III
Risk Assessment

Introduction to Risk Assessments

The IT Service Management Model described in this section is derived from the results of audits of IT service delivery activities undertaken by different SAI's, mainly during the last decade. The model defines six areas of IT service delivery activities that should be managed in public agencies, and also a seventh overall 'entity' aspect. The entity aspect, as well as the interaction between the activity areas, are visualised by the arrows. The model is followed by a brief definition of each area. Further information on Risk Management can be found at Annex 5.

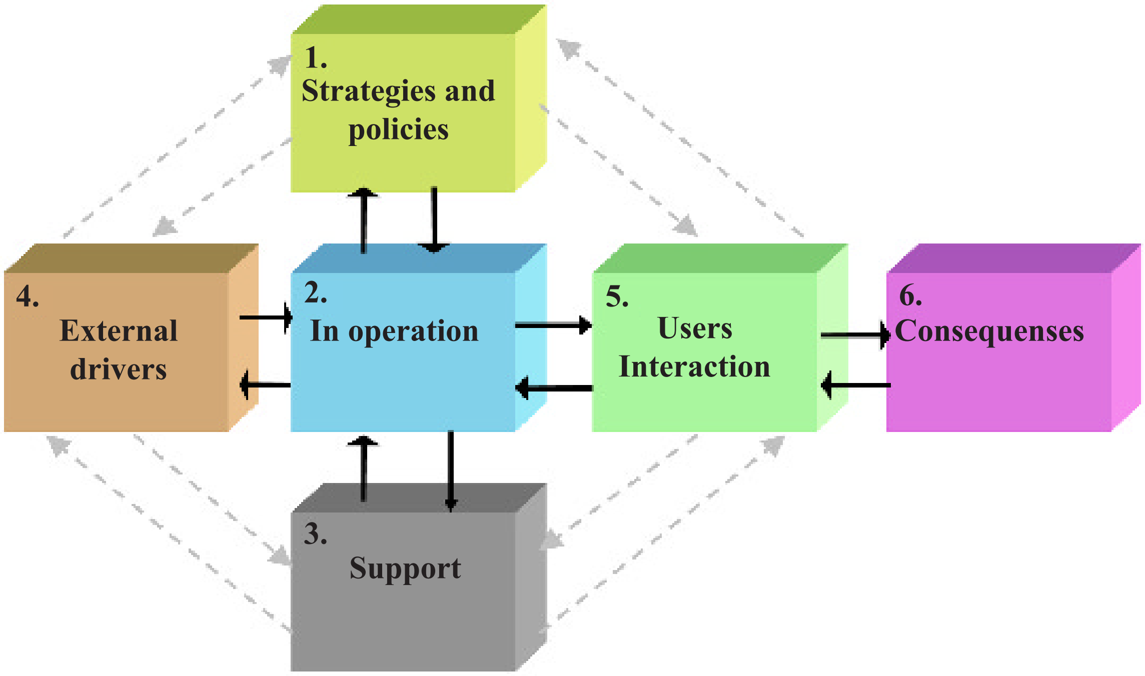


Figure 1 - IT Service Management Model

Activity areas

Entity area

Failure to manage IT services effectively could affect an organisation's ability to achieve its planned business objectives. The Entity area reflects top management's responsibility for managing all areas of activity.

No 1 – Strategies and policies

This area deals with the operational strategies and policies that are necessary to ensure that IT services support business strategy and organisational objectives.

Organisations generally regard policies on IT services to be essential, but these are not always supported by strategies. An IS related policy should be seen as a specified and documented set of aims and objectives that govern the provision of IS systems and services through all stages of their life cycle (that is, *identification, planning, development, implementation, operation, review and disposal*). Policies may also relate to wider organisational and management issues arising out of the governance of IS within an organisation. Some policies will affect both customers – the end users of IS – and both internal and external providers to the organisation.

Annex 1 contains further information on IT strategies.

No 2 – In Operation

This area deals with the IT department's delivery of IT services. Delivery includes activities and conditions that represent risks to the achievement of business objectives; they are development, operations, maintenance and IT service support. The requirements that are necessary to perform these activities effectively are:

- Strategies and policies linked to business objectives
- An appropriate level of IT security
- Funding
- Human resources

Annex 4 contains further information on service management processes.

No 3 - Service support

This area deals with the financial, human and technical support needed in order to ensure that IT infrastructure contributes to planned business objectives.

No 4 – External drivers for change, regulations and constraints

This area focuses on an agency's obligation to assess, adopt and implement external demands and formal regulations when delivering IT services.

No 5 – User Interaction with IT services

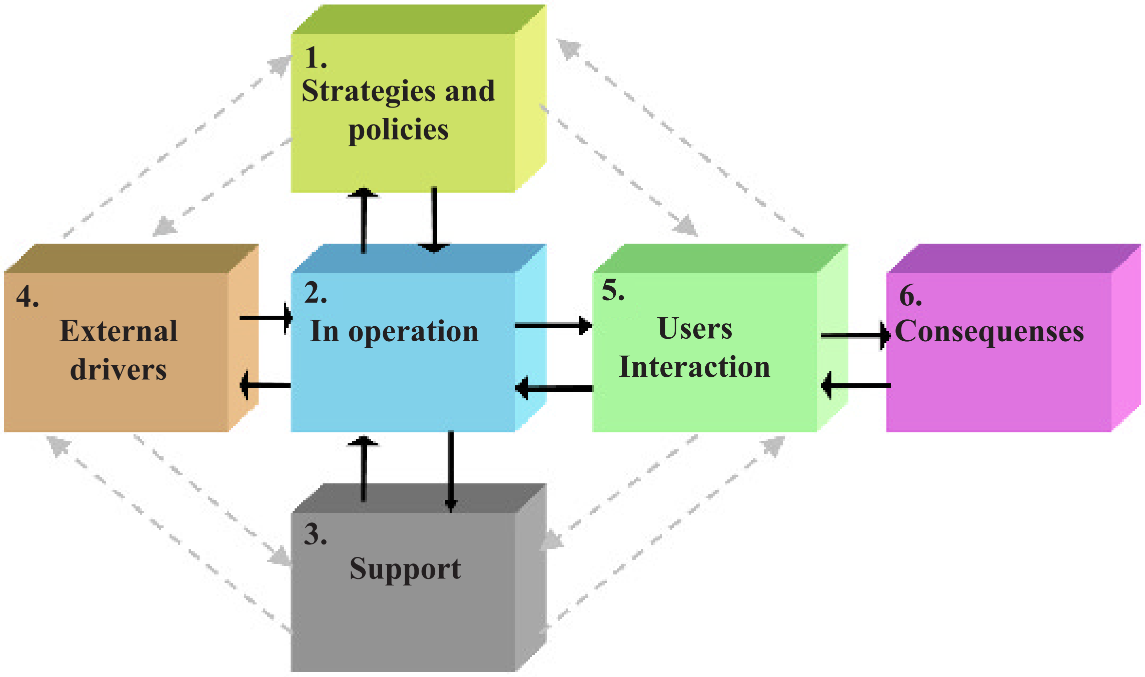
This area covers the use that internal and external users make of a service. It focuses on accessibility, and on other service delivery issues that affect the user's perception of quality, such as ease of use.

No 6 – The consequences of ESD (electronic system delivery) on society, citizens and organisations

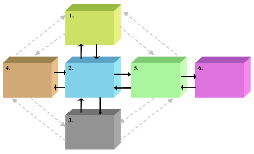
This area deals with consequences of ESD on society, citizens and organisations. This means focusing on the needs of service users rather than on the convenience of government departments.

Risk Assessment

Entity Area



Definition Entity Area



The IT Service Management Model presented in the *Introduction to Risk Assessments* introduced the concepts of "Activity Areas" and an "Entity Area". Activity areas represent primary activities in which risks have to be identified and managed to enable the area to support organisational objectives.

The Entity Area reflects top management's responsibility for managing the activity areas. Top management is responsible for co-ordinating activities across an organisation, making optimal entity decisions.

The tasks of managing IT services

Managing IT services comprises four main tasks:

- **Planning**
- **Organising**
- **Leading**
- **Monitoring**

In order to perform these tasks successfully, some vital conditions need to be considered:

- Top management need to understand the contribution that IT makes to their achievement of business objectives.
- Top management need to understand the agency's IT services and the activities to be managed.
- Top management should understand their role as drivers for change and innovation, making public services more efficient, effective and accessible through electronic service delivery.

Government organisations rarely deliver IT services as a core activity. However, as technology develops, delivering electronic services become more important. Most managers are well aware that IT is a key issue. Some even think it is the key issue, treating IT as an isolated and outstanding function, regardless of its supportive function to business objectives.

Another vital condition necessary when managing IT services is to clarify what activities are to be managed. The IT Service Management Model could be used as a framework for defining the elements of the IT service.

Top management objectives

These top management objectives are based on what we consider to be the overall responsibility for managing IT infrastructure activities. Top management also has an overall responsibility for managing the individual activity areas. Risks connected to this responsibility are considered under the respectively risk assessment.

The auditor should be aware that the objectives presented in the Entity Area Assessment are considered to be those that are generally necessary to achieve satisfactory IT service management. There might be other objectives to consider, depending on the agency's particular role and operational environment.

Planning

> ***Aim: Top management should develop a strategic plan to help align their use of IT infrastructure with their corporate objectives. They should ensure that the strategic plan is implemented and is effective.***

Preparing the strategic plans involves:

1. Recognising opportunities and problems that confront the organisation in which Information Technology and Information Services can be applied cost effectively.
2. Identifying the resources needed to provide the required Information Technology and Information Services
3. Formulating strategies and tactics for acquiring the necessary resources
4. Establishing achievable and measurable objectives

Organisation

> ***Aim: Top management should ensure that the organisation of IT service activities achieves the stated organisational objectives.***

The planning function establishes goals and objectives for information systems within the organisation. The organising function gathers, allocates, and structures resources to enable these goals and objectives to be achieved. Unless top management performs the organising function properly, the IT services are unlikely to be effective an efficient.
A major responsibility for top management is to acquire the resources needed to accomplish stated objectives. These resources include hardware, software, personnel, finance and facilities. The funds must be expended in a planned, systematic way to ensure that adequate resources are available when and where they are needed.

Leading

> ***Aim: Top Management must provide leadership in developing the IT service delivery necessary to create a suitable environment for sustaining prosperity, performance and growth.***

Top management should provide leadership designed to achieve harmony in attaining their objectives. Individual and activity area objectives must not conflict with the organisation's objectives. The process of leading requires managers to motivate staff, direct them, and communicate with them. In the management of IT infrastructure, this concerns the leadership of middle managers, IT staff and the internal users of IT.

Ensure control and monitoring procedures

> ***Aim: Top Management should establish procedures for controlling and monitoring IT infrastructure activities.***

In order to be able to manage the entity, there is a need for Top Management to establish procedures designed to identify any material deviations from the achievement of organisational objectives or, preferably, identify the *risks* of possible material deviations. In this connection, a Risk Management strategy is recommended.

Risk Assessment

***Aim:** Top Management has to develop a master plan for an effective and efficient use of IT Infrastructure as an integrated part of the organisation's strategy, and make sure that the plan is implemented and effective in order to reach the organisation's overall objectives.*

Risk	Impact	Risk management strategy
1. Poor awareness of IT among Top Management.	a. Low quality services.	– Recruiting and educating procedures have to be established to ensure that top management has ability to manage an organisation with a comprehensive IT Infrastructure. – There has to be clear policies on using IT experts, to support Top Management i.e. IT Management involvement in strategic planning.
2. IT function is regarded as an outstanding function and not as a supportive function.	a. Exaggeration of funds provided to IT related investments. b. Investments are not adequate or necessary for providing IT services.	– Ensure focus on core activities. In public organisations there are demands, for instance from Ministry level on key deliveries (Core activities). – Assess how IT function contributes or will contribute to Core activities.
3. IT's level of contribution to core activity is not appreciated by Top Management.	a. Underestimating the signification of IT. b. Lost opportunities.	– Define the significance of the IT function. This could be done by analysing in what degree delivery of service is influenced by electronic delivery based on the following criteria: – *Accessibility of the services.* – *Users participation.* – *Service concept.* – *Interaction.* – If the value of these criteria is affected positively it indicates high significance and dependency of the IT function and IT infrastructure.
4. IT service activities areas are not defined, or the survey is not complete. The allocation of economic, human and technological support is inappropriate.	a. Important areas are neglected or not sufficiently managed. For instance, management will not consider external regulations when developing a system, or will not evaluate the consequences it might have on society.	– Top Management needs to define relevant activity areas to be managed. This could, however, be based on the IT Infrastructure Management Model introduced in the Introduction Paper.
5. IT service objectives do not support organisational objectives or vision.	a. Services delivered are not in accordance with organisational objectives.	– Clarify vision, define object and establish superior objectives. Make sure there is consistency between lower level objectives and superior objectives. Every single action should support an objective.
6. The objectives established are not achievable.	a. Low motivation, high uncertainty if IT infrastructure is supporting organisational objectives.	– Obtain realistic planning by interaction and communication with everyone responsible. Provide ownership and obligation by participation when setting objectives.
7. The objectives are not measurable.	a. Those responsible do not know what to obtain, or when or if objectives are achieved.	– Objectives at this level ought to be "closed", expressing distinctive figures such as days, cases, monetary unit etc.

Aim: Top Management should ensure effective and efficient IT service organisation to enable stated organisational objectives to be achieved.

Risk	Impact	Risk management strategy
1. IT service activity areas to be organised are not defined, or the survey is not complete.	a. Important areas are neglected.	– Top Management needs to define relevant activity areas in order to be able to allocate resources adequately. This could, however, be based on the IT Infrastructure Management Model introduced in Introduction part.
2. Top Management are unable to communicate the financial needs to governmental authorities allocating funds.	a. The organisation do not receive sufficient grants and will not be able to achieve organisational objectives.	– Provide sufficient plans and reports concerning services, activities and projects accomplished and planned. Communicate actively with granting authorities.
3. Top Management are not capable of assigning funds or human resources adequately between competing IT service activities.	a. Some activities will not be allocated sufficient funds or human resources, and will be unable to contribute satisfactorily to IT service delivery, while others are overestimated. Both might impact on other dependent activities.	– Effective and efficient budgeting procedures. The organisation needs to adopt effective estimating techniques and ensure interaction and co-operation through budget meetings and feedback. – Verifications of estimates. Estimates should be based on planned activities and projects.
4. Shortage of skilled and experienced personnel.	a. Adequate support is not available in time. Constantly hiring external help could lead to cost overruns.	– Work out organisational plans for building competence. – Gather information of education needs and wishes among staff by handling out questionnaires. – Arrange for external or internal education programmes. – Plan staff requirements.
5. Insufficient or inappropriate technology.	a. Electronic services are not delivered effectively and efficiently due to under or over capacity. b. Inadequate data processing capacity.	– Work out an investment program and implement an on-going capacity-planning programme.

***Aim:* *Top Management must provide leadership in developing the IT services necessary to create a suitable environment for sustaining prosperity, performance and growth*.**

Risk	Impact	Risk management strategy
1. Poor motivation among staff dealing with IT service issues.	a. Conflicting management objectives leading to low performance among employees. b. Reduces the ability of achieve key objectives.	– Identify the factors for motivating IT personnel and end users. – Create environments for communication through conscious teambuilding. Include everyone responsible for IT infrastructure issues. Establish procedures for frequent meetings at all levels.
2. Staff hesitate taking further education or education programmes to improve their IT skills.	a. Lack of skills throughout the organisation. b. Reduces the ability to achieve key objectives.	– Motivation by financing further education, paid leave when studying prioritised subjects, career development programs etc.
3. Important management information is not available.	a. Affects ability to manage at all levels. b. Human, economic, legal and/or technological impacts, both external and internal.	– Create environments for confidence and frankness. Acknowledge contributions. This requires a management "close" to their staff. – Assign responsibility for identifying, classifying and recording information; legal, technological, customers need etc.
4. Inadequate awareness of technical trends and developments.	a. Budgets are underestimated, business opportunities are not exploited, low customer satisfaction, low motivation among staff.	– Establish the aimed technological level in IT policies. – Allow staff time to update their knowledge by free membership in IT associations, subscriptions to IT periodicals etc. Establish internal forum for exchanging knowledge. Communication throughout the organisation.

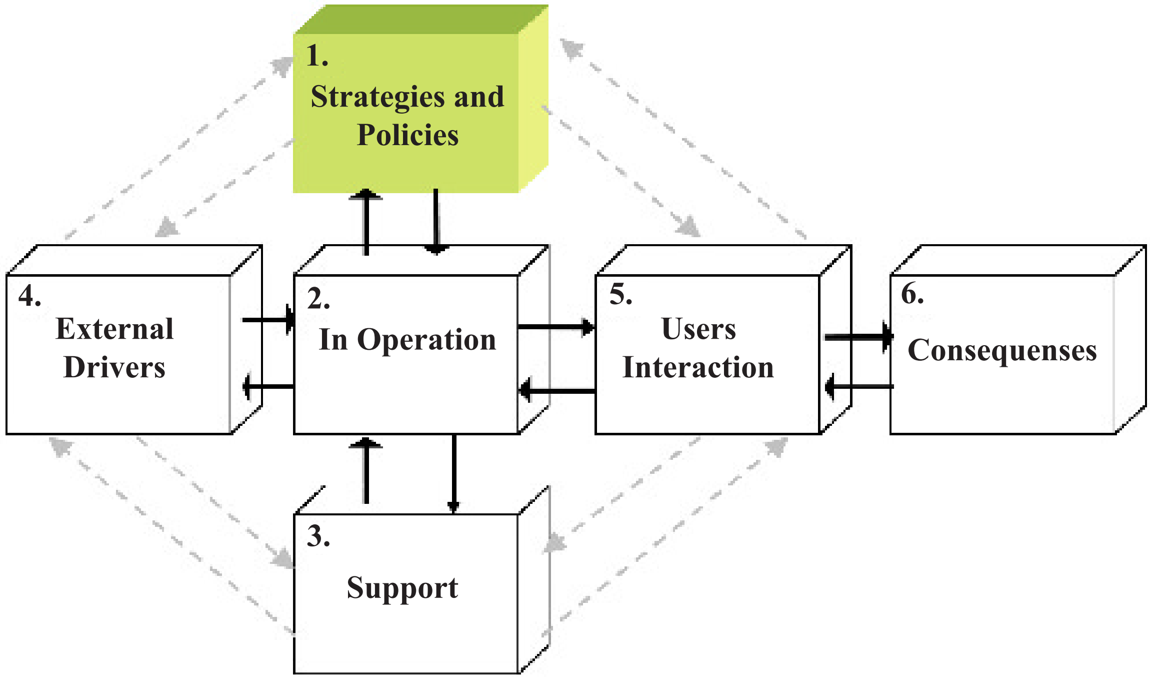
Aim: Top Management should establish procedures for controlling and monitoring IT service delivery activities.

Risk	Impact	Risk management strategy
Activity control and monitoring – Risk Management		
1. Top Management are not familiar with Risk Management theories and models.	disproportionate amount of resources be spent on risks not having high likelihood or impact.	The risk management model described in this guide should be adopted.
2. Top Management does not see the importance or the benefits of using formal Risk Management procedures.	a. Actors responsible might implement individual procedures, or the risk management might be informal. There might be no procedures for monitoring activity areas risks effectively. b. Lack of awareness and high likelihood for not achieving a balanced entity management. Mixed signals downward and low motivation in the organisation.	a. Gather information of the benefits and the costs of implementing Risk Management Model. b. Identify and analyse own risks as an experiment and decide if their likelihood and impact indicates permanent procedures to be implemented.
3. Top Management do not promote risk awareness or they do not promote it effectively.	Low motivation.	Appropriate risk awareness training programmes should be for all staff.
4. Top Management do not see the importance of motivating those responsible for risk management.	Risk Management could be informal or incomplete. Staffs do not see the point of spending valuable time on RM.	Carry through monitoring procedures frequently. Communicate with those responsible about results and actions to be taken. Arrange frequent meetings.
5. Top Management fails to implement effective and efficient procedures for Risk Management.	The foundations for making decisions are incorrect or incomplete. Necessary changes are not implemented. Part of, or the whole IT infrastructure fails to contribute of to achieving organisational objectives.	Gather information and make a survey. Identify which part of the process fails. Interact with those responsible.
Financial control and monitoring:		
6. Top or, most likely, middle managers do not have adequate financial management skills.	IT management focuses on IT service delivery without considering the financial issues.	Work out organisational directives and procedures in accordance with governmental directives for financial management. Obtain knowledge and focus on this issue through education programs.
7. Reports and information supporting financial management are incomplete or incorrect.	Cost overruns and poor cash flow are not identified. Decisions are based on unreliable information, resulting in important activities not receiving proper management attention.	Implement an effective financial information system, offering flexible financial reporting facilities.

Risk	Impact	Risk management strategy
8. Lack of or inadequate procedures for budgeting and reporting costs.	Delayed information or lack of information. Staff deliberately exaggerate or underestimate their funding requirements. This could lead to project costs and benefits being incorrectly stated, and projects being incorrectly prioritised. Exaggeration leads to undeserved credit when budgets are "in the black".	Introduce procedures for frequent reporting, weekly or monthly. Arrange frequent budget meetings with all staff responsible. Work out procedures for feedback. Undertake quality assurance on draft estimates and budgets. Work against rewarding systems or performance measuring systems that could lead to sub optimisation. Verification of estimates and withdrawing funds not spent at Year-end.
Manage changes:		
9. Political changes result in changed funding levels and/or priorities.	Top management is unable to make the necessary changes to It systems or projects to implement the new requirements.	A management framework together with procedures for re-defining plans and objectives, and for re-allocating resources.

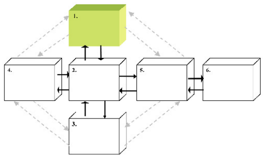
Risk Assessment

1. Strategies and policies



1.1 Definition

1.1.1 Organising for IS Strategy



IT now pervades every aspect of business management. It is important, therefore, that all major stakeholders are represented including activities that may appear to be peripheral to core business activities (for example, staff recruitment and training; the management of office accommodation; auditing and information security). The usual approach is to operate a structure of committees, sub-committees and planning teams that between them provide the breadth of perspectives and skills that comprehensive planning requires. In a large organisation it may be necessary to maintain a permanent team to help co-ordinate and administer planning activities on a day-to-day basis.

There must also be a clear reporting line from the top of the organisation. This provides the direction and authority that ensure that detailed planning remains firmly linked to business aims and objectives.

1.1.2 Planning for IT Services

Large sums of money can easily be wasted in developing IT services that fail to work properly (or at all), cost far more than was anticipated, take an excessive amount of time to deliver, or any combination of these. Planning IT services carefully and then controlling their implementation can significantly reduce the risk of such failure occurring.

There are numerous reasons why an IT service should be carefully planned. These include:

- the need to identify the business objectives and end-user requirements that an IT service is to satisfy, which in the latter case especially can be a lengthy and involved process;
- careful thought needs to be given to design to ensure that the technical system(s) that supports the service can achieve the identified business objectives and user requirements *in a cost-effective manner*;
- the lead time necessary to procure hardware and software; to let contracts for the provision of support services (such as hardware maintenance, data communications circuits); the installation of cabling infrastructure; and whatever building alterations are necessary to create a suitable environment;
- whatever is built or procured should be tested to ensure that quality criteria are met in terms of functionality, security, availability, serviceability and capacity;
- other activities that also absorb time include information security and business continuity planning, developing and delivering staff training, converting and migrating data from an existing to a new system, and planning a system implementation strategy.

1.1.3 The underlying thinking

The thinking that underlies strategic planning can be described as a series of questions:

- **what is the scope?** What do we need to address in our current planning, in what sequence and in what time-scale?
- **where are we now?** Do we understand our existing business; its aims, objectives and constraints; its working methods and the views of its stakeholders?
- **where do we want to be?** Do we understand how our business is likely to evolve over the planning period? Do we understand what problems can be addressed and new business opportunities created through technological developments?
- **how do we get there?** This is about planning "migration" from where we are now to where we want to be. What constraints exist in terms of finance, skills and manpower? What options and combination of options exist for moving forward? What would happen if we did nothing? What would the consequences be of doing everything? What intermediate solutions exist? What are the costs and risks?

1.1.4 The stages in the cycle

Changes in business needs, together with continuous developments in what IT can offer the business, mean that an IT strategy is not a static plan. It needs to be monitored (to ensure that it is delivering what was expected), reviewed and updated periodically. This involves a cycle of events:

- **scoping**: establishing the boundary for a strategy study (or perhaps more than one study), defining its outputs, and identifying any matters that require resolution before the main strategy study commences (e.g. resources, top management commitment)
- **undertaking the study**: analysing the business area under review and its environment, its existing use of IT, and identifying options for improvements
- **strategy definition**: bring together the findings and options from the strategy study, identifying constraints, and creating a blueprint for the future deployment of IT. A further important output from this stage is to define the managerial and technical policies that will underpin the strategy.
- **implementation planning**: producing a timetable for progressing the strategy; producing accurate estimates of resource requirements; and defining the scope, purpose and terms of reference for each implementation project;
- **monitoring, tuning and review**: this is an on-going activity, the aim of which is to ensure that there is satisfactory progress against the plan, tuning it more closely to business needs, and taking corrective action where it is required. IT services

1.1.5 Strategic planning outputs

IT strategy studies will vary in the nature of interim outputs. Some will evolve throughout the process. Many will be of value for other planning initiatives and will provide a starting point for later reviews.

Outputs from a strategy study will typically include:

- a scoping study report – the end product from the scoping study
- those relating to the business and its environment. These are usually embodied in

the strategy study report, but are sometimes provided as interim working papers for management comment and endorsement. They include:

  - description of the business environment
  - objectives and priorities
  - models of the business

- those concerned with the current and future use of IT. These also provide elements of the strategy study report, including:
  - review of existing use of IT
  - candidate applications for improvement
  - options for improvement
- the Strategy Report – the formal deliverable from the strategy study
- the definition of the "strategy", and its supporting documents, including:
  - the Strategy Statement
  - management and technical policies
  - plans (management and migration)
  - portfolio of implementation projects to be delivered
  - resource, funding and benefits profiles
  - business case and investment appraisal

These deliverables will be produced as documents, normally supplemented by management presentations, when the essential features of a number of deliverables will be covered.

1.1.6 Examples of management and technical policies

A very important output from a IT strategy study is to define the technical and managerial policies that will guide the organisation in their development and operation of IT services. The following are some examples of the policies that an organisation might adopt:

IT development

Policy:

- to minimise development
- to avoid high risk, leading edge technology
- to avoid bespoke development if commonly available products would meet most of the requirements
- to use proven commercial software packages wherever possible, considering an off-the-shelf solution in all feasibility studies
- where development work is undertaken, to use appropriate corporate standards (e.g. the use of ORACLE RDBMS) unless an exception is granted by the Director of IT
- to accept, where necessary, some loss of desirable (as opposed to mandatory) functionality in order to enable an off-the-shelf solution and reduced development
- to chose standard, modern equipment and software wherever possible, using only

bespoke software where it provides better value for money.

Audit and control of IT developments

Policy:

- to conform with formal procedures for control at the pre-project stage (*project authorisation and prioritisation*), during projects (PRINCE 2 standard for project management method) and after its completion (to ensure systems are delivering anticipated benefits), and that resources are used cost effectively in support of the Strategy
- to monitor project to ensure that they remain conformant to the IT Strategy.
- to set appropriate targets and performance measures for measuring benefits from new systems (e.g. response times to customer enquiries and to the resolution of service problems)
- to use control procedures (such as setting priorities, using PRINCE 2) to ensure that IT staff and users only spend time on authorised tasks.

Systems architecture

Policy:

- to base the systems architecture on *workgroups*
- to standardise on a limited range of hardware platforms
- to make workgroups as large as possible (but with due regard to the "need to know" information security policy requirement)
- to evaluate a limited number of platforms for conformance with the corporate standard version of Windows NT, and to implement systems only on those platforms that are demonstrably compatible with the operating system.

Standards

Policy:

- To use internationally agreed standards wherever possible.

1.2 Objectives

Against the background set out in the previous section, the IT department should:

1. Clearly understand their business aims, objectives and corresponding timescales, and the role that IT services are to play in meeting them.

This understanding should be incorporated in a written “IT Strategic Plan” designed to provide consistent understanding and direction for those who are to provide and manage IT services on a day-to-day basis, and to set benchmarks for measuring their success.

2. Have in place a management structure for implementing, monitoring the cost-effectiveness of, and updating the IT strategic plan.

3. Identify the standards, methods and software tools that are to support the application of the strategic plan.

4. Periodically reviews the outcome of their IT strategic planning, and make adjustments as necessary.

The Risk Management Strategy in the table relates to the Objectives identified above, and numbers indicates the links to the objectives.

1.3 Risk Assessment

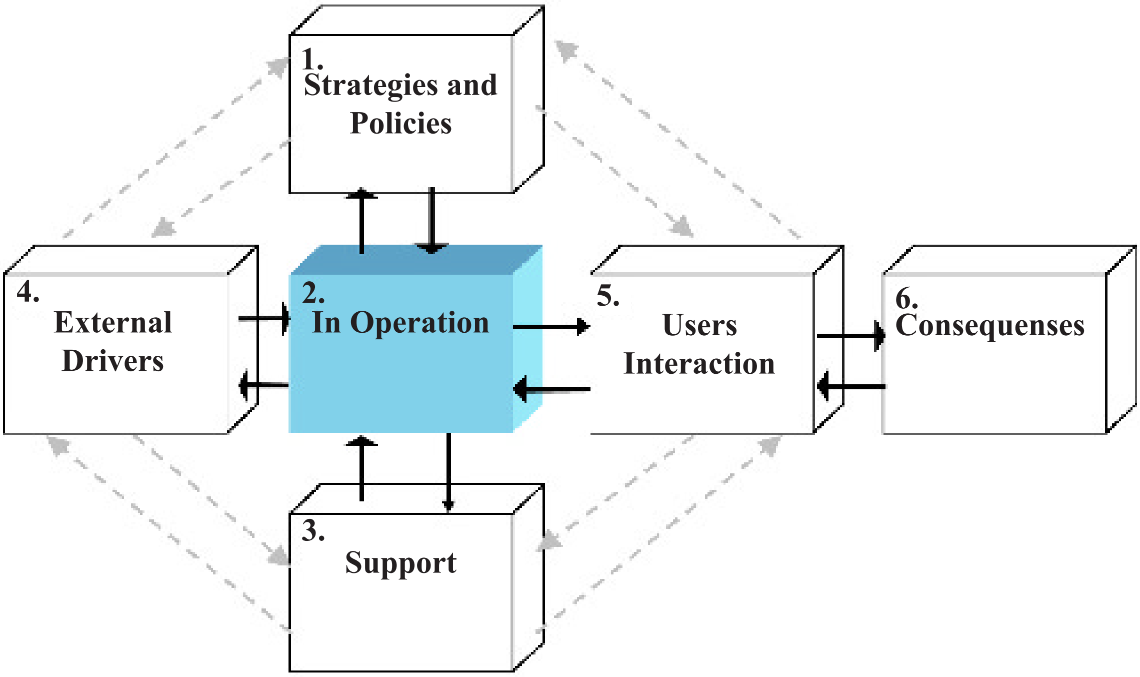
Risk	Impact	Risk management strategy
1. A new IT service(s) is not delivered on time.	a. Failure to meet statutory or contractual obligations. b. Missed business opportunities. c. Failure to deliver government policy on time.	Develop a strategic plan for IT to cover *at least* the next three years. The plan should link projected business needs and IT service requirements. (Objective 1). Develop a detailed tactical plan to prioritise delivery of the strategic plan over the next twelve months, and to plan the delivery in detail. (Objective 2). Review and update the strategic and tactical plans in the light of changing circumstances. (Objective 2). Implement programme and/or project management techniques to control the development and implementation of IT services (Objective 3).
2. The new IT service(s) development costs exceed/ are exceeding budget or economic justification.	a. Wasted investment (project possibly abandoned). b. Limited funds diverted from worthwhile projects. c. The service lacks essential functionality due to the need for unanticipated economies.	Develop a standard to control how a business case is to be developed, authorised and monitored. (Objective 3). Produce a formal business case to justify IT projects and programmes (e.g. options, and the related costs, benefits, strategic fit and risks). (Objective 1). Independently audit data and assumptions contained in major business cases. (Objective 1-4). Establish authorisation and accounting rules for project and programme expenditure. (Objective 3). Periodically validate actual project/programme expenditure against the business case. Re-validate the risks and assumptions contained in the business case. (Objective 4). Submit regular financial out-turn reports to top management. (Objective 4).
3. There are significant change(s) to requirements during the course of an IT project and/or programme.	a. Project/programme cost over-runs. b. Project/programme abandoned through excessive cost. c. Unanticipated technical problems/risks associated with the changed requirements. d. Delay in implementing the new service due to the need for additional development time. e. Higher operational and maintenance cost than anticipated.	Enforce formal change control procedures. (Objective 3). Where possible, defer significant changes until after the initial project and/or programme is complete. Define a formal business case to justify project and programme changes. (Objective 1). Obtain top management authorisation for any change that exceeds specified level of expenditure (beware of disaggregation! – splitting change requests into a number of small packets to bypass authorisation levels). (Objective 2). Revise the business case and project/programme plan following significant changes to requirements. (Objective 3).
4. The new IT service lacks important functionality.	a. The service is unable to satisfy important business needs. b. Failure to meet statutory or contractual requirements. c. Failure to produce acceptable accounts, where important accounting requirements are not addressed (e.g. audit trails). d. Security failure, where important security requirements are not addressed (e.g. strong logical access controls).	Ensure that project objectives are clearly stated and thoroughly understood before development work commences. (Objective 1). Formally specify service requirements and acceptance criteria, and use as a basis for acceptance testing. (Objective 3). Develop a standard for specifying and prioritising service requirements (e.g. list the interested parties to be consulted; hold workshops; one-to-one interviews with key personnel; opinion surveys for the general public). (Objective 3).

Risk	Impact	Risk management strategy
	e. The IT service is under-utilised or ignored by the public (resulting in wasted investment; failure to meet government policy, etc.).	Independent audit of requirements specification. (Objective 4). Build mock-ups of the live system using prototyping tools. (Objective 3). Consider building a prototype service to study functionality in a low risk environment. (Objective 3). Involve all interested parties in system acceptance testing. (Objective 3).
5. The new IT service(s) is unfriendly and difficult to use.	a. Higher operating costs due to low productivity. b. High error rate. c. Poor staff morale. d. The service is under-utilised or ignored by the public (resulting in wasted investment; failure to meet government policy, etc.).	Take care in specifying the user's interface with the service. Use workshops together with prototyping tools to get the user interface 'look and feel' correct. (Objective 1). Consider providing a Service Desk to provide advice on problems with service use. (Objective 3) Involve users in acceptance testing the new service. (Objective 4). Careful attention to the development of training material and user manuals. (Objective 3). Consider focus/user groups for discussing common problems, developing workarounds, and providing feedback to the service operators/ developers. (Objective 4).
6. The new IT service is unresponsiveness.	a. Need for excessive overtime working resulting in high operating costs. b. The IT service is under-utilised or ignored by the public (resulting in wasted investment; failure to meet government policy, etc.). c. Service failures due to over-loading. d. Low morale among personnel (e.g. due to poor systems to support their work and a constant need to contain emergencies).	Use capacity management techniques (pay careful attention to processor, storage and network capacity). (Objective 3-4). Undertake independent quality checks on program design and coding. (Objective 4). Consider developing a prototype system to study system response characteristics at the feasibility study stage of development. (Objective 3). Consider using automatic traffic generator software for load and stress testing. (Objective 4). Use 'demand management' to discourage high load activities at busy times (e.g. ban background tasks - such as backing up - during the on-line day; apply variable service charging rates). (Objective 3).
7. The new IT service(s) lacks satisfactory availability and/or serviceability.	a. Low morale among personnel (e.g. due to poor systems to support their work, and constant 'fire fighting' to contain emergencies). b. Failure to meet business deadlines. c. High operating costs (e.g. due to need for frequent system recovery and re-working).	Define policy on including resilience in new services (e.g. dual processors, dual LANs, and excess disc capacity). (Objective 1). User requirements to include availability (downtime as a percentage of agreed service time), the number of service breaks per period, and the maximum tolerable length of any one break. (Objective 3). For contracted out services, specify the required availability, failure and service recovery levels. (Objective 2) .

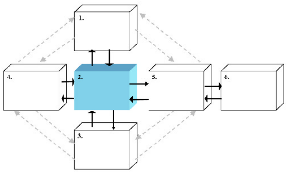
Risk	Impact	Risk management strategy
8. The new IT service(s) is difficult to maintain and/or change.	Missed business opportunities. Failure to deliver government policy on time. IT services are expensive to operate. System changes expensive to change and vulnerable to error and failure.	Define what hardware, software and design standards are to be followed as part of IT strategy. (Objective 3). Undertake quality inspection during development projects to ensure conformance with design standards. (Objective 4). Ensure that all aspects of service design, operation and use are documented to an agreed standard, that documentation is kept up-to-date, and that it can easily be located and recovered. (Objective 4). Implement IT service management practices. (Objective 2).
9. The IT service(s) cannot be scaled up to accommodate business growth (e.g. more users and/or functionality).	Missed business opportunities. Failure to deliver government policy on time. Cost of service re-development.	Ensure that IT strategic planning includes a requirement for analysing service use and predicting service growth.(Objective 1). Implement capacity management to provide advance warning of possible service capacity problems. (Objective 4). Ensure so far as possible that service designs (hardware, software, communications, etc.) are scaleable. Transfer the risk – outsource the delivery of the service to a major commercial provider. (Objective 2).
10. The new IT service(s) is insecure.	Hacking, mischief, service failures. Fraud. Individuals placed at personal risk (e.g. through inadequate information security or software error). Wasted investment – e.g. the public ignore the service because of security concerns.	Define IT security policy. (Objective 1). Undertake IT security risk assessment. (Objective 1). Define a management structure to implement, monitor and maintain IT security policy. (Objective 2). Provide specialist advice on IT security risk assessment and risk management. (Objective 2). Define IT security incidents, and implement a process for reporting, recording and investigating security incidents. (Objective 3). All information resources have a nominated ‘owner’ to be held accountable for their security and use. (Objective 2). All important information resources should be backed up regularly, with at least one copy stored remotely. (Objective 3). There should be appropriate, workable business continuity arrangements. (Objective 3). All personnel should receive IT security training that is appropriate to their particular role. (Objective 1). Audit the IT security management process for compliance and effectiveness. (Objective 2).

Risk Assessment

2. In Operation



2.1 Definition



This section provides advice on the audit issues that are relevant to the effective and efficient delivery of IT services.

IT service delivery includes the following main activities:

- Development
- Running
- Maintenance
- Support

The main requirements for performing these activities are:

- Developing strategies and policies for the organisation;
- Implementing effective IT security;
- Funding;
- Human resource management;
- Managing external demands.

In order to perform these activities, the following objectives need to be met.

2.2 Objectives

The IT-Department has to deliver IT services effectively and efficiently in order to support business goals.

Changes in focus on IT 's importance in business leads to changing requirements, in particular when it comes to leading an IT Organisation. There will be less focus on IT managers' technical skills, and more focus on their ability to lead, ensuring that the organisation is supporting business goals. Increasing importance and usage of IT makes this less a technical part of the organisation, and more an integrated part of overall business functions. Therefore IT management's leadership ability will be brought more into focus. One solution is to organise the management of the IT department to correspond to different parts of the business structure.

The IT-Management risks are often closely connected to Top Management's overall risks. Operations management is responsible for the daily running of hardware and software facilities so that (1) production application systems can accomplish their work and (2) development staff can design, implement, and maintain application systems. Due to the indispensable importance of the information systems to numerous organisations, many operations managers see themselves as the " engine" when it comes to running and maintaining the daily business in their organisations. The tasks they perform can be critical to an organisation's success.

2.2.1 Ensure system development

Aim: To ensure that system development processes are established in order to support the stated organisations objectives.

System development management has responsibility for those functions concerned with analysing, designing, building, implementing and maintaining information systems. There is no approach to system development that can be used on all systems and situations. They all have advantages and disadvantages, and leave management with a range of choices.

Projects should be initiated using well-defined procedures to communicate the organisation's needs to responsible management. These procedures often require detailed documentation identifying the need or problem, specifying the desired solution and relating the potential benefits to the organisation. All internal and external factors affected by the problem and their possible impacts on the corporation should also be identified. This documentation is then reviewed by a senior management committee that will determine the priority of the user's request for a resolution.

2.2.2 Ensure continuity in delivery of IT services

Aim: To ensure continuity in delivery of IT services in accordance with the organisation's stated goals that are formed in:

- Business strategies
- Functional strategies
- Operational plans

There should be procedures and strategies designed to ensure continuity of operations. Routines for input and output controls, proper monitoring and problem solving are essential to the daily running and delivery of IT-services. Within the organization, there should be policies dealing with how to handle software-licening issues. The success of the IT Organisation depends upon satisfying end users processing and service requirements. These services include accuracy, completeness, timeliness and proper distribution of output related to application processing. Services delivered have also to be in accordance with stated security policies and procedures.

Business continuity planning

An important aspect of the System Security Policy is a requirement to produce business continuity plans that are both workable and consistent with the criticality of IT services to the organisation.

Most organisations now rely on It services, some to the extent that if key services are unavailable for a matter of hours the business can be severely affected. It is generally impossible to fall back on manual methods, either because it is not technically feasible (e.g. in network services), or there are insufficient staffs to process the volume of work, or staffs no longer has the necessary skills; or a combination of these.

Although in practice business continuity planning is often forgotten or put to one side, the formulation of workable plans should form part of development projects. New services should enter live use with workable plans in place to cover various failure and disaster scenarios.

Business continuity plans need to take into account the relative importance of individual services to the organisation - this should be established using risk assessment techniques - and against this background plan how alternative computing facilities are to be provided. Following a service breakdown or disaster, critical services need to be restored first, perhaps in a matter of hours, whereas the time-span available for restoring non-essential services may run to weeks. The maximum recovery time available for each service will determine the type and cost of the standby arrangements that are necessary.

In general, standby options include:

- "Do nothing"; perhaps an option for unimportant services;
- Manual fallback procedures may be feasible in some cases;
- Reciprocal arrangements made with other organisation, although these may be ineffective due to informality and lack of a legal foundation;
- "Fortress" approach - building in such a high level of protection and resilience that a service is unlikely to be affected by major breakdowns or disaster;
- "Cold start". Providing alternative accommodation equipped with power, environmental equipment, and telecommunications connections installed, but empty in all other respects. Can be either fixed or mobile;
- "Hot start". Providing an alternative fully equipped computer and operations suites, either within the organisation or using an external disaster recovery contractor, and on either a fixed or mobile basis;
- "Mirrored" services to cover the most critical applications of all. These are geographically separated locations using systems that are updated in parallel, with arrangements to switch communications and processors on command.

Other aspects of continuity planning, which should also be addressed during development, are the means whereby business users can also be re-located and connected to the stand-by system if necessary. The need for alternative voice and data communications, for copies of important paper documents to be stored off site (e.g. user manuals, important contracts), and for procedures for clerical processing financial data until the stand-by service is available, are also often over-looked.

2.2.3 Obtain the level of maintenance as required

Aim: To obtain the level of maintenance as required ensuring continuity in IT-services.

Hardware must be routinely cleaned and serviced to ensure proper operation. Maintenance requirements may vary based on Information Systems size and complexity. Maintenance should be scheduled to closely coincide with vendor-provided specifications. The procedures used to carry out maintenance to programs are often important to ensure service continuity. If controls over maintenance are not properly performed, unauthorised, inaccurate, or incomplete codes could be implemented in a production program. Controls must exist to ensure that changes in production programs are formally approved, and that the process of designing, coding, testing, and implementing the modifications required is monitored carefully.

2.2.4 Obtain necessary support

Aim: deliver sufficient support in order to enable the organisation to utilise the IT- Services provided.

End-user support for information systems covers:

- Taking the requirements of end users into account in the specification, design, development, implementation and operation of information systems and services;
- Considering the support requirements of in-house users and, as appropriate, of the general public;
- Ensuring that users are fully involved in and supported by IT -related programs of business change;
- Ongoing training and development facilities for end users;
- Provision of support facilities such as Help Desks for end users of information systems;
- Promulgation of policies and Codes of Practice on the use of in-house IS/IT facilities by staff

Where a system is managed or maintained on behalf of users by an internal or external service provider, users and provider should formally agree on the range and levels of services to be delivered.

A Service Level Agreement (SLA) is a written agreement between the customer of an IT service and the service provider. It does not constitute a legal contract in itself but may be an essential component of it. Without an SLA there is a risk that system performance will not be related to any measure of service that users understand or require. An SLA should therefore define the required performance of the system in terms of its availability to users, response times, numbers of transactions processed, and any other appropriate criteria meaningful to the user. Performance indicators will need to be agreed, and the delivered level of service should be regularly monitored against that specified.

An SLA should also define the level of technical support to be provided to users (for example in training, help desks), the procedures for proposing changes to the system, standards of security provision and administration (e.g. system and data access controls; monitoring system and network use); contingency requirements; and a schedule of charges for the services to be provided.

Work on defining the SLA should have been started during the System Design Stage when the shape of the eventual operational system began to emerge. During the implementation phase, the SLA will need to be completed in detail, and signed off by both the System Owner and the Service Provider.

2.3 Risk Assessment

Ensure system development

Aim: ***To ensure that system development processes are established in order to support the stated organisations objectives***

Risk	Impact	Risk management strategy
1. An IT project is not in accordance with corporate agency plans or IT-strategy.	a. IT systems don't support business goals. b. Ineffective use of recourses. c. Project delivery is not accepted by users.	– Management on all levels has to commit to all authorised projects initiated. – The organisation of the project has to be effective. Accepted System Development Methods have to be used.
2. The IT Infrastructure does not interact effectively and efficiently with the organisations goals.	a. IT-organisation does not consider the organisations needs. b. Top management has little awareness on the importance of IT.	– IT-plans should be consistent with and integrated into senior management's long-range plans. The IS-departments long-range plans should recognise organisational goals, organisational changes, technological advances, and regulatory requirements.
3. Level of confidentiality on information has not been considered.	Unwanted exposure of information; – Internal. – External.	– The management has to declare in their business strategy, on what level of confidence the organisation information is to be handled.
4. Unrealistic budgeting in both time and cost, deliberately or not.	a. Acquisition and development are not delivered on time. b. Higher costs than budgeted. c. Loss of credibility; – Internal. – External.	– Ensure that projects are initiated by organisational needs and not by people with a special field of interest. – Implement Benefit Management procedures.
5. Ownership to systems is not in place.	a. No overall responsibility for the day-to day system security is established. b. No overall responsibility for system changes, updating etc.	– An overall accepted system development Methodology will ensure that a system ownership is established. This is, among other factors, to ensure system updating, user commitment and allocation of cost.
6. The new IT service(s) fails to attain optimum performance.	Failures to optimise return on investment. User productivity less than anticipated. Operating and/or maintenance cost greater than anticipated. Continuing user dissatisfaction with the system. Failure to learn lessons for future projects.	Undertake an independent (i.e. of the project team) post implementation review and act on its findings. Consider undertaking further post implementation reviews at intervals throughout the life of the service to ensure that maximum business benefits continue to be obtained in the face of changing use. Implement user groups to provide feedback and suggestions for enhancements.

Ensure continuity in delivery of IT services

Aim: ***To ensure continuity in delivery of IT services in accordance with organisation's stated goals formed in:***
- Business strategies
- Functional strategies
- Operational plans

Risk	Impact	Risk management strategy
1. The organisation has no awareness of security issues.	a. This can lead to loss of business. If industrial secrets are exposed it might, in worst-case lead to business failure.	– Awareness on all levels. Security strategy. Classification of sensitivity. – Implement the most effective and efficient security measures.
2. The organisation of the IT – department does not prevent unauthorised access to data.	a. The organisation exposing itself to malicious alter-action of data and theft of corporate assets. b. Unwanted exposure or loss of data. c. Intruders inside and outside the organisation can access data. d. Change of standing data.	– Segregation of duties or develop alternate controls. These should be supervised and checked. – The organisation should have a security policy that includes the security of Breach of confidentiality, loss of integrity and reduced availability. The security policy should also include monitoring.
3. The IT-function fails to deliver due to lack of capacity.	a. Tasks cannot be carried out. b. System fails due to lack of capacity planning. c. IT-resources are not efficiently used (IT-capacity is not used).	– Planning to ensure that cost-justifiable capacity always exists to process the workloads agreed between the service provider and customer(s). – Providing the required performance quality and quantity. – Monitoring the systems used and the services provided to check that the work can be processed and the performance levels experienced are as specified in service level agreements, and recommend corrective action if they are not. – Identifying the work and the levels of service that can be supported on available or planned capacity.
4. Backup and recovery procedures are not in accordance with the organisation's stated level of services.	a. Loss of data. b. The organization may not deliver services on time. c. (Backup/recovery procedures are to be comprehensive compared with organisations needs i.e. use of hot sites when this is not necessary). d. The procedures are not efficient.	– Uninterruptible Power Supply (UPS) are installed and regularly tested. – Estimation of loss is made to help in assessing level of backup procedures i.e. critical systems are identified. "Down time" is stated. – Testing of procedures is undertaken.
5. There are no Change Management procedures.	a. Problems with system compatibility. b. Changes lead to problems that easily could have been detected and prevented.	– Changed management procedures have to be clear and known. – Complete and up-to-date application and configuration documentation is available. – An independent process for verification of the success or failure of change is implemented.
6. Difficulties in recruiting qualified personnel.	a. Slows down production speed. b. Forces the organisation to use alternative solutions such as temporary staff recruitment agencies. c. Loss of knowledge.	– There has to be an up to date human resource plan. – Have sound policies on adjusting salaries to the private market, if possible. – Emphasise the advantages of working in public sector, when recruiting staff.

Risk	Impact	Risk management strategy
7. Network failures.	a. The organisation can become unable to deliver services.	– An important tool that operators use to manage a WAN (Wide Area Network) is a network control terminal. This terminal provides access to specialised systems software that allows a number of functions to be performed. – Alternative routed circuits can be established. – Redundant circuits are also an alternative that can be used to provide resilience. – Within LANs (Local Area Networks) there also are a wide range of controls that can be performed: – Available disk space on a file server can be monitored. – Utilisation activity and traffic patterns within the network can be monitored. For a complete network audit there is a lot of material available, not covered in these risk assessments.
8. Wrong versions of programs are utilised.	a. Loss of data. b. Incorrect data. c. Program failure.	– File library has to be established. – There has to be a library function for documentation and programs. – There has to be established Version control and software release procedures.
9. Applications software is used without legal software license.	a. Illegaly use of copied software. b. The organization could be held economically responsible for using illegal applications software.	– The organization ought to have a procedure, to prevent that application software is used without proper software licence. – The organization should keep/file the entered software-licence contract.

Obtain the level of maintenance as required

Aim: ***To obtain the level of maintenance as required ensuring continuity in IT-services.***

Risk	Impact	Risk management strategy
1. The organization fails to achieve an adequate level of service availability.	a. Unsatisfied customers and users. b. The organization losing credibility.	– Organisational strategy and plan, IT strategy and plan, and other plans concerning the delivery of services, have to be consistent with the overall anticipated level of service. – Procedures for monitoring the service levels achieved, for taking remedial action on under-performance, and for improving quality of service delivery are to be established.
2. Roles and responsibilities for third parties are not clearly defined.	a. Third parties fail to accept their responsibility. b. Problems in continuity of services. c. The organization has no legal protection if loss of business appears due to failure in third party deliveries.	– Clearly defined service requirements and performance measures are established. – Third party providers have a quality assurance programme established. – Contracts are signed after a legal review. – Processes are established in order to classify service problems based up on their importance and their required response.
3. Critical components of the infrastructure are not identified and monitored.	a. Failure in delivery of services.	– Critical systems, applications, network solutions amongst others, have to be identified in order to ensure system continuity. – Hardware and software plans have to take in to consideration the existing infrastructure and prioritise the replacement purchases.
4. The organisation has no uniform approach to the purchase of hardware and software components.	a. Difficult to maintain the infrastructure. b. Unnecessary expensive maintenance routines due e.g. several smaller maintenance agreements with third parties, instead of a few more efficient routines. c. Problems with vendor commitments.	– Develop an organisation-wide purchasing policy to guide in purchasing decisions. – Ensure proper implementation of the stated policy on purchasing issues.

Obtain necessary support

Aim: ***Deliver sufficient support in order to enable the organisation to utilise the IT-Services provided.***

Risk	Impact	Risk management strategy
1. End-users cannot use the application system.	a. Tasks cannot be carried out. b. Loss of data due to inexperienced users.	– The organisation has a help-desk function. – System development-/acquisition routines have to consider the need for user training when new systems are implemented, or when major system changes are made.
2. There are no functions to inform end users of problems.	a. Loss of credibility. b. Failure to meet users requirements. c. Changes will be made on the systems by "clever" employees due to lack of responsibility.	– In order to minimize e.g. system failure impacts, there should be an information strategy present. – Known system maintenance that could lead to error has to be informed of in advance. – Accepted "down-time" in the organisation has to be communicated to users on all levels. – Form a Service Level Agreement (SLA), which is a written agreement between the customer of an IT service and the service provider. See 4.2.4 above.

Reference Material In Operation:

Handbook of IT Auditing,
by Warren, Edelson, Parker.

BS 7799 and Guide to BS7799, Risk Assessment and Risk Management
By British Standard Institution

COBIT (3rd Edition) Management Guidelines
By Information Systems Audit and Control Foundation

Information Systems Control and Audit
By Ron Weber, 1999

Anbefaling til God IT-skikk(Recommendations for Best practice on IT)
By Information Systems Audit and Control Association, Norway Chapter And Den Norske Dataforening

Management Information Systems, 6th edition
By Laudon & Laudon

Auditing IT Service Management (this report)

Other Reference material:

Free resource - **Why IT Project fail** at http://www.citu.gov.uk/succesful_it.pdf/

Free resource - **The IS Management Handbook** at http://www.ogc.gov.uk/handbook/

Free resource - **Programme Management Overview at**
http://www.ogc.gov.uk/prince/progmgtoverview.rtf

Free resource - **Procurement at** http://www.ogc.gov.uk/pdfs/proc_hbook21_12_00.pdf

Free resource - **IT Infrastructure Management Self Assessments** at

Service Support: http://www.itil.co.uk/online_ordering/serv_supp_graphs/serv_desk.htm

Service Delivery: http://www.itil.co.uk/online_ordering/serv_del_graphs/itserv_cont.htm

Various free resources at http://www.ogc.gov.uk/ogc/publications.nsf/pages/publications.html

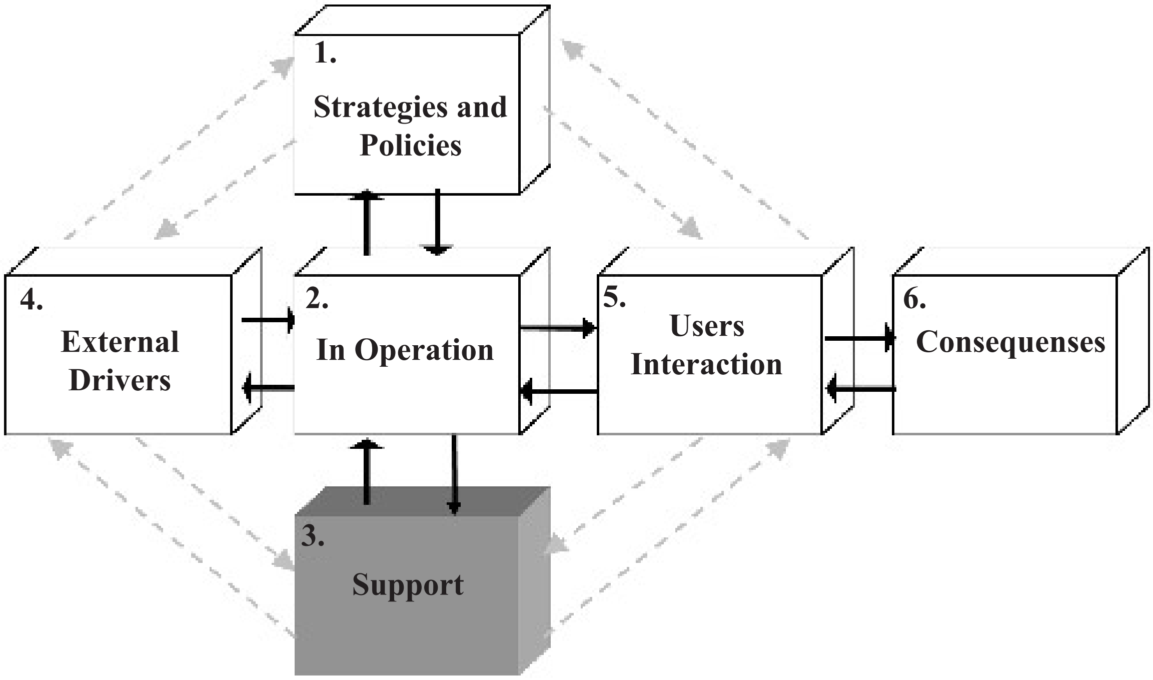
Reference to commercially available material on IT Infrastructure Management - http://www.itil.co.uk/

Reference to commercially available material on PRINCE 2 - http://www.ogc.gov.uk/prince/

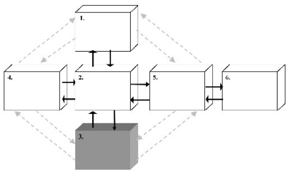
UK government "E-government" strategies http://www.e-envoy.gov.uk/egovernment/index.htm

Risk Assessment

3. Support



3.1 Definition



This section provides advice on auditing IT infrastructure support, which aims to ensure the effective and efficient achievement of the organisation's stated business objectives.

The operation of IT-systems is included in the "In Operation" activity area.

Support is defined as:

- Financial
- Technical
- Human resources

Managers must do more than manage what already exists. They must also create new products and services and re-engineer the organisation's systems from time to time. A substantial part of management is creative work driven by new knowledge and information; IT can play a powerful role in redirecting and redesigning the organisation. This is why effective IT service support is important.

3.2 Objectives

Management on all levels are aware of, and take advantage of the opportunities provided by a flexible IT infrastructure.

3.2.1 Manage Human Resources

Aim: Ensure that there are sufficient human resources to develop and maintain the IT services.

In most organisations there will be a minimum need of IT skill and experience covering operating, developing and maintaining IT-services. Effective routines for installation, operation and maintenance of both hardware and software are necessary to ensure efficient use of IT resources. IT personnel are difficult to recruit due to an enormous growth in the "Internet Industry". This makes it even more important to have a plan for recruiting and educating IT infrastructure support staff.

In addition to IS skills, people working within, or delivering IT services to an organisation will need some knowledge and understanding of the business, its technology, processes and business activities. These skills will be specific to the organisation or to the industry. For public sector organisations skills will need to be relevant to their area of operation, but they will also need the skills required for effective IS governance, and for achieving government objectives. The skills required for the effective exploitation of IS can be considered from the following perspectives:

- Professional IT skills
- Business/management skills
- End user skills

To ensure that the organization will continue to have access to the right mix and quantity of skills, business managers should establish formal policies and procedures for the management of skills in the organisation.

3.2.2 Provide Funding

Aim: The organisation receives sufficient funds to enable IT infrastructure to be developed to meet organisational objectives.

The investments made in Information Systems often from a “productivity paradox”. The paradox pertains to the phenomena that organisations are continuing to invest substantial amounts of money in information systems, sometimes without any apparent payoffs from this investment. The payoff may occur in terms of improved effectiveness of the services delivered. The improved effectiveness might lead to increased value for the users, but can be difficult to measure as increased “profitability” for Government. It is always important to focus on these factors when there is a discussion on new IT services to be delivered. A post implementation review can be performed on comparable existing systems, to determine two things: 1. How well this system is meeting its stated objectives. 2. Evaluate the adequacy of the system development process used to design and implement the system. The first part can be used to discuss implementation of new services. When evaluating the post implementation reviews the auditors always should assess the underlying motivation for the evaluation made in the organisations.

Further information on Post Implementation Review can be found at Annex 3.

3.2.3 Exploit Technological Opportunity

Aim: The organisation should exploit the opportunities provided by new technology in order to achieve organisational objectives effectively and efficiently.

Business process re-engineering (BPR) is the process, used by private firms, for responding to competitive economic pressures and customer demands in the business environment. Similar thinking can be used in public organisations to exploit new possibilities to offer their services. Advantages of BPR are usually experienced where the re-engineering process appropriately suits an organisation’s need. BPR has increasingly been used as a method for achieving cost savings through streamlining operations and gaining the advantages of centralisation within the same process.

Outsourcing is another issue that can be discussed for parts or all of the IT-function. There is an increasing focus on this in governmental organisations, though the long-term effects are yet to be seen. One problem can be that the organisations are dependent on the service provider when it comes to exploiting technological opportunities.

The Internet is creating a whole new area of business. It creates new possibilities for government service providers to distribute services to the public more effectively. A common factor of new technology is that it offers a means for organisations to increase service levels and reduce costs.

3.3 Risk Assessments

Manage human resources

Aim: Ensure that there are sufficient human resources to develop and maintain the IT infrastructure

Risk	Impact	Risk management strategy
1. Lack of skilled employees to ensure continuity in IT service.	a. Problems in deliver services at the right time. b. Quality. c. Relevant IT systems. d. Turn over. e. Inexperienced staff. f. Reliance on few key personnel.	– There should be a plan for managing human IT resources. Management on all levels has to support and commit to the IT human resources plan. – There has to be consistency between the IT strategic plan and the IT human resource plan. – Appropriate training is available to fulfil the needs of the IT human resources plan.
2. The technological infrastructure is not consistent, and use of incompatible systems leads to increased cost for the entire organisation.	a. Failure to deliver services. b. High maintenance costs.	– There has to be policies and procedures for: – Implementing and managing the IT Infrastructure. – Support the sharing of information between users and across business applications. – System acquisition and maintenance plans should be formed and updated. – Technical Infrastructure overviews should be kept up-to-date. – Be able to move application systems between different hardware and software platforms. – Adhere to well articulated management and technical policies. – Have clear management ownership and responsibility for infrastructure components. – Compatibility between infrastructure components, making change possible without disruption. – Have clear, well-designed change management processes and procedures.
3. Ineffective use of resources.	a. Lack of support from the employees. b. Loss of competitiveness.	– Communicate all changes in IT systems to interested parties to ensure understanding for priorities been made. – Use BPR (Business Re-engineering techniques when a wish for new services are being made.
4. Ineffective use of resources due to unskilled users.	a. Loss of credibility because users don't find the services useful. b. Wrong decision is made due to incorrect use. c. IT resources spend too much time resolving error caused by unskilled users.	– Training should be provided on a fair and regular basis to all employees. – Changes in systems should naturally be followed by a training course.
5. The operational service does not comply with legal and regulatory requirements.	a. An IT service is not in accordance with the organisation's stated objectives and goals. b. Loss of credibility. c. Cost of remedial action. d. Possible legal consequences due to processing transactions in an unlawful way.	– When developing new strategies, plan to ensure that all parts of the organisation have sufficient skilled employees. – Develop a human resource plan where there exists a requirement for skilled IT personnel. – Be aware of, and maintain a register of the legal and statutory requirements that relate to each business process. – Take professional legal advice when defining a specification for a new or amended business process to ensure proper compliance with legal and regulatory requirements.

Provide funding

Aim: ***The organisation should receive sufficient funds to enable IT infrastructure to be developed to meet organisational objectives.***

Risk	Impact	Risk management strategy
1. The IT infrastructure is not up to date.	a. The organisation may fail to meet stated objectives. b. The Infrastructure does not contribute to organisational progress and/or social change. c. The IT infrastructure is difficult and expensive to maintain. d. Problems with recruiting skilled personnel who understand the old technology. e. Problems with recruiting necessary personnel, both in the technical and business departments/ functions. f. High operating costs running and maintaining legacy systems.	– Managers are responsible for making decisions on how to use IT in the business processes. – There has to be consistency between the stated use of IT and the availability of resources. – Funds must be expended in a planned, systematic way to ensure adequate resources are available when and where they are needed. – Developing IT strategies in accordance with the Corporate Plan. – Monitor progress against the strategy, investigate and take action on variations.
2. Difficulties in gaining user acceptance i.e. the benefits are difficult to measure, or are not being achieved fast enough.	a. Loss of business/dissatisfied customers. b. Difficulties with end user acceptance. c. Low productivity and falling staff morale.	– IT-Management has to clearly communicate the benefits of implementing new solutions. – Ensure that a clear connection exists between the Corporate Plan and the IT Strategic Plan. – Undertake a post implementation review to identify problems – act on the PIR recommendations. – Monitor productivity levels, and investigate the causes of peaks and troughs.
3. Higher staff turnover rate than the organization can tolerate in order to ensure continuity.	a. IT Infrastructure development plans are delayed or abandoned. b. Increases uncertainty in IT-service delivery. c. Higher costs, due to continuous training of new employees. d. Low productivity and falling staff morale due to lack of continuity.	– Implement a Human Resource Plan, as mentioned above (See 5, page 50). – Personal development planning can be a way to reduce staff turnover. – Implement a comfortable working environment ("ergonomics") and use up-to-date technologies.
4. Unable to identify, measure or control IT infrastructure costs.	a. Over/Under budgeting. b. No commitment in the organization to IT development. c. Difficult to measure advantages of the new system(s).	– Establish ownership of IT investment projects. – Ensure that financial targets for system development and for day-to-day operation are included as part of the justification for new systems and services. Subject estimates to quality assurance. – Implement IT infrastructure accounting as a means of identifying and measuring cost components.
5. IT investment fails to provide value for money (Investment risk).	a. New investment will be hard to justify.	– There has to be analyses of cost vs. benefit of the project prior to development. The management ought to carry out quality assurance of these analyses. – Use methods identify Critical Success Factors to help in system development. See also the 'In Operation' section for details on project management.

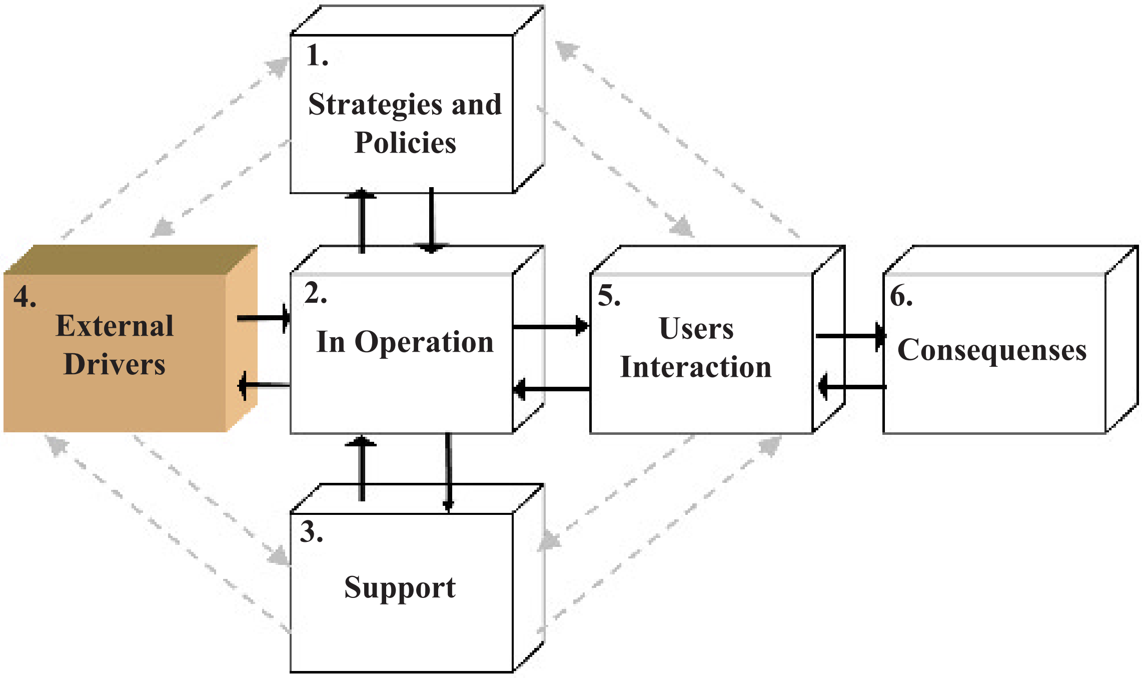
Exploit technical opportunities

Aim: The organisation should exploit the opportunities provided by new technology in order to achieve organisational objectives effectively and efficiently.

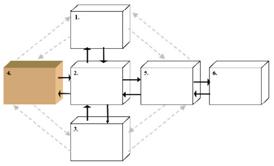
Risk	Impact	Risk management strategy
1. Top management are unaware of the business opportunities made possible by IT infrastructure developments.	a. The effectiveness and efficiency of the IT infrastructure will not be optimised. b. Obstructs the introduction of "electronic government". c. Excessive costs due to the retention of inefficient and uneconomic paper-based and legacy IT systems.	– Appoint a top manager to "champion" the organisation's use of electronic business techniques. – Promote electronic business awareness campaigns at all levels of the organisation, and make sure everyone knows about and understands what changes are planned and how they will benefit from them. – Appoint an IT Steering Committee that has overall responsibility for the activities of the IT-function. – There should be established goals and objectives for Information Systems within the IT Strategic Plan, and regularly monitor progress against them. Investigate the reasons for under-performance.
2. New IT investments are driven by, and conducted by IT-personnel.	a. Wasted investment on 'technical fashion' rather than on legitimate business needs. b. Wasted investment on replacing systems that have not reached the end of their economic life. c. Systems contain excessive functionality, and are therefore more difficult to use and more expensive to maintain.	– Define corporate policies and procedures for controlling capital investment. – Ensure that a senior management committee (including and chaired by business area representatives) approves all IT infrastructure investment proposals. – Ensure that IT infrastructure investment proposals come out of the IT Strategic Plan. – Introduce a system of budgetary control within the IT-function, to be run in conjunction with IT cost accounting. – Ensure that the IT Strategic Plan is clearly linked to the Corporate Plan.

Risk Assessment

4. External Drivers



4.1 Definition



This section of the guide focuses on the following principles concerning external regulations, constraints and other drivers for IT services. There are the needs to manage:

- formal regulations
- demands from target groups
- third party opinions
- drivers from new IT knowledge.

Together they indicate the need for organisations to act to minimise the likelihood that their IT Infrastructure fails to meet external demands and requirements (drivers, regulations and constraints) from Parliament, Government and other organisations.

4.2 Objectives

4.2.1 Manage formal regulations and policies

Aim: to ensure that the organisation recognise formal regulations that have an impact on IT Services and the IT infrastructure that supports them.

Organisations need to identify and analyse formal regulations in order to assess in what degree such regulations have an impact on the IT services and the IT infrastructure that supports them. Formal regulations to be analysed are produced by Parliament, Government and other public agencies. Relevant regulations are common regulations (integrity, secrets, archive, security etc), special IT-regulations (procurement, development, maintenance, IT security, Government regulations for the specific field of actions (service to be delivered) and special regulations from public agencies. The risk of failing to identify and analyse regulations is that the developed IT services will not comply with the law.

In society there are several drivers for increased and more developed use of IT that organisations sometimes find it difficult to assess and to decide how to react to. There are several sources of IT drivers, such as Government policy on the use of IT in public administration (e g Modernising Government through IT), competing organisations developing IT, and universities and other research institutions developing good practice in IT infrastructure development.

Management should therefore promote a regulation analysis policy that focuses on identifying regulations having impact on the IT services.

4.2.2 Manage demands from target groups

Aim: to ensure that the organisation understands who its customers/user are, and their particular needs.

Organisations need to undertake research at the earliest stage of development of an IT service to establish the end-users' business requirements. This kind of early end-users analysis needs to be reviewed on a regular basis in order to ensure that the demands from target groups are known and up to date. Otherwise the IT service will runs the risk of failing to meet their requirements.

Management should therefore ensure that careful research is carried out to identify and prioritise the user requirements for a new service.

4.2.3 Manage opinions from third parties

Aim: to ensure that organisations get relevant opinions from third parties concerning the IT service involved

Organisation often uses third parties to deliver, develop or operate parts of the IT service based on contracts. Sometimes an organisation outsource the whole or a part of the IT service to an external “service provider”. Organisations need to undertake research or review activities in order to establish the service provider’s opinion about the IT service efficiency. Otherwise the risk is that the organisation will miss opportunities to make IT service improvements.

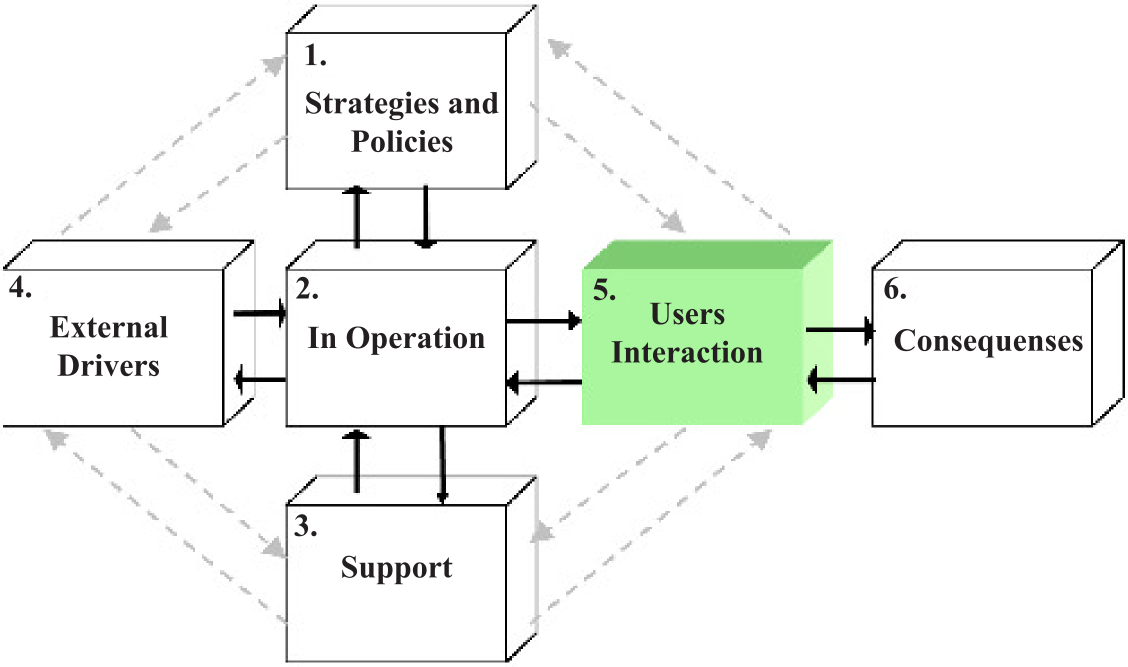
Management should therefore encourage service providers to make suggestions for improving the IT service delivery.

4.3 Risk Assessment

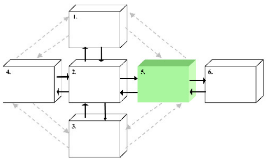
Risk	Impact	Risk management strategy
1. Top Management fail to see the area as an area of management.	The organization is unable to respond quickly to external drivers for change, resulting in: ● political embarrassment. ● delay in implementing government policy. ● excessive costs due to greater need for overtime working and the need to use consultants.	Managing the organization of the risk area: – establish the context and awareness. – identify the external risks and maintain a list of risks and sources from where they arise. – analyse the risks and sources. – assess and prioritise. – manage risks. – regularly monitor and review the outcome.
2. Failure to identify and monitor external risks.	The information to be used in decisions about the IT service is incomplete. Poor decision-making due to management strategies and policies on IT Infrastructure being based on unreliable information.	Managing the interaction with external agencies: – identify sources of information on external risk factors; – develop good relationships and interactions with the most relevant external agencies. Maintain a dialogue about planned, changed or new business drivers, demands and constraints; – monitor external sources of risks (e.g. agents on the Internet, join web based communities); – develop a strategy for recording and evaluating external risk factors.
3. Failure to interpret and understand identified external risk factors.	Decisions about IT service are not taken, or are based on unreliable information. Poor decisions about operational IT infrastructure strategies and policies, result in insufficient IT infrastructure in operation and support.	Managing the quality of the knowledge about external risk factors: – use experts to analyse the information gathered in terms of its impact or consequences for the IT infrastructure. – ensure that the conclusions concerning the impact of external risk factors on IT services is based on sound and well articulated arguments.
4. Failure to exchange the knowledge about external factors to other managers.	IT service managers are unaware of external risk factors, resulting in decisions being based on unreliable information.	Manage the exchange of information on external risks with other managers in the organisation. Ensure that: – there is sufficient interaction with other managers (e.g. through committee meetings, intranet, mail etc). – other managers are well informed. – other managers understand external risk factors. – external risk factors are taken into account when making decisions about the organisation's IT infrastructure.

Risk Assessment

5. Users Interaction



5.1 Definition



The concept “use” refers to the different users’ capacities’ to obtain data or information etc. from the system that meets their requirements (both in content and in ease of access)

The guide focuses on three guiding principles, which are to manage:

- Accessibility to the services delivered by the IT Infrastructure;
- Service support and user training
- The communication quality between the user and the IT services

It is necessary to establish a management process to help ensure that both internal and external users can utilise electronic services efficiently and effectively.

5.1.1 Training

Training must address both the needs of the staff that are to use the system, and also those who will be responsible for operating and maintaining it. Within these two broad categories, training should also address the needs of managers whose use of the system may differ from that of their staff; for example they may need to provide electronic authorisations; obtain ad hoc reports to assist with business planning and administration, etc.

Staff should not be trained too early, or there is a risk that they will have forgotten their skills before cutover to the new system takes place; also, staff may leave or transfer to other parts of the organisation during the intervening period. Ideally, staff should be able to work with the new system as soon as they have completed their training. Involving them in system testing and in parallel operation will help to maintain and develop their skills.

Where users are geographically dispersed, training might need to be done on a “cascade” principle. This approach involves one or two of the more apt users from each location being selected for intensive training. On completion they are then given responsibility for training the others in their work area.

It is important to monitor the quality of training as it takes place as it can easily be of limited value. For instance, where packaged systems are procured, the operational requirement often stipulates that the supplier provides training. Although suppliers generally know their product, they cannot be expected to know how it will fit into a particular organisation’s business environment, or have detailed knowledge of the supporting clerical procedures. The project team may need to deliver additional training to address this deficiency.

During training, the students’ views of the system should be canvassed. Even at this late stage it may be possible to identify potential problems or deficiencies, which may be easily cured or rectified.

5.1.2 User groups

User Groups are useful for feeding back to management, and the System Owner in particular, solutions to problems and ideas for developing and enhancing the system, and generally making it more useful to the organisation.

The System Owner should, ideally, chair a user group. It should represent the various business areas covered by the system, generally at junior management level. Its aim is to meet periodically to discuss problems presented by the new system, consider how these may best be resolved, and to discuss ways in which the system might usefully be improved or enhanced. The Group should also provide a forum for exchanging ideas on how to bypass particular problems until a permanent solution can be provided in a future release of the system (temporary solutions of this sort are sometimes referred to as “workarounds”).

A system analyst might also attend meetings to provide a technical perspective on ideas, and to help in formulating system change proposals.

5.2 Objectives

5.2.1 Manage the user accessibility to the IT services

Aim: to ensure that internal and external users are able to access IT services.

In the description of activity area “In Operation” it was stated that the IT organisation delivers IT services to different kind of users. This is only one side of the delivery. The other side of the delivery should be seen from a user perspective. The services delivered have to be easy to access to ensure the use of services. The competence needed, and technical platform for the solution will affect the accessibility for the users. Perceived usefulness is linked to whether the users will gain rewards form their use of an information system and therefore the attitudes they have toward using the systems. If their attitudes are favourable, they are likely to use the system more frequently and more effectively. If their attitudes are unfavourable, however, they are not likely to use the system.

5.2.2 Manage user support and training.

Aim: to ensure internal and external users receive an adequate level of service support and can use the service effective and efficient.

An IT-service requires a support function to resolve problems in the use of the system. This is often provided by means of locally based specialists (sometimes called “Local Service Administrators”) and/or a central service support function (sometimes called a “Help Desk” or a “service Desk”). In both cases the service support function may need to refer difficult problems to technical support technicians for resolution (sometimes referred to as a “Problem Management Function”).

The help desk/technical support function has two primary responsibilities. First, assist end users to employ end-user hardware and software, such as microcomputers, spreadsheet packages, database management packages, and local area networks. Second, it provides technical support for production systems by assisting with problem resolution. There are two important requirements for the help desk/Technical support to function effective and efficient. First, competent and trustworthy personnel are essential.

Second, a problem management system that provides inventory, logging and reporting capabilities must be available to support the activities of the area. When users report some type of difficulty or request some advice, this should be logged into a system. Support personnel then can analyse the problems and use this information to improve the service delivery.

It will be necessary to implement a user-training programme to provide users with the practical skills necessary to use the service efficiently and effectively. Training could be delivered through a conventional training course, or by using a computer-based training module.

Another important issue is that system manuals are continuously updated. If manuals are paper based, this requires distribution routines to ensure updating to all users. User manuals are often built in to new systems, which help the distribution and updating work. On-line help facilities are also an easy way for the user to solve problems fast. The time it takes from a problem occurs until it is solved by the helpdesk is always important for the users. That the problem solving is fast helps in ensuring continuous use of the services.

The risks of failing to ensure that users are capable of using an IT-service are a high level of user errors; service facilities being under-utilised through ignorance and lack of understanding; and users becoming disillusioned with the service and avoiding its use.

Management should therefore promote user training and development activities.

5.2.3 Manage the communication quality

Aim: to ensure that the dialogue between users and IT service has the right communication quality

As for perceived usefulness, perceived ease of use shapes the users' attitudes toward a system. If their attitudes are favourable they are likely to use the system more frequently and more effectively. If not they are unlikely to use the system. There are some factors to be considered:

- Users perceive that it is easy for them to learn to operate the system
- Users perceive that it is easy for them to get the system to do what they want
- Users perceive that they can interact with the system in a clear and understandable way
- The interaction is flexible, the system is easy to use and it is easy to become skilful with the system.

5.3 Risk Assessment

Manage the user accessibility to the IT services

Aim: to ensure that internal and external users are able to access IT Infrastructure services.

Risk	Impact	Risk management strategy
1. Top management fail to identify the risk of a poor user interface with IT services.	A poor user interface with the service resulting in: – an under-utilised service (and wasted investment in its development). – low productivity through difficulty and problems in service use. – unreliable data and poor decision-making. – disillusioned staff and low morale.	Managing the organising of the risk area: – establish the context and awareness of IT-service users. – identify the risks and keep an up-dated list of risks and sources concerning IT-service users. – analyse the risks and sources. – assess and prioritise. – treat risk. – monitor and review. – set standards for user interface design. – set standards for validating data captured from users, and data transferred to other systems (e.g. control totals, inter-system reconciliation's/run-to-run totals).
2. Failure to provide user-focused, accessible IT services.	The service is under-used through failure to thoroughly understand what it is to achieve. In particular: a) the services fails to provide the required functionality; b) the service is not available for use at convenient times; c) the preferred means of access are not provided; d) the service is not accessible over a sufficiently wide geographical area; e) the service is expensive to access; f) the service is unfriendly and difficult to use; g) the service cannot be used by foreign language speakers; h) no provision is made for face-to-face contact with end-users.	A comprehensive user requirements survey to establish: a) who the service users actually are; b) why they will need to use the service and what they expect to receive from it; c) the times when, and places where, users are likely to want to use the service; d) whether or not to charge users for access (e.g. by using a free-phone numbers); e) what access channels to offer (e.g. Internet, call-centre, digital television, local offices, letter post); f) helpful and intuitive designs for: – screen layouts and navigation (for terminal access); – voice menus and navigation (for call-centre access); g) requirements for on-line help screens and an enquiry desk; h) information security requirements. For example: – the sensitivity of the data to be processed; – whether electronic signature will be required for authentication and legal purposes; i) whether to cater for foreign language needs, and which languages to include; j) whether accessibility would be improved by using private sector IT infrastructure (e.g. siting service access points in supermarkets); k) what physical contact to maintain with users (office, post).
3. Electronic Service Delivery (ESD) fails to deliver significant improvements in service quality.	Wasted investment. Public dissatisfaction and adverse publicity. Inefficient and under-used services.	Electronic Service Delivery (ESD) creates new opportunities, capabilities and expectations, but their exploitation is not just a matter of automating existing systems together with their inefficiencies. It means taking a fresh look at the business and its processes. Business process re-engineering should be carried out as part of the process of defining (and maintaining) a corporate information system strategy (see paper 1).

Risk	Impact	Risk management strategy
4. A major design failure is revealed following ESD live implementation.	Delay and wasted investment. Adverse publicity. Need to revert to or perpetuate inefficient legacy systems. Adverse impact on staff morale. Embarrassment due to inability to meet political and legislative deadlines.	Major failure can be due to concept and/or technical design. ESD has in some cases been a victim of its own success and has as a result failed to satisfy demand (i.e. capacity problems). There may also be unforeseen problems in its use; for example due a poorly designed user interface or to the initial justification for the service changing or disappearing. The software, hardware and communications may also fail to operate as expected. These types of problems can to some extent be addressed by testing, but the real test of end-to-end operation only comes in live use. Developing a pilot system enables the ESD concept and its technical operation to be tested in live use with limited and affordable risk. A 'phased' approach to implementation enables problems to be addressed as they arise, with the possibility of halting implementation where serious problems are encountered. Both these implementation strategies help to avoid expensive, high profile disasters. However, in the case of pilot projects *it is important to ensure that the pilot is capable of being scaled up to its eventual size – this should not be taken fore-granted*. Furthermore phased implementation takes longer than 'big bang', so a balance has to be struck on what is acceptable.
5. ESD compares unfavourably with comparable developments elsewhere.	Failure to optimise opportunities and savings from ESD. Unfavourable public comment. Political embarrassment.	Build on the success of others and adopt good practices that have been successful elsewhere. Organisations should benchmark their achievements against their peers, both at home and abroad. Where it is difficult to compare at the system level, it may possible instead to focus on overall strategy, and achievement against it.

Manage the user support and training.

Aim: ***to ensure internal and external users receive an adequate level of service support and can use the service effective and efficient***

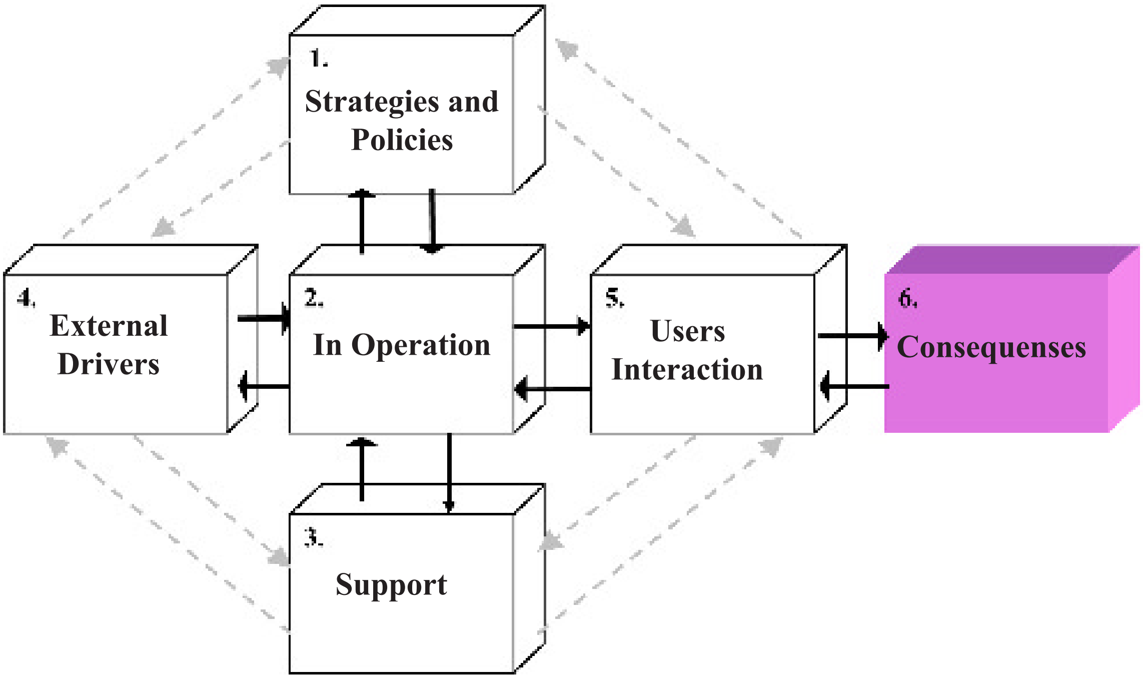
Risk	Impact	Risk management strategy
1. Users are unable to use a service efficiently and effectively due to lack of, or inadequate training.	Low productivity/poor standard of service. Users avoid using the service, resulting in wasted investment. Poor value for money in achieving corporate goals. Political embarrassment.	Manage users skills and access to the IT-service: – Top Manager should give a statement that it is the Business Unit Managers responsibility to ensure users skills and support then using IT-service. – Identify different kinds of user categories and develop special skills strategy for each group. – Follow up and evaluate the skill demands for the IT-service user. – Follow up and evaluate user skills, behaviour and their problems about the technical dialogue with IT-service. – Follow up, evaluate and adjust user education and training programs. – Follow up, evaluate and give advice concerning users different technical environment. – Follow up, evaluate and adjust the user support.
2. Failure to ensure understanding.	Ignorance can result in a range of problems, including: a) the service being under-used, through failure to understand what it can do, or how it should be used to satisfy a particular need; b) high error rates and re-working due to incorrect use; c) missed opportunities through failure by business managers to exploit the service fully due to lack of understanding; d) service malfunctions and failures due to incorrect operation by support staff; e) unresponsive service, malfunction and failure due to poor technical maintenance by support staff.	Define a training and awareness policy and strategy designed to address personnel needs. Issues to address in formulating the policy and strategy include: a) a management structure to oversee training; b) a training needs analysis covering: internal end-users; technical support staff; middle and senior managers; c) quality control standards and procedures covering training material and training delivery; d) training and case study material; e) linking planned business and system changes to the training needs assessment; f) maintaining individual training records; g) maintaining individual training needs assessments as part of staff appraisal; h) on-line help facilities, and a help desk; i) user and technical focus groups; j) publicity aimed at keeping all personnel aware of service issues and future plans; k) development of user manuals; l) development of technical support manuals and operating procedures. m) Linked to the ‘user requirements survey’ at 1. above, the needs of external users (e.g. citizens and trading partners) who access the service also need to be addressed. Issues to consider include: n) publicising the service externally and explaining, for example, what it can offer, how and when it can be accessed, and from where help can be obtained; o) designing on-line help screens (for terminal accessed services) and voice menu options (for call centre services); p) Provision of printed guidance on demand.

Manage the communication quality

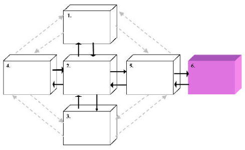
Aim: ***to ensure that the dialogue between users and IT service has the right communication quality.***

Risk	Impact	Risk management strategy
1. That the interaction between user and IT-service will not meet communication quality requirements.	There will be users spreading data with lacking quality into the system leading to negative consequences for other actors. There will be users mistrusting the IT-service results.	Managing the communication quality between user and IT-service: – Follow up and evaluate the interactions between user and IT-service to get knowledge about problems in the interactions from both sides. – Follow up and evaluate user trusts in the IT-service from a business point of view. – Follow up and evaluate how user are working with the IT-service concerning giving data.

6. Consequences from IT Services on society, citizens and organisations



6.1 Definition



This section of the guide provides advice on the audit issues surrounding the exploitation of IT services to deliver government services electronically. It focuses on the consequences on society, citizens and organisations, and is based on five guiding principles. These are the need to manage:

- information
- change
- manage information security
- the working environment
- the consequences on citizens, society and organisations

6.2 Objectives

6.2.1 Manage information

Aim: to ensure that organisations recognise that information is a vital resource and manage it securely and to best effect.

The transition from paper-based to electronic business is often accompanied by a failure to manage data and electronic business records effectively, or at all.

Management should therefore take steps to ensure that:

- different business systems can use and exchange corporate data in an unproblem atic manner;
- electronic business records can be traced, recovered and read, perhaps years after their creation;
- should the need arise, it is possible to demonstrate that important business ecords are reliable, perhaps to the extent of their being used as evidence in a court of law.

6.2.2 Manage change

Aim: to ensure that changes to electronic services are implemented in an unproblematic manner

Changes to electronic services can range from minor technical changes to major enhancements to business applications.

Many electronic service problems and breakdowns can be attributed to failure to manage change effectively. At a higher level, service changes need to be managed strategically to ensure that they deliver the correct functionality, take place at the right time, and meet cost targets for their delivery and on-going maintenance. But all levels of changes bring with them the risk of unforeseen problems occurring.

Management should therefore ensure that:

- changes to electronic services are justified;
- there is an effective management structure for managing change;
- there are effective change management procedures.

6.2.3 Manage information security

Aim: to protect the confidentiality, integrity and availability for use of corporate data in a cost-effective manner, and to inspire confidence within the user community.

Information security addresses the need to protect the integrity and confidentiality of corporate data, and its availability for use. A further heading that is particularly important in electronic business is 'authentication', which concerns the need to be sure:

- about the true identity of the individuals or organisations who are participating in an electronic transaction, and be able to link them to the transaction;
- that the information exchanged between participants has not be tampered with.

The public will not use electronic services if they are not confident that their personal information is protected from disclosure and abuse. Security failures can also have dramatic impacts on business management; for example, as organisations become increasingly dependent on electronic services, service failure (availability) can easily bring the business to a standstill.

Management should therefore ensure that:

- information security policy, appropriate to their business, is developed and maintained;
- there is a management structure for implementing, monitoring and maintaining the information security policy, and for investigating failures.

6.2.4 Manage the working environment

Aim: to promote good productivity and morale by providing a safe and congenial working environment.

"Ergonomics" is the application of biological science to study the relation between workers and their environments. The growth and development of IT infrastructure is such that a diminishing number of those employed in an 'office' environment are able to work effectively without it. However, good productivity and morale in the workplace do not only rely on effective training and user support, but on a safe and congenial working environment.

IT brings with it health and safety risks. This need to be managed to avoid industrial injury and ill health among users, and in some countries there is also a legal obligation to manage health and safety in the workplace.

Increasingly personnel are being required to work in the home rather than in a traditional office environment. "Teleworking" can offer significant advantages to both employer and employee, but again it brings with it risks (e.g. health and safety issues, and security) that need to be carefully considered. Management therefore needs to be aware of the ergonomic issues that stem from their use of IT in the workplace - be it at home or in the office - and manage the legal and social obligations that arise.

6.2.5 Manage consequences on citizens, society and organisations

Aim: to ensure focus and awareness of both intended and unintended consequences from development and changes on Electronic Service Delivery.

Developing ESD in public administration claims conscious focus and awareness of what consequences it might have on citizens or organisations affected by the changes effectuated. The transition from manual delivery of services to electronic delivery can lead to both fortunate and unfortunate spreading consequences that need to be managed in order to ensure credibility. In some countries, there is increasingly focus on management liability, forcing managers to take precarious action. Poor risk management leading to severe consequences on citizens is an obvious reason to replace one or several managers.

On the other hand, consequences could lead to opportunities. Introducing Electronic Service Delivery that meets end-users demands in a successful way could lead to social increase of IT-skills and knowledge. This opportunity needs to be exploited.

6.3 Risk Assessment

Manage information

Aim: ***to ensure that organisations recognise that information is a vital resource and manage it securely and to best effect.***

Risk	Impact	Risk management strategy
1. Failure to manage information effectively.	a) Electronic inter-working ("joined up services") cannot be exploited due to: • ignorance about: – where and when the data to be exchanged was obtained; – what the data represents; – who can legitimately/legally access the data, and uses that they can put it to; • incompatible data formats. b) Loss of accountability through inability to: trace, recover or read electronic business records; demonstrate the authenticity of electronic business records.	Implement data management. Management should: a) develop policy and standards on the acquisition and management of data, and on the technical formats for data items; b) implement a management structure to control and monitor data policy and standards; c) maintain metadata (i.e. "data about the data"); d) implement information security policy to define legitimate/legal data access and use; e) ensure conformance to the requirements of data protection legislation; f) collaborate with those responsible for system recovery and business continuity planning to ensure that data is protected from corruption and destruction. Implement electronic records management. Management should: g) develop policy and standards for capturing, naming and filing corporate records in electronic form to facilitate their recovery, perhaps after many years in storage; h) develop and implement technical standards for the format in which electronic records are to be stored. Ensure reliable migration when changes to storage standards take place; i) implement information security policy on record access and use; j) ensure conformance to the requirements of data protection legislation; j) collaborate with those responsible for system recovery and business continuity planning.

Manage change

Aim: to ensure that changes to electronic services are implemented in an unproblematic manner.

Risk	Impact	Risk management strategy
1. Ineffective change management.	Badly managed change can introduce problems with the functionality and responsiveness of an electronic service, and high error and failure rates. These in turn can result in: a) wasted investment through failure to satisfy user requirements properly; b) missed business opportunities through inability to respond quickly and effectively to changing business needs and objectives; c) high operating costs due to the need for system recovery, re-working and lost production; d) dissatisfaction among the workforce with unreliable systems; e) public complaint and political embarrassment resulting from service malfunction and/or failure to provide an adequate level of service.	There should be policy and procedures for managing service changes. The main issues to consider are to define policy and procedures, and to implement a management structure to control their operation. Lower level issues include: a) the categorisation of different classes of change (e.g. from routine, through significant to major changes), and the procedures that will apply to the management of each category; b) the requirements for justifying major changes and for setting benchmarks against which to assess the outcomes; c) how different change categories are to be authorised and funded; d) when to apply project and programme management (links to Domain 1 paper); e) the approach to identifying and specifying user and technical requirements, and for identifying the service components to be changed; f) risk assessment procedures, including links to other IT infrastructure management processes for identifying how a change will impact on, for example, network capacity and business continuity planning. The impact on training plans may also need to be assessed; g) quality assurance procedures (e.g. inspections of documents and designs; technical testing of modules, systems and services; load and stress testing including network capacity; end-user acceptance testing); h) building and implementing service releases; i) developing back-out plans; j) the need for additional awareness and training; k) post-implementation review on the outcome.

Manage information security

Aim: ***to protect the confidentiality, integrity and availability for use of corporate data in a cost-effective manner, and to inspire confidence within the user community***

Risk	Impact	Risk management strategy
1. Ineffective information security.	Ineffective information security can have dramatic impacts on business operations. It can also have far wider reaching impacts on the public's perception of electronic services (particularly where fraud is involved), resulting in a general loss of confidence. More specific impacts include: a) unauthorised disclosure of sensitive business and/or personal information, which could result in further damaging impacts on the business and on individuals); b) unauthorised manipulation of information, which could in turn result in such impacts as fraud and corruption of personal data (e.g. due to software error or virus attack); c) loss of service availability, for example due to inadequate resilience against breakdowns or lack of effective continuity plans in the event of prolonged failure; d) physical damage to IT components due to inadequate physical and environmental security. Failure to maintain adequate information security may also result in legal impacts where there is failure to comply with contractual, statutory (e.g. data protection) or regulatory requirements.	An information security policy should be defined, and there should be a management structure for implementing the policy, and for controlling and monitoring its operation. In general terms information security policy should: a) provide a general explanation of information security, its importance to the business, and a statement of top management commitment; b) describe the main roles and responsibilities for implementing, operating and monitoring the effectiveness of security policy, and for complying with relevant legislation; c) the organisation's approach to, and requirements for undertaking security risk assessments, and the provision of expert help and advice; d) what is to be achieved with regard to: • classifying and protecting information in terms of its sensitivity and criticality; • controlling access to premises, information systems, and information; • checking the backgrounds of new personnel, including consultants and temporary staff; • controlling unauthorised software; • virus prevention, detection and response; • authenticating individuals in on-line transactions, and the integrity of information exchanged; • the use of data encryption techniques; • reporting and responding to security incidents; • business continuity planning.

Manage the working environment

Aim:* *to promote good productivity and morale by providing a safe and congenial working environment

Risk	Impact	Risk management strategy
1. Failure to manage the working environment – health and safety.	a. Sick absence. b. Claims for compensation. c. Prosecution for contravention of regulations. d. Low productivity. e. Poor morale.	a. Define management policy on the ergonomics raised by IT in the workplace. b. Appoint a senior manager to be responsibility for IT-related ergonomics. c. Allocate an annual budget for ergonomic projects. d. Provide expert source of advice on IT-related ergonomics. e. Undertake periodic expert inspections of the workplace to include: ● fire hazards and fire precautions. ● dust and cleanliness. ● natural and electric lighting, ventilation, heating and humidity. ● noise and vibration. ● standards of electrical insulation (including static electricity). ● adequate spacing of equipment and furniture. ● appropriate furniture for IT users (e.g. load-bearing, user posture, foot and wrist rests, safety of cabling; safe storage of media, screen glare). ● obstructions, such as those posed by IT equipment, patch panels, electrical and communications cabling, plugs and sockets. f. Define policy on rest breaks for those making intensive use of terminals. g. Maintain statistics on health and safety problems related to the use of IT. h. Periodic meetings of a representative committee. i. Regular written reports to top management on the outcome of workplace inspections, statistics, projects and on any further recommendations.
2. Failure to manage the working environment – teleworking.	a. Prosecution/fines for infringement of legal requirements. b. Increased operating costs. c. IT security failures. d. Low productivity. e. Outputs of unsatisfactory quality.	Develop a strategy for teleworking. Issue to consider should include: a. environmental requirements for office accommodation in the home (e.g. adequate space, separation from home distractions, such as noise, cabling, and the ergonomic factors listed in table 3a); b. office technology requirements (separating office communication links from domestic circuits; types of communications links, telephones, fax, printers, scanners, PCs); c. physical security (e.g. adequate lockable doors and windows; facilities for safe storage of paper documents and other storage media; intruder detection and alarm; physical locks on PC; removable hard disc); d. logical security (PC security software; smart card/biometric reader; firewall; remote data backup and recovery from backup); e. external access to an on-line help desk; local hardware and software maintenance support; f. secure access to corporate systems and services; remote conferencing facilities. Consider legal requirements. For example: a. application of health and safety at work regulations to the home;

Risk	Impact	Risk management strategy
		b. the need for adequate insurance (e.g. value of the equipment; public liability insurance). c. legal restrictions on work from domestic premises; planning permission on building extensions. d. possible impact on taxation (e.g. local property tax rates may increase when domestic premises are used for business; the tax on house sale may alter if viewed as an ‘office’). Undertake individual site inspections and risk assessments against the strategy to establish the suitability of the premises and the overall requirements. Define and monitor benchmarks for measuring the success of teleworking. Implement teleworking via a pilot project, and then in a phased manner to gain experience.
3. Skills redundancy.	Unemployment. Damage to staff morale.	Part of the business case for on-line services is that it will further automate the work process. Its development cost will be funded in part by the gradual disappearance of paper-handling jobs, and the need for many fewer people in these types of tasks. Other jobs will become much more ‘IT-assisted’, and older people in particular may find it difficult to accommodate the change. Much more emphasis will need to be placed on continual professional development programmes, than on formal qualifications that are likely to become obsolete more quickly. Other programmes will need to be put in place to re-train personnel whose skills become redundant.

Manage consequences on citizens, society and organisations

Aim: ***to ensure focus and awareness of both intended and unintended consequences from development and changes on Electronic Service Delivery.***

Risk	Impact	Risk management strategy
1. Citizens are unaware of ESD (Electronic Service Delivery) and its advantages.	New services are underused. Wasted investment. Failure to achieve efficiency gains. Government strategic objectives (e.g. on-line learning, on-line medical advice, freedom of information) are not achieved.	It is essential to market new on-line services in order to make people aware of them and ensure they are successfully taken up, and to realise the benefits they can provide. Marketing must communicate the existence of new services and also issues that concern customers, such as security, confirmation of transactions, and how to use the service. Providing incentives also helps, particularly where new systems run in parallel with conventional paper-based methods. In the UK the taxation authority offers a cash discount for electronically submitted tax returns. Organisations may also commit to processing electronic transactions more quickly than those submitted on paper.
2. Citizens lack the ability to exploit ESD.	ESD is under-used. Wasted investment. Failure to achieve efficiency gains. Government strategic objectives (e.g. on-line learning, on-line medical advice, freedom of information) are not achieved.	Bringing ESD to the citizen can be achieved through providing awareness and incentives, but there are many in society who are not confident enough, or able to use it through lack of education. Special programmes will need to be developed to target sectors of society, especially the elderly, unemployed, disabled and the poor. Government staff must also be educated in order that they may use ESD effectively in delivering better quality services to the public.
3. Social exclusion.	Citizens are unfairly excluded from access to ESD; for example, through: - physical disability - language barriers - geographical isolation - social deprivation - lack of education - failure to re-educate. Under-used services. Possible legal implications (e.g. through 'equal rights' legislation).	Online services should be easy to use and accessible to all. This includes providing services for minority language groups and those with disability or limited mobility. A choice of electronic delivery channels should also be offered, but traditional delivery channels should be preserved in the medium term to ensure social inclusion. The overall commitment should be to make it easier for everyone to get access to services, whether individually or through community facilities. Digital TV and mobile phones will become increasingly important as a means of accessing the Internet, but the telephone will remain a preferred means of contact for many. Call centres should give their staff access to information networks that will enable them to provide better service. Better information systems should support those who have face-to-face contact with the public. Working methods will change. Greater emphasis will be placed on home working rather than travelling to the office every day. This will involve changes to people's homes, to their home insurance and security. Cultural changes will also be needed to enable people to work effectively without face-to-face contact with colleagues.
4. Information cannot be readily exchanged within and between different public sector organisations.	IT infrastructure fails to support improvements in policy-making, ESD and more efficient working.	Information is a valuable and vital resource. Implementing IT strategy requires organisations to adopt coherent and compatible information policies. A ***"System Interoperability Framework"*** should be established, its aim being to set out the technical policies and standards for achieving interoperable and coherent information systems across the public sector. Training, best practice guidance, toolkits and centrally agreed data schemas should support it, and its use should be mandatory.

Risk	Impact	Risk management strategy
5. The ‘System Interoperability Framework’ is, or becomes, ineffective.	Information cannot be readily exchanged within and between different public sector organisations.	It is essential to ensure that the Framework remains up to date, aligned to the requirements of all stakeholders, and is able to embrace the potential of new technology and market developments. It should therefore be managed as an ongoing activity and be supported by robust processes and clearly defined accountabilities. Accountabilities should include the roles and responsibilities of key stakeholders, and of committees, management and working groups.
6. ESD suffers from an unacceptable level of system errors and service failures.	High operating costs. Unresponsive systems. Inadequate/ineffective information security. Poor morale among support staff due to the need for constant "fire fighting" and numerous customer complaints. Public dissatisfaction, frustration and adverse publicity. Political embarrassment. Possible legal implications (e.g. on data protection issues, freedom of information).	The technology should be fast, robust and well managed. Successful front-line ESD applications also depend on robust and reliable back-office capability. Suitable national and international standards and codes of practice covering the development and operation of ESD systems should be considered for adoption, and personnel trained in their use. For example: *TickIT ((British Standards Institution)* – Guide to software quality system construction and certification; *British Standard 15000* – IT Service Management; *British Standard 7799* – Information Security Management (to become ISO 17999 in 2001); *PD0005 (British Standards Institution)* – Code of Practice for IT Service management; *PD5000 ((British Standards Institution)* – Electronic documents and e-commerce transactions as legally admissible evidence.
7. ESD compares unfavourably with comparable developments elsewhere.	Failure to optimise opportunities and savings from ESD. Unfavourable public comment. Political embarrassment.	Build on the success of others and adopt good practices that have been successful elsewhere. Organisations should benchmark their achievements against their peers, both at home and abroad. Where it is difficult to compare like with like at the system level, it may possible instead to focus on overall strategy, and achievement against it.