5

July 2000

IT SERVICE DELIVERY AND SUPPORT

CONTENTS

PREFACE

In today's digital world, the management of information, information systems and the communication of information to interested parties is key to the success of every organization. This is because of:

- *The increasing dependence on information and on the systems and communications that deliver the information.*
- *The scale and cost of current and future investments in information.*
- *The potential of technologies to dramatically change organizational and business practices, create new opportunities and reduce costs.*

Many organizations recognize the potential benefits that technology can yield. But, with those potential benefits, come risks. To provide effective direction and adequate control, executive management of successful organizations must not only appreciate the possible benefits, but also properly manage the risks and constraints of information technology.

In this guideline series, the International Federation of Accountants, through its Information Technology Committee, seeks to promote executive understanding of key issues affecting the management of information and communications. ***This series of guidelines is written for management.***

This guideline is the fifth in the series and covers ***IT service delivery and support****. In addition to describing the nature of the IT infrastructure required to provide services and support for an organization, this guideline provides an understanding of the main principles behind the approach to managing this area.*

Executives in various capacities (for example, accountants, financial controllers, auditors or business managers) are frequently asked to manage, participate in, assess or comment on the delivery and support of IT services and, indeed, to approve the budgeting requirements associated with this function. They can do this only if they have a sound knowledge of the principles and practices required to manage the delivery and support of IT services.

IFAC's Information Technology Committee would like to thank the various contributors who provided valuable input for this document:

Authors

John Frisken, ISG Consulting
Judith Merryweather, Alexer Pty Ltd
Charles Micallef, Micallef Computer Consultants Pty Ltd

Review Panel

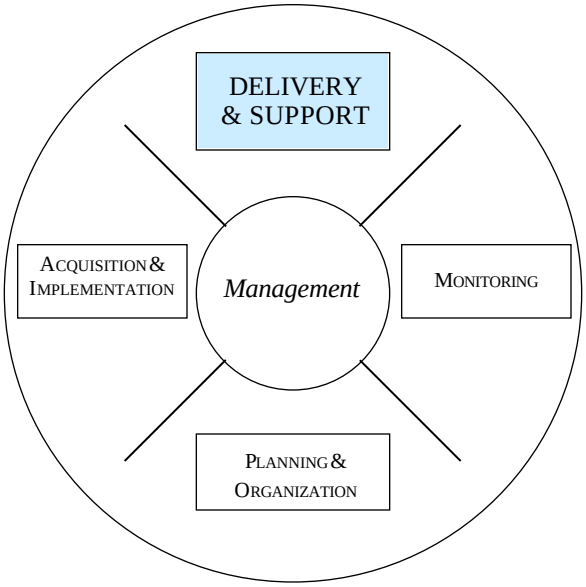
Stephen Arnold, Ernst & Young
George Cascales, South Eastern Area Health Services
Paul Eriksson, Sara Lee Intimate
Bob Hennessy, Westpac Financial Services
Kurt Huth, Bankers Trust Australia Limited
Gary Knep, Com Tech Communications

EXECUTIVE SUMMARY

WHY?

1. The IT Management Series provides Statements of Best Practices associated with the management of information technology (IT). While there are many methodologies and approaches to IT management, this series addresses the topic under the broad headings:

   - Planning and Organization
   - Acquisition and Implementation
   - Delivery and Support
   - Monitoring



2. This publication discusses the delivery and support of IT services, which range from traditional IT operations through to service level management, continuity of services, training and cost management. Terminology used in this publication is defined in the section "Key Definitions." This series also includes the actual processing of data by applications in line with the CobIT approach. This guideline should, therefore, be read in conjunction with the other titles in the series for an overall appreciation of the issues associated with IT management.

   Note: Security, which is an essential part of the overall delivery and support of IT services, is the subject of a separate IFAC publication (***International Information Technology Guideline 1: Managing Security of Information,***

January 1998). Similarly, the topic of outsourcing has been excluded from this publication and will be the subject of a separate IFAC IT Committee publication

3. Most businesses today rely on technology either directly, as IT customers, or indirectly, by relying on the information that is produced by information systems. To realize the maximum benefit from the investment in technology, organizations require sound applications, information systems and an IT infrastructure that meets the expectations of its IT customers.

4. Business success will not, however, depend solely on buying or installing the latest or most expensive technology or systems but, rather, from making sure that any new technology or information systems are appropriate and relevant to the people who will use them. Careful planning and monitoring are essential.

5. IT environments are more complex today, and there are more demands for IT services and support. Delivering these IT services requires skilled, experienced staff and a technology infrastructure that is easily supported, is flexible enough to process the volumes associated with operational peaks and can support the increased demands generated by growth in the business.

6. Technologies such as client/server environments, Internet/Intranet technologies, electronic commerce and Enterprise Resource Planning (ERP) are providing increasing challenges for IT management. Responsibility for the delivery and support of IT services is becoming more fragmented. In some organizations, business units share the responsibility for certain functions previously handled by the IT staff, and the infrastructure can be widely dispersed throughout the organization. In these circumstances, IT management must be highly organized and follow consistent practices to ensure uninterrupted business operations.

7. To realize such a goal for the organization, IT must be an integral part of its business strategy. IT management must be included in the planning processes to ensure that the information systems and technology infrastructure provide the delivery and support that the organization requires.

WHAT?

8. Although the information technology infrastructure and reliance on information systems varies from one organization to another, there are broad fundamentals that can be applied to all IT environments and that should be considered in the delivery of IT services and support.

   These core principles are:

   - ***ACCURACY*** — Information delivered to the business must be accurate and timely.
   - ***AWARENESS*** — Training, education and support services are provided to all IT staff and IT customers.

- ***COST EFFECTIVENESS*** — Systems and facilities should be aligned with business needs and not put undue financial burdens on the organization.
- ***CUSTOMER-FOCUSED*** — The organization's systems should be easy to operate and supportive of its business operations.
- ***DISCIPLINED APPROACH*** — Information technology should have adequate controls, a well-defined structure and consistent policies and procedures.
- ***FLEXIBILITY*** — Systems and facilities should exhibit a degree of flexibility to cater for fluctuations in business volumes and staffing levels and, wherever possible, be capable of being easily modified to handle changes in business practices.
- ***MEETING PERFORMANCE EXPECTATIONS*** — The delivery of, and support for, IT services must meet the expectations of IT customers, be available at agreed-on times and be measurable and measured.
- ***PROTECTED ENVIRONMENT*** — Business data and the facilities and information systems used to process them should be safe and secure. The environment should also offer a safe working environment for IT customers and staff.
- ***RELEVANCE*** — The systems and facilities should be appropriate and aligned with the organization's business needs. They should also be fit for purpose and conform to the user requirements.
- ***RELIABILITY*** — Information systems should be robust and reliable.

WHEN?

9. Delivery and support infrastructure for information technology must be available when the organization is about to deploy information technology. Such delivery and support mechanisms need to cover service level management, management of third-party services, performance and capacity, business continuity, security, budgets and cost allocation, training, customer service, configuration management, problem reporting, data management, facilities management and operations management.

   Unlike other phases, such as acquisition and implementation, which may depend on specific projects, delivery and support of IT services is continual. Certain functions, e.g., establishing budgets, will be performed according to corporate timetables. The majority of processes will, however, be performed almost daily and will require regular monitoring and review.

WHO?

10. The delivery and support of an organization's IT services is normally the responsibility of the Chief Information Officer and senior IT management. Depending on the size of the installation, some of the functions required to

deliver and support IT services may be fulfilled by the same person. Third-party suppliers may also fulfill some of the functions. This area is one of change, and current trends are for outsourcing certain functions. Despite the approach taken, the organization still has a responsibility for the delivery and support of IT services to its various business units.

As client/server technologies, Intranets and desktop computing proliferate, many of the functions may be fulfilled by personnel located within the business units rather than by specialized IT staff. Some aspects, such as security, are the responsibility of all corporate personnel and depend on a clear set of policies and procedures that are understood throughout the organization.

HOW?

11. To manage the delivery and support of IT services, we need to understand the expectations of the organization, its IT customers and, in particular, its senior management. These needs will vary according to how the organization uses technology but may include:

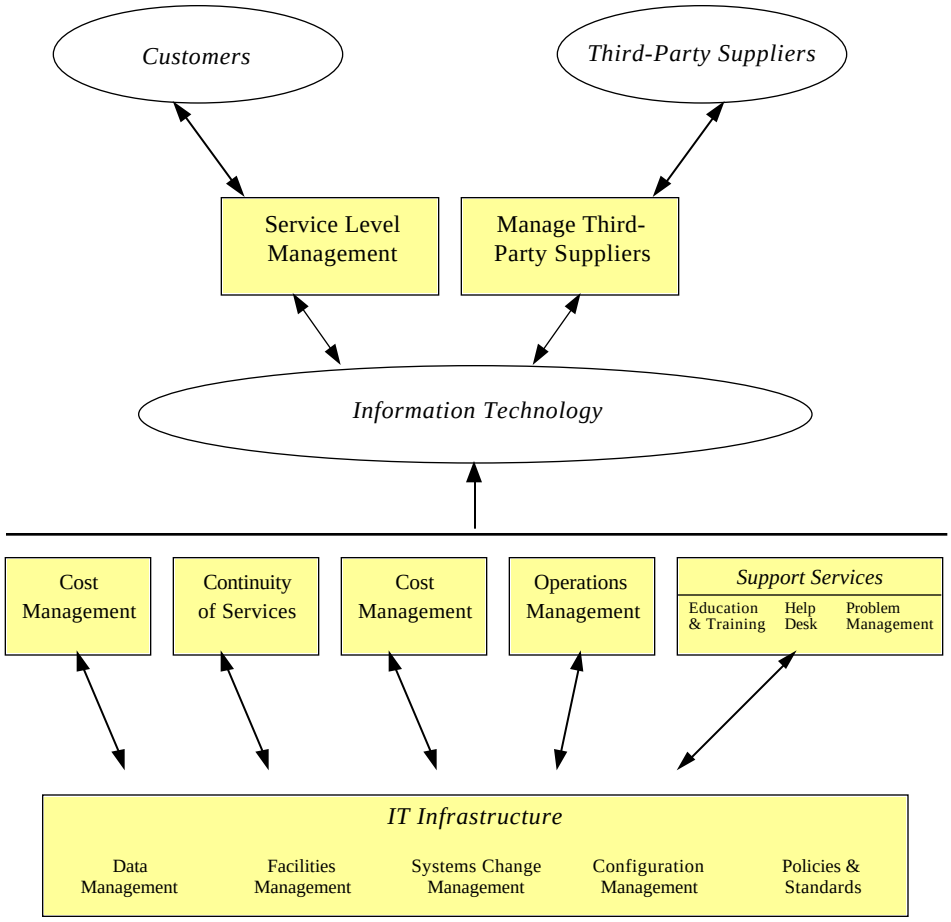
    - availability of services and facilities as and when required;
    - accessibility to information as and when required;
    - confidentiality and security of data;
    - good performance of systems and facilities;
    - timely training;
    - appropriate tools and facilities;
    - help and support when required;
    - problems and requests for enhancements resolved promptly.

12. Managing the IT services and processes to ensure that IT customers are satisfied involves delivering effective services, providing support and maintaining a reliable IT infrastructure.

    The diagram below depicts the linkages and relationships between the functions involved with both the delivery and support of IT services. Just how formalized the processes are will depend on the size of the organization and the nature of the business.

13. Functions involved in the delivery and support of IT services include the following, each of which is described in more detail later in this guideline.

IT Service Delivery and Support



Service Level Management: Service Level Agreements (SLAs) should be negotiated and established to define the clear requirements and expectations of customers and external suppliers. Management of the SLAs will ensure that services continue to meet the business needs.

Manage Third-Party Suppliers: Relationships with external suppliers must be built and managed to ensure they deliver value to the organization and that they continue to offer it the optimal solution.

Cost Management: Information technology requires a significant capital investment and represents a commitment to the future. The development and management of IT budgets and expenditure requires consultation, controls to

ensure the equitable recovery of expenditures and monitoring to ensure the realization of benefits.

Continuity of Services: With IT as the backbone of many organizations, steps to reduce the risks of failure of the technology infrastructure or the information systems are paramount to the organization's success. Continuity of IT services and the ability to recover after disasters should be aligned with the overall requirements for continuity of business operations.

Performance Management: Maintaining the agreed performance levels of IT is key to meeting the expectations of IT customers. This requires balancing the capacity available to deliver and meet the operational peak volumes today, and the capacity that will be required to meet the organization's future needs.

Operations Management: Many of today's information systems rely on the availability of specific technology infrastructure, the successful completion of jobs, the availability of networks and access to online services. Management of these aspects is key to delivering and supporting effective and efficient business operations.

Education and Training: To gain the most benefit, IT customers must be able to use the information systems and equipment properly. Appropriate training and education about the infrastructure, IT systems or processes involved will ensure that customers can use the systems efficiently and effectively, and that IT staff can adequately support IT customers.

Help Desk: Over recent years, the "Help Desk" has emerged as a necessary first line of support to IT customers. Management of this area, monitoring of calls and having appropriate skills for responding to the calls is essential to maintain the agreed levels of support.

Problem Management: Closely associated with the Help Desk is the need to manage reported problems that cannot be fixed on the spot. Problems requiring hardware or software upgrades need to be logged and monitored to ensure that the change does not have an adverse impact across other business units.

Data Management: Data is the core of the organization's information requirements. IT management must have sound management practices in place to protect, secure and maintain integrity of the organizational data.

Facilities Management: Resources, including human, physical and consumables, are required to deliver consistent, high-quality IT services. In addition, the facilities and environment in which they operate must be safe, secure and satisfy the organization's business needs.

System Changes Management: Problems requiring changes to systems or infrastructure need planning, prioritizing and scheduling to ensure that business interruptions are minimized.

Configuration Management: Programs, software, data and equipment can exist in many versions and under different licenses. Management and control of these versions and the licenses is necessary to ensure a continuous high level of IT service and also to meet all legal requirements.

Policies and Standards: Underlying all IT functions and processes and, in particular, the delivery and support of IT services, are a set of policies and standards. These policies and standards must be clear, kept up to date and the details widely promulgated.

KEY DEFINITIONS

14. **Applications:** computer programs, specifications, procedures, physical devices or techniques required to input, store, process, share, transmit or retrieve data and information relating to one or more groups of business processes.

    Authorized Use: use in a manner intended or otherwise sanctioned by the owner of the data.

    Communications: the transmission and reception of messages including both voice and data communications.

    Data: the representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation or processing by human beings or by automatic means.

    Data Definition: the characteristics associated with data held within a repository related to its source, currency and format.

    Data Disposal: the process of archiving, removing or destroying no-longer-required data within a repository.

    Data Integrity: where data conforms to the definition of data held within a repository with respect to its source, completeness and currency.

    Information: the meaning assigned to data by means of conventions applied to that data.

    Information Systems: the infrastructure of information technologies together with data and information that may be recorded, stored, processed, shared, retrieved or transmitted by them.

    IT Customers: those who use information systems or the technology infrastructure. Although this will generally be employees, in some instances, IT may support remote customers who are not employees but who use the organization's IT services.

    IT Staff: the human resources required to plan, operate, manage, develop, monitor and support information systems and IT infrastructure.

    Job: a collection of related computer programs that perform a regular business function.

    Management Procedure: any computerized or manual procedure designed to provide assurance that a function or process has been properly performed.

    Personal Data: data about a natural person describing his/her identity (name, date of birth, gender, family background, place of residence, etc.), religious beliefs, details of education, employment or professional associations, health

or medical history, purchasing patterns, or details of commercial and credit transactions.

Process: a series of manual and/or computerized tasks or instructions designed to perform a specific function.

Repository: any computerized or manual file used to store data about a subject or activity.

Resources: any piece of physical or human resource infrastructure required for the ongoing delivery of information system services to the organization. This will include processes, buildings, networks, terminals or personnel.

Threat: any potential or real source of risk to resources.

Technology Infrastructure: the hardware and software components and their interconnections required to support the applications.

Sabotage: deliberate actions carried out with the intention to cause destruction of facilities, inflict loss or otherwise hinder normal operations.

Service Level Agreement: a written agreement between information technology and the organization's business units spelling out the IT products and services to be delivered, and stating the performance criteria to be met.

Unintentional Loss: a loss that arises as an unintended consequence of a mistake or adverse incident occurring without malicious intent.

IT SERVICE DELIVERY AND SUPPORT

Service Level Management

15. Overview

A "Service Level Agreement" (SLA) is a written contract between a provider of a service and the consumer of the service. The purpose of the SLA is to establish measurable targets of performance with the objective of achieving a common understanding of the nature of and levels of service required.

IT management should have formal SLAs with all of their IT customers because these contracts provide:

- defined levels of service;
- accountability for the service;
- evaluation criteria and a basis for improvement;
- performance criteria;
- methods and processes of delivering the service;
- a method for communicating service expectations and actual performance;
- a basis for costing IT services to their customers.

The agreement defines the responsibilities of both parties and should encompass the following aspects:

- availability;
- reliability;
- performance;
- support;
- business continuity planning;
- security;
- service charges;
- capacity for growth;
- change management;
- penalties for non-delivery.

IT management should establish a benchmark for measuring performance to meet the agreed-on quality and quantity of service.

16. Common pitfalls

- Performance criteria are not specific.
- Customer obligations are not adequately defined.
- Service levels are not reviewed regularly.
- Performance is not monitored on a regular basis.
- Performance expectations are unrealistic.
- Method of delivery is not agreed on.
- Requirements are not adequately defined.

17. Outcomes

- Delivery and support of IT services meets the service levels defined in the SLA.
- IT customer expectations can be managed efficiently because the SLA provides an effective communication and performance measurement tool.
- Definitions of responsibilities, response times, volumes, charges, etc., are clear, objective and understood by all parties involved.
- Service levels should improve over time.

Manage Third-Party Suppliers

18. Overview

In today's business environment, many organizations use third-party service providers to deliver various information technology services. Third-party services include the supply of contractors and applications, provision of Web Site content, telecommunications services and fully outsourced IT functions. The reasons companies use third-party suppliers include:

- Management hopes to reduce cost while continuing to meet or exceed customer expectations.
- Downsizing means there are fewer staff to provide services in-house.
- The organization lacks core competencies needed to use advanced technologies.
- Third-party contracts enable the organization to concentrate on its core business.
- Internal IT staff are unable to meet the business needs.
- Applications and the majority of technology infrastructure have been purchased from third-party suppliers who provide ongoing upgrades and support.

While contracting out services to third parties has become a common practice, organizations need to exercise care in evaluating the need for outsourcing and how it is done. IT management also has a responsibility to manage the services to ensure that the expected benefits are realized. Use of third parties requires planning, management and discipline. Use of third parties does not just involve locating the required outside competencies, but can also involve (in the case of outsourcing) the searching out of a business partner who is competent and shares the organization's service delivery objectives.

19. Common pitfalls

- The organization fails to convey its business goals and objectives to its IT third-party service providers.
- The organization fails to identify the IT services that can be serviced by a third party.
- Service levels are not set, agreed on or monitored.
- The third party selected does not have the competencies required.
- The service contract is not enforceable.
- Contracts are often managed from a viewpoint of minimizing risks and not sharing rewards.

20. Outcomes

When managed correctly, third-party service contracts may provide the realization of expectations as outlined in the original proposal used to contract out the service, which could include the following outcomes:

- The provision of IT services at the current level but at reduced cost.
- The expansion of IT services to IT customers without the need for increased IT expenditures.
- The provision of more current IT systems to IT customers that allow the organization to fulfill its long-term corporate objectives.

- The organization is able to concentrate on its core activities while the third party provides it with the IT services required to carry on those activities.
- IT costs are fixed and can be more easily budgeted for.

Cost Management

21. Overview

Many organizations misunderstand the nature and extent of IT costs, both direct and indirect. Much of this can be related to the high costs of providing reliable, quality IT services and the inability to measure, and subsequently realize, the full benefits from IT.

Budgeting for the delivery and support of IT services must be done with the full knowledge and support of corporate management. Sound and realistic budgets will depend on a clear understanding of corporate goals, plans and priorities. In some organizations, SLAs may already be established, providing the basis for costing and, therefore, the necessary input to the budget. Once a budget is established, prudent controls must be put in place to ensure that expenses are controlled and that IT services are delivered within the operating budget.

There are many different funding sources for operations and projects, and they all need managing. Management must also decide the policy to be adopted in terms of cost allocation, e.g., charge-back schemes, and representation within the overall business. This policy should also recognize that there are many hidden IT costs within the organization's various business units.

Costs must be monitored constantly to ensure that trends for high expenditures are identified early and problem areas managed. Appropriate tools will assist in the collection of accurate job accounting and resource usage information for calculating accurate and full cost information.

22. Common pitfalls

- Market forces are not taken into consideration in the planning and budgeting process.
- Benefits of IT upgrades for the organization overall are underestimated.
- Business units and IT develop their budgets in isolation.
- Value for money is not seen as a key driver; instead, there is too much emphasis on cost.
- The full cost of running a complex IT service organization is not understood or measured.

23. Outcomes

- Senior management understands the costs and benefits of IT and, therefore, supports necessary budgetary expenditures.
- Charge-back schemes can help develop an understanding of IT costs and benefits. The organization's business units become more accountable for their IT demands and usage.

- Identifying IT as an unallocated cost center can stimulate usage, experimentation and understanding of IT.
- Management of total cost of ownership.

Continuity of Services

24. Overview

Management has the responsibility to maintain the continuity of mission-critical activities to meet organizational goals and objectives.

The organization requires a "Business Continuity Plan" (BCP) to ensure the uninterrupted availability of all key business resources required to support essential business functions.

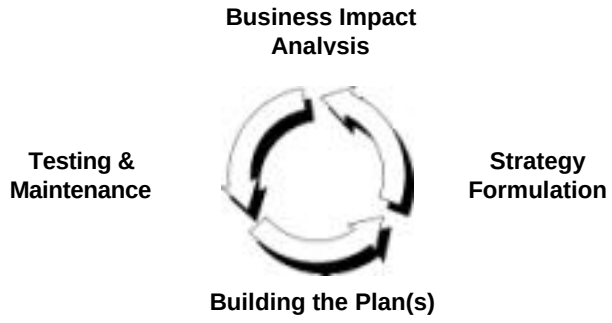
While this definition emphasizes the entire organization, IT management must provide a framework that minimizes the potential disruption to IT services of a significant event such as fire, loss of power or denial of access. Given the time-sensitive nature of many applications, the need for continuous IT service delivery is paramount to business survival. For an organization to survive a disaster, the restoration of essential systems must be accomplished as quickly as possible. This requires careful planning.

The purpose of a BCP is to ensure that steps are taken in advance to maintain continuity of essential business functions should a crisis occur. IT management should prepare and maintain a written plan in accordance with the overall framework for restoring essential information services in the event of a disaster.

Planning for continuity of services should consider:

- *Prevention*: What can be done to prevent the crisis from occurring in the first place?
- *Detection*: What can be done to ensure timely detection of the crisis?
- *Correction*: What can be done to respond to, and recover from, the crisis?

and should be based on a methodology such as the following diagram:



25. Common pitfalls

- Business impact analysis is not performed.
- Worst-case scenarios are not developed.
- BCPs are not tested.
- BCPs are not maintained.

26. Outcomes

- The delivery and support of the organization's IT services continue within an acceptable timeframe after a disruption.
- The roles and responsibilities, alternative processing facilities and alternative procedures to be used subsequent to a disaster have been well defined.
- IT staff familiar with the BCP and the recovery procedures have been identified.

Performance Management

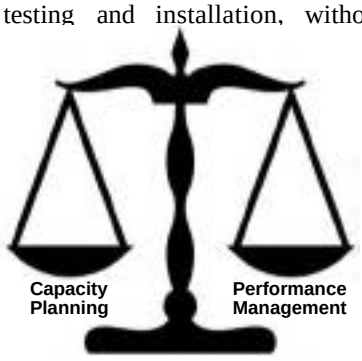
27. Overview

Organizations depend on timely access to business information, efficient processing of data and effective reporting of information. As electronic business becomes an integral part of operations, the demands for speedy and reliable access increase correspondingly. Associated demands, such as increased storage requirements and access to resource-hungry applications, are placing increased pressure on planning for future growth while continuing to meet the expectations of IT customers.

Not only must IT departments work within existing resource constraints, but they must also continually stay up to date with technology to ensure that appropriate services are available to support the organization. Logging system resource usage and monitoring results is essential to balance the IT resources available with the demands of the organization's business units.

Business peaks and trends for increased volumes should be considered and plans established to maintain delivery and support throughout all business cycles. Modeling and forecasting tools can provide projections of the likely impacts on the organization to allow IT to develop plans and acquire appropriate equipment to ensure the continuity of agreed-on service levels. Forecasting methods include rules of thumb, simulation, benchmarking and analytical models.

IT must strike a balance between the detailed and specific information required to resolve and address a performance issue and the more general trend information required for forecasting and capacity planning. When additional capacity is required, the acquisition should be timely and allow sufficient time for testing and installation, without affecting existing business schedules, p



28. Common pitfalls

- Business units give insufficient notice when ordering additional equipment or capacity and operations suffer as a result.
- IT is not informed of major business decisions affecting the organization or user environments.
- Poor performance can frustrate staff and lead to work-arounds or implementations of one-off solutions.

29. Outcomes

- Service level expectations of response times, access and systems support are met. IT customers will get the agreed-on level of IT support.
- Organizational schedules operate efficiently, and peak periods are handled with little or no disruption.

Operations Management

30. Overview

Failures in the "Operations" function increasingly jeopardize the entire organization. While these "back-room" operations often suffer from cost and resource cutbacks, management should not ignore this crucial part of IT.

Operations management involves many of the day-to-day activities associated with running the IT infrastructure, such as scheduling regular jobs, scheduling workload arrangements, planning systems maintenance, managing the computer networks and managing communications. Job scheduling is a complex task, requiring a balance between the run times of the jobs, the priorities for the organization, the frequencies of the jobs and the resources required to run the jobs. Where shift work is involved or where several staff members are involved with operations, management must ensure that there are appropriate hand-over procedures in place to ensure the continuity of jobs and operational activities.

Operations management requires the planning, monitoring and recording of all activities, the prioritization of tasks and scheduling of resources to deliver IT services to the organization. All personnel must understand the business priorities and requirements and ensure that a balance is achieved with the available resources. Availability of operational equipment relies on regular maintenance procedures, which must be scheduled and completed to minimize the impact on the daily business operations.

As more and more business functions are delivered in real time and online, the management of networks is fast becoming a core activity of IT delivery. The convergence of computing and telecommunications, the introduction of Intranets, adoption of Internet technologies and the emergence of electronic commerce generate enormous expectations for access to information and, thus, for the availability of sound and reliable networks.

31. Common pitfalls

- Under pressure from IT customers for continuous access, maintenance activities are often delayed, causing problems and costly urgent repairs.
- No processes are established to communicate with IT customers about operational problems, thus creating frustration among those customers.
- Ongoing battles with user groups over priorities.

32. Outcomes

- IT customers receive information that is timely and up to date.
- The organization's business units have access to equipment that works efficiently and effectively to support their work.
- Equipment is maintained as required on a cost-effective basis.

Education and Training

33. Overview

A comprehensive understanding of the uses and impacts of IT on the organization can often remove some of the barriers to the use of systems and technology, while timely training to support the introduction of new systems or technology can also provide substantial benefits.

IT customers have varying levels of IT skills and knowledge. To ensure the smooth delivery of services and the maximum use of the facilities, IT management must first have a clear understanding of the current skills base of its customers. With this baseline, often prepared in conjunction with the Human Resources Department, the needs of IT customers can be defined and appropriate education scheduled. Relevant and timely training must accompany all changes to business systems and all new systems implementations.

Appropriately skilled and knowledgeable IT staff are also key to providing relevant and satisfactory support to the organization. Keeping staff up to date with developments and emerging technologies will foster staff loyalty and continuity of IT service delivery and support.

Training curricula for particular functions and particular business units will enable the organization to match appropriate skill levels to the business goals and resources available. Various approaches can be used to support the necessary training, including in-house training, self-study, computer based training (CBT), mentoring, external providers or strategic partnerships. Major upgrades, new systems implementations and changes may also require review of the training curricula and the development of new courses.

34. Common pitfalls

- Training is not timely.
- Organizations do not invest in maintaining the currency of the skills and knowledge of their IT Staff.
- No formal procedures are established for training and inducting new staff into the IT practices of the organization.
- External provider training for one group of IT customers, or for one particular package, differs significantly from other internal practices throughout the organization.
- IT customers who are insufficiently trained will call the Help Desk repeatedly, wasting the valuable time of this resource.

35. Outcomes

- IT customers can effectively use the technology and systems to perform efficient business operations.
- IT customers are more self-sufficient and have a consistent approach to the use of IT.

Help Desk

36. Overview

With an increasing reliance on technology in the workplace, the Help Desk has become a crucial factor in ensuring effective and efficient operations. The Help Desk, which is the first-line area for IT customers with problems, has become the focus of high service level expectations. Organizations may establish a composite Help Desk facility utilizing both internal resources and the services of an external Help Desk for specialized systems or facilities. IT customer requirements for a Help facility may be closely linked with the assessment undertaken for education and training and the education programs ultimately implemented.

IT management must ensure that Help Desk strategies are aligned to the changing technological environment and to the organization's needs. As most desktop applications are mission-critical to the company's success, it is essential that the Help Desk staff have appropriate tools to log, monitor and manage the calls to ensure that IT customers can resume normal operations as soon as possible. Knowledge systems or expert systems may be developed to capture the expertise of the Help Desk staff. This will assist when new staff are recruited for this function and create awareness of recurring problems.

Strategies must be in place to address problems that cannot be readily fixed, including ensuring that unresolved problems are flagged for follow-up and not forgotten. Regular reporting of Help Desk performance can assist in establishing reasonable service level expectations and in highlighting problem areas where further action is required, e.g., specific education and training programs, upgrades to hardware or software systems.

37. Common pitfalls

- If IT customers do not receive adequate training up front, the Help Desk can become a pseudo training facility, and some of its resources will be wasted.
- Many IT customers have no idea of the workload of the Help Desk staff members, who often end up the object of IT customer frustration, anger and derision.

38. Outcomes

- The organization operates smoothly, using IT facilities, and IT customers can depend on having problems resolved quickly.

Problem Management

39. Overview

Problem management refers to managing the problems and incidents logged by the Help Desk. Logged problems must be given an appropriate level of resources so that they can be resolved in a timely manner.

Organizational management should help make decisions on prioritizing problems to ensure minimal disruption to normal business operations, and regular reports should be provided on problem resolution progress. Guidelines should be agreed on for dealing with reported problems that may take some time to resolve, the impacts of those problems on the business or implications for other systems and IT customers.

Problem management has a proactive role in identifying weaknesses in the applications or infrastructure and areas of concern in the service support. Once these adverse trends are recognized, problems can be highlighted and corrective action initiated, e.g., forwarded to systems change management or further education and training.

40. Common pitfalls

- Problems are logged but IT customers are not notified of progress.
- Problems are analyzed in isolation, and common trends and underlying problems are not addressed.
- Urgent problems are not given due priority, are not identified for follow-up and disrupt IT customers.

41. Outcomes

- Problems are resolved quickly, minimizing business interruption.
- IT customers receive the expected level of service from IT, and changes to applications are performed as quickly as needed.

Data and Information Management

42. Overview

Organizations collect data as part of their normal business operations. Data can be held within both computerized and physical repositories and can be

processed using manual or computerized processes. It can take a wide variety of forms, including data held within accounting applications, manufacturing, process control, engineering or other specialized applications. Data also includes documents such as manual forms, written correspondence, digital images, e-mail, maps, plans and virtually any other pertinent document, observation or item of knowledge held by, or known to, an organization's employees.

Data management refers to the processes and applications that an organization puts in place to collect, store and dispose of corporate information, including the data used to create that information. Information management is a related series of techniques referring to the processes and approaches of managing computerized and manual data in an orderly manner to permit ease of storage, retrieval and reporting by users and applications.

Important considerations for the management of data include:

- Developing standards defining responsibility for ownership, management and use of data with the organization. These standards should be reviewed on a regular basis.
- Conducting risk assessments of threats to corporate data.
- Protecting data of a confidential, private or proprietary nature from unauthorized disclosure and using it only for approved purposes.
- Establishing policies and procedures to ensure that data input into business applications is accurate, authorized, complete and processed in an accurate and timely manner.
- Developing policies defining the length of time that various classes of data and business records should be retained and destroying, on a regular basis, all records and business data exceeding the specified retention periods.
- Regularly backing up business data and applications; back-ups should be securely stored in an appropriate environment.
- Establishing controls and processes over access to and use of corporate data by external parties.

43. Common pitfalls

- Lack of independent review of controls.
- Controls are not based on an assessment of risks to data and, thus, are ineffective.
- Procedures over confidential, personal or proprietary data are inadequate.
- Data is not managed as a corporate resource.
- Data back-up and recovery procedures have not been tested.

44. Outcomes

- Data is managed as a valuable corporate resource and the value of data to the organization is continually enhanced through use and refinement.

- The integrity and security of data is protected through the implementation of an appropriate control framework that responds to the threats to an organization's data resources.
- The net benefits associated with the management and protection of data are maximized.

Facilities Management

45. Overview

Information technology utilizes substantial resources in terms of the costs of physical equipment and the costs associated with personnel employed within the function. This investment in IT resources must be protected and developed to ensure the organization can continue operating in a cost-effective manner.

Physical resources comprise the computer room, computer equipment and consumables, communication networks, local area networks, terminals and PCs. They may also include remote facilities.

Human resources consist of the employees who operate the computer facilities, develop information systems or provide IT services to user departments.

Management of these resources is essential to protect and develop an organization's investment in physical and human resources, and to meet its service delivery expectations. This management will take various forms, including evaluation of employee performance, availability of appropriate training and education for IT personnel, and the development of policies and procedures regarding the effective operation of corporate IT facilities.

46. Common pitfalls

- Threats are not clearly identified.
- Visitors are not challenged.
- Business continuity plans have not been tested or maintained.
- There are no offsite contingency plans.
- Insurance is inadequate.

47. Outcomes

- Resources are protected from misappropriation or destruction.
- Risks to facilities and resources are identified and effectively managed.
- Human resources are adequately protected.
- Business continuity plans are in place for essential corporate infrastructure.

Systems Change Management

48. Overview

Systems change management refers to managing ongoing systems changes. Changes can be triggered by problems logged by the Help Desk or by changing business needs, changes in the environment or bugs lying dormant in the system until a specific set of circumstances arise. Formal procedures should be established to ensure that changes are properly authorized and controlled. All applications changes or new infrastructure implementations should be thoroughly tested and follow the guidelines established for version control before being used in the production environment.

Organizational management should participate in making decisions on prioritizing system changes. Guidelines should also be agreed on for emergency changes and for resolving problems that have been outstanding for a long time, with attention paid to the impacts those problems might have on the organization or implications for other systems and IT customers.

49. Common pitfalls

- IT customers and other business units may lobby to get changes into production before they are adequately tested.
- Inadequate version control can lead to changes being made to old versions of programs.

50. Outcomes

- Business interruptions created by problems or fixes are minimized.
- IT customers receive the expected level of service from IT.
- Changes to systems are performed as quickly as needed.

Configuration Management

51. Overview

Configuration management provides a mechanism for identifying, tracking, controlling and maintaining the organization's hardware and software. Configuration management is a prerequisite to change management because it establishes the baseline against which all changes are made. In many cases, earlier versions of some of the software are still in use and must also be maintained and controlled.

ISO 9000-3 1991 states that software configuration management should:

- uniquely identify the version of each authorized item (software or hardware) and record it;
- identify the versions of each software item that constitutes a specific version or build of a complete software product;
- identify the build status of software products in development or production;
- control simultaneous update of a software item by more than one person;
- provide coordination for the updating of multiple products in one or more locations;

- identify and track all actions and changes from initiation through to release.

These characteristics of software configuration can be expanded to IT configuration in general. All components that make up the IT environment must be under configuration control, including:

- application software;
- system software;
- hardware.

Configuration management activities require definition in a "Configuration Management Plan" and involve identifying and recording the characteristics of all hardware and software. The specification that the IT customers have accepted, called a "baseline," serves as a basis for formal change procedures. Changes to baselines must be controlled. Only authorized changes should be implemented.

IT management should establish and maintain procedures to record, manage and report on the status of all configuration items. Periodically, the organization should perform an audit to verify and validate the extent to which the configured baselines reflect the actual physical and functional content.

52. Common pitfalls

- Initial baselines for configuration items are not established and frozen.
- Changes to configuration items are not controlled so that amendments made to a baseline in one version of a configuration item are overwritten by amendments made to another baseline.
- There are no configuration management plans for identifying the mechanisms for implementing configuration management.
- Mechanisms are not put in place so that amendments can be rolled back should they fail in production. These amendments lack traceability.
- Mechanisms are not implemented to ensure that only authorized modifications to configuration items are implemented.
- Unauthorized/unlicensed software is implemented and used within an organization.

53. Outcomes

- All modifications to configuration items are controlled. No unauthorized changes to configuration items can be implemented.
- Modifications are not overwritten by the release of new versions of configuration items.
- Traceability for all changes to baselined items is provided.
- All modifications to baselines can be reversed, if necessary.

Policies and Standards

54. Overview

The main objective of the standard-setting process is to provide the management framework and context within which ongoing operations are managed to deliver IT services. The development of standards provides the opportunity for the organization to influence, and become responsible for, IT decisions without requiring managers to become involved in reviewing every decision.

Policies and standards provide high-level guidance for IT decision making and provide the key linkage between business and technology strategy. Standards and policies are derived from, and support, the achievement of the organization's business goals and corporate values on an ongoing basis. They provide the basis for establishing a well-managed IT facility and are a crucial component of corporate governance.

The existence of standards and policies is an essential mechanism for measuring the quality of IT service delivery and maintaining accountability for key information technology activities. The effective implementation of IT standards and policies will ensure greater consistency in decision making in relation to the management of information technology service delivery.

Common areas where it is anticipated that policies and standards would normally be developed in relation to ongoing IT operations include:

- organization and responsibility for IT-related activities;
- management of IT personnel;
- electronic communication, including e-mail, telephones, faxes and modems;
- management of computing devices, networks and communication systems;
- relationship with user departments;
- management of technology;
- preferred hardware, communication and database vendors;
- guidelines for acquisition of new technology;
- interoperability of applications databases and operating systems;
- system development and maintenance procedures and methodologies.

In some circumstances, it may not be appropriate to always enforce standards. There should be a process to approve exceptions where it can be demonstrated to be appropriate and of benefit to the organization.

55. Common pitfalls

- Policies and standards are not documented.
- There is a lack of business input and ownership.
- Standards are not updated on a regular basis.

- Compliance is not evaluated.

56. Outcomes

- IT service delivery quality is improved.
- Risks are mitigated.
- Consistency is achieved.

SUMMARY OF OTHER DOCUMENTS

The Committee has issued one Information and Communications Technology Project, as summarized below. To obtain copies of this document, please visit the IFAC Web site at www.ifac.org or contact the IFAC Secretariat.

Information and Communications Technology Project
Executive Checklist
Issued October 1999

The checklist was developed to provide questions senior management should ask before authorizing any investment in an IT project. Questions are organized around the key stages of an IT project: the strategic dimension; checking the benefits; appraising the project; managing the change; managing the risk; legal compliance; and security issues. It was designed to help executives control costs and be more proactively involved in the key stages of an IT project.