

2nd Issue, December 1, 2005

# Bayside

**An Introductory  
Overview Of ITIL**

**Mainframe Security  
Issue**

**The REGION JCL  
Parameter**

# Advisor

Winter 2005

## Table of Contents

▶ An Introductory Overview of ITIL	3
▶ Featured Articles	
▶ Mainframe Security Issue by James Smith	21
▶ The REGION JCL Parameter by James Smith	24

# An Introductory Overview of ITIL

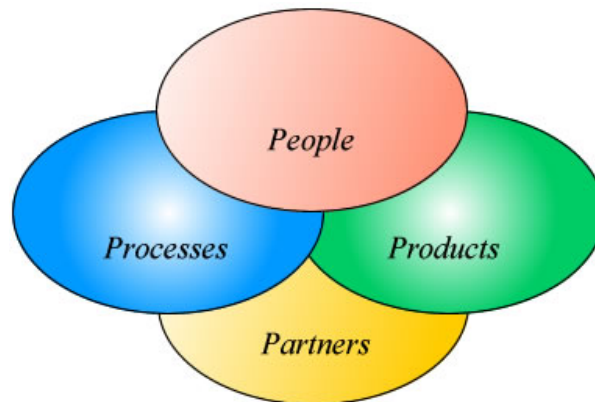
## 1. Introduction

In recent years it has become increasingly recognized that information is the important strategic resource that any organization has to manage. Key to the collection, analysis, production and distribution of information within an organization is the quality of the Information Communication Technology (ICT) systems and IT services provided to the business. It is essential that we recognize that ICT systems are crucial, organizational assets and therefore organizations must invest appropriate levels of resource into the support, delivery and management of these critical IT services and the ICT systems that underpin them. However, these aspects of IT are often overlooked or only superficially addressed within many organizations.

The key issues facing many of today's senior Business Managers and IT Managers are:

- IT and business strategic planning
- Integrating and aligning IT and business goals
- Acquiring and retaining the right resources and skill sets
- Implementing continuous improvement
- Measuring IT organization

- effectiveness and efficiency
- Reducing costs and the Total Cost of Ownership (TCO)
- Achieving and demonstrating Value For Money (VFM) and Return on Investment (ROI)
- Demonstrating the business value of IT
- Developing business and IT partnerships and relationships
- Improving project delivery success



**Figure 1: The Four Ps**

- Outsourcing, insourcing and smart sourcing
- Using IT to gain competitive advantage
- Delivering the required, business justified IT services (i.e. delivering what is required, when required and at an agreed cost)
- Managing constant business and IT change
- Following the sun and offshore operations
- Demonstrating appropriate IT governance.

The challenges for IT managers are to co-ordinate and work in partnership with the business to deliver high quality IT services. This has to be achieved while reducing the overall TCO and often increasing the frequency, complexity and the volume of Change. The main method of realizing this goal is the operation of effective processes and the provision of appropriate, value for money services. To achieve this, the correct processes need to be developed and implemented with in-built assessment and improvement mechanisms. IT management is all about the efficient and effective use of the four Ps, people, processes, products (tools and technology) and partners (suppliers, vendors and outsourcing organizations).

Management therefore needs to develop joint strategies and plans for all four areas within Figure 1. However, many organizations, in the past and still today, recognize the four Ps but do not use them for maximum advantage. All too often products are bought to manage areas of technology and then the processes, partners and people's roles are engineered to fit the technology and its limitations. The people and processes issues must be addressed first and this is one of the core principles of ITIL.

## 2. What is IT Service Management?

What do people mean when they refer to “**Service Management**”?

Different people use the term in different contexts. Some use it to refer specifically to just the Service Delivery and Service Support ITIL books while others use it to include all of ITIL. In reality, Service Management should refer to any aspect of the management of IT service provision and therefore should include the whole of ITIL and not be limited to just two of the core modules. This is the definition and interpretation of the Service Management term used throughout this guide and is a core principle of ITIL.

Another core principle of ITIL and IT Service Management is the provision of quality Customer service. This is achieved by ensuring that Customer requirements and expectations are all times. The satisfaction of business and Customer requirements is fundamental to the whole of ITIL and there are a number of key activities that are vital to the success of ITIL processes within this area:

- Documenting negotiating and agreeing Customer and business quality targets and responsibilities in Service Level Agreements (SLAs)
- Regular assessment of Customer opinion in Customer feedback and Customer Satisfaction Surveys
- IT personnel regularly taking the ‘Customer journey’ and

sampling the ‘Customer experience’

- IT personnel taking the Customer and business perspective and always trying to keep Customer interactions as simple and enjoyable as possible
- Understanding the ICT infrastructure.

### Tip:

To keep interactions as simple and enjoyable for the Customer as possible use language that they understand and don’t use technical IT terms.

ITIL recognizes that there is no universal solution to the design and implementation of an optimized process for the management and delivery of quality IT services. Many experts, authorities, leading practitioners and exponents within the IT industry have contributed to the development of ITIL and the result is a framework that provides a “**common sense**”, structured approach to the essential processes involved. ITIL has been developed to be process driven and yet scalable and sufficiently flexible to fit any organization from Small, Medium Enterprises (SMEs) to global multi-National Organizations.

Each organization whether an internal service provider or an external third party service provider should adopt the guidelines, principles and concepts of ITIL and adapt them to fit their own unique environment-“**adopt and adapt**”.

IT management must recognize the importance of their role in

underpinning the operation of the business. They must coordinate and work in partnership with the business, facilitating growth, rather than letting the technology and IT dictate and drive the business. It is essential therefore that the issues and expectations of business managers are closely aligned with objectives and deliverables of IT management. Therefore IT processes must be developed based on their ability to deliver true business benefit.

The only way of achieving this is design, plan and implement IT services using ICT infrastructure and management processes that deliver the information and solutions required by the business. The more effective organizations of today design the people’s roles, partner’s roles and the processes first and then configure the technology to support and automate them. In the truly efficient organizations these roles and processes are aligned to the business, the business requirements and the business processes. This ensures that the business and IT management processes and systems have aligned targets and goals.

ITIL provides “**best practice**” guidelines and architectures to ensure that IT processes are closely aligned to business processes and that IT delivers the correct and appropriate business solutions. ITIL is not a standard, nor is it rules or regulations and therefore neither tools, processes or people can be deemed “**ITIL compliant**”. Processes and organizations can be assessed against BS 15000, the IT Service Management standard. However, neither tools nor individuals can

be certified against BS 15000. Further information about BS 15000 is contained in section 12 of this guide.

### 3. Why Implement Service Management?

One of the main objectives of ITIL is to assist IT service provider organizations **“to improve IT efficiency and effectiveness whilst improving the overall quality of service to the business within imposed cost constraints”**

- The specific goals of IT are to develop and maintain IT services that:
- Develop and maintain good and responsive relationships with the business
- Meet the existing IT requirements of the business
- Are easily developed and enhanced to meet future business needs, within appropriate time scales and costs
- Make effective and efficient use of all IT resources
- Contribute to the improvement of the overall quality of IT service within the imposed cost constraints.

Benefits realized by many IT organizations through implementing ITIL and processes based on **“best practice”** guidelines are:

- Continuous improvement in the delivery of quality IT services
- Reduced long term costs through improved ROI or reduced TCO through process improvement

- Demonstrable VFM to the business, the board and stakeholders, through greater efficiency
- Reduced risk of not meeting business objectives, through the delivery of rapidly recoverable, consistent services
- Improved communication and better working relationships between IT and the business
- The ability to absorb a higher rate of Change with an improved, measurable rate of success
- Processes and procedures that can be audited for compliance to “best practice” guidelines
- Improved ability to counter take-over, mergers and outsourcing.

Examples of some of the savings made by organizations include:

- Over 70% reduction in service downtime
- ROI up by over 1000%
- Savings of 100 million per annum
- New product cycles reduced by 50%

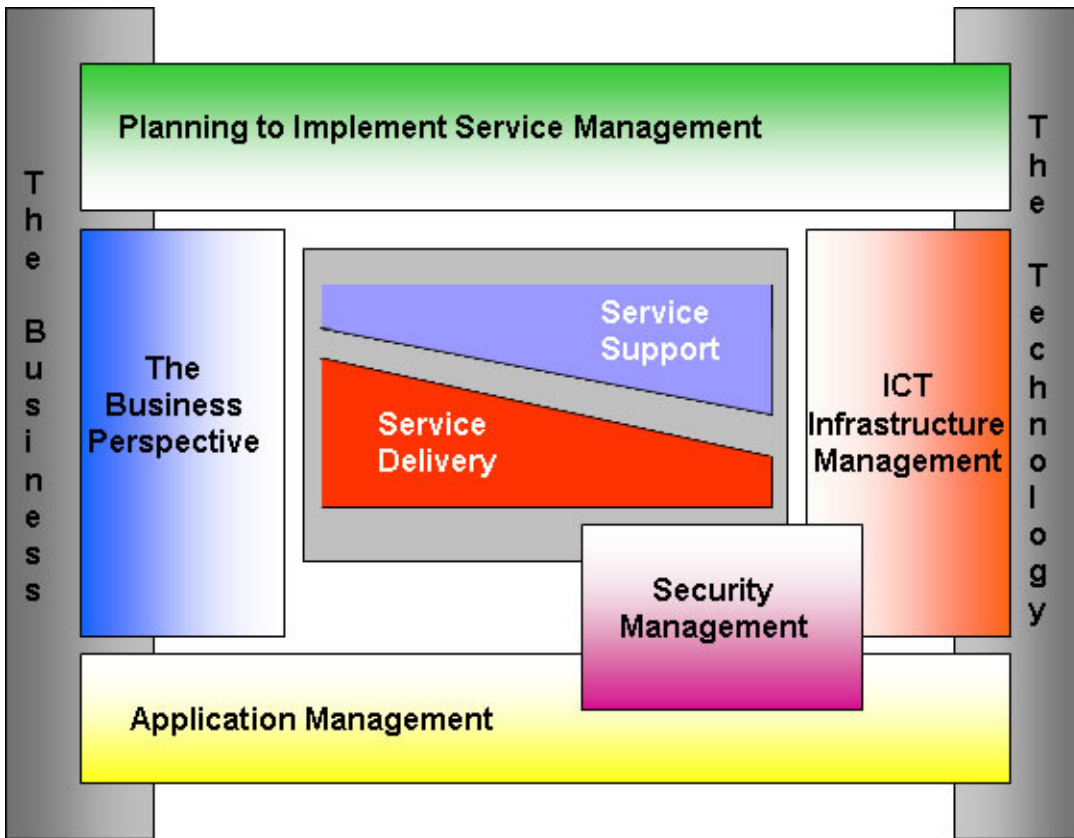
However, care must be taken when developing IT Service Management within an organization. It is easy to view and interpret ITIL as bulky and bureaucratic and as a result implement processes that inhibit Change rather than facilitate it. It is important that ITIL is implemented with an “adopt and adapt” approach so that effective and appropriate processes are put in place. This can only be achieved where business driven metrics, Critical Success Factors (CSFs) and Key Performance Indicators

(KPIs) are put in place to measure the success of the process implementations and their continuous improvement. Quality and the measurement of quality, in business related terms, is yet another core principle of ITIL.

### 4. The ITIL Framework

ITIL provides comprehensive “best practice” guidelines on all aspects of “end-to-end” Service Management and covers the complete spectrum of people, products and the use of partners. ITIL was initially designed and developed in the 1980s but has recently been revised and updated to bring it in line with modern practices, distributed computing and the internet. ITIL is the most widely used management approach to the delivery and support of IT services and infrastructure, world-wide. ITIL and its constituent modules were scoped and developed within an overall framework.

Figure 2 shows the overall environment and structure within which the modules were produced. It illustrates the relationship that each of the modules has with the business and the technology. From the diagram it can be seen how The Business Perspective module is more closely aligned to the business and the ICT Infrastructure Management module is more closely aligned with the technology itself. The Service Delivery and Service Support module provide the heart of the process framework.



**Application Management:** describes how to manage applications from the initial business need, through all stages in the application lifecycle, up to and including retirement. It places emphasis on ensuring that IT projects and strategies are tightly aligned with those of the business throughout the application lifecycle, to ensure that the business obtains best value from its investment.

**The Business Perspective:** provides advice and guidance to help IT personnel to understand how they can contribute to the business objectives and how their roles and services can be better aligned and exploited to maximize that contribution.

**Figure 2: The ITIL Framework**

These seven modules constitute the processes core of ITIL. Its recent revision has improved the structure of ITIL, and the new scope, contents and relationships of the various modules are in essence as follows.

**Service Delivery:** covers the processes required for the planning and delivery of quality IT services and looks at the longer term processes associated with improving the quality of IT services delivered.

**Service Support:** describes the processes associated with the day-to-day support and maintenance activities associated with the provision of IT services.

**ICT Infrastructure Management (ICT IM):** covers all aspects of ICT Infrastructure Management from identification of business requirements through the tendering process, to the testing, installation, deployment, and ongoing operation and optimization of the ICT components and IT services.

**Planning to Implement Service Management:** examines the issues and tasks involved in planning, implementing and improving Service Management processes within and organization. It also addresses the issues associated with addressing Cultural and Organizational Change, the development of a vision and strategy and the most appropriate method of approach.

**Security Management:** details the process of planning and managing a defined level of security for information and IT services, including all aspects associated with reaction to security incidents. It also includes the assessment and management of risks and vulnerabilities, and the implementation of cost justifiable countermeasures.

Figure 3 illustrates the scopes of each of the core ITIL modules together with the main deliverables from each of the individual processes, as shown

within each of the individual process boxes. The lines between processes indicate where the deliverables of each process are principally used outside of their own process area.

Each of the separate modules is expanded in the following sections.

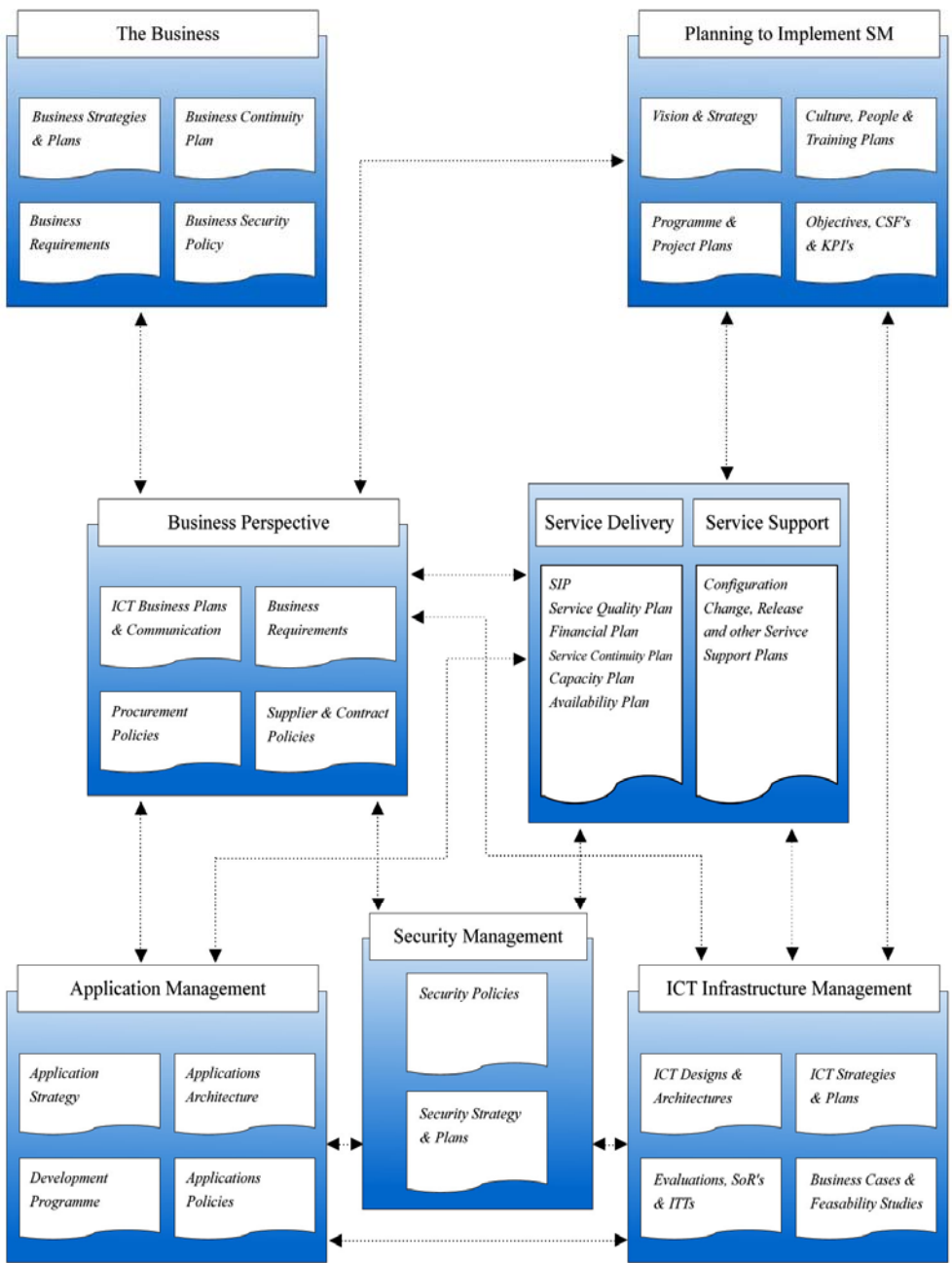


Figure 3: The Deliverables and Interfaces

## 5. Service Delivery

The Service Delivery module of ITIL covers the more forward-looking delivery aspects of service provision and consists of Service Level Management, Financial Management for IT Services, Capacity Management, IT Service Continuity and Availability Management. These processes are principally concerned with developing plans for improving the quality of the IT services delivered.

Figure 4 illustrates how Service Level Management (SLM) provides the major interface to the business and it also shows the major deliverables from each of the Service Delivery processes.

The SLM process negotiates, documents, agrees and reviews business service requirements and targets, within Service Level Requirements (SLRs) and Service Level Agreements (SLAs). These relate to the measurement, reporting and reviewing of service quality as delivered by IT to the business. The SLM process also negotiates and agrees the support targets contained in Operational Level Agreements (OLAs) with support teams and in underpinning contracts with suppliers, to ensure that these align with business targets contained within SLAs.

The other major roles of the SLM process are the production and maintenance of the Service Catalogue, which provides essential information on the complete portfolio of IT services provided, and the development,

co-ordination and management of the Service Improvement Program (SIP) OR Continuous Service Improvement Program (CSIP), which is the overall improvement plan for continuous improvement in the quality of IT services, as delivered to the business.

Financial Management for IT Services provides the basis for running IT as a business within a business and for developing a “**cost conscious**” and “**cost effective**” organization. The principle activities consist of understanding and accounting for the costs of provision of each IT service or business unit and the forecasting of future expenditure within the IT Financial Plan. There is also another optional, but preferred activity, the implementation of a charging strategy, which attempts to recover the IT costs, from the business, in a fair and equitable manner.

SLM demonstrates the level of service being delivered to the businesses day in and day out. As long as the service meets the business’ specified requirements, when cost models or a charge back mechanism are implemented under Financial Management, you can show the financial value of those services. This provides a baseline for assessing the financial viability of a service or adjusting charges in line with changing service requirements i.e. in general, a better service costs more money.

The Capacity Management process ensures that adequate capacity is available at all times to meet the requirements of the business by balancing “**business demand with IT supply**”. In order to achieve this,

a Capacity Plan closely linked to the business strategy and plans is produced and reviewed on a regular basis. This covers the three principle areas of Business, Service and Resource Capacity Management (BCM, SCM and RCM). These three areas comprise the activities necessary for ensuring that the IT capacity and the Capacity Plan are kept in line with business requirements. The common activities used within these areas are Performance Management, Workload

Management, Demand Management and Application Sizing and Modeling.

IT Service Continuity produces recovery plans designed to ensure that, following any major Incident causing or potentially causing disruption of service, IT services are provided to an agreed level, within an agreed schedule. It is important for each organization to recognize that IT Service Continuity is a component of Business Continuity Planning (BCP). The

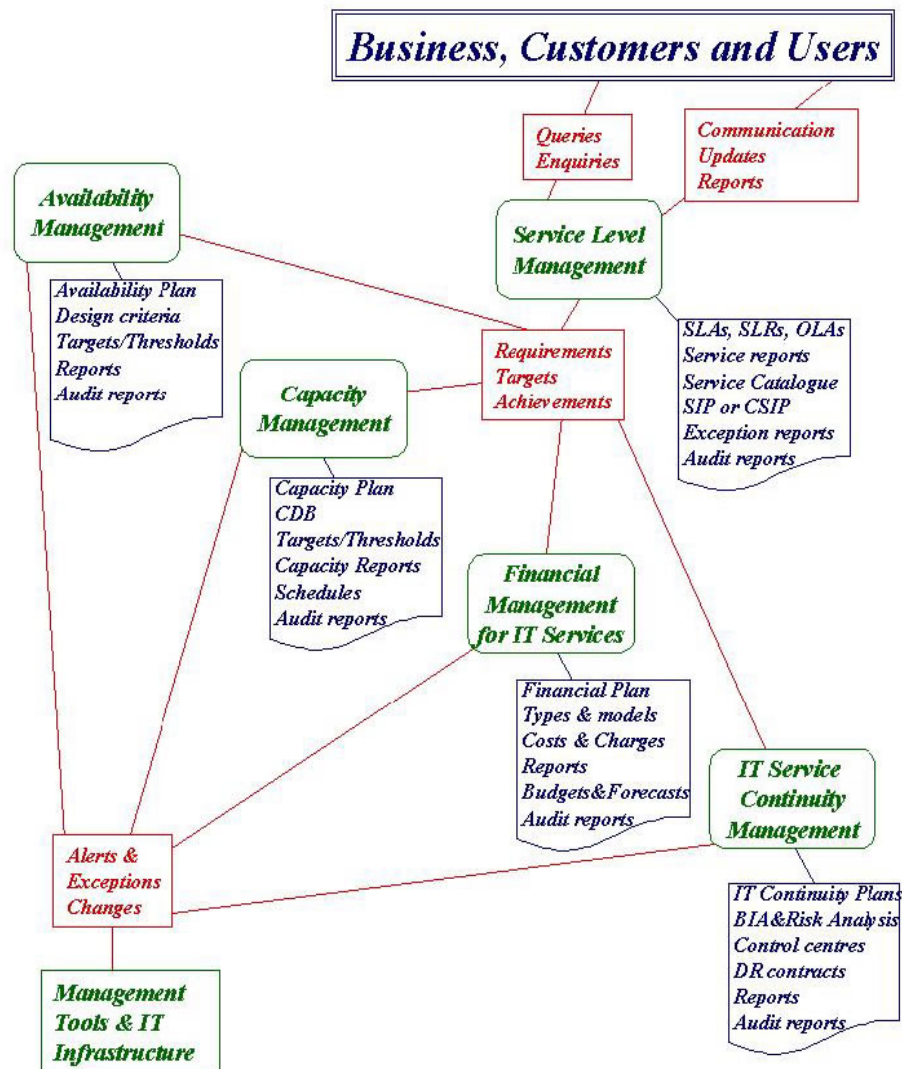


Figure 4: The Service Delivery Processes

objective of IT Service Continuity is to assist the business and BCP to minimize the disruption of essential business processes during and following a major Incident. To ensure that plans are kept in line with changing business needs Business Impact Analysis, Risk Analysis and Risk Management exercises are undertaken on a regular basis together with the maintenance and testing of all recovery plans.

Availability is a key aspect of service quality. Availability Management is responsible for ensuring that the availability of each service meets or exceeds its availability targets and is proactively improved on an ongoing basis. In order to achieve this, Availability Management monitors, measures, reports and reviews a key set of metrics for each service and component, which includes availability, reliability, maintainability, serviceability and security.

## 6. Service Support

The Service Support component of ITIL deals more with the day-to-day support and maintenance processes of Incident Management, Problem Management, Change Management, Configuration Management and Release Management plus the Service Desk function.

Figure 5 illustrates that the Service Desk function provides the major interface to the business and it also shows the

major deliverables from each of the Service Support Process.

The Service Desk provides a single, central point of contact for all Users of IT within an organization, handling all Incidents, queries and requests. It provides an interface for all of the other Service Support processes.

Incident Management is responsible for the management of all Incidents from detection and recording through to resolution and closure. The

objective of Incident Management is the restoration of normal service as soon as possible with minimal disruption to the business.

The goal of Problem Management is to minimize the adverse impact of Incidents and Problems on the business. To achieve this, Problem Management assists Incidents and Problems, while endeavoring to record all workarounds and 'quick fixes' as Known Errors where appropriate, and raising Changes to

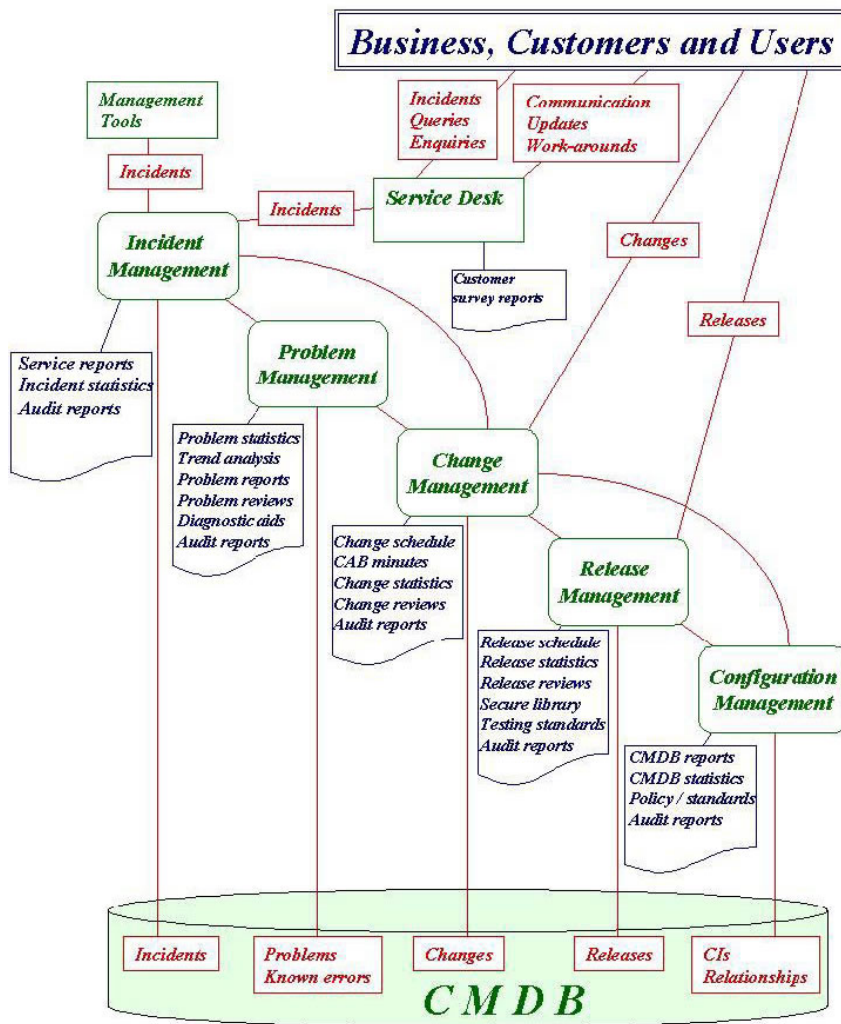


Figure 5: The Service Support Processes

implement permanent structural solutions wherever possible. Problem Management also analyses and trends Incidents and Problems to proactively prevent the occurrence of further Incidents and Problems.

A single centralized Change Management process, for the efficient and effective handling of Changes, is vital to the successful operation of any IT organization. Changes must be carefully managed throughout their entire lifecycle from initiation and recording, through filtering, assessment, categorization, authorization, scheduling, building, testing, implementation and eventually their review and closure. One of the key deliverable of the process is the Forward Schedule of Change (FSC) a central program of Change agreed by all areas, based on business impact and urgency.

The release Management process takes a holistic view of Changes to IT services, considering all aspects of a Release both technical and non-technical. Release Management is responsible for all legal and contractual obligations for all hardware and software in use within the organization. In order to achieve this and protect the IT assets, Release Management established secure environments for both hardware

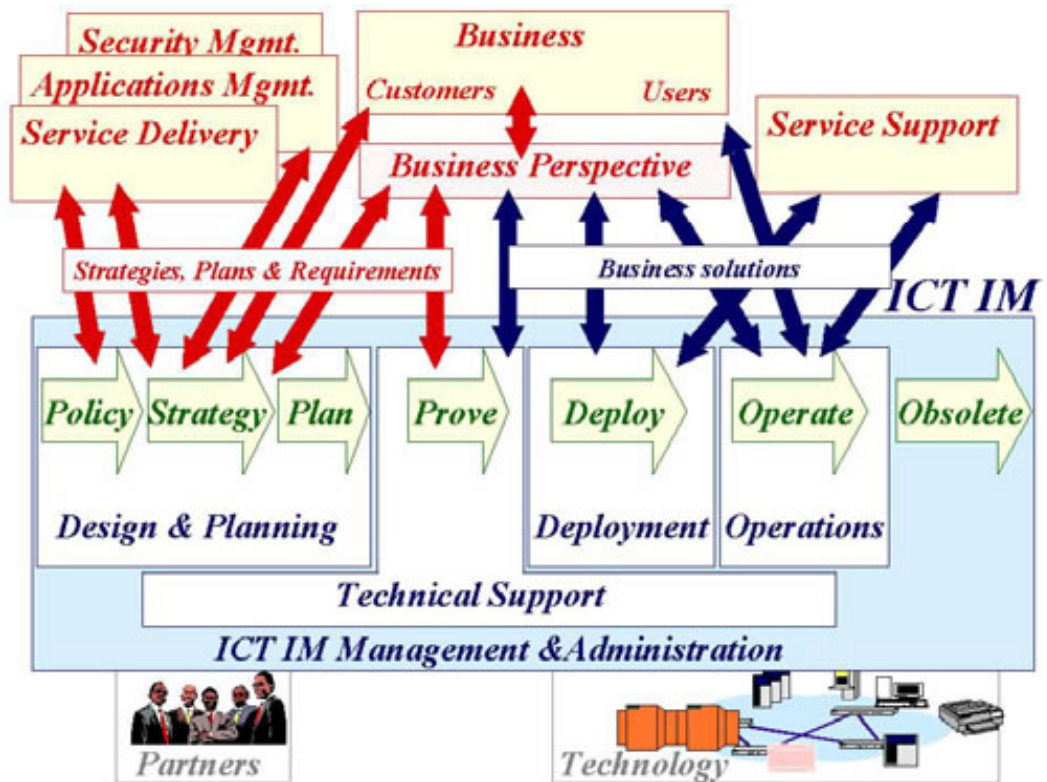
in the Definitive Hardware Store (DHS) and software in the Definitive Software Library (DSL).

Configuration Management provides the foundation of successful IT Service Management and underpins every other process. The fundamental deliverable is the Configuration Management Database (CMDB), comprising one or more integrated databases detailing all of the organization's IT infrastructure components and other important associated assets. It is these assets that deliver IT services and they are known as Configuration Items (CIs). What sets a CMDB apart from an ordinary asset register are the relationships, or links, that

define how each CI is interconnected and interdependent with its neighbors. These relationships allow activities such as impact analyses and 'what if?' scenarios to be carried out. Ideally the CMDB also contains details of any Incidents, Problems, Known Errors, and Changes associated with each CI.

## 7. ICT Infrastructure Management

ICT Infrastructure Management (ICT IM) looks at the challenges associated with the management of the ICT infrastructure and covers overall



**Figure 6: The Major ICT IM Interfaces**

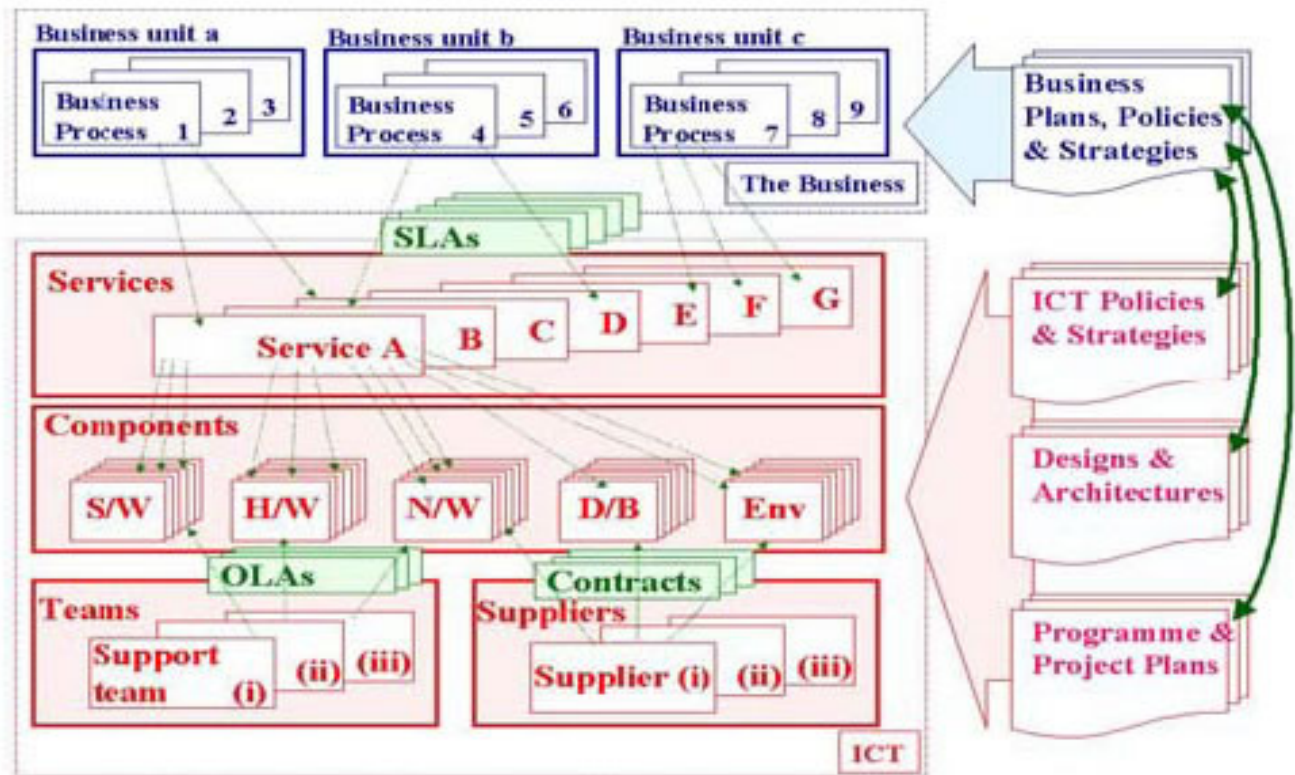
Management and Administration, Design and Planning, Technical Support, Deployment Operations.

ICT IM processes are closely associated with the ICT infrastructure on which the IT services run. They are all about managing the four Ps (see Figure 1) but concentrate on those areas of IT most closely related to the actual tools and technology as illustrated in Figure 6. The ICT IM processes

the ICT Operations processes and are responsible for ensuring that all operational events are appropriately managed and that all operational service targets are achieved.

The Management and Administration areas of ICT IM are responsible for creating the most appropriate environment under which a secure infrastructure is maintained for the delivery of quality IT services to the business both currently

a part of a Business Change program, by working with ICT Steering Group (ISG), through participation in quality and audit reviews, and also in crisis management situations. They also need to ensure that the support processes are in place so that all other areas of IT can operate effectively and efficiently. This requires their involvement, together with all of the other ITIL processes, in all stages of the service lifecycle from requirement analysis, through



**Figure 7: The ICT Infrastructure Model**

are responsible for managing a service through each of the stage in its lifecycle, from requirement, through design, feasibility, development, build, test, deployment, operation and optimization to retirement. The operation and optimization stages are the responsibility of

and in the future. The goal is to improve the effectiveness and efficiency of the ICT infrastructure, while maintaining the overall quality of the IT services provided.

ICT Infrastructure Managers play a key co-ordination role as

design, feasibility, development, build, test, deployment, implementation, pilot, operation and optimization, to eventual retirement.

The Design and Planning function is responsible for all of the strategic issues associated

with the running of an ICT function. They liaise with the business regarding future business plans and from the information provided, and in consultation with all other areas of the business and IT, develop the plans, architectures and strategies required for the provision of current and future ICT business solutions. One of the key tasks of Design and Planning is to include all requirements, not just the functional requirements, for a new service, considering them at the initial requirements stage and at each subsequent stage of the service lifecycle. This ensures that services are designed for “operational excellence” and that all business, Service Delivery, Service Support, operational and maintenance requirements are included at the earliest possible and most cost effective moment within the service lifecycle.

Another vital role of Design and Planning is to work closely with all business managers and planners, ISG, IT managers and planners, following the Business Perspective approach, to ensure that all business and ICT plans and strategies, as illustrated in Figure 7 are closely coordinated and aligned.

The Deployment process deploys new and changed ICT solutions to the business to agreed quality, cost and timescales. Deployment principally involves establishing projects and project methodology to ensure that new ICT solutions are delivered to the business with minimum disruption to business processes and that use of ICT resources is optimized. This is achieved by liaising closely with the business

and agreeing training, methodologies, handover processes and acceptance criteria.

The operational IT services and environments are managed and controlled within the Operations Management function. Operations use all of the management tools available to ensure that all services and components meet all operational targets, as agreed with the business and other teams in SLAs and OLAs. Operations are also responsible for the tuning and optimization of all operational areas of the ICT infrastructure.

Technical support ensures that the necessary support, skills and knowledge are available to underpin the overall service delivered by ICT IM. They maintain a pool of in-depth technical expertise to provide information guidance and actual resources for the research and development of new technology solutions, and third line technical support for all other areas of IT.

## 8. Planning to Implement Service Management

This module addresses the task of implementing or improving ITIL within an organization and considers aspects such as where and when to start, Organizational Change, Cultural Change, Project and Program Planning, Process Definition and Performance Improvement.

Using the approach in Figure 8 the overall vision for IT is produced first. An IT Service

Management vision is a mutually agreed statement of desire and intent between the business and IT. It describes the aim and purpose of the Service Management CSIP.

Once the vision has been determined it is important to establish “**Where are we now?**” This can be assessed using an overall IT organizational growth model that determines the current maturity of the IT organization in terms of:

- Vision and Strategy
- Steering
- Processes
- People
- Technology
- Culture

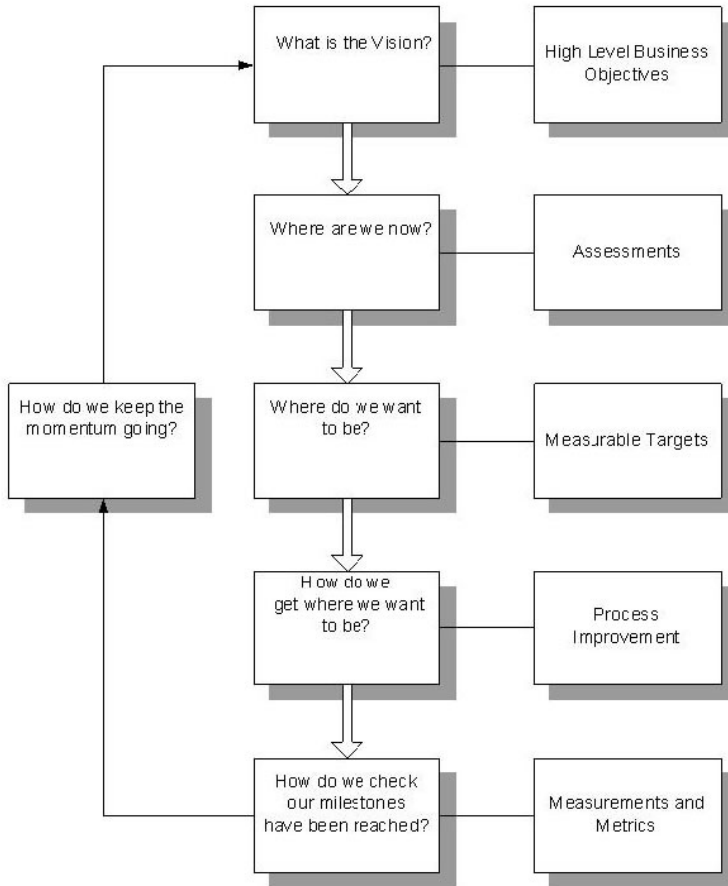
Other techniques which can be used for assessing current status include internal review, external benchmarking or process assessment against industry standards and guidelines (e.g. ITIL and BS 15000).

The business and IT must then agree the future role and characteristics required of the IT organization, to understand “**Where do we want to be?**” This stage involves the completion of a gap assessment report, together with a business case for the CSIP. Wherever possible, ‘quick wins’ must be identified, provided they do not inhibit the achievement of long term objectives.

A plan must then be produced for the CSIP project of “**How do we get where we want to be?**” This considers:

How the Changes are going to be achieved?

- Where to start?
- Which elements are



**Figure 8: Planning to Implement Service Management - Continuous Improvement**

essential to address within the CSIP?

The answers to these questions determine the approach, final scope and terms of reference for the CSIP project.

A set of measurable milestones, deliverables, CSFs and KPIs must be agreed to assess the progress and performance of the CSIP, i.e. **“How do we check milestones have been reached?”** All of these areas need to be regularly measured and reviewed at each stage of the project to ensure success. It is important to include measurements that directly relate to business benefits and quality business improvements.

Having started a CSIP, one of the hardest issues to address is maintaining the focus and commitment, i.e. **“How do we keep the momentum going?”** Sustaining improvement is made more difficult by the continued acceleration of the rate of Change within IT. The success of any ‘quick wins’ can be used to maintain the momentum during the project. Each improvement, once achieved, must be consolidated into everyone’s everyday practice, in job roles and job descriptions.

Throughout all CSIP activities the key messages of maintaining business focus, priority, impact and alignment must be emphasized and re-emphasized to ensure that all

improvements relies true business benefits.

## 9. Application Management

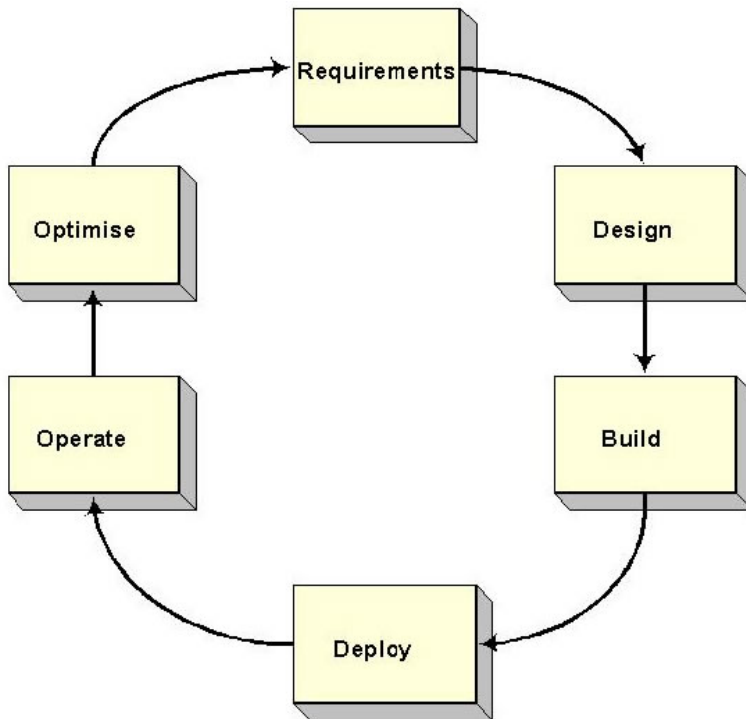
A key issue that has existed for some time is the problem of moving application developers and IT Service Management closer together. The lack of Service Management considerations within all phases of the application lifecycle has been seriously deficient for some time. Applications need to be deployed with Service Management requirements included, i.e. designed and built for operability, availability, reliability, maintainability, performance and manageability, and to be tested for compliance to specification.

To fully understand Application Management, it is necessary to compare it with Service Management and Application Development:

- Application Management is the superset which describes the overall handling, or management, of the application as it goes through its entire lifecycle (see Figure 9)
- Application Development is concerned with the activities needed to plan, design, and build an application that can ultimately be used by some part of the organization to address a business requirement
- Service Management focuses on the activities that are involved with the Release, delivery, support and optimization of the

application. The main objective is to ensure that the application once built is documented. A method for managing a complex applications environment is

state, based on the readiness assessment, to a desired state, as determined by the business drivers.



**Figure 9: The Application Lifecycle**

and deployed can meet the service level that has been defined for it.

It is essential that the requirements of all areas of the business and Service Management are considered at each stage of the application lifecycle. Having IT and the business jointly develop their strategies, as a mutual effort, needs to be a precursor to beginning any Application Development or deployment project. This ensures that IT and the business agree to objectives that are clear, concise and achievable. Once an organization has a common understanding of the alignment between business and IT, it faces a new problem, ensuring that the increasing number of applications are appropriately

through the use of an application portfolio, which provides a mechanism for viewing and evaluating the entire suite of applications in the business enterprise.

Organizations need to assess their ability to build, maintain, and operate the IT services needed by the business. A readiness assessment provides a structured mechanism for determining an organization's capabilities and state of readiness for delivering a new or revised application to support business drivers. The information obtained from an assessment can be used to determine the delivery strategy for an application, IT service, or ICT system. The delivery strategy is the approach to move an organization from a known

Application Management sees Application Development and all areas of Service Management as interrelated parts of a whole, which need to be aligned. The implication of this is that Application Development; Service Management and ICT IM units need to co-operate closely to ensure that every phase in the lifecycle dedicates the appropriate attention to service creation, delivery and operational aspects. The emphasis must be on the importance of dealing early in the lifecycle with those issues as this can have a large impact on the effectiveness and efficiency of service delivery and operation.

For each application lifecycle phase a management checklist can be developed to ensure appropriate Service Management aspects are fully considered and addressed, identifying the key Application Management roles that need representation to ensure that activities are completed comprehensively.

Within each phase of the application lifecycle, and likewise for the service lifecycle, each of the key Application Management roles has very specific goals to meet. It is crucial that organizations find some way of measuring progress and performance with respect to achieving these goals. To be effective, measurements and metrics must be woven through the complete organization, touching the strategic as well as the tactical and operational levels.

## 10. The Business Perspective

The Business Perspective approach to the delivery of IT services focuses on the key principles and requirements of the business organization and their operation. Especially to understand how they relate to and interface with the provision of IT within all areas of Service Management. This awareness of the business enables Service Management to ensure the most effective relationships, interfaces and delivery, which is aligned to the business, and so maximizing business benefit that can be delivered by IT.

The objectives of the Business Perspective approach to delivering IT services are:

- To enable IT personnel to understand how they contribute to business objectives
- To enable IT personnel to deliver/improve IT services to underpin business objectives
- To enable IT personnel to assist the business in maximizing the exploitation of IT
- To enable a complementary and integrated culture with the business
- To influence, innovate and enable Change for business advantage
- The alignment of IT with the business.

Effective processes ensure that IT services are aligned to business requirements and that the supplier elements also

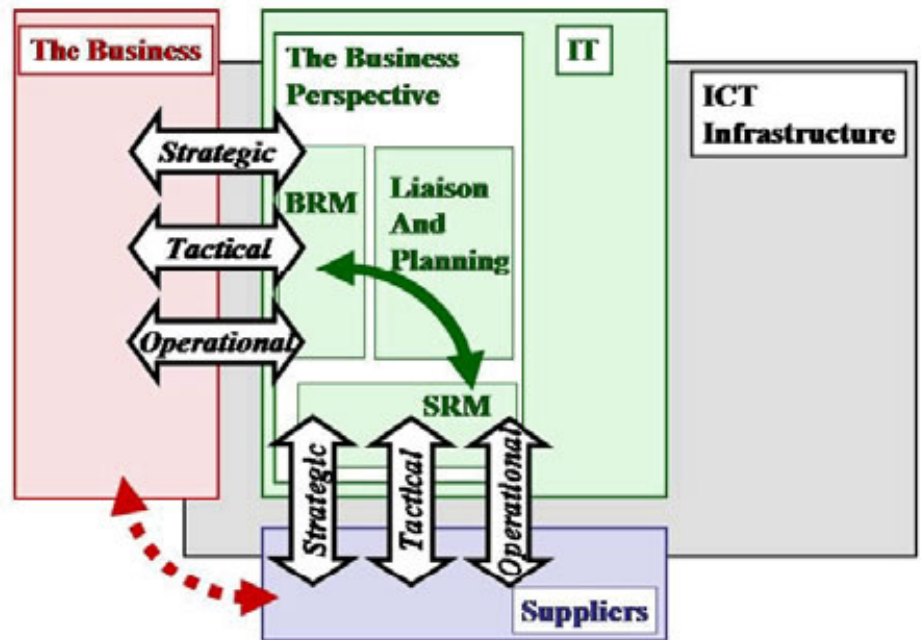
underpin and support that alignment. It is therefore essential that partnerships are forged between IT and the business, and IT and its suppliers to ensure that a “business-led” IT organization develops.

To be effective this approach consists of a number of processes aimed at aligning the business and IT. The alignment does not just cover current, but also future ICT systems and IT services. There is therefore a requirement for alignment at strategic, tactical and operational levels as illustrated in Figure 10.

To achieve this alignment of interests a number of process areas and roles need to be considered. The key processes are:

- Management (SRM)
- Review, planning and development of IT
- Liaison, education and communication of IT.

Developing and nurturing relationships with Customers has always been an important issue for all organizations. It is just as important for IT service providers to develop relationships with their Customers and business managers. It is equally important for them to develop relationships with their major suppliers, especially where aspects of the overall service are outsourced to these suppliers and they have a direct interface to and a direct impact upon the quality of service delivered to the Customers and the business. Establishing BRM and SRM processes is the preferred method of achieving this.



**Figure 10: The Business Perspective**

- Business Relationship Management (BRM) It is crucial that the people working within the BRM process
- Supplier Relationship Management (SRM)

appreciate the value of IT and its role within the business value chain and continually publicise this and reinforce the message of business and IT alignment. They need to have synergy and empathy with the business units and represent their views to the rest of IT.

SRM needs to ensure that supplier relationships are maximised to business advantage. This includes recognising the need for different types of suppliers together with their appropriate relationships, a Supplier Catalogue, the contract lifecycle, integration of suppliers into the “end-to-end” Service Management processes and supplier performance management.

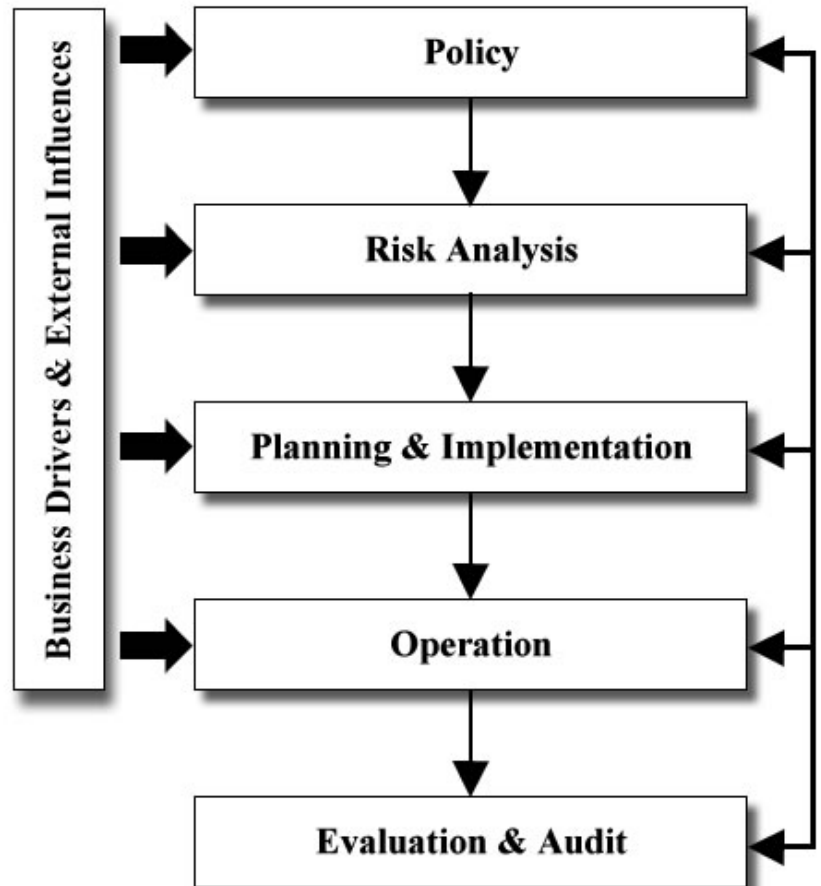
Effective relationships at operational, tactical and strategic levels between the business and IT, and IT and its suppliers can also ensure effective and innovative use of IT for business advantage, e.g. identifying new technologies, facilitating business transformation and meeting ever increasing, rapidly changing business demands.

It is key for IT organisations to endeavour to align their organisation, delivery and culture as closely as possible to that of the business. Close alignment can achieve significant benefits for the business, especially in areas such as continuity, risk, Change and SLAs, bringing improved delivery focus and achievement of key business objectives. Alignment needs to start at the top, with alignment of IT strategies, governance and culture to those of the business.

IT management needs to review their organisation and services against the business and improve business alignment through CSIPs.

At tactical and operational levels,

business, together with management of new service introduction, business expectations, continuous improvement and the development of organisational culture.



**Figure 11: The Information Security Model (ISM)**

in terms of managing IT service provision, alignment and business involvement must be considered for all process areas within Service Management. This ensures “end-to-end” integrated processes delivering the advantages of synergy and partnership working across the organisation. The approach also considers use of the Service Catalogue and SLAs to market IT and its services to the

The Business Perspective approach also focuses on liaison between the business and IT, improving information flows, planning business communication, and particularly co-ordinating the activities of the BRM and SRM processes to ensure consistency of approach.

## 11. Security Management

IT Security Management is the process of managing a defined level of security for information, IT services and infrastructure. IT Security Management enables and ensures that:

- Security controls are implemented and maintained to address changing circumstances such as changed business and IT service requirements, IT architecture elements, threats, etc
- Security Incidents are managed
- Audit results show the adequacy of security controls and measures taken
- Reports are produced to show the status of information security.

IT Security Management needs to be part of every IT manager's job description. Management is responsible for taking appropriate steps to reduce the chances of a security Incident occurring to acceptable levels. This is the process of risk assessment and management.

Corporate executive management is accountable to stakeholders and shareholders for security, and is responsible for defining the corporate security policy. IT Security Management is governed by that policy. The existence of the policy registers and reinforces the corporate decision to invest in the security of information and information processing. It provides management with guidelines and direction regarding the relative

importance of various aspects of the organisation, and of what is allowable and what is not, in the use of ICT systems and data.

Figure 11 illustrates the information security process as seen by the business. It covers all stages, from policy setting and initial risk assessment, through planning, implementation and operation, to evaluation and audit.

Every organisation must have an information security policy that is widely circulated, committed to by everyone within the organisation and actively enforced and reviewed.

Figure 12 provides an overview of the ITIL IT Security Management Process. The process shows the complete route from the collection of a

Customer's requirements, through planning, implementation, evaluation and maintenance – under a framework of control - with regular status reporting to the Customer closing the loop.

Intrinsic elements of all activities within the IT Security Management process are risk and vulnerability assessment, and management and the implementation of cost justifiable countermeasures to reduce vulnerability and risk to an acceptable business level. These activities must be closely co-ordinated with all other areas of Service Management, especially the Availability and IT Service Continuity Management processes.

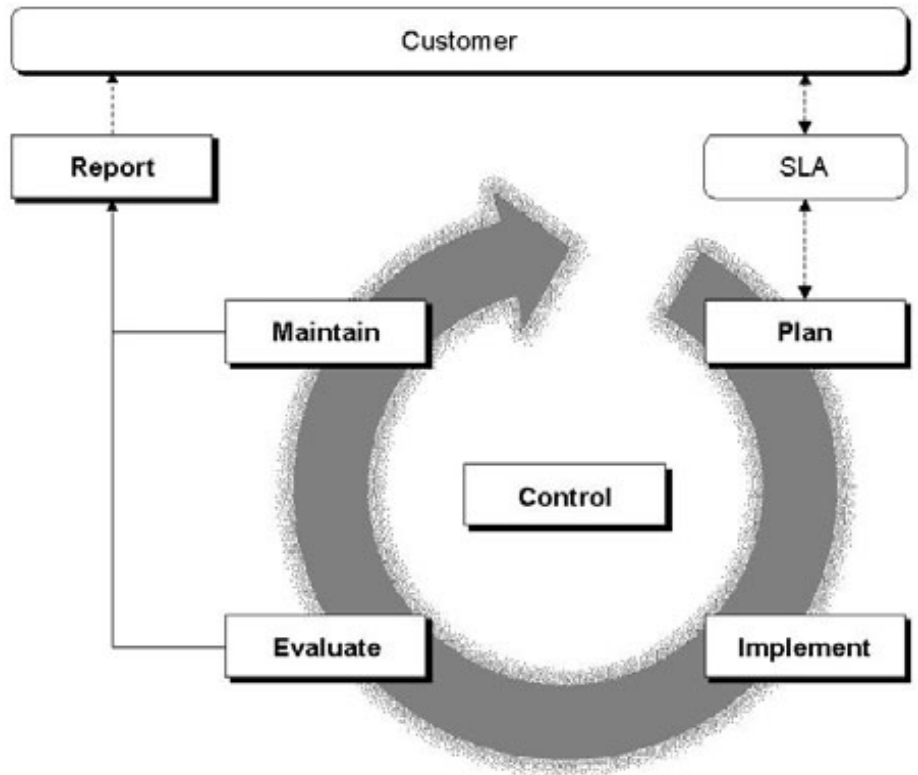


Figure 12: The IT Security Management Process

## 12. Related Standards and Complementary

ITIL consists of modules containing advice and guidance on “best practice” relating to the provision of IT services. ITIL has subsequently been used as the basis for the development of a British Standard for Service Management. The standard and ITIL are aligned and the standard has itself been recently revised and is now documented in the following set of documents:

- BS 15000-1:2002, IT Service Management (Part 1: Specification for Service Management)
- BS 15000-2:2003, IT Service Management (Part 2: Code of Practice for IT Service Management)
- PD 0005:2003, IT Service Management – A Manager’s Guide
- PD 0015:2002, IT Service Management – Self Assessment Workbook.

These documents provide a standard against which organisations can be assessed and certified with regard to the quality of their IT Service Management processes.

A BS 15000 Certification scheme was introduced in July 2003. The scheme was designed by the itSMF and is operated under their control. A number of auditing organisations are accredited within the scheme to assess and certify organisations as compliant to the BS 15000 standard and its content. The BS 15000 standard is now progressing towards an International (ISO) standard on Service Management.

A complementary book on Software Asset Management (SAM) has also been added to ITIL. This concentrates on the specific demands of managing software assets within an organisation and the related issues associated with the use of those software assets. The book definition states that “SAM is all of the infrastructure and

processes necessary for the effective management, control and protection of the software assets within an organisation, throughout all stages of their lifecycle”.

The overall objective of all SAM processes is good corporate governance, namely to manage, control and protect an organisation’s software assets, including management of the risks arising from the use of those software assets. An overview of the process areas for SAM is shown in Figure 13.

The objective of the Overall Management processes is to establish and maintain the management infrastructure within which the other SAM processes are implemented. Each of the other process areas can then achieve their objectives as follows:

- Core Asset Management processes: to identify and maintain information about software assets throughout their lifecycle, and to manage physical assets related to software
- Logistic processes: to control all activities affecting the progress of software through its lifecycle
- Verification and compliance processes: to detect, escalate and manage all exceptions to SAM policies, processes, procedures and licence use rights
- Relationship processes: to manage all relationships within the business, and with partners and suppliers, to agreed contractual, legal and documented service terms and targets relating to the use of software.

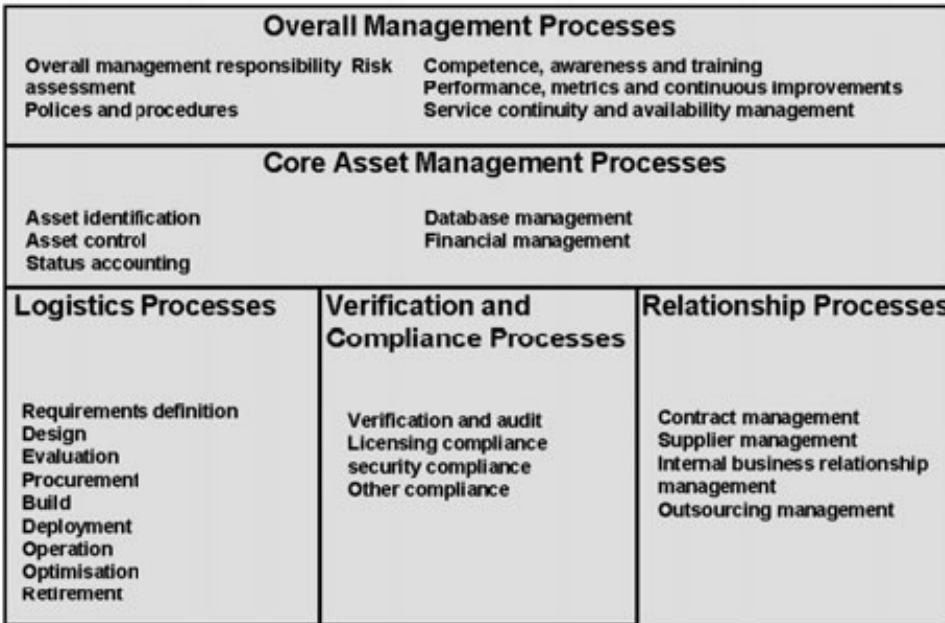


Figure 13: The SAM Process Areas

### 13. Summary

Many organisations still see IT service management as being predominantly a technology issue. ITIL promotes a much more "joined up", "end-to-end" approach to IT service management replacing the 'technology silos' and isolated 'islands of excellence'. The focus of IT management has been changing for some time and in the future management will be even less focussed on technology and still more integrated with the overall needs of the business management and processes. These new systems and processes are already starting to evolve and will continue to evolve over the next few years. This development will accelerate, as the management standards for

the exchange of management information between tools become more fully defined, by organisations such as the Distributed Management Task Force (DMTF). This integration process may gather speed now that the itSMF is an Alliance Partner with the DMTF. In essence, management systems will become:

- More focussed on business needs
- More closely aligned to business processes
- Less dependent on specific technology and more "service centric"
- More integrated with other management tools and processes as the management standards evolve.

This will allow "joined up", "end-to-end" IT management processes to be developed that

will replace the 'technical silos' and isolated 'islands of excellence' that have previously existed within IT organisations.

This will only happen if we adopt practices and architectures that are focussed on business needs and business processes. The OGC's ITIL framework gives a sound basis for achieving all of this once management tools and interfaces evolve to fully support them. The "big picture" of how all of these areas and processes together provide "end-to-end", "joined up" Service Management is illustrated in Figure 14.

Several organisations have already used this approach to significantly improve the quality of IT services delivered to the business. The benefits gained have included:

- Greater alignment of IT services, processes and

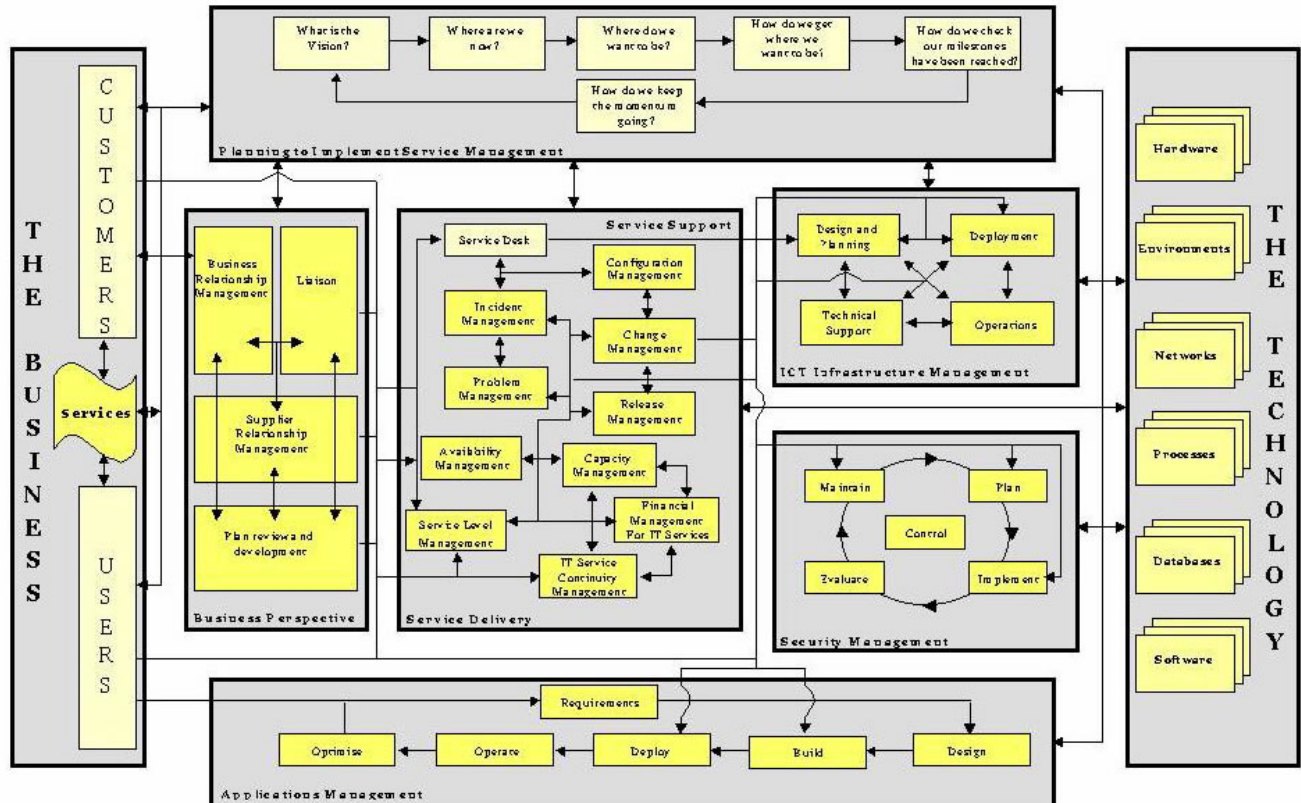


Figure 14: The "big picture" of ITIL Processes

- goals with business requirements, expectations and goals
- Improved business profitability and productivity
  - Support staff that are more aware of business processes and business impact
  - A reduction in overall management and support costs leading to a reduced TCO
- Improved service availability and performance, leading to increased business revenue
  - Improved service levels and quality of service.
- However, care must be taken when developing IT Service Management within an organisation. It is easy to focus on the internal aspects of IT process rather than on the Customer and business needs and requirements. The processes should always be designed primarily to make the Customer experience simple and enjoyable and secondly to make the backend IT processes effective and efficient. This can only be achieved when business and Customer driven measurements metrics, CSFs and KPIs are put in place to measure the quality of service and its continuous improvement.



## Bayshore Consulting & Services Co., Ltd

Rm 209, Zhongchen Building, No.1, Lize Zhong Er Lu,

Chaoyang District, Beijing, China, 100102

Tel: (010) 6439-1733 Fax: (010) 6439-1582

<http://www.bayss.com>

Featured Article

## Mainframe Security Issue

By James Smith

INFORMATION security in general is given very little attention, even in these most turbulent of times. Some may successfully argue that is not true and that there is a lot of discussion on security issues these days. Yes, there is talk, and there is debate, and there is concern. But when it comes to budgeting and allocating funds for security projects, it is a different story—security gets a smaller and smaller piece of the budget pie each year. Ask yourself how much of your IT budget is set aside to protect your most precious resource – your corporate data.

The reason for this is simple, although sometimes difficult to accept—security is like buying insurance, and not many companies are willing to invest in this “optional” item. Why spend money on security when there are newer, shinier toys to buy, such as that latest Java application, or the newest Websphere software?

Such is the state of security in general. When it comes to mainframe security, the situation is even worse. The prevailing thought at many installations is that these dinosaurs of the computer age will some day go away, so why waste precious resources on them? It matters little when you point out that this talk of mainframe obsolescence has been going on for the last two decades, and mainframes are still going strong, thank you.

Listed below are the main issues plaguing mainframe installations. Your installation may have as their security software either RACF from IBM, or ACF2 or Top Secret from Computer Associates International. It matters little. The issues are generic in nature. Of course, all items do not apply to all installations; there are some that have taken steps to address these issues, with the banking industry often leading the way, and have spent the necessary funds to achieve their security goals. But these apply, in varying degrees, to quite a few installations.

### LACK OF STAFF TRAINING

This is one of the most serious issues facing mainframe security professionals. Long since gone are the days of almost ‘unlimited’ IT training budgets. These days, the security administrators are too busy doing the day to day administrative work, and have no time to go for training, even if a budget existed.

The security staff themselves are quite often reluctant to bring up the training issue, lest they be viewed in a negative light by their bosses. The fear of losing their job is foremost in their minds, not training. But proper training can bring to light better methods of doing the daily security administration work, and in the long run can mean faster turnaround times for security requests.

Older methods are not only inefficient, they are sometimes even inaccurate. Only by proper training, and by regularly examining the daily workload, can you bring in efficiencies. All three security software products, RACF, ACF2 or Top Secret, bring in newer features that are seldom implemented because the staff members are not properly trained.

### THE DAILY GRIND

Security administration, by its very nature, entails doing the daily tasks of adding new userids and deleting old ones, and changing user accesses all day long. While this is important to the business, and must be done as quickly as possible, this daily activity does not leave time to invest in smarter, proactive measures. There is no time to step back and look at the big picture.

The Security Manager should ask questions like: Are there more efficient methods to grant the security access? Is old security access removed when not needed? Who is making sure that necessary approvals are requested before access is granted? Is anyone verifying that the approvers are still valid?

There is no time to ponder these and a host of other questions.

### COPING WITH ORGANIZATIONAL CHANGES

Security administration is dependent on how the company is organized into departments,

divisions, job functions, and so on. This is because, in most cases, security accesses are granted to entire departments or business units, to simplify security administration work. And there is nothing wrong with that. In fact, that's how it should be. The problem arises when organizational changes occur. Examples are—departments merge; business units get bought or sold; even entire companies get merged, bought or sold. Because security is dependent on departmental and divisional structures, it follows that when there are organizational changes of this nature the security database needs to be re-examined to realign itself with the latest organizational structure.

But this is easier said than done. Reorganizing the security database requires elaborate planning and preparation, not to mention special, onetime-only type of skills. So this item may be put on the back burner. An interesting point to note here is that, even if the security database is not aligned with the company's organizational structure, security will still work! There is no pressing need to address the issue. Of course, you now may have inappropriate access, wrong access, and even too much access. But the system works, and the concern is that the issue may go unaddressed.

Over time, however, this situation, coupled with employee transfers and terminations discussed below, may cause the entire security structure to crumble, until the daily administration itself is affected. Then drastic steps are often required to correct the situation. What is needed is a proactive process whereby smaller, piecemeal changes

take place as they are needed, so there is no deterioration in security architecture, and the need to take drastic measures sometime in the future does not arise.

### EMPLOYEE TRANSFERS AND TERMINATIONS

Employee transfers, terminations and resignations quite often go unnoticed by the security department. Usually, there is a process for immediate terminations. The Human Resources Department sends out an email for immediate action to the security department to terminate all userids for the terminated person.

But what about all those other "normal" terminations and resignations that take place regularly? These employees' access to the system should be removed as soon as possible to prevent misuse. And what about employee transfers within the company? These, too require security changes to reflect the employee's new role within the company. At many places, all these changes are seldom made to the security database, if at all. Sometimes these are piled up and left unattended; to be done when there is no other work!

What procedures do you have in place to deal with employee terminations or resignations?

### REPORTING AND MONITORING

Apart from the daily administration work, a good security department should have procedures for regular monitoring and reporting of all security activities. These include producing reports and monitoring such activities as invalid logons, unauthorized

access attempts, persons having special security privileges, monitoring of accesses to important data sets, and so on. In some shops these reports are produced, but not regularly monitored, and allowed to collect dust. In others (although these shops are few) they are not even produced. Some individual needs to be made responsible (and accountable) for this task, because only then will it be done properly.

This is probably one of the most difficult areas for the overworked security administrator as most security products provide very limited reporting mechanisms. As a result we have seen an increase in the use of products such as the CONSUL/RACF suite of tools that better help you manage and administer your RACF security system. Even IBM has finally pitched in with the introduction of RACFICE to generate some very useful security reports.

### SECURITY POLICIES

Each company should have in place a security policy. The policy is a statement that establishes the guidelines and responsibilities to protect the information assets of your corporation.

A clear security policy shall clearly define:

Data Ownership – the Data Owner responsibilities include:

- Determine the sensitivity of data, judge its value and importance, and classifies it accordingly (as discussed in the data classification section).

- Determines who will have access to the data and to what extent.
- Specifies the necessary security controls to be placed on the data, and communicates them to the Security Administrator.

**Data Custodian** - The Data Custodian is the manager(s) of the data processing department which will maintain, store, process and produce information for the Data Owner. Data Custodian responsibilities include:

- Ensures the availability of data for processing in a secure manner on a continuing basis.

**Data User** - Data Users are the individuals in user departments who have permission from the Data Owner/custodian to access and use the data. Data User Responsibilities include:

- Responsible and accountable for all data access made by their identification code.
- Complies with all security controls designated by either the Data Owner or Security Administrator.
- Does not disclose confidential data to anyone without the consent of the Data owner.
- Does not disclose their password to anyone.

**Security Administrator** - The Security Administrator is the person responsible for the security administration function within the business. Security Administrator responsibilities include:

- Provides data access controls as specified by the Data Owner.

- Ensures that proper logical and physical safeguards are in place to protect the data.
- Provides adequate procedural controls to protect the data from unauthorized access.
- Ensures that ownership and classification have been established for all data used at the computing facility.
- Reviews access activities against the data and communicates violations to the Data Owner.

#### HELP DESK MENTALITY

Some managers view security administration as little more than a Help Desk activity. In fact, there are some installations that have merged the two areas, in the hope of saving costs. This is unfortunate, for there is more to security than just granting and removing access, and adding and deleting userids. At the very least, it is a specialized skill requiring skilled staff.

When security is lumped with other activities, the quality of security administration deteriorates, eventually forcing the company to completely overhaul the security database. This is much more expensive than having security professionals do the job correctly in the first place.

#### NEW SECURITY FEATURES NOT IMPLEMENTED

The three main security products on the mainframe, RACF, ACF2 and Top Secret, all introduce newer features all the time. These, when implemented, can not only provide improved security, but often they can speed up the security process itself.

However, time, effort and skills are needed to implement these new features.

A case in point: in RACF, for UNIX System Services (USS) security, there is a need to assign unique "UID's" to users. However, under the older versions of RACF, this task of keeping UID's unique was a manual one, and was the responsibility of the security administrator. Newer versions of RACF have addressed this problem, automation of unique UID's is possible, but it is up to the installation to implement this new feature.

#### INADEQUATE STAFFING LEVELS

This is a chronic complaint in some shops. They try to do with the bare minimum of staff, and often the mainframe person has to do network security as well. Or the non-mainframe security person is asked to do mainframe security. The result is that there is no time to identify security weaknesses and address them. Not only is it important for the mainframe security person to administer security but they should also have enough mainframe knowledge to understand the impact of any changes.

#### CONCLUSION

The list of issues discussed here is by no means complete. There are other issues as well, of a lesser significance. What is needed is a healthy discussion to bring to the attention of management that security issues will not go away unless they are addressed. And we don't want to wait until a security "incident" happens before we react.

Featured Article

## The REGION JCL Parameter

by James Smith

The JCL REGION parameter is one of the most confusing of all JCL parameters. Using it correctly can be crucial to getting vastly improved throughput for many batch jobs. The confusion about the REGION parameter stems from many factors. Some are historical. Others are due to misconceptions. I will attempt to explain as many of these factors as possible and hopefully, clarify the REGION parameter's usage.

### REGION DOES NOT ACQUIRE STORAGE

This is the first misunderstanding that needs clarification. I'll state this as: If a REGION= parameter is coded in a JCL stream or at TSO logon, this DOES NOT cause any storage to be acquired by the operating system. Or, if I code "REGION=0M" on a job card, my job does NOT attempt to GETMAIN all of the virtual storage on the operating system. Coding a REGION parameter influences only two data values within a control block known as the Local Data Area (LDA, DSECT IHALDA). These two binary fullword values store the maximum amount of virtual storage that address spaces can GETMAIN. Be clear on this: Programs being executed acquire storage. Not the JCL

itself. Why two values? Simple: one field stores the 24-bit ("below the 16 megabyte line") maximum and the other stores the 31-bit ("above the 16 megabyte line") maximum. This dual nature of the REGION parameter, limiting both 24 and 31 bit storage, is critical and will be fully explained later.

### JOB CARD CODED REGION OVERRIDES STEPCODED

#### REGION

If you code a REGION=50M on your jobcard, it will apply to all steps in the job—even steps that code a different REGION value. Knowing that the REGION declaration doesn't actually acquire any storage but instead, establishes a limit, I recommend always coding REGION on the jobcard. Why code it multiple times when you can code it once.

### DEFAULTS AND EXITS

This is where the REGION processing gets tricky. I am going to try to explain this as clearly as possible but be forewarned: The defaults and exit-modified values for REGION vary widely from installation to installation. I can't speak in absolutes here because every single z/OS site

usually has a different set of default values.

### WHAT IS THE DEFAULT FOR REGION?

All REGION discussion that follows applies to what are known as "V=V (or ADDRSPC=VIRT) type of job steps—99.999% of all work on z/OS.

There is a single question to ask and get answered before you can accurately determine the default limiting amounts for REGION at your site. That question is:

Has your installation established its own defaults by way of either the IEFUSI or IEALIMIT exits? Or, have IBM's "factory defaults" been left in place?

### REGION VALUES FALL INTO RANGES

Much of the following discussion is based upon the explanations in —REGION Defaults—in the z/OS (or OS/390) MVS JCL Reference manual. I suggest reading this bit of IBM documentation in conjunction with my explanations. I have tried to simplify things a bit and to underscore the fact that the values coded on a REGION parameter fall into **ranges** when it comes to what type of

REGION you are seeking to limit.

#### REGION=0M OR REGION=0K

The value of zero is a special case. Coding a zero REGION size sets the limits to all of the 24-bit and 31-bit virtual storage available to the address space. Typical defaults are between 8M-10M for 24-bit storage and between 1600M-1900M for 31-bit storage. It **DOES NOT** acquire any memory and may be further limited by an IEALIMIT or IEFUSI exit.

Also, remember that the REGION parameter applies only to virtual storage limits for the address space (job, step, TSU, etc.) that it is coded on. To view the available private storage for an address space (the REGION= amount you can potentially use), you would need an RMF post processor VSTOR report or some other tool that displays a virtual storage map—something like, TASID, ShowMVS or MXI. If your site has one installed, MVS monitors like OMEGAMON, TMON and MAINVIEW can also display a virtual storage map.

#### REGION=1K THROUGH REGION=16384K

When you code a value between 1K and 16M (note that 16384K = 1,024 X 16), the limit will be applied only to 24-bit storage. For the 31-bit limit, the job will either get the IBM default of 32M or an exit-modified 31-bit limit value.

Note that there is a range of “below the line” limiting values that I will call *impossible values*. These values fall between approximately REGION=11M

to 16M. If an exit doesn't intercept these *impossible values* and alter them dynamically (to an amount less than the 24-bit maximum amount), your job will get an S822 abend every time if it uses REGION values in the impossible range.

The impossible range is limited by the amount of below-the-line PRIVATE storage that is available. Check RMF or TASID, SHOWMVS or some such like tool to the size of your below-the-line PRIVATE region.

#### REGION=16385K THROUGH REGION=32768K

REGION values between 16M (+ 1K) up to and including exactly 32M limits the job step to the defined site maximum for 24-bit storage. The 31-bit limit will always be either 32M or an exit-modified 31-bit limit value.

#### REGION=32769K THROUGH REGION=2047M

REGION values between 32M (+ 1K) up to and including exactly 2047M limits the job step to the defined site maximum for 24-bit storage. The 31-bit limit will be either the coded value or an exit-modified 31-bit limit value.

In the IBM documentation, the following sentence appears several times when describing how the region below 16 megabytes might be influenced:

*“The resulting size of the region below 16 megabytes depends on system options and what system software is installed.”*

This varies from site to site but a typical default maximum for “below the line” storage is between 9M-10M. In other

words, no job step can EVER request more below the line storage than this. If it does, this is considered an impossible REGION value and either your job will abend with an S822 or the impossible value will be lowered by an exit.

#### CONCLUSION

Certainly, the REGION parameter of z/OS JCL is one of the most confusing of all JCL parameters. One thing to keep in mind is the very nature of a language such as JCL. JCL, like HTML, is what I call a “static” language.

It is designed to create a framework for the invocation of programs, nothing more. It doesn't have the capability of taking its own actions. All of its many keywords and parameters define existing or newly created run-time components. Some JCL parameters set limits or establish other runtime variables but JCL itself has no ability to acquire storage, move values or do anything other than establish a run-time environment for programs.

With this in mind, remember these three key things about how the REGION parameter influences virtual storage in a z/OS JCL stream:

1. It **NEVER** acquires any storage. It only sets limits.
2. A REGION value coded on the job card overrides any step-coded values.
3. The values coded fall into ranges. Below 16M, the REGION value limits 24-bit storage. Above 32M, you are limiting 31-bit storage.



**Bayshore Advisor**  
2nd Issue, December 1, 2005