

Realtime
publishers

"Leading the Conversation"

The Definitive Guide[™] To

Converged Network Management



Ken Camp

Chapter 10: Asset Reporting, Audit Compliance, and IT Documentation	212
FCAPS and Asset/Administration/Accounting Management.....	212
Accounting/Administration/Asset Management.....	212
Managing Billing	213
User Accounting	214
The Asset Management View	214
Why Documentation? Why Process?.....	215
Creating Repeatable Processes	215
Revisiting the Importance of Knowing Your Environment.....	215
Be Prepared: Protecting Against Future Business Issues	216
Legal and Regulatory Issues to Consider.....	217
SOX.....	217
Risk Assessment	218
Control Environment	218
Control Activities.....	218
Monitoring	219
Information and Communication.....	219
GLBA.....	219
HIPAA	220
Methodologies in Best Practices for Management and Oversight.....	223
ITIL.....	223
Service Support.....	224
Service Delivery.....	225
The Business Perspective.....	227
ISO 17799	227
Managing and Protecting the Network	232
Inconsequential Risk Classes.....	232
Significant Risk Classes.....	232
Reducing Risk for Single Occurrence Losses.....	233
Addressing the Risks.....	234
Risk Management Life Cycle	234
Summary	235
Download Additional eBooks from Realtime Nexus!	235

Copyright Statement

© 2007 Realtimepublishers.com, Inc. All rights reserved. This site contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtimepublishers.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 Realtimepublishers.com, Inc or its web site sponsors. In no event shall Realtimepublishers.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.

Realtimepublishers.com and the Realtimepublishers 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 Realtimepublishers.com, please contact us via e-mail at info@realtimepublishers.com.

[**Editor's Note:** This eBook was downloaded from Realtime Nexus—The Digital Library. All leading technology guides from Realtimedpublishers can be found at <http://nexus.realtimedpublishers.com>.]

Chapter 10: Asset Reporting, Audit Compliance, and IT Documentation

This final chapter will explore asset and audit compliance methods and procedures. They're the last component of the FCAPS model. As this guide comes to a close, it will examine why documenting IT process is critical to business operations. Earlier chapters have made brief mention of approaches such as ITIL and ISO 17799 as best practice methodologies. This chapter will probe into those a bit deeper.

For many enterprises, regulatory requirements to comply with SOX, GLBA, and HIPAA raise concerns about the impact on managing an integrated service network with VoIP. This chapter will close with a review of managing the network life cycle with an eye toward holistic risk management.

FCAPS and Asset/Administration/Accounting Management

Over time, and depending on what business the enterprise is engaged in, the "A" in FCAPS has stood for accounting, administration, auditing, and asset management. That variation is perhaps a good reinforcement that the FCAPS approach is a model, not a process. FCAPS is simply a holistic model that suggests you look at multiple domains within the service network—fault, configuration, accounting, performance, and security—to provide comprehensive service management.

Accounting/Administration/Asset Management

In the commercial services market, whether delivering traditional telephony services or enhanced VoIP services, accounting becomes vital to successful service delivery. A Call Detail Record (CDR) in telecommunications contains information about system usage. This includes the identities of call originators, the identities of call recipients, call duration, any billing information about the call, information about time used during the billing period, and other usage-related information.

Managing Billing

CDRs are created constantly throughout the business day, with every telephone call. The telephone calling patterns within an enterprise can provide a great deal of information about customers, business partners, and internal relationships. In many VoIP systems, CDRs are stored in databases on the VoIP servers. A SQL server in the VoIP segment may be just as vulnerable as one sitting elsewhere in the network.

Internal Billing

For many organizations, IT and telecommunications services represent a business within the business. For enterprises that treat these services as a cost center, billing within the organization may drive either real dollar transfers or cost center cross charges for tracking the cost of doing business. CDRs and call accounting systems provide the means to generate and control this recordkeeping function within the service delivery network.

Billing as a Service Provider

Advances in unified communications technologies have dramatically lowered the barrier to entry to the VoIP services business. It's become relatively easy and cost effective to become a voice service provider in the converged network environment. As a result, hundreds of service providers offer a wide range of integrated services, many focused in niche and vertical markets. For many global enterprises, the deployment of self-managed infrastructure makes sense. In these enterprises, affiliates and business units are often paying customers of the services delivery organization.

Whether CDRs are used to bill paying customers or to track system utilization doesn't matter. The data collection and analysis of usage statistics provides the same baseline knowledge about what's going on in the network. In traditional telephony, carriers billed for minutes of usage. In the integrated services environment, there are several new factors that need to be accounted for.

Bandwidth utilization is the primary accounting factor for many enterprises. Although it might not provide the granularity of detail that some facets of the network offer, bandwidth can be used to account for WAN links, based on the speed of the link. In large enterprise networks, it helps delineate the cost differences in delivering 10Mbps, 100Mbps, or Gigabit Ethernet connections within the LAN. These port speeds become more critical factors as the enterprise evolves from a legacy LAN environment into an integrated voice, data, and video service network.


Disk space and CPU utilization become increasingly important in the converged service environment. Adding a voice service introduces codecs, signaling, and control processing that consumes resources, not just in the network, but sometimes in nodes across the network.

Minutes of use may seem like an obsolete billing mechanism in the new integrated services network, but that isn't always the case. Many enterprises rely on telecommunications services to derive information about peak business hours during the day or week. For businesses that are very voice-centric in nature, minutes of use, and when they are used, continue to provide key business intelligence information about the ebb and flow of work throughout the business day. Collected over time, this information is used by dynamic organizations to assist in managing staffing requirements.

User Accounting

As we touch on a variety of regulatory and compliance issues, user accounting becomes a vital recordkeeping and auditing component of the service network. With heightened requirements for audit trails and accountability, the integration of VoIP and video into the enterprise operational network raises the need for effective user accounting mechanisms.

User administration tools have widely permeated the IT and telecom services environment. They're common enough that today, reference to an "AAA server" or service may not raise any questions, but for many organizations, the adoption of new services for authentication, authorization, and accounting/auditing may be new.

 Chapter 9 discusses the importance of authentication, authorization, and accounting/auditing.

Tracking UserIDs, passwords, and user permissions becomes more important as service networks mature. As a more diverse suite of services is available, it's important to track which users have permission to use which services. From a regulatory and compliance viewpoint, you might focus more on who the services were used by and what activity was performed.

When crafting the enterprise converged services network, one factor to consider is a backup methodology. Recovery of auditing or accounting information impacts compliance for many organizations.

The Asset Management View

Another facet of the FCAPS approach is the challenge of asset management. Current unified communications technologies introduce a plethora of new devices and equipment into the network. Chapter 8 discussed configuration management. In the integrated services network, management and monitoring tools are vital service delivery support mechanisms.

As part of configuration management, the NMS commonly incorporates an asset management module. These tools in the NMS help in managing the IT asset life cycle. As this guide has noted throughout, every facet of network and services management has its own life cycle component. The integrated services network is a series of life cycles within life cycles. In this area, we focus on:

- Asset evaluation and selection
- Asset procurement
- Asset maintenance and support
- Asset disposal at end of life

As you adopt a comprehensive FCAPS model, many organizations are inclined to take a singular view on asset management, auditing, or accounting for billing purposes. It's wise to consider a more holistic view and incorporate all three into the enterprise management model.

Why Documentation? Why Process?

Throughout this guide, there has been a recurring thread reinforcing the need for process and documentation. As we wrap up in this closing chapter, let's touch on why these are so important in the integrated service network of voice, data, and video.

Creating Repeatable Processes

When we deliver services of any kind, we strive for a predictable and consistent service quality; VoIP and video services in the converged network present some technical challenges. Traditional networks dealt with bursty non-real-time data. Voice and video services place new demands for real-time services on the network. Real-time services can be designed to overcome a number of network impediments, but doing so requires predictability.

We put great effort into repeatable processes in every facet of the service delivery network because repetition brings consistency. With consistency, we can achieve the quality we commit to, whether those commitments are via service level agreements (SLAs) or through tacit user expectations in the enterprise.

Additionally, repeatable processes can free time and resources in many organizations; those resources can be better spent on more creative work that requires focused attention. Not every project or task in the enterprise requires repeatable processes, but those things that routinely consume resources are more efficiently managed with thorough documentation and process controls.

Revisiting the Importance of Knowing Your Environment

In the information economy, our business intelligence is a corporate asset. For many enterprises, the information we have about our own business processes, workflows, and information resource tools may be the most valuable asset the company owns.

The more we know about the environment, the better armed we are to manage the business. The more we know about our integrated services, how they're used, when they're used, and who uses them, the better prepared we are to support the enterprise mission.

Documenting processes provides sustainability. Too often, especially in small and midsized businesses, there is a corporate culture of reliance on key individuals who know what to do. These people who carry corporate information in their heads are perceived as being high-value resources, when in fact they present great risk. The problem is depth of coverage. When a single individual is the only resource with expertise in a particular subject area, there is a risk that an event changing the status of a single person can create problems. If a single IT person handles cyber security incidents, for example, what happens if that person is out ill or leaves the company. It's vital that business processes not rely on "one deep" personnel. Documentation eases cross-training of other staff, and helps ensure long-term viability of business processes. Thorough documentation of business intelligence information—whether it's about the integrated services network or a customer account—protects the organization from the danger that critical institutional knowledge exists solely in the hands, or brains, of a single individual.

Be Prepared: Protecting Against Future Business Issues

There is another reason to document IT service delivery processes and workflows. It has to do with budgeting. Information services networks tend to change more rapidly than legacy telephone networks. In the past, an enterprise telephone system might have a 10-year lifetime. The LAN and WAN environment has proven to be more dynamic. In many enterprises, the IT services network undergoes extensive redesign and re-architecture every 3-to-4 years, with continual upgrades taking place along the way.

As our integrated voice, data, and video services become more widespread, they become more tightly coupled with daily business operations. Enhancements and upgrades to the service network become, for many, key business drivers.

The budgeting process of calculating costs, building a business case, proving return on investment (ROI), and preparing acquisitions all require documentation. In order to be prepared for business contingencies, in the IT services network, one commonly adopted best practice is to maintain and regularly update the requirements, including replacement costs for high-level elements of the service:

- **Hardware**—A comprehensive inventory of the network infrastructure can ensure that no components are overlooked in the life cycle evolution.
- **Software**—A library of software used, including version information, not only documents the current environment but also provides a quick recovery checklist when problems arise.
- **Services**—An inventory of every service delivered and the user or customer to which it is delivered can prove vital during potential business continuity events. Knowing who the users of every service are can ensure good communications and information sharing during an incident.
- **Staffing**—Training, cross-training, and skills retention requirements need to be documented and continually updated.

Legal and Regulatory Issues to Consider

Although this guide can't begin to address the spectrum of legal and regulatory issues to which private and public sector organizations may need to adhere, let's take a brief look at a few of the most visible and compelling concerns.

SOX

In 2002, SOX was passed. Entitled the Public Company Accounting Reform and Investor Protection Act of 2002, it's been very controversial and raised a lot of debate. This law arose from the furor over corporate accounting scandals at WorldCom, Enron, Tyco, and others. This flurry of visible accounting scandals and fraud in business reduced public trust in business management and in accounting and reporting practices. Named after sponsors Senator Paul Sarbanes and Representative Michael G. Oxley, SOX passed in the House by a vote of 423-3 and by the Senate 99-0.

This wide-ranging legislation introduced new standards and bolstered existing ones for the boards, management, and accounting firms that represent public companies. Although SOX doesn't correlate directly to telecommunications or IT services, its impact has been far-reaching, well beyond publicly owned companies.

Major SOX provisions include:

- A Public Company Accounting Oversight Board (PCAOB) was created
- Public companies are required to both evaluate and disclose the effectiveness of their internal controls
- Financial reports must be certified reports by both Chief Executive Officers (CEOs) and Chief Financial Officers (CFOs)
- Companies listed on stock exchanges must have independent committees overseeing relationships with auditors
- Most personal loans to executive officers and directors have been banned
- Both criminal and civil penalties for securities law violations have been increased
- Willfully misstating financial reporting by corporate executives is punishable by significantly longer maximum jail sentences and larger fines

Although SOX might not apply to all organizations because of its focus on financial accountability, the principles contained in the act have been widely embraced and adopted across the private and public sector. What is for some a legal requirement has quickly become a generally accepted best practice for many. The fundamental SOX focal areas easily extend down into IT management and delivery of services within the enterprise.

The impact of SOX on business practices surrounding financial and auditing controls has been widely felt. But the impact isn't solely in the financial area of business. IT has felt some impact as well. Those impacts are mostly felt in five areas: risk assessment, control environment, control activities, monitoring, and information and communication.

Risk Assessment

Every organization is faced with a variety of internal and external risks that must be taken into consideration. Establishing objectives is a precondition to risk assessment because we are actually evaluating the risk posed to achieving business objectives. Before we can determine how to manage risks, we have to understand what they are in relation to specific business goals.

For example, IT managers have to both assess and understand the risks around financial reports, particularly in the areas of completeness and validity, before they can implement necessary control mechanisms. Thus, service delivery managers must understand how services, systems, and resources are being used, and document accordingly.

Control Environment

The control environment sets the tone for the organization and influences human behavior. This control environment addresses business factors such as management style, organizational ethics, and delegation of authority and staff development processes.

IT and service delivery groups thrive in an environment in which employees take accountability for and receive recognition for the success of their projects. This encourages that issues and concerns are escalated in a timely manner and dealt with effectively. For many organizations, this means that service delivery employees need to be cross-trained in design, implementation, quality assurance, and deployment so that they can engage in the complete life cycle of the converged services technologies.

Control Activities

These are the corporate policies and procedures that govern how to ensure management directives are accomplished. They help guarantee that appropriate actions are being taken to mitigate the risk that might interfere with meeting objectives. Control activities occur throughout every organization, and include routine tasks at all levels and in all functions. They include a broad range of activities—approval processes, authorization acquisition, verification, financial reconciliations, operating performance reviews, and asset security.

In the past, many ERP and CRM systems were used to collect data that fed into spreadsheets for analysis. Manual spreadsheets are prone to human error. Organizations will need to document usage rules for the integrated services and create an audit trail for each. These systems support business services and often contribute financial or other key business intelligence information. It's important that corporate policies define the business requirements and other documentation necessary for each and every IT and telecommunications service project.

Monitoring

Internal control systems within the service environment need to be routinely monitored. This helps assess the quality of the system's performance over time. This is best accomplished through a combination of both ongoing monitoring activities and periodic evaluations. Problems and anomalies identified during monitoring should be reported and documented and corrective action should be taken. This ensures a continuous improvement in the delivery of fully integrated services.

Within the service delivery environment, specialized auditing and review processes may be appropriate to address high-risk areas. Those services and systems that are mission-critical to the enterprise often require focused attention. The service delivery team should perform frequent internal assessments of these vital systems and services. One important consideration may be to have independent third-party assessments performed on a regularly scheduled basis to augment the work performed by employees. The management team needs to clearly understand the outcomes of these audits and assessments. As these services roll up to larger corporate business and financial reporting, the management team will be held accountable for the outcomes.

Information and Communication

Information systems play a pivotal role in all our internal business controls. They provide reports that make it possible to run and manage the business. These reports contain operational, financial, and compliance-related information. Effective communication aids the flow of information throughout the organization.

Service managers can't identify and address risks without timely, accurate information. Timeliness in reacting to issues as they occur is vital to maintaining the integrated services environment and ongoing business operations.

GLBA

GLBA was designed to open competition among banks, securities companies, and insurance companies. These companies make up what is known as the financial services industry. GLBA really governs how these companies can merge and own one another. Because people invest money differently in differing economic times, GLBA introduces controls so that investment banking firms, for example, might also participate in the insurance business. Banks haven't traditionally participated in insurance underwriting, but consolidation of the financial services sector led to the need for new regulation.

Although a great deal of consolidation in this industry has taken place since the passage of GLBA, it hasn't been as widespread as anticipated. For most businesses outside the financial services industry, GLBA is of no concern. It represents another set of requirements, similar in many ways to SOX, for financial services. Again, we see regulatory efforts and compliance requirements for one industry or set of industries being adopted as common best practices in other sectors.

HIPAA

Congress enacted HIPAA in 1996. The primary goal of HIPAA Title I is to protect health insurance coverage for workers and their families in the event of change or loss of their jobs. Title II of HIPAA had wide-ranging impacts on the health care industry. It set in place requirements for national standards of health care transactions and identification mechanisms for health care providers, insurance plans and providers, and employers.

As part of Title II, a section called Administrative Simplification also addressed the security and privacy of individuals' health-related information. The intent of this section was to bring about standardization in systems and encourage electronic data interchange (EDI) within the U.S. health care sector.

Within HIPAA, there is a Privacy Rule that took effect in 2003. This rule provides regulations for what is termed Protected Health Information. PHI is comprised of information that can be linked to any individual about the status of that person's health, health care being provided, or payment for that health care. The rule has been broadly interpreted to include any portion of either a patient's complete medical record or payment history.

The Privacy Rule dictates what may or may not be disclosed by law and to help ensure treatment. Health care organizations have to take great care to disclose only what is necessary and take measures to protect all information from undue disclosure.

Beyond the Privacy Rule, there is also a Final Rule on Security Standards that was issued in 2003, with a compliance requirement date in 2005. This Security Rule is intended to complement the Privacy Rule. It defines three types of safeguards that healthcare entities must put in to place to comply:

- Administrative
- Physical
- Technical

Each of these types has specific security standards that must be adhered to for compliance. Some of the standards are required; others are "addressable" or flexible enough to be uniquely addressed based on circumstances.

Although the intent of this guide isn't to provide a detailed evaluation of HIPAA requirements and impacts, because the act is so broad in scope—even to the point of impacting many enterprise Human Resources organizations—this information is included to give an appreciation of these regulatory compliance needs as they may overlap into service delivery requirements. These descriptions of administrative, physical, and technical safeguards are liberally extracted from a number of resources widely available online. HIPAA has been very widely documented and many resources say the same things.

Administrative Safeguards:

- Organizations covered under HIPAA must adopt written privacy procedures and designate a privacy officer. The privacy officer is responsible for developing and implementing all required policies and procedures.
- Management oversight and organization buy-in to compliance and security controls must be documented within the organizational procedures and policies.
- Classes of employees that are permitted access to PHI must be documented in organizational procedures. Employees should have access only to the subset of PHI needed to perform their jobs.
- Organizations must demonstrate they have implemented an ongoing training program regarding the handling of PHI, and that it's provided to all employees that perform any administrative health plan functions.
- If an entity outsources some part of their business process to a third party, that entity must document that their vendors also have the procedures and policies in place to comply with HIPAA requirements. In most cases, organizations accomplish this through contractual clauses as part of third-party service agreements. One area of concern is the possibility of a vendor further outsourcing data handling functions to yet another vendor farther downstream. At each step of the way, appropriate contracts and controls need to be established.
- Health care entities are responsible for data backups and disaster recovery procedures. A documented emergency contingency plan should be established that documents data priority and failure analysis, testing activities, and change control procedures.
- HIPAA dictates an internal audit process that continually reviews compliance and the potential for security violations. Enterprise policies and procedures need to document the frequency and scope of audits, and the specific details of the audit procedures. Under HIPAA, audits should be both regularly scheduled and event driven.
- Procedures for mitigating security breaches should be well documented.

Physical Safeguards:

- The network must include controls governing the introduction and removal of both hardware and software. Equipment that has reached end of life must be retired in such a way that PHI cannot be compromised.
- Access to systems that contain health information should be diligently monitored and controlled.
- Only authorized individuals may access systems hardware and software.
- Access controls must include security plans for facilities, maintenance records, and visitor sign-in (including a process for escorts).
- Workstations should not be placed in public or high-traffic areas. Monitor screens should not be viewable by the public. Policies addressing proper workstation use are required.
- If contracted employees are used, they too must be fully trained on their responsibilities.

Technical Safeguards:

- Systems that house PHI must be protected from intrusion. If data is transmitted over an open network, some form of encryption is required. If private or closed networks are used, existing access controls may be sufficient to eliminate the need for encryption.
- Every entity involved in the transmission and handling of PHI data is responsible for ensuring that the data within its systems has not been modified or deleted.
- Data integrity should be maintained and corroborated using check sum, double-keying, message authentication, and digital signature techniques.
- Message authentication between parties covered under HIPAA is required. Each party should corroborate that an entity is who it claims to be. Common examples of this authentication include: password, two or three-way handshakes, telephone callback, and token systems (including digital certificates).
- Organizations covered under HIPAA must make their documentation available to the government to determine and verify compliance.
- IT documentation should include a written record of all configuration settings on the elements of the service network. This is in addition to other policies and procedures because these components are complex, configurable, and constantly changing. For many service delivery organizations, this presents a huge challenge.
- Risk analysis and risk management programs must be implemented and documented.

Whether the regulatory issue is SOX, GLBA, or HIPAA, it's obvious by now that any enterprise that is required to comply takes on an added set of documentation requirements that necessitates diligence and attention to detail. Some regulations apply only to specific areas in the private sector. Public sector groups may have other requirements at the federal, state, and local level. Although this guide can't begin to touch on the privacy issues surrounding the protection of personally identifying information (PII), as of this writing 46 states have active PII legislation in place.

For many enterprises, another entity's regulatory challenge can be used as a diligent best practice with some adaptation. Many best-in-breed organizations adopt a blend of compliance with the regulations we've described coupled with the practices that follow in the remainder of the chapter.

Methodologies in Best Practices for Management and Oversight

This section will delve into two widely accepted best practices methodologies: the Information Technology Information Library (ITIL) and ISO 17799.

ITIL

ITIL is a collection of industry best practices that has grown out of earlier efforts by the Central Computer and Telecommunications Agency (CCTA) in the UK. It provides a collection of industry best practices, taken from both private and public sector organizations, for information technology services across all IT infrastructure and operations.

ITIL is published as a series of books, hence the library approach. At one point, there were 31 volumes incorporated in ITIL. ITIL v3, termed a refresh of the library, was due to be released in May of 2007 but has been slightly delayed as of this writing. ITIL v3 will contain five volumes:

- Service Strategy
- Service Design
- Service Transition
- Service Operation
- Continual Service Improvement

The framework in ITIL has been widely adopted by many enterprise organizations. ITIL contains an area that addresses IT Service Management (ITSM), which garners a great deal of attention from service delivery organizations. Although ITSM and ITIL aren't directly related, they're used in tandem to provide a customer-focused set of service delivery best practices. Their shared heritage dates back to the IBM Yellow books and W. Edwards Demings' Total Quality Management (TQM) principles. Today, these principles are found in a number of widely embraced approaches including Six Sigma, Capability Maturity Model Integration (CMMI), and Business Process Management (BPM).

It's perhaps noteworthy to remember that early work in quality management and process engineering was oriented toward manufacturing. What we see here is the evolution of how the lessons learned in the manufacturing sector evolved over time and are now being applied to the delivery of information services in today's converged data, voice, and video networks.

Some of the benefits of a systematic, ITIL-based approach to managing IT services include:

- Cost reduction
- IT service improvements based on best practices
- Increased customer and end user satisfaction
- Enhanced auditability through process and documentation
- Productivity improvements through incorporation of repeatable processes

Service Support

ITSM can bring many benefits through the adoption of best practices. It's driven by both technology and the many businesses engaged in ITSM, so it's continually evolving and changing.

It's a fact that many service provider organizations have turned to ITIL for guidance to help deliver and support their services. ITIL provides useful guidelines, yet it does not actually provide the service management processes. Service providers are still expected to define the processes themselves. This is often accomplished with help from outside consultants.

The service management processes alone are not enough. Staff who are expected to follow the processes also require more detailed work instructions behind the processes.

ITIL provide some guidelines for service management applications, yet does not provide the tool settings. Thus, after a service provider organization has defined its service management processes, the organization still needs to find or develop the appropriate application to support these processes.

Today, nearly all service management applications claim to support ITIL and work out-of-the-box. Reality requires more work. It's not unusual for it to take somewhere between 2 weeks and 4 months to configure a service management application so that it can support the processes that a service provider organization has defined. And that's the easy part, after all the processes have been defined and documented.

There are several views of how ITIL might be used. One leading company is Alignability. Figure 10.1 shows a widely adopted view called the Alignability Process Model.



Figure 10.1: The Alignability view of ITIL service support and delivery processes.

Service Delivery

Given that ITIL is a library, covered in a series of books developed over many years, this short mention cannot begin to do justice to the complexity of this very thorough approach. In the visuals that follow, we see some flows and concepts specific only to incident management that are widely adopted by service delivery organizations embracing the ITIL model. Each box in Figure 10.1 has a detailed and specific set of documentation and process flows to support that facet of operations.

Incident management is a daily part of operations for every service delivery organization. In Figure 10.2, we see one ITIL view of incident management and response. This is provided as an example and may not be applicable as shown for every service delivery organization. The example provides, as does the entire ITIL collection, a framework that an organization can use for modeling its own specific process documentation.

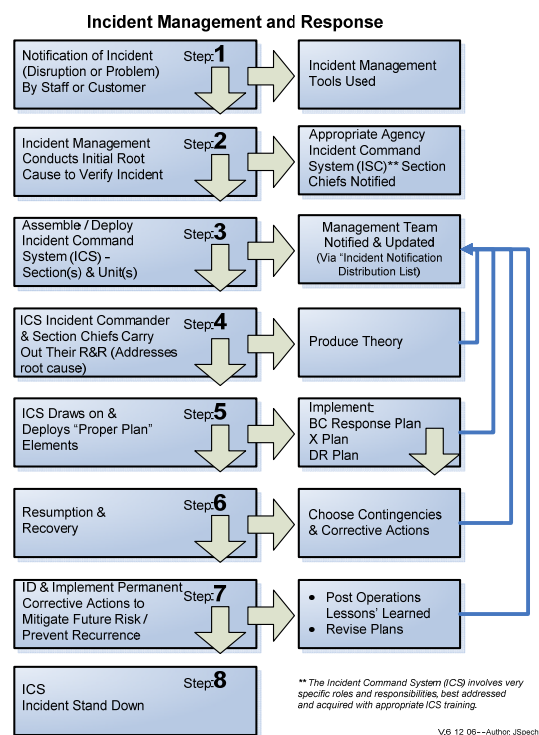


Figure 10.2: The ITIL incident management and response flow.

In Figure 10.3, we see one tool for a small part of the incident management and response flow. Every incident has an impact, and associated with that impact is some sense of urgency to achieve resolution. For most organizations, this simple three-by-three matrix will provide enough granularity to prioritize every possible incident and contingency from a flu pandemic to natural disaster to minor power failures or service disruptions.

IMPACT				
Extreme (Critical) Major Incident And, Multiple agencies cannot conduct core business		High Cannot conduct core business	Medium Restricts ability to conduct business	Low Does not significantly impede business
URGENCY	High Requires immediate attention	1	2	3
	Medium Requires attention in near future	2	3	4
	Low Does not require significant urgency	3	4	5

Figure 10.3: Incident prioritization matrix.

Figure 10.4 simply provides an example of drilling down another level. Once priorities have been applied to a given incident, established responses need to be engaged.

Each priority is related to a certain recovery time . . .

<p>Priority 0: Major Incidents - Larger global incidents <small>Multiple agencies cannot conduct core business. Other global incidents may include: Fire, natural disasters, such as floods, earthquakes or volcanic eruptions. Human and animal disease outbreaks. Hazardous materials incidents. Terrorist incidents, including the use of weapons of mass destruction. Civil unrest, labor strikes, picketing.</small></p>	<p>Immediate Attention <small>24/7 effort until resolved /contained n hour escalation / communication</small></p>
<p>Priority 1: Significant damage, must be resolved / recovered immediately</p>	<p>Immediate Attention <small>24/7 effort until resolved /contained n hour escalation / communication</small></p>
<p>Priority 2: Limited damage, should be resolved / recovered immediately</p>	<p>N hours <small>24/7 effort at managerial discretion</small></p>
<p>Priority 3: Significant damage, does not need to be resolved / recovered immediately</p>	<p>N hours / business day</p>
<p>Priority 4: Limited damage, does not need to be resolved / recovered immediately</p>	<p>N business day(s)</p>
<p>Priority 5: Non-urgent – no impact on the customer’s ability to work. Could become a project oriented issue</p>	<p>N/A</p>

Figure 10.4: Prioritization response matrix.

The Business Perspective

What we see in this quick series of examples is that the ITIL approach to incident management provides a consistent methodology for prioritizing and responding to incidents. Coupled with established process flows, the integrated services delivery organization possesses a complete, methodical tool set for managing and delivering consistent and predictable integrated network services.

This consistency and set of repeatable processes ensures that enterprise operations continue on an even keel no matter what happens. They provide sustainability. For service providers, these tools ensure business survival, as these integrated services represent the customer revenue stream. For other enterprises, appropriate modification allows them to support the enterprise mission and sustain the work that goes into meeting corporate objectives.

ISO 17799

ISO 17799 is actually entitled Information technology - Security techniques - Code of practice for information security management. It was revised in June 2005 by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). It offers best practice recommendations on information security management. Many organizations are today embracing ISO 17999 as a broader part of service management and business operations, folding it into the larger set of corporate compliance efforts. Although focused primarily on the protection of confidentiality, integrity, and availability of network services and resources, ISO 17799 reaches far beyond security.

Business Continuity Planning

Business Continuity Planning (BCP) has grown and evolved from what in the past were disaster recovery initiatives in the enterprise. Like every other facet of managing a unified communications services network, BCP strategies continually mature as processes are developed. BCP focuses on organization recovery and service restoration when a disaster or extended disruption occurs. For many organizations, BCP digs deeper than network services into what is frequently called an “all hazards plan.”

BCP is simply how an enterprise plans and prepares for future events that could jeopardize business mission and overall operational health. It’s often a path to discovery of weak processes and tightly coupled with efforts toward improving information security and risk management practices. Typically, BCP yields some organizational documentation for use before, during, and after a business disruption.

BCP methodologies today scale to fit both large and small businesses but initially grew primarily from the efforts of regulated industries. Common sense indicates that every organization should have a plan to guarantee sustainable business.

One view that is widely represented in a number of scholarly articles on business continuity management process consists of the following six procedures.

- **Disaster Notification Handling**—At this stage, an on-duty manager becomes aware of either an existing or impending disaster. This procedure is used to assess the situation using established checklists and determine what protective and recovery actions are warranted.
- **Service Recovery**—In the recovery phase, management and recovery teams follow predefined plans for service recovery.
- **Return to Normal Operations**—Once service recovery has been completed, the continuity manager or incident commander implements a predefined return to normal operations. This collaborative effort shifts the focus of operational control from the recovery team back into the hands of the normal operations team.
- **Service Recovery Testing**—The continuity manager and service recovery team remain engaged to ensure that recovery is complete and the process, as followed, provides for reliable service recovery and restoration to normal operations.
- **Continuity Manual Maintenance**—The business continuity team must complete an after-action analysis and update business continuity process manuals to ensure that action is taken on any lessons learned from the event.
- **Continuity Plan Maintenance**—Business continuity planners need to continually revise the continuity plans for the service infrastructure of the integrated network that provides mission-critical enterprise services.

There is a great deal of evidence indicating that many organizations don't invest enough time or money in BCP. Statistically, building fires permanently close 44 percent of the businesses they affect. In the World Trade Center bombing in 1993, more than 42 percent, 150 of 350, businesses didn't survive. Conversely, in the attacks of September 11, 2001, many businesses had extensive business continuity plans and were back in operation within days of the devastation.

For many organizations, the plan can simply be a binder stored somewhere away from the main work location that contains contact information for management and general company staff, a list of clients and customers, and vendor partners. It's wise to include any other work process documentation including the location of the offsite data backups, copies of insurance documents, and other materials vital business survival.

For large enterprises, with more complex needs, the plan may well include:

- A failover, disaster recovery, or business continuity work site
- A process to routinely test technical requirements and readiness for disaster
- Backup systems for regulatory reporting requirements
- A mechanism to reestablish physical records, perhaps from tape, drive, or microfiche
- A means to establish a new supply chain when vendor partners are also impacted
- For manufacturing operations, the means to establish new production centers may be required

Every organization, large or small, needs to ensure that their business continuity plans are realistic. It's vital that they be easy to use during a crisis. BCP is a crucial peer to crisis management and disaster recovery planning. It is part of every organization's overall risk management strategy.

Development of a business continuity plan can be reduced to five simple steps:

- Analysis
- Solution design
- Implementation
- Testing and organization acceptance
- Maintenance



Figure 10.5: Five-step BCP life cycle.

A great deal of BCP material is available on the Internet, sponsored by consulting firms who provide fee-based services. It's worthwhile to note that there are many freely available basic tutorials that can help those organizations that are motivated to prepare but financially constrained from hiring consultants. The simple act of establishing the role of a business continuity planner can greatly improve organizational readiness for events that cannot be predicted.

System Access Control

System access control includes several techniques addressed earlier in this guide. Chapter 9 looked at the “Golden Rules” of authentication, authorization, and audit. Rather than dig into the details of each, we’ll just revisit the basics.

Authentication is the act of ensuring that the user is who they claim to be. Best practices also drive server or system authentication in the opposite direction, giving the user authenticated proof that the system or server is indeed the one it purports to be and not a spoofed system somehow inserted in the traffic flow. Authentication can range from simple passwords to more complex token-based and/or biometric verification tools.

Factors for Authentication

Simple passwords are often viewed as a very weak form of authentication. Two-factor authentication is generally considered more acceptable and appropriate for many business applications today. There are four generally accepted authentication factors that might be used in combination to provide strong user authentication:

- Something you know—Usually a password or PIN; it’s assumed that only the owner of the account would know this information
- Something you have—Often a smart card or token; again, assumes only the owner of an account will have the associated token
- Something you are—Most often a biometric solution: a fingerprint, palm print, voice or retinal scan
- Somewhere you are—May be as simple as inside or outside the corporate firewall for matters of trust; it might also be a more extensive ring-back system that allows a user to dial in, and then calls back at a predefined telephone number to grant access; RFID devices may play a role in future use of location-based authentication.

Authorization is the process of matching the authenticated user or system to a profile that identifies what that user has permission to do. It’s a combination of services the user is allowed to use and service network resources to which the user has been granted access. These might include permission to read-only access or to write files and the ability to execute programs. Read, write, and execute are the most common authorization focal points.

Audits provide the proof details that may be required later in some form of incident or event investigation. This includes system logs and history files that provide information about what the user actually did during a session. Audits provide the documentation for who performed what function and when. Audits provide accountability, associating users with actions.

Physical and Environmental Security

Beyond the systematic controls of authentication, authorization, and auditing at the system level, we have physical controls to protect systems. Door locks, controlled work areas, card key scanners, and automated systems all aid in securing the physical location where systems delivering key integrated services reside. Physical security may be as simple as a locked door. For many small organizations, this simple precaution is adequate. Other enterprises may require guards, video monitoring, metal detectors, and complex personnel tracking systems to eliminate any chance of unauthorized access.

Hiding resources by simply not advertising their availability provides a very minimal and weak approach often termed “security by obscurity.” Proponents of discretion will point out that, conversely, putting a big sign on the data center door advertising what is inside is probably unnecessary and inappropriate.

Compliance

ISO 17799 isn't really a regulation or code that organizations comply with directly. It's really a code of practice that helps shape the corporate culture and behaviors. Businesses use ISO 1799 to help avoid breaking any laws or regulations. For many companies contracts, SLAs and security policies become part of ISO 17799 adoption. The intent is to ensure that all internal systems comply with documented corporate policies and standards.

Asset Classifications and Control

IT asset management (ITAM) is another set of business best practices. ITAM brings financial, contractual, and inventory functions together to manage the IT environment life cycle. This information is used to make decisions about architectural and service changes in the enterprise based on knowledge of what is known about the operational environment. It includes both hardware and software management.

Software management commonly includes licensing to ensure businesses aren't running on unlicensed copies of commercial software. Beyond this, software asset management ties closely to configuration management of corporate systems. Lastly, software asset management is frequently used as a tool to document compliance with SOX, GLBA, HIPAA, copyright laws, and so on. There are a number of commercial tools available to assist in managing the enterprise software inventory.

Hardware asset management focuses on the physical components. In the integrated services network, this includes all the network elements, nodes, and even cables that deliver mission-critical business services. Under the umbrella of ISO 17799, many organization document practices surrounding procurement, administration, re-use, and retirement of hardware assets.

Security Policy

At a high level, the enterprise security policy simply provides a definition of what it means to be secure. The security policy describes acceptable behavior and approved uses of resources and often delineates specific security elements to impede unauthorized access. The security policy speaks to the flow of information by elaborating on what information may enter or leave the corporate network or zones inside that network.

Managing and Protecting the Network

Managing and protecting the enterprise network is a daily, ongoing exercise in managing risk. As we've begun to learn in this brief overview of regulatory and compliance concerns, we find that to some extent we must embrace risk. We recognize risks exist. We assess the impact it may have on business and we develop strategies to either counter, manage, or mitigate it.

In some cases, we can avoid risk entirely by taking some alternative safe approach. In some cases, we'll defer the risk to a third party, like an insurance carrier. Sometimes we can reduce the negative impact, but other times we simply accept the full risk consequences. Each approach needs to be the result of a conscious business decision.

Chapter 9 introduced Jacobson's Window for simple risk modeling. This is a good point to refer back and bring our thoughts together as we work toward the closing of this guide. We'll do a quick review here and revisit some key points.

Inconsequential Risk Classes

Inconsequential risks fall into two distinct categories. One inconsequential risk is so unlikely to occur that it doesn't warrant concern. This risk has a low occurrence rate but a high impact should it ever occur. We used the example of a meteor striking our data center in Chapter 9, but we could just as likely take into account a continental power failure or any other very rare event. When they happen, they are completely outside our control and so devastating to business operations that spending time brainstorming contingency plans is simply a wasted effort.

At the opposite end of the spectrum is the risk event that has a high rate of occurrence but a low impact. Spam email provides a perfect example. We get spam email in our inboxes every day. For most of us, the impact is minimal. We click delete, and it's gone. Although we may have to do this several times in the course of a day, the impact to the company is low. In both these cases, we're simply accepting the risk rather than investing efforts to mitigate and respond to the consequences.

Significant Risk Classes

The more significant risk classes are those that have either low-low or high-high occurrence and impact rates. This is where the majority of all risk analysis and management efforts fall. We build remediation and mitigation strategies to reduce the risk, spread it across the organization to reduce the impact, or transfer it through outsourcing, insurance, or some other means. In each case, we're striving to minimize disruption to services in the network.

Reducing Risk for Single Occurrence Losses

Chapter 9 used the following illustration to show how risks spread in the real world. This view is helpful in placing the risks in different quadrants as we determine what our plan or response might be to a particular type of event.

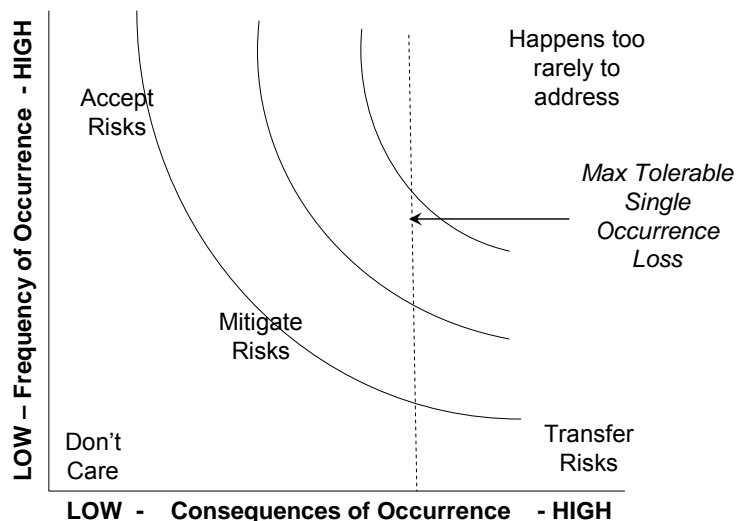


Figure 10.6: Modeling risks.

This spectrum of risk is very identifiable in real-world planning for business operations. Over time, losses across this spectrum of risk tend to have similar organizational impacts. From an actuarial standpoint, the notion of annualized loss expectancy (ALE) is used to quantify risk. This is often expressed in terms of occurrences per year and the loss resulting from a single occurrence.

Although ALE is useful for comparing risks, it's difficult to achieve credible estimates of occurrence rate for risk events that rarely occur. It's fairly easy to estimate the consequences, but not as easy to estimate occurrence rate. Computer network risks frequently stem from human actions such as simple configuration errors, but fraud, sabotage, viruses, and malicious attacks may come into play unexpectedly. These occurrence rates are very difficult to quantify.

Despite this difficulty, it's often wise to define a set of risks that might have disastrous effects should they occur as a one-time event. Some one-time events might be planned for, while others might result in circumstance for which there can be no pre-planned business strategy. The exercise of documenting a brainstorming session for these types of events often leads to creative, workable strategies for other similar events.

Addressing the Risks

Typical risk management focuses on risks that come from known and identifiable causes—natural disasters, fires, accidents, death, and so on. Risk is anything that threatens the successful, ongoing operations of the business. The main objective of risk management is to reduce risks to tolerable levels. What is tolerable will vary from organization to organization and is based on a number of factors including technology, people, organizations, and sometimes politics.

Ideally, risk management follows a prioritization scheme like that described in Chapter 9. Jacobson's Window offers just one way of looking at risk prioritization. One simple view of the risk management process is offered from the Nonprofit Risk Management Center at <http://www.nonprofitrisk.org/>.

Risk Management Life Cycle

Like every facet of network services we've touched on throughout this guide, risk management has a life cycle of its own. We see in Figure 10.7, the risk management life cycle, from identification, assessment, response development, to control and closure.

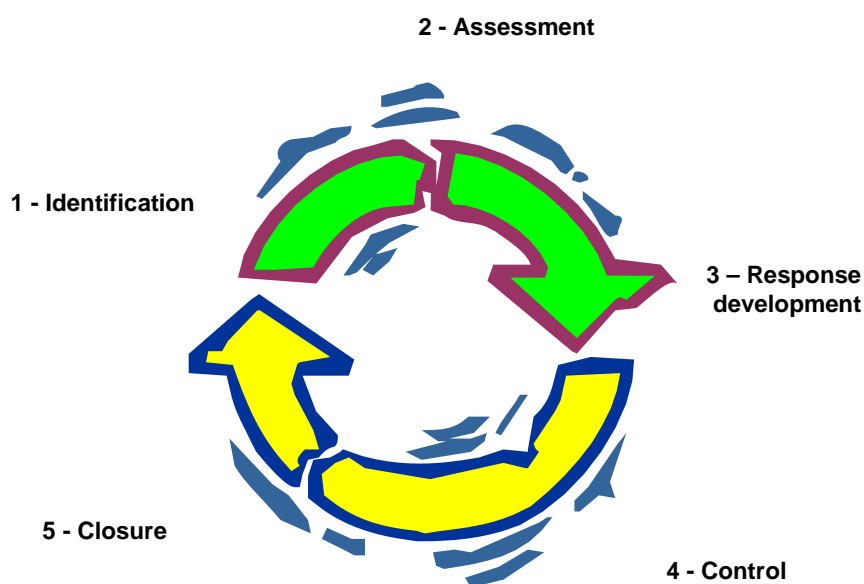


Figure 10.7: The risk management life cycle.

In simple thinking, we assess the risks to the business and determine what the core needs are to protect the corporate mission. This assessment typically identifies gaps between the current operational state and what poses acceptable risk. This gap analysis feeds the development of new policies, procedures, and controls.

As policies and procedures adapt and change to mitigate risk and meet business needs, it's vital that they be widely disseminated across the organization. This may present the greatest challenge, but a policy isn't effective if employees aren't aware it exists or what purpose it serves. Continuous monitoring of policies and controls will lead to ongoing improvements—a life of risk management within the life cycle of the enterprise itself.

Summary

For much of this guide, we focused on the FCAPS model as a tool for managing faults, configurations, accounting, performance, and security. FCAPS is a model from industry-driven standards groups and has been widely adopted in the telecommunications industry as a method for delivering voice and data services.

It's important to openly acknowledge that FCAPS isn't the only model and may not be the best approach for every organization. Today, many service providers take excerpts from the FCAPS approach and fold them into the ITIL model, creating an enterprise-specific framework from the array of best practices tools and techniques available in the marketplace.

For most organizations, there is no one model that fits all needs. The process of compiling the best facets of each approach is a learning process, maturation. As part of ITIL adoptions, most organizations perform a maturity self-assessment exercise to identify where they feel they fit along the curve of maturity as an IT services organization. Very few companies starting the process place themselves toward the mature end of the scale. The act of beginning, of assessing where your organization fits and documenting each step of the way, is a recognized best practice to delivering sustainable, reliable data, voice, and video services in a converged network. At the end of the day, the highly successful service delivery organization doesn't have just the ITIL library. They have the enterprise library of policies, procedures, and practices that, honed over time, document the best practices for managing the needs of that enterprise.

Download Additional eBooks from Realtime Nexus!

Realtime Nexus—The Digital Library provides world-class expert resources that IT professionals depend on to learn about the newest technologies. If you found this eBook to be informative, we encourage you to download more of our industry-leading technology eBooks and video guides at Realtime Nexus. Please visit <http://nexus.realtimepublishers.com>.