Annex 1:

IT services management overview

Strategic planning for information systems

The provision of IT services requires investment in people, technology and environment. IT infrastructure can rarely be bought off-the-shelf and brought into use in quite the same was as a PC software package. In generally requires significant investment and lead-time, and in common with other forms of major investment it should be carefully planned to ensure a successful outcome.

Strategic planning involves taking a long-term view of how a business is to develop, and a comprehensive view of all the significant factors. This will involve:

- understanding business aims and objectives
- establishing customer requirements
- outlining the required IT services
- agreeing policies and plans for developing and implementing the required services, and examining alternatives and corresponding risks in order to identify the best option
- identifying the financial and manpower resources that will be necessary to implement the strategy
- managing, reviewing an evolving the strategy in the face of changing business needs and constraints. Business aims and objectives rarely stand still for long, whilst technological developments continue to offer new business opportunities and solutions.

Strategic planning often crosses the boundaries between different organisations – this is particularly true in government - and these principles must be extended to address co-operative and collaborative working.

Business needs constantly change, whilst developments in IT continually create new business opportunities and better ways of doing things. Strategic planning for IT should therefore be regarded as an on-going activity or "cycle" of events. The strategic planning cycle is described in more detail at Activity Area 1.

Managing large-scale programmes of change

Implementing a strategic plan often runs over a considerable period of time and involves numerous separate "projects", each of which is designed to deliver a component part of the overall plan. The problem that faces top management is that of co-ordinating the activities of a number of projects, some of which may have competing demands on limited resources, and utilising their deliverables to move the organisation along the path set out in the strategic plan. This over-arching management activity, described as "programme management", is illustrated in figure 1.

Programme Management is defined as the selection and planning of a portfolio of projects to achieve a set of business objectives; and the efficient execution of these projects within a controlled environment such that they realise maximum benefits for the resulting business operation.

Failure to manage large-scale programmes of change effectively can be dire, involving:

- **cost over-runs**, resulting from inadequate control and co-ordination of activities; failure to resolve conflicts and priorities; failure to align individual projects to one another, to the current business, to the method of operating and to the future business;
- **lost benefits and opportunities**, due to failure to clearly assign the responsibility for realising them or through lack of common understanding on how they are to be realised;
- **loss of direction**, if no clear vision is expressed at the outset; if the vision and the plan to achieve it are not constantly monitored and revised in response to developments, and communicated to those who bring it about and are affected by it; if individual projects are pursued at the expense of the broader programme;
- **under-achievement by the current business**, if the incorporation of change and the delivery of benefits are not effectively planned and managed;
- **failure to identify and contain the unexpected** through failure to analyse and manage risks effectively, or at all.

The programme management environment

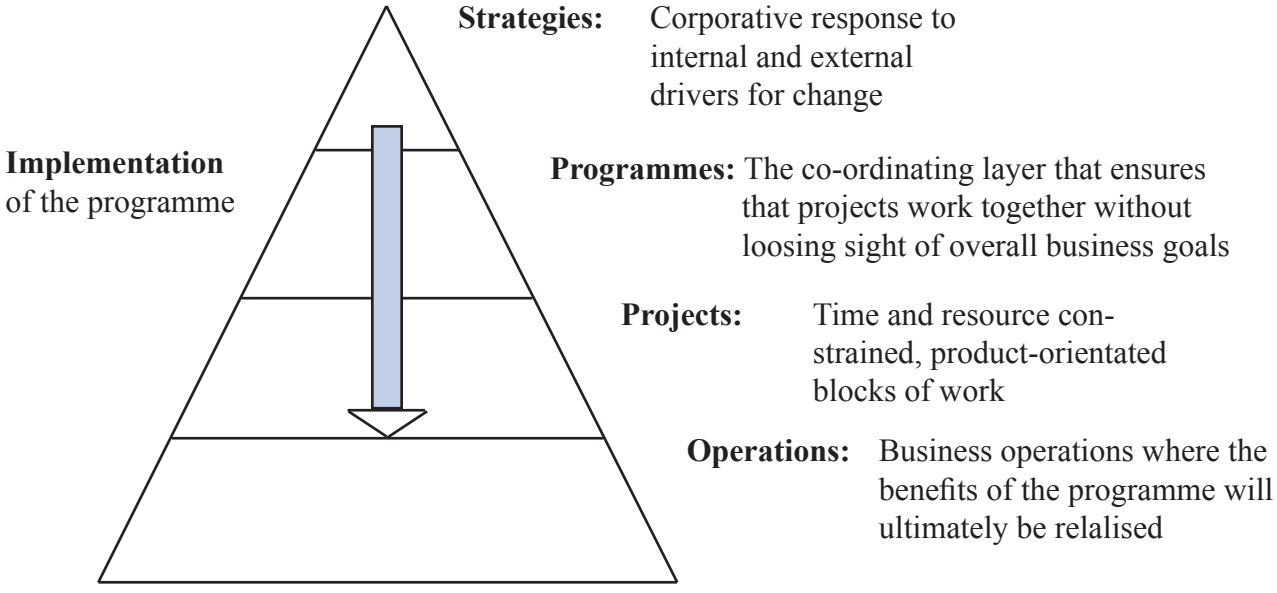

Figure. 1

IT infrastructure planning

The requirements for new or revised IT infrastructure arise from the formulation or review of IS Strategy and the identification and definition of one or more programmes, as outlined above. In most cases the IS Strategy will have been developed in the context of considerable existing investment in IT infrastructure, and much of the planning process will be devoted to developing a path along which to migrate from what currently exists to what is planned.

Planning and designing an organisation's IT infrastructure has to take account of numerous factors. These include new requirements that emerge from the definition of programmes and from existing IT infrastructure commitments, whilst the constraints imposed by the technical policies and standards laid down in the IS Strategy must also be taken into account. IT infrastructure planning is therefore a highly iterative process; it often takes several months to define:

- the user communities
- the IT:
- services required
- capabilities to be developed
- components to be procured
- the IT infrastructure costs to be borne by programmes
- implementation priorities and time-scales
- dependencies and risks
- people issues (resource management, skills acquisition, training needs, etc.)

Once these issues have been decided, the IT infrastructure framework can be defined. This will include models of the IT capabilities required to support the information systems developed or required by the development programmes - sometimes described as the "*goal architectures*" of the IT infrastructure.

Migration to the goal architectures occurs through the successful implementation of one or more IT infrastructure "projects". These move the operational capability of the business progressively from its current to its future state through a series of transitional steps.

IT project management

A project is an intense, focused activity that is driven by the product(s) that it is to deliver.

IT infrastructure projects in particular require careful management for several reasons:

- they often span organisational divides. This involves the co-operation of individuals from different parts of the line management structure, and sometimes from different organisations
- project staff brings different skills to the project, have different backgrounds and are subject to different pressure from their non-project work (only part of their time may be assigned to a project). They may also have different expectations about how they should be managed and their work assessed and rewarded. But it is essential that they work productively together during the life of the project

- projects tend to have peaks and troughs of activity (e.g. whilst awaiting top management decisions or the delivery of components), and requirements often change during the life of the project

Experience shows that managing IT projects is particularly fraught with difficulties, and that part of the reason for this is the view that IT personnel are also capable of managing IT projects. This is not necessarily the case; project management requires skills that are not necessarily IT-related, include the ability to:

- manage and lead a project team
- plan, and take decisions
- communicate

A project manager therefore needs to be carefully selected and given adequate authority to underpin responsibility.

The adoption of a standard approach to project management also provides an aid (but not a solution) to success. A method provides a framework, which, through training, helps to ensure a common understanding of how a project will be planned, managed and controlled. There are numerous approaches to project management. What is important is that the method is understood and does not become an end in itself - it should be used as a tool for:

- providing senior managers with a common approach to project management
- promoting conscious and effective senior management control
- empowering the Project Manager (responsibility with authority)
- controlling the activities of external contractors by providing a standard to which they too must adhere
- promoting the control of quality, change and risk
- helping to ensure that the right people make the right decisions at the right time

Implementing IT services

Introduction

Implementing a new or updated IT service comprises a number of activities, the successful completion of which should result in an operational service. These activities form the bridge between a development project and an operational IT service. Careful attention to detail during this stage of its life can pay dividends in customers' on-going perceptions of the new service.

Implementation issues

Service implementation can involve numerous activities, and requires careful planning. Activities that will need to be considered include:

- building and testing the new service in its operational environment
- migrating any existing data from the existing to the new platform

- allocating roles and responsibilities and transferring operational responsibility to the service management team;
- creating operational procedures, and training both business users and technical support staff in them;
- finalising support contracts and agreements for the new service;
- developing and testing business continuity plans

It is not just a matter of deciding who is to do what; timing is also important. Implementing a new system at certain periods may be inadvisable because. For example, during holiday periods, key staff may be unavailable; at financial year-end, the accounts staff will not wish to take on the risk of service failure; or coincident with other major business changes. And training users too soon means that their new-found skills may have been forgotten by the time the new service goes into operation.

Service cut-over

"Cut-over" is the process of transferring the live workload from an existing to a new service. The most obvious way of achieving this is simply to transfer operations by "the throw of a switch", a strategy sometimes referred to as "big bang". However, while big bang may be an acceptable strategy for implementing centralised, non-critical applications, it may be unsuitable in other situations. ***The risks need to be assessed***.

The importance of reviewing projects

Introduction

Business managers need to be sure that their investment in information systems and services represents the most effective choice for the organisation, both now and in the future. Information systems and their supporting information technology should:

- be deployed to support the organisation's business needs and objectives in full
- represent the best value for money in doing so
- meet the demands of changing business needs

Reviews provide the opportunity to assess the effectiveness of IS/IT and determine what actions need to be taken to make improvements. Effectiveness is monitored by checking the alignment of IS/IT to business objectives, measuring actual performance against that predicted in the business case(s) and making recommendations for action to maximise that performance. Reviews allow the organisation to respond quickly and appropriately to internal and external pressures, and learn valuable lessons for the future.

The range of reviews undertaken, their scope and frequency will depend on what the organisation needs to know. Some reviews are part of the strategic planning process, taking place at planned intervals; others may be triggered at specified milestones, such as a post implementation review of a new system or a service review at a contractual breakpoint.

The benefits of reviewing IS/IT projects

All IS/IT projects should positively contribute towards the achievement of an organisation's business objectives, represent best value for money in doing so, and meet the demands of changing business needs (although some projects will only do so indirectly). Reviews contribute to the following:

- ensuring that IS/IT aligns fully with corporate objectives
- allowing the organisation to recognise and respond quickly to and appropriately to internal and external pressures
- ensuring that benefits are managed and maximised
- allowing costs and risks to be tracked, managed and minimised
- allowing the organisation to decide whether its IS provision represents value for money
- allowing useful generic lessons to be learned for future projects.

Different types of project review

Reviews of IS/IT projects take place as part of the overall strategy cycle. They are concerned primarily with implementation and management of IS/IT investment to ensure the effectiveness of IS-enabled change.

There are two types of review to consider which, together, make up "post project evaluation".

Project Evaluation Review (PER)

A PER concentrates on a project's success in meeting its objectives. It examines how well the project was managed, and how ell the deliverables (e.g. an information system, training, user manual) meet the agreed specification.

A PER should be conducted should be conducted at, or shortly after, project closure whilst the Project Manager and key participants are still available and their recollection of events is clear. The review should determine the efficiency and economy of the project (*management method, organisation, development method, procurement, etc.*) and the quality, cost and timely delivery of business products against the forecast in the business case. Useful generic lessons will emerge which should be fed back into the organisation's project management processes and procedures for the benefits of future projects.

Post Implementation Review (PIR)

A PIR is much broader in scope, and may be undertaken on a number of occasions during the life of a system or service.

A PIR concentrates on the effectiveness of the business change enabled by the project - at a point in time - and measures the extent to which the objectives of the business case have been met. It aims to make recommendations for any changes that are necessary to optimise benefits, costs and risks.

Service management

Introduction

Once services are acquired, the next step is to ensure that they continue to provide the best value for money. This will greatly depend on the robustness of the management processes adopted, and the effectiveness of co-operation between the service provider and both customers and third part suppliers.

IT service management policy

A policy should be defined to scope the requirements and objectives to be achieved by service management. There are many views on the exact scope of service management. Those described in this section represent the consensus view of the industry in the UK.

A policy should also set out the approach to risk assessment and risk management, and the approach to take to monitor and continuously improve the quality of service management. This should highlight the key roles and responsibilities required within the service management team, together with the use of third party suppliers.

The link back to business strategy

This is the point in fig. 1 where the loop is completed – where the operation of "what you've got" delivers the business benefits that meet the aims and objectives in the corporate plan.

The process of formulating IT services begins at a high level, when developing and interpreting the organisation's business strategy. What services to offer is a business decision, whilst the form in which they are to be delivered (e.g. using e-business techniques) is partly a function of business and of IS strategies. How to deliver the services is partly a function of implementing the business and IS strategies, and partly of the acquisition strategy (e.g. service delivery may be outsourced). The delivery details may be left to the service provider under contract.

IT service management processes

Service management comprises a number of closely related processes aimed at providing the best possible services to meet an organisation's business needs within agreed resource levels; i.e. service that is professional, effective and has minimal risk. These processes can be grouped, as follows:

- ***Service design & management*** processes form the largest group, and are generally proactive. They comprise processes aimed at managing:
- service levels
- service capacity
- service availability
- service costs (including cost recovery)
- information security
- service availability and continuity
- service reporting.

- ***Supplier processes*** are those that involve the interface between the supplier and the customer. The supplier may be the in-house service team and the customer the organisation's business-based staff. But increasingly the supplier is a third party providing services to the in-house group under a service-based contract. These processes comprise managing:
- customer relations
- suppliers.
- ***Resolution processes*** are focused on resolving and preventing service incidents. They comprise:
- incident management
- problem management.
- ***Release processes***. Release management caters for the roll-out of new software and hardware, and is strongly linked to control processes.
- ***Control processes*** are central to the whole operation. They are targeted at preventing interruptions to services and are dominated by risk management. They are therefore fundamental to the long-term quality and cost-effectiveness of the service. They comprise:
- configuration management
- change management.

Business benefits

With the increasing use of IT to support businesses and the diverse range of technologies available, many service providers struggle to maintain high levels of customer service. Working reactively, they often spend little time planning, training, reviewing, investigating, and working with customers. Those same organisations and departments are being asked to provide improved quality, lower costs, greater flexibility and faster response to customers. Providing an infrastructure for the controlled operation of service delivery using formalised and disciplined management processes helps to address these requirements.

Some useful standards

A standard is a *recommendation* to do something (e.g. to design a product or use a testing method) in a certain way. Applying a standard helps to make things simpler, ensures reliability and saves manufacturing costs. The format of sheets of paper is a common example: an A4 sheet of paper will fit most printers, copying machines, envelopes, files, drawers, etc.

Another example is the RS-232C standard, which allows manufacturers to make modems that will work with any PC, MAC or terminal, or other RS-232C complaint system. As long as the system to be connected to a modem has serial ports that meet the requirement, all that is needed is a serial cable with the correct connectors. Indeed, standards are particularly important throughout IT because their use enables systems to exchange data regardless of their manufacturer or country of origin, or the network to which they are connected.

In addition to standards that apply to the characteristics of IT components and to data communications protocols, standards also exist that define the objectives that

management processes should conform to. Such "process control standards" enable:

- IT service providers to advertise their management capabilities in terms of an independently verified measure of quality
- organisations seeking tenders for IT service delivery, to advertise their requirements in terms of a potential supplier's quality capability.

Process control standards all help in harmonising the manner in which organisations work that regularly exchange data, such as different government departments. For example, in the UK electronic business techniques are being exploited increasingly by government to exchange data with citizens and with businesses. Much of the data obtained from the public in this way is used by more than one department. In order to provide the public with confidence that their data is not being disclosed to unauthorised people, the government have taken the decision to implement the British Standard for Information Security Management (BS 7799) in all key government systems.

In the context of IT infrastructure management, the British Standards Institution is soon to publish the British Standard for IT Service Management (BS 15000) to accompany the existing code of practice for IT service management, PD 0005 (which will become Part 1 of BS 15000 in 2002). BS15000 defines the requirements to be met in the following IT service management activities:

- general organisation and management:
- service management planning
- professional competence
- audit evidence
- demonstrating compliance (*with the standard)*
- and all the management processes

In addition to guidance published by the British Standards Institution, the CCTA (a UK government agency set up to provide advice and guidance on IT) have published a large library of information on IT infrastructure management, the "IT Infrastructure Management Library" (ITIL). The library contains over 30 volumes of guidance ranging from IT service provision and infrastructure management, through It service support and delivery, to a range of environmental issues.

Annex 2:

Aspects of programme management

Identifying the programme's scope:

- identify relevant strategies and change initiatives; assess their impact on the business areas affected by them and defined the required benefits
- identify candidate groupings of projects and evaluate them for business benefits, economies of scale and compatibility with other projects and plans for delivering IT services
- select as a programme the grouping of projects that achieves the best balance between strategic objectives and affordability, achievability and acceptable risk
- define and document each group as a programme, and obtain authorisation for the business case.

Defining and planning the programme:

- prepare and maintain a clear model of the improved business operation – this can be thought of as a "blueprint" for the affected business area(s)
- ensure that the "blueprint" is owned by the business area(s) and is seen to be practical, relevant and achievable
- ensure that objectives and priorities of the constituent projects are clearly driven by their impacts on the business operation – test them against the blueprint.

Structuring the programme:

- organise roles and responsibilities at both programme and project levels
- divide the programme into tranches of work to facilitate its management, synchronisation with planning and funding cycles, and the delivery of benefits
- co-ordinate projects within each tranche with the aim of achieving some of the planned benefits at the earliest possible time
- plan review points ("islands of stability") between tranches of work to review progress, direction and achievement of planned benefits
- ensure that plans for and changes to support facilities are co-ordinated across all projects.

Managing programme risks, quality and change:

- assess and manage risks associated with the programme, its projects and the planned changes to business operations

- ensure that the assessments of quality and fitness for purpose fully represent the requirements of the business
- ensure that progress reporting is open and effective so that problems can be f oreseen and dealt with
- be aware of developments that are external to the programme (such as legislative or policy changes) and take action to accommodate them.

Managing the impact on the business operation:

- involve personnel in the affected business area(s) to prepare them for change – for example, with training, awareness and the planning of procedures
- throughout the programme manage the take-on of project deliverables to ensure a smooth transition to the new business operation
- ensure that support services are able to accommodate changes in the business operation.

Ensuring that the programme delivers its planned benefits:

- look for measurable improvements in business operations
- identify benefits from the programme as a whole as well as from individual tranches of work
- actively manage the delivery of benefits throughout the programme
- provide time at the end of each tranche of work and at the end of the programme to reassess benefits and to tune the changes.

When to use programme management

Programme management should be used when one or more of the following conditions apply:

1. **Shared objectives:**
   - there is a need to co-ordinate several initiatives affecting a business area
   - the proposed projects support a strategy, a strategic change or a similar type of initiative, with significant impact on the organisation
   - a set of proposed projects and activities address a common problem or deliver a common set of business benefits.
2. **Management of complex changes:**
   - the set of changes cannot be managed as a single project because of their size or complexity
   - a set of changes covers too wide a range of business areas or development skills for a conventional project management structure
   - there are strong interdependencies between projects that require co-ordinated management.

3. **Shared resources:**
    - the use of resources from a common pool can be optimised by co-ordination across projects.
4. **Advantages of scale:**
    - the grouping of projects gives cost savings by avoiding duplication of effort
    - the grouping of projects provides the increase in scale to justify necessary infrastructure
    - the grouping of projects justifies the employment, recruitment or training of specialist skill groups
    - the grouping of projects leads to risk reduction; for example, by closely controlling vulnerable project interfaces.

Organising a programme

Programme management disciplines supplement, rather than replace, project management disciplines. Programme managers need to take a broader and more flexible view than project managers. They should be concerned to achieve not just product delivery, but also the actual realisation of business benefits. Programmes should therefore be led by senior management, whose commitment and involvement are essential.

In common with any major business initiative, there should be a clearly defined management framework for controlling activities and taking decisions. Overall authority and responsibility should be assigned to a ***Programme Director*** who is best drawn from the group of seniormanagers whose areas of the business are targeted for improvement. The Programme Director should have personal responsibility for the success of the programme in terms of realising its benefits, and therefore needs the status and authority within the organisation that are necessary to deliver that success.
Key supporting roles for the day-to-day management of a programme are:

- **Business Change Manager** – responsible for the blueprint, business case, management of change and benefits management
- **Programme Manager** – responsible for ensuring that the programme is carried out efficiently and delivers according to plan
- **Design Authority** – responsible for ensuring that the overall design and quality of the programme's outputs remain consistent and comply with the organisation's standards and policies.

For a small programme these roles may simply be expansions of existing responsibilities, whilst for a large and complex programme full-time roles, with additional support, would be justified.

Annex 3:

Post implementation review

Aim

The aim of a Post Implementation Review (PIR) is to establish the degree of success achieved by a project and to make recommendations, which may include identifying lessons that can be applied to improving the development process.

In practice a PIR is often avoided. It is sometimes seen as an unnecessary cost and, where a new system has failed to meet its objectives or realise the anticipated benefits, it may also be an uncomfortable process for the key participants.

The Post Implementation Review

The full scope of a PIR will depend largely on the scale and complexity of the project. Overall it should establish - in an impartial manner - whether a new system or service has met its:

- business objectives (delivered within budget and deadline; is producing predicted savings and benefits, etc.)
- user expectations (user friendly, carries the workload, produces the required outputs, good response time, reliable, good ergonomics, etc.);
- technical requirements (capable of expansion, easy to operate and maintain, interfaces with other systems, low running cost, etc.).

During the PIR it is also important to identify any lessons which can be used to improve the organisation's development process.

Timing

The timing of a PIR is much a matter of judgement. In general it should not be undertaken until after any changes and tuning that are necessary to achieve a stable system have been completed and any significant problems have had a chance to surface. Sufficient time should also be allowed for the system's users to become familiar with it. These criteria are generally met between six and twelve months after implementation. If the PIR is delayed beyond twelve months there will be an increasing risk that changing requirements - leading to further releases of the system - will obscure the outcome from the original development, or that the need for a PIR will be overtaken by other priorities.

If there are obvious and significant problems with a new system or service a PIR may need to be undertaken sooner than would otherwise have been the case in order to identify the nature of the problem(s), their case(s), and to recommend a suitable course of action.

The PIR team

In order to achieve an impartial outcome, the team should be substantially independent of the original system development team. It may therefore be advisable to employ an external IS consultant to manage the review. It may also be necessary to employ other external support to assist in evaluating the delivery of technical (e.g. project management, system design) and specialised functions (e.g. in financial and management accountancy), and to make appropriate recommendations where necessary. Internal Audit might help assess the effectiveness of internal controls.

In order to facilitate control, the PIR should have terms of reference, authorised by the approving authority, defining the:

- scope and objectives of the review;
- criteria to be employed in measuring the achievement of objectives;
- management and organisation of the review team;
- review budget and reporting deadline.

Activities to be undertaken

During a PIR the team should, according to their terms of reference, review:

- the main functionality of the operational system against the User Requirements Specification;
- system performance and operation;
- the development techniques and methodologies employed;
- estimated time-scales and budgets, and identify reasons for variations;
- changes to requirements, and confirm that they were considered, authorised and implemented in accordance with change and configuration management standards;
- set out findings, conclusions and recommendations in a report for the authorising authority to consider.

In addition to reviewing the functionality delivered by the new system, the review team will also need to look back to the Business Case on which the system was originally based to confirm that all the anticipated benefits, both tangible and intangible, have been delivered. This will involve investigating the reasons behind benefits that where not achieved, perhaps involving recommendations for remedial action, and using survey techniques to establish the extent to which intangible benefits (such as improved staff morale) have been realised.

It is also possible that the PIR will identify benefits that where not anticipated in the Business Case. These should be included in the PIR Report as additional justification for the investment, and to identify benefits that might be realised in other IS development projects.

Following their deliberations on the PIR Report, the authorising authority may either:

- endorse continuation of the system;
- approve plans to modify the system;
- terminate the system and made arrangements for a new course of action.

Annex 4:

Service management processes

Service design and management processes

Service level management

The process of agreeing, documenting and managing the quality and quantity of delivered IT service according to a written agreement or contract between the customer(s) and service provider. When invoked in conjunction with charging for the use of IT services, service level management forms a basis for running the service as a business or profit centre.

Capacity management

Capacity management is concerned with having sufficient IT capacity and with making the best use of it. Capacity management embraces the following:

- 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
- using capacity in an optimum way.

Costs and cost recovery

Addresses the identification, accounting and apportionment of service costs, and its recovery from customers where this is applicable.

Information security

Addresses the risks associated with inadequate protection of services from:

- disclosure of sensitive information to unauthorised parties
- inaccuracy or incompleteness of information
- non-availability of information when it is required.

Information security management processes have the objectives of ensuring that:

- all risks to services are identified
- manageable levels of risks are agreed
- procedures to achieve and maintain that manageable level are in place.

Service availability and continuity

Availability and continuity management processes form a continuous process committed to delivering services without interruption:

- **availability management** is concerned with identifying what can and cannot be controlled, and then dealing with and avoiding expected occurrences
- **service continuity management** is concerned with dealing with the unexpected.

The two processes must work together to ensure the right level of protection.

Service reporting

A timely, reliable, clear, concise and meaningful report enables its user to make informed decisions. Receiving an informative report at the right time means that the customer can fully understand the resource/cost/business impact of service provision. The success of service management is also heavily dependent on the monitoring, reporting and use of the information provided in service reports.

It is impossible to list all the service management reports that could usefully be produced. There are many, and their importance will vary from one organisation to another. However, in general they should cover metrics with regard to least the following areas of activity:

- workload and problem management
- financial reporting
- change and configuration management.

Supplier processes

Customer relations

An IT service manager should aim to provide quality services within the resources that are available. Quality is determined by fitness for purpose, and quality services are those that consistently meet the customer's business needs. Managing customer relations is about:

- providing customer support (advice, guidance, joint planning, liaison)
- conducting contacts with customers in an efficient, honest and courteous manner
- customer liaison initiatives (customer satisfaction surveys, publicising service management, etc.).

Supplier relations

No organisation is completely free of the influence of suppliers, both internal and external. For many, the achievement of business objectives may depend to a large extent on the performance of their suppliers.

Managing supplier relations involves:

- development of formal agreements with suppliers, and negotiation of discounts
- monitoring the use and performance of suppliers, identifying non-compliance and

instigating corrective action
- co-ordinating supplier activities
- arranging for briefing on suppliers' capabilities and products
- liaison with contract/legal and procurement teams.

Resolution processes

Incident management

Incident management is principally a reactive process. It translates a communication into a recorded support requirement. Communications may be about incidents, problems, requests for change, and questions. The incident management process potentially covers the management of all inbound communications as items of work.

The management process involves:

- call reception, recording, initial impact and urgency assessment and classification
- first line resolution or referral
- call tracking and management
- call request verification and closure
- first line customer liaison
- communicating short term changes to customers.

Problem management

Problem management differs from incident management in that its main goal is the detection of underlying causes and their eradication or circumvention.

The problem management process includes:

- problem investigation, diagnosis and resolution of problems
- impact and urgency assessment
- providing temporary workarounds
- problem record closure
- incident and problem prevention.

Release management

Many service providers and suppliers are involved in the release of hardware and software in a distributed environment. Good resource planning and management are essential to package and distribute a release successfully to the customer, and to manage the risk to the business.

Release management comprises:

- release planning, communication, preparation and training
- designing, building and configuring the release
- release acceptance
- distribution and installation.

Control processes

Configuration management

Configuration management is a discipline which can be used for controlling all components of an IT infrastructure. These include hardware items, software components, network items, documentation, and any part of the IT infrastructure or items associated with it that the organisation wishes to control. It involves:

- specifying the versions of configurations items in use and in existence in an IT infrastructure, and information on:
    - their status (in use, archived, under test, etc.)
    - who owns each item
    - the relationships between items
- maintaining up-to-date records containing this information
- controlling changes
- auditing the IT infrastructure to ensure that it contains the authorised items, and only the authorised items.

Change management

IT is becoming more integrated into the business of organisations, and more integrated with the work of their staff and customers. As a result the pace and frequency of change (changing requirements, and IT service changes to address the requirements) is increasing.

Experience shows that a high proportion of IT quality problems can be traced back to a change that has been made to some part of a system or service. A significant reduction in quality of service problems can be achieved if systematic change management procedures are introduced.

Change management comprises:

- raising and recording changes
- assessing the impact, cost, benefits and risk of changes
- developing the business justification and obtaining approval
- implementing changes, and monitoring and reporting on implementation
- closing down and reviewing change requests.

Annex 5:

Risk management

"The process of analysing exposure to risk and determining how to handle such exposure"

"Risk" is the potential for unwanted consequences. Whenever there is an opportunity there is a risk; risk of not seizing an opportunity and risk of failing when an opportunity is taken. The better these risks are understood and managed, the more competitive the organisation becomes and the better placed it will be to sustain its advantage.

Although we are rarely conscious of it, we identify, assess and manage risks throughout our everyday lives; for example, when we cross the road or buy a house. However, the subject needs some explaining in the context of developing and managing electronic services.

The impact of IT-related risks in particular may easily prevent an electronic service from achieving its stated objectives. This is clearly unsatisfactory, and particularly so in an age when the public increasingly depend on the delivery of electronic services. It should therefore be a central part of any public service manager's role to:

- understand what risk is
- be able to identify and assess the risks that threaten the successful delivery of electronic services
- manage risks so that service management objectives are achieved.

Deciding on an approach to risk management

Considering risk in an appropriate way throughout an organisation improves the chances of success for the organisation and all its activities. The management of risk should therefore be built into the overall management process and not treated as something extra that can easily be forgotten.

The processes of risk assessment and risk management should not be conducted just once for a particular strategy, programme, project or operational activity. They should be carried out throughout their lifetime from initiation; through development, operation and evolution; to completion or termination.

It is necessary to adopt appropriate risk assessment and risk management techniques at each level within an organisation because the nature of the threats and vulnerabilities changes. When the underlying principles are understood, appropriate processes can then be defined and implemented to ensure effective risk management. But even then it is essential to monitor process operation so that lessons can be learned and used to improve the process for the future.

A model based upon Guide to BS7799 is describing the process of risk assessment and risks management as follows:

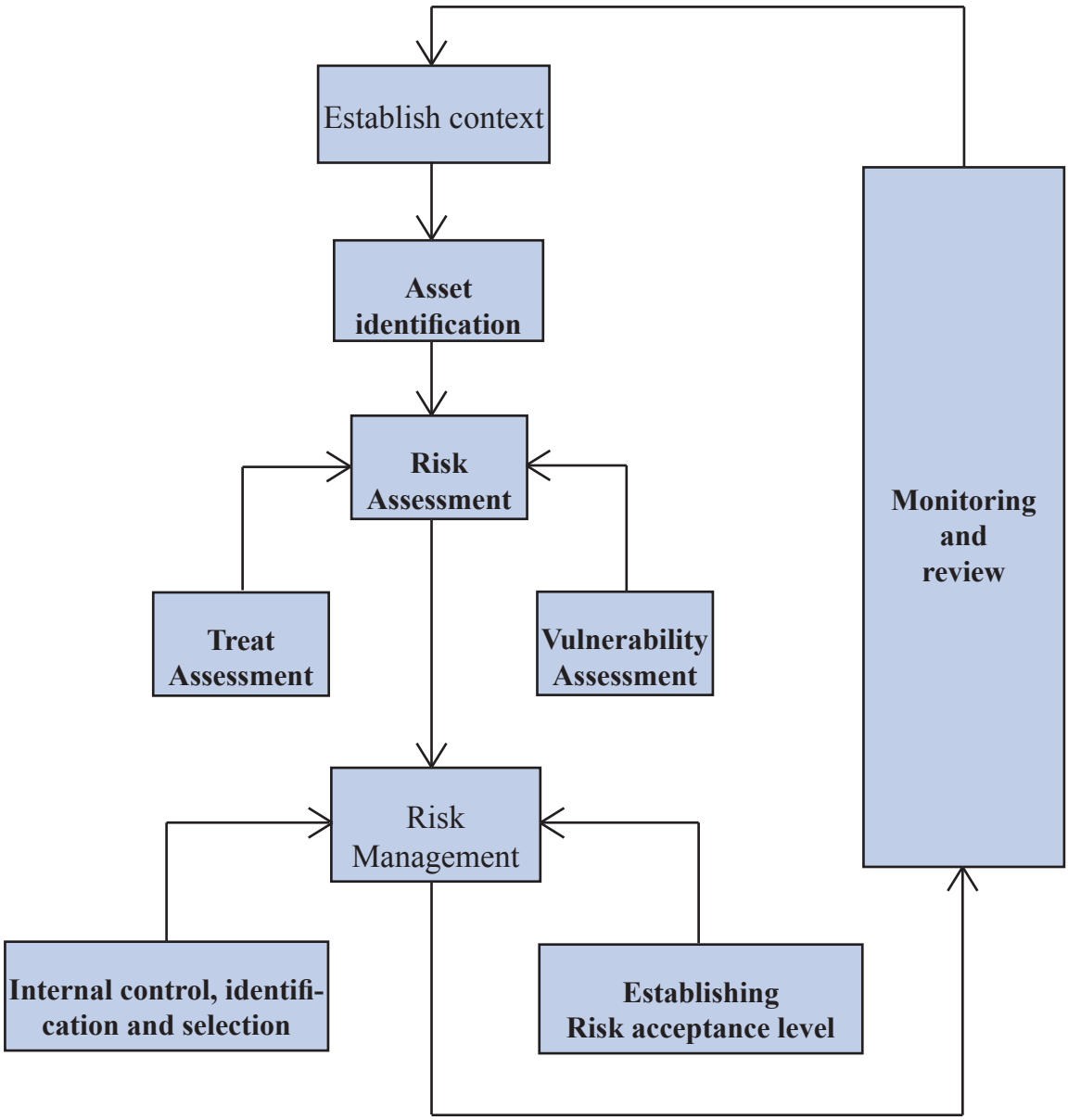

Figure 3 – Risk Assessment and Risk Management Model

1 - Establishing the context

The Risk Management Model starts by establishing the organisation's strategic aims and objectives, and then identifying the processes and controls that are necessary to achieve them.

Strategic context: Defines the relationship between the organisation and its internal and external environment, identifying its strengths and weaknesses, opportunities and threats (SWOT analysis). This stage of the process should also involve identifying and communicating with the organisation's owner (superior authority) and determining their expectations and requirements.

Organisational context: requires an analysis of the entity's goals, objectives and policies, which then contributes to the establishment of criteria for the risk assessment process. The consequences of goals and objectives not being achieved should be considered at this stage.

Risk management context: Involves determining the goals, objectives, strategies, scope and parameters of the actual risk management process itself. It is an advantage to define the structure of the process by separating the risk analysis into a set of manageable elements. The risk management context also examines the need for information and research. In this product risk has the following elements:

- Threats to, and vulnerabilities of, processes and/ or assets (including both physical and information assets)
- Impact on assets based on threats and vulnerabilities
- Probabilities of threats (combination of the likelihood and frequency of occurrence).

IT- risks in this context are often defined by the potential for loss of confidentially, availability or integrity of information.

2 - Asset identification and valuation

Many risk assessment methodologies start with the identification and classification of the assets which need protection because they are vulnerable to threats. All assets within the review boundary should be identified. After fulfilling the objective of asset identification, values should be assigned to each of these assets. The values assigned should be related to the cost of obtaining/replacing and maintaining the asset, and the potential adverse business impacts from loss of confidentiality, integrity and availability.

3 - Risk assessment

The objective is to identify and assess the risk to which the organisation and its assets are exposed, in order to identify and select appropriate and justified internal controls. Risk are a function of the values of the assets at risk, the likelihood of threats occurring to cause the business impacts, the ease of exploitation of the vulnerabilities by the identified threats, and any existing or planned controls which might reduce the risks.

4 - Threat assessment

Different functional groups within the organisation must be used to support a threat assessment. They could be personnel department staff, facilities planning and IT specialists. The organisation must identify the nature of threats and their targets, and then assess their likelihood.

Threat assessment should consider the following:

- Frequency – how often a threat might occur
- Deliberate threats – motivation; the capabilities of, and the resources available to possible attackers; and perceptions of the value and vulnerability of an organisation's assets
- Accidental threats – geographical factors such as proximity to chemical or petroleum factories, in areas where extreme weather conditions are always possible, and factors that could influence human errors and equipment malfunction.

5 - Vulnerability assessment

When an organisation considers vulnerability, it should consider weaknesses relating to:

- The physical environment, for example location in an area susceptible to flooding
- Personnel, management and administration procedures and controls, for example lack of policies for the correct use of telecommunications media and messaging
- Hardware, software or communication equipment and facilities, for example lack of effective change control procedures.

It is important to assess how severe each vulnerability is in relation to each threat that might exploit it in a particular situation.

6 - Identification and selection of internal controls

The risk management process follows risk assessment. It involves identifying and selecting appropriate, cost-justified controls, a process that should be supported by the results of the risk assessment. The strength of a control depends on its costs, ease of use, reliability, and the number of different threats it will manage (e.g. vetting new recruits covers quite a range of potential threats, as does securing the entrances to a building. On the other hand a biometric control only covers the threat of impersonation).

7 - Identification of existing and planned internal controls

Internal control includes five categories of control that management designs and implements to provide reasonable assurance that its control objectives will be met. These are called the "components of internal control", and include the control environment, risk assessment, control activities, information and communication, and monitoring. Without an effective control environment the other four components are unlikely to result in effective internal control, regardless of their quality.

Risk assessment might determine that an existing or planned control is not justified. The organisation should then check whether it should be removed, replaced by another, more suitable control, or whether it should stay in place.

8 - Reducing the risks

Controls can reduce the assessed risks in many different ways. They can act to:

- Avoid the risk (for example, the risk of external hacking of a computer system can be avoided by having no external network connections)
- Transfer the risk (for example, outsourcing IT services to an external service provider)
- Reduce the threats (for example, a ban on smoking reduces the threat of fire)
- Reduce the vulnerabilities (for example, constructing with fire-resistant materials reduces vulnerability to fire)
- Reduce the possible impacts (for example, backing up data can reduce the impact of system failure/disaster)
- Detect unwanted events, react, and recover form them (for example, by reviewing computer usage logs to detect unauthorised activities, and then investigating and taking action on them).

It is always important to match the controls to the specific needs of the organisation, and to justify their selection. Control selection should always include a balance of operational and technical control supporting and complementing each other.

9 - Risk acceptance

Risk management rarely eliminates risks, and some "residual" risk is likely to remain after appropriate controls have been implemented. It is a management issue to decide what level of residual risk is acceptable. Risks in excess of this level should be reduced by the implementation of more stringent controls. Risks below this level should be evaluated to determine if an excessive level of control is being applied, and if removing or reducing these controls can reduce costs.

10 - Monitoring and Review

Organisational priorities change through time, as does the IT environment, and both risks and their management should be monitored and updated as part of the on-going management cycle. Periodic review is essential to ensure that risk management strategies remain relevant. It is also beneficial to monitor the effectiveness of the management system set up to control the implementation of risk management strategies.

Annex 6:

How to audit the management of IT infrastructure risks

Audit Methodology

Audit methodology is a set of documented audit procedures designed to achieve planned audit objectives. The approach to audit is governed by the main audit objectives. Some of the most common types of audit service are:

- Financial auditing – which aims to express an audit opinion on the reliability and presentation of an organisation's financial statements;
- Performance auditing – which focuses on the economic, effective and efficient expenditure of public funds;
- Compliance auditing – which focuses on compliance with statutes and regulations.

SAIs often adopts one or more audit methodologies. Auditors can use this guide regardless of which methodology they use.

Audit Approach

There are several possible approaches to auditing an organisation's IT service delivery risk assessment and risk management processes.

This guide assumes that, regardless of formal risk management procedures, organisations implement some kind of internal controls. The process of implementing internal controls is mainly a result of risk awareness.

Auditing the management of IT service related risks involves assessing:

- whether the organisation has adopted an approach to IT service delivery risk assessment
- whether the selected approach is in accordance with best practice
- risk assessment and risk management operates effectively
- whether there are effective quality assurance and quality control processes over the management of IT service related risks.

It is reasonable to assume that audit scope will vary depending on an SAI's overall audit risk analysis and their level of materiality. A number of potential audit boundaries need to be considered when deciding on an audit strategy:

1. Auditing management of IT infrastructure risks on a **central government level.**
2. Auditing management of IT infrastructure risks on a **government agency level.**
3. Auditing management of risks on selected parts of an IT service within any given level.

4. Comparing the management of IT service related risks in a selected **sample of government agencies.**

It is important to appreciate that this guide focuses on managing IT service related risks as an isolated subject, although in practice this forms only part of an organisation's overall risk management strategy.

If the Risk Management Model or a similar risk management process underlies an organisation's approach to IT service management, the auditor could use this guide as a tool to evaluate management's control over IT service related risks. Audit conclusions would then be based on the quality of the risk assessment and risk management processes. Conversely, failure to find the Risk Management Model or a similar risk management process in operation could indicate a lack of risk awareness (or lack of knowledge). The Guide then provides the auditor with advice on typical risk areas and risks, and on business impacts based on international experience obtained through case studies. The audit findings could also be used to justify deploying further audit resources, either on a detailed investigation or on investigations into other areas that are similarly affected by IT service management weaknesses.

Examples of common audit approaches:

Risk-based audit approach

A risk-based audit approach is usually adapted to develop and improve the continuous audit process. It is used to assess risk and assist the auditors decide whether to adopt a controls-based or a direct substantive testing audit approach. In a risk based audit approach, the auditor considers risks and controls for managing them against knowledge of the organisation and their business. The auditor may use this guide to identify the main risks within IT infrastructure management in order to concentrate audit resources in these areas.

Problem-based audit approach

In a problem-based audit approach, the auditor reviews one or more issues within in a number of organisations with the aim of drawing an overall conclusion(s). When following this approach the auditor selects the appropriate sections of this guide, and then uses them to support audit testing within each organisation.

Annex 7:

Some examples from SAIs on IT Service delivery and project failures

An IT service's exposure to risk

Audit projects often reveal that agencies have significant problems in obtaining a satisfactory contribution to organisational objectives from their IT-related investments. Some problems are technical whilst others concern management, and in particular IT service management. This indicates a need for more efficient IT service management processes. Audit experiences from different SAI's also reveal that there is often a lack of risk awareness combined with a lack of knowledge of how to manage risks. Any IT service is exposed to various risks that could result in it failing to make a full contribution to achieving the organisation's business objectives. In our study we have identified the following main risks:

External demands and requirements from Parliament, Government and other organisations are not met.

One problem is to identify external demands and other requirements. For example a study (SNAO[1] 1991) showed that during the development of a major IT system, the agency failed to consider some important legal requirements. The project had to be suspended, and this caused a big delay in further project work.

The SNAO have shown that complex IT systems can have serious problems handling fresh demands from new or amended legislation (SNAO, 1991, 1993). Sometimes, due to political reasons, organisations have to change their IT infrastructure quickly without having the necessary time to analyse new external demands thoroughly. It seems that some organisations are not well prepared for implementing a rapid succession of externally imposed changes.

In a study three central agencies were to co-operate in developing a strategy for a big IT-system, the cost of which was not to exceed 260 million SEK. This estimate was based on the agencies' own calculations. Some months after the IT project started, the agencies told the Government that the cost had risen to 360 million SEK. This caused the Government to ask the SNAO to audit the project costs. The audit resulted in several recommendations for reducing them (SNAO, 1997).

IT infrastructure strategy is not aligned with business strategy

In 1992 the SNAO audited the relationship between business strategy and IT infrastructure strategy within a number of public agencies. (SNAO, F 1993:34). In one case study the main audit conclusion was that the agency's business strategy was not driving the IT infrastructure. There was a big difference between the delivered IT Infrastructure and what was required to meet business objectives.

Insufficient knowledge and experience of IT infrastructure management

One important support area is the knowledge and experience that is necessary to manage IT infrastructure efficiently and effectively at all management levels. Several studies have shown that there is significant need for improvement (SNAO, 1993).

Shortage of IT project management skills

Several IT audit projects undertaken by the SNAO during the 90s revealed that agencies often have significant problems managing IT development projects and maintaining their IT Infrastructure (SNAO 1992, 1993, 1998, 2000). The SNAO attributed these problems to insufficient IT project management skills, particularly to poor standard of project planning and estimating. In the late1980s the SNAO observed that the demarcation between business and IT department managers was unclear, and that this led to confusion in the maintenance of IT systems (SNAO 1987).

A poor standard of operational procedures

An SNAO study in 1991 attributed many IT problems to poor communications with other departments.

A study carried out by the SNAO in 1987 revealed a poor standard of security in IT infrastructure operations. Agencies did not collect and analyse information about IT security incidents in order to identify trends and fundamental problems.

In a study of Y2K matters, the SNAO revealed that some agencies did not have adequate contingency plans for responding to significant IT security incidents (SNAO, 1999).

Late and incompatible IT systems

Sometimes IT systems are so delayed that the users build their own IT system instead (SNAO, 1993). Another problem is that systems are sometimes unable to exchange information with other systems (SNAO, 1993).

In another study it was shown that the data delivered from one IT system to another was late and technically insufficient because the two IT systems were incompatible. This resulted in wasted investment (SNAO, 1993).

The users of the IT Infrastructure service do not use it efficiently.

A study revealed that the users of an IT system were unable to use it efficiently and to its full potential because it was complicated and time-consuming to use (SNAO, 1995).

In another study the users did not trust the information produced by the system (SNAO, 1996).

The system fails to deliver the planned business benefits due to unreliable outputs.

In a study carried out in 1995, the SNAO observed serious problems in obtaining the planned benefits from an IT system. The system was running at several agencies that used it to exchange information with each other. One central agency received information from the others and stored the data in a central database to be used for statistical purpose. Altogether information gathering cost 100 million SEK, but due to poor quality the information could not be used as intended. As a result the central agencies could not deliver important statistics to Parliament.

Managers dealing with IT infrastructure matters do not communicate effectively.

One study stated that managers did not co-ordinate the development and maintenance of IT infrastructure efficiently. They had not developed a management framework for discussing, planning and steering IT infrastructure developments and operations, neither had they analysed the business strategy in order to give appropriate directives to the IT-Department. In one case the top managers placed the responsibility for the IT infrastructure in the Administration Department. (SNAO, 1993).

The above list of risks is taken from investigations and studies of IT projects performed by the SAIs of the UK, Sweden and Norway.

Annex 4 contains further case studies based on work undertaken by the UK National Audit Office.

An example from an Electronic Service Delivery in Norway

Over ten years ago, the Norwegian Customs and Excise (NCE) developed an electronic clearance system (TVINN). The system uses EDI messages that conform to EDIFACT (the EDI[2] standard of United Nations). One of the reasons for developing TVINN was to make the clearance procedure more effective and efficient, for both NCE and the private industry. Approx. 95% of the total number of customs declarations are processed by this system.

TVINN is considered by its users to be a successful electronic service. The OAG[3] of Norway has, however, raised some criticisms of the system. These mainly concern a lack of transaction trails connected to the debtors' ledger; insufficient routines for analysing extended controls performed by the NCE; and that system changes are not being recorded. Also, the EDI solution replaces traditional paper with electronic vouchers. The OAG has legal access to any debtors' account and voucher files for purposes of auditing and examining the quality of NCE's revenue determination procedures. Nevertheless,

this is considered as a resource-intensive audit approach.

NCE has also recently launched “TVINN-Internet”, a simplified clearance solution that makes it possible for citizens to pay duty on goods they import by mail order. The citizen can use a personal computer to access TVINN over the Internet. However, a problem with this service is that customers don’t always collect their goods when they realise the exact amount of duty to pay. This leaves NCE with arrears, and the postal services with unclaimed property.

(Footnotes)

[1] SNAO reports are available in Swedish only

[2] EDI: The interchange of standard formatted messages between the computer application systems of trading partners and/or administrations with minimal manual intervention.

[3] OAG: Office of the Auditor General

Project	Problems experienced	Impact of problems	Lessons
The United Kingdom Passport Agency In 1997 the Passport Agency let contracts to the private sector to undertake some of its activities and to introduce a new computer system. The objective was to improve the efficiency of the passport issuing process and improve the security of the United Kingdom passport. The Agency had planned to roll-out the new processing system to all its offices within a tight timetable before the busy season, but this was postponed following difficulties at the first two offices. In the spring and summer of 1999 there were serious delays in processing passport applications by the United Kingdom Passport Agency, partly as a result of problems with the implementation of new IT driven passport issuing arrangements in the Liverpool and Newport passport offices.	• Although the specification for the new computer system broadly mirrored the processes and functions of the existing system, it did incorporate more sophisticated software and technology. Agency staff found the system more complex to use and it took some time for output to return to previous levels. • Most elements of the system development had been completed successfully prior to launch, but project delays meant that the productivity of the new system was not thoroughly tested by the Agency prior to going live. • The Agency's roll out timetable was short and allowed little room for manoeuvre should problems arise. The second office went live despite the first office failing to meet the criterion of output for continuing the roll-out. • When the Agency took its decision to halt roll out it had no contingency plan. Despite considerable effort, at no point during early 1999 did the Agency process sufficient output to catch up on the rising backlog.	• From early 1999 the Passport Agency encountered increasing difficulties meeting demand for passports. • The unit cost of producing a passport in 1999-2000 is was estimated to be £15.50, compared to the Agency's £12 target. • Processing times reached 50 days in July 1999. The problems received widespread publicity and caused much anxiety for members of the public. The Agency's telephone service became overloaded, and members of the public had to visit and queue at one of Agency's offices. • The Agency employed additional staff, and optimised the efficiency of its examination processes, consistent with the need to maintain the integrity and security of its issuing procedures. Only the introduction of emergency measures enabled the Agency to reduce its backlog.	• Organisations must examine carefully the full implications of the introduction of changes to IT systems, including the impact of any policy changes that may affect demand for services. • It is essential that bodies draw up contingency plans to cover the risk that the system will not be delivered on time. Such plans should include an assessment of potential compensation payments to customers.
Council for the Central Laboratory of the Research Councils (CCLRC) – Integrated accounting system The CCLRC decided to replace their old and outdated cash-based accounting system with an integrated accruals based system to record all financial transactions, produce their accounts and provide meaningful internal management information.	• The integrated accounting system was due to be introduced on 1 April 1997 for full operation by June 1997. The Council ceased to operate their old system on 31 March 1997, but did not follow the normally accepted practice of running the two systems in parallel. CCLRC estimated this would have incurred costs of up to £2.5 million in 1997-98, although a more reasonable estimate was between £0.75 million and £1million.	• The system was still not fully operational in early 1999, two years after the planned implementation date and costs had overrun by 84%. • The original contract value was £544,000, but the Council estimated that they incurred further, unanticipated, direct costs of some £458,000 on additional hardware, training, legal and audit fees and temporary staff.	• There are very significant risks in not introducing back-up procedures, such as the continuation of the outgoing system for a limited period. Full consideration of the risks and a realistic analysis of the case for parallel running must be undertaken. • It is not acceptable for the body concerned to rely on the contractor to manage the project.

Project	Problems experienced	Impact of problems	Lessons
	• The Council encountered problems with the operation of the new system, together with delays and errors in the migration of data from the previous system, • The project management structure failed to comply with best practice, particularly in terms of ensuring clarity of roles, responsibilities and accountabilities. There had also been a failure to ensure clear reporting lines to senior management consistent with their responsibilities. • The project team was not equipped to manage a situation where the contractor progressively withdrew before the project was completed and demonstrated a lack of effective control over the contractor. • Scrutiny of the project was compromised because the Audit Committee was presented with insufficient and over-optimistic information on the problems being encountered.	• Inadequate controls over manual payments made to ease the backlog in payment processing on the new system led to nearly 500 overpayments to staff and suppliers, totalling some £270,000, most of which were subsequently recovered. • A fixed asset module did not account correctly for the Council's large capital asset base, forcing them to resort to a spreadsheet register to support their 1997-98 accounts. • The Council were also unable to reconcile their general ledger to their bank statements. There was an original difference of some £1m, which was eventually reduced to £48,000, which was written off at the end of the year. • The new Chief Executive had taken prompt action to address the problems he had inherited and various parties to the contract were continuing to work together to ensure the system became fully operational in 1999-2000.	• Organisations must recognise that introduction of a bespoke financial and management accounting system to a demanding timetable is a business critical operation, requiring good project management skills. • If an organisation has reservations about the technical viability of a proposal, they should seek expert advice before proceeding. • Sponsor bodies should be notified directly of significant problems impacting on their IT systems.
<u>The Hospital Information Support Systems Initiative</u> By the late 1980s, many acute hospitals had developed their own computer systems. They were not linked together and as a result the recording of information was slow and inefficient. The NHS Executive launched the Hospital Information Support Systems Initiative (HISS) in 1988 to explore the costs and issues involved in implementing integrated systems in NHS hospitals in England. The Comptroller and Auditor General examined 6 of the sixteen projects funded under the Initiative.	• In 1996 there was a gap between the Executive's plans and achievements in implementing integrated systems, and Executive needed convince those trusts not already involved of the value of the systems. • The Executive went ahead with one project despite high costs and the significant risks involved. The fact that two major suppliers did not believe it was feasible did not act as a warning.	• All six projects examined by the National Audit Office had experienced delays, and likely to have had an adverse effect on the quality of care those hospitals could provide.	• It is essential that organsiations learn from the lessons of previous projects. • The commitment of users such as clinicians is crucial to the success of such projects. All users need to be involved in the development of these systems. • There are considerable dangers in trying to implement projects too quickly and not preparing sites properly.

Project	Problems experienced	Impact of problems	Lessons
	• The NHS Executive selected the three pilot projects under the Initiative within the very short period of two months. Subsequently, each of the projects suffered problems and delays. • These delays may have stemmed, at least in part, from the Executive's failure to prepare the hospitals to run their projects, and that they might have obtained better value for money had they taken more time to ensure hospitals were fully prepared. The Executive argued that in view of the innovative and complex nature of these projects all reasonable steps had been taken to manage them effectively. • The projects proceeded without sound business cases being established. Although the aim was to learn lessons to inform the development of integrated systems in other hospitals, development of formal evaluation mechanisms was only started four years after the start of the initiative. The Executive considered that full business cases for early pilot sites, as defined by today's standards were not realistic given the decision to invest in order to understand the issues.		• Projects should not proceed without first establishing that there are sound business cases for doing so, and without undertaking full investment appraisals and risk analyses. • The need to consider evaluation mechanisms at an early stage is integral to all initiatives of this kind.
Ministry of Defence : Support Information Technology The Ministry of Defence use IT for management and administration, and for planning and conducting military operations. The National Audit Office examined their performance in delivering IT systems and improving the planning and management of information technology.	• The complexities involved in implementing IT in a large organisation such as the Ministry of Defence are large, but the cost of the learning process was unacceptably high.	• All nine systems examined had suffered delays varying from five months to two years, postponing the achievement of predicted benefits. • Of four systems subjected to post implementation review, only one had achieved all intended financial and operational benefits.	• Clear definitions of user requirements were important before going ahead with projects. • The Department recognised the need to break projects down into shorter tranches and apply strict control over requirement changes during development.

Project	Problems experienced	Impact of problems	Lessons
	• There were a number of problems with the LANDSCAPE project. It suffered from successive delays due to changing user requirements, the contractor's achievement on the software was imperfect and the hardware was unsuitable for the project. • Fundamental misjudgements were made on the SEMA project which led to a nine-fold increase in the development effort required. • User involvement in IT had been insufficient to ensure the systems were capable of meeting business needs. • The 1988 IT strategy identified project management weaknesses as a factor in the failure to fully realise the benefits of investment in IT.	• The LANDSCAPE project had resulted in a loss of some £6 million. • In the mid-1980s the Department recognised the need for co-ordinated planning and in 1988 approved a strategy for support IT.	• Post-implementation reviews are crucial in ensuring that expected benefits have been achieved and in identifying lessons for the future.

Glossary of Terms

Introduction

This glossary of terms is designed to assist those who use the INTOSAI Guide to IT Service Audit to understand the terms used in the Guide. Although it contains over 20 pages, it is by no means comprehensive in the sense of being a dictionary of IT terminology. If you require an on-line dictionary of IT terms try……

http://www.zdwebopedia.com or

http://whatis.techtarget.com/

The words that are defined may have different meanings when used in different contexts. The definitions provided here are those that are normally used within in the context of IT infrastructure management and information security.

To enable quick navigation between definitions, ensure that you select the "web" toolbar option (View, toolbars, web) before using the dictionary.

Access controls Controls that are designed specifically to reduce the risk of the unauthorised use of resources (including the use of resources in an unauthorised way), or damage to, or theft of resources. Access control mechanisms include a combination of physical (barriers, CCTV, security guards), technical (e.g. passwords, biometrics, computer logs) and administrative (e.g. personnel vetting, management supervision) controls (see physical access; logical access).

Accountability An information security principle whereby system users are uniquely identifiable and are held responsible for their actions. Being able to identify users uniquely enables security violations to be traced to individuals; sharing passwords defeats this objective.

Active-X Active X is an integration technology developed by Microsoft. Its main use is for web pages, which it can make more useful and, visually, more exciting. However, Active X controls have powerful processing ability, and the onus lies with the user whether or not to accept them. Web browser settings control whether Active X controls are to be downloaded and run, or whether they are blocked; however, blocking Active X may limit the information provided by the web page the user is trying access.

Active X controls (See also Active X). Active X controls are objects in a web page that allow interactive between the user and the web server. Besides enlivening web pages for aesthetic value, controls can be used to create interactive forms for ordering merchandise, collecting information, and other purposes.

After image See - Before and after image.

Algorithm In computing, a finite set of well defined rules for the solution of a problem in a finite number of steps (see encryption algorithm).

Applet A small Java program that can be embedded in an HTML page. Applets differ from full-fledged Java applications in that they are supposed to be restricted to provide some security to the user.

Application A system that has been developed to serve a specified purpose, for example to pay suppliers' invoices, place orders with suppliers and maintain stock records. An application incorporates both clerical and computerised procedures; controls over transaction input, processing and output; and file management. It should also maintain an audit trail (see also system software; program).

ASCII American Standard Code for Information Interchange. ASCII was developed to standardise data transmission among disparate hardware and software systems, and is built into most mini and personal computers. It is a coding scheme using 7 or 8 bits that assigns numeric values to up to 256 characters. These include letters, numerals, punctuation marks, control characters and other symbols. ASCII text is often referred to as a "plain text" (see EBCDIC).

ASCII file A document file in ASCII format, containing characters, spaces, punctuation, carriage returns, tabs and an end-of-file marker, but no formatting information. Also sometimes referred to as a text file, text-only file or plain text.

Asset In Information Security, the information or information processing resources that are to be protected by the application of controls.

Asymmetric encryption A cryptographic algorithm that employs a public key for encryption and a private key (see secret key) for decryption; or in authentication, a private key for signing and a public key for signature verification. Public and private keys are related and form an asymmetric key set.

Audit trail A chronological set of records that collectively provide documentary evidence of processing, sufficient to enable reconstruction, review and examination of an activity.

Authenticity The attribute of genuineness. For evidence to be authentic it must be all that it purports to be.

Authentication (1) The act of determining that a message has not been changed since leaving its point of origin. (2) A process that verifies the claimed identity of an individual.

Availability The ability to access and use a system, resource or file, where and when required.

Backup A duplicate copy (e.g. of a program, of an entire disc or of data) made either for archiving purposes or for safeguarding valuable files from loss should the active copy be damaged or destroyed. A backup is an "insurance" copy.

Back door see Trapdoor.

Bandwidth A measurement of how much data can be sent across a communications circuit at the same time. It is usually measured in bits per second (BPS).

Baseline A snapshot of the state of a CI and any component CIs, frozen at a point in time for a particular purpose.

Bastion host A specific host that is used to intercept packets entering or leaving a network and the system that any outsider must normally connect with to access a service or a system that lies within an organisation's firewall.

Before and after image In database updating, the transaction is first applied to a copy of the record to be updated (the "before image") held in memory to produce an image of the record after updating (the "after image"). The updated image is then committed to the database, after which the after image is compared with the database record. If they do not match the process can be rolled back by the DBMS.

Benefit Management procedures Identifying, optimising and tracking expected benefits to ensure they are achieved.

Biometrics In access control, automated methods of verifying or recognising a person based upon behavioral or physical characteristics (e.g. fingerprints, handwriting, and facial or retina geometry).

BIOS The set of essential software routines that test hardware at start-up, start the operating system, and support the transfer of data among hardware devices. BIOS is an acronym for Basic Input/Output System. On PC-compatible computers, the BIOS is stored in read-only memory (ROM) so that it can be executed when the computer is turned on. Although critical to performance, the BIOS is usually invisible to computer users.

Bit Shortened term for binary digit. It is the smallest unit of information handled by a computer. One bit expresses a 1 or a 0 in a binary numeral, or a true or false logical condition, and is represented physically by an element such as a high or low voltage at one point in a circuit or a small spot on a disk magnetised one way or the other. A single bit conveys little information a human would consider meaningful. A group of 8 bits, however, makes up a byte, which can be used to represent many types of information, such as a letter of the alphabet, a decimal digit or other character.

Black box testing Testing that involves no knowledge of the internal structure or logic of a system.

Boot The process of starting or resetting a computer. When first turned on (cold boot) or reset (warm boot), the computer executes important software that loads and starts the computer's operating system and prepares it for use. Thus, the computer can be said to pull itself up by its own "bootstraps".

Boot disk A floppy disc that contains key system files from the operating system and that can boot, or start, the PC. A boot disk must be inserted in the primary floppy disc drive (usually drive A:) and is used when there is some problem with starting the PC from the hard disc, from which the computer generally boots.

BSI British Standards Institution. The UK national standards body. Widely used standards first developed and published by the BSI include ISO 9001 (BS5750 – quality management systems) and ISO 17799 (BS 7799 – information security management).

BS 7799 A UK standard published by the BSI. It consists of two parts. Part 1 (A Code of Practice for Information Security Management) provides a baseline set of information security controls. Part 2 contains the auditing criteria against which formal certification against the standard may be obtained.

Browser See web browser.

Browsing Searching through storage to locate or acquire information, without necessarily knowing of the existence or the format of the data being sought.

Buffer In computing, an area of storage that is temporarily reserved for use in performing an input/output operation, into which data is read or from which it is written. In data communications, a storage area used to compensate for differences in the rate of flow of data, or time of occurrence of events, when transferring data from one device to another.

Bug An error in programming code that produces an undesirable variation from design performance in a program during execution.

Business A commercial or government enterprise, and the people who comprise it.

Business continuity A formal plan, or integrated set of plans, designed to enable key business processes to continue in operation following a major system failure or disaster. Essential ingredients include the identification of key business processes, adequate system backups and a workable continuity strategy.

Business impact review In business continuity planning, a review designed to identify the impacts (over time) of loosing information systems.

Business process re-engineering (BPR) Modern expression for organizational development stemming from IS/IT impacts. The ultimate goal of BPR is to yield a better performing structure, more responsive to the customer base and market conditions, while yielding material cost savings. To reengineer means redesigning a structure and procedures with intelligence and skills and being well informed about the entire attendant factors of a given situation, to obtain the maximum benefits from mechanization as basic rationale.

Byte A unit of data generally comprising 8 bits. A byte can represent a single character, such as a letter, a digit or a punctuation mark. Because a byte represents only a small amount of information, amounts of computer memory and storage are usually given in kilobytes (1,024 bytes), megabytes (1,048,576 bytes), or gigabytes (1,073,741,824 bytes).

Call centre A central point where customer and other telephone calls are handled by an organisation, usually assisted by some amount of computer automation. Typically, a call centre has the ability to handle a considerable volume of calls at the same time, to classify calls and forward them to someone qualified to handle them, and to record calls. Call centres commonly handle such activities as customer services, order entry, reservations, help desk facilities, dispatch systems, telesales and collections. Telephone banking, insurance and share dealing are among financial applications.

CASE Computer Aided Systems Engineering. Software tools that support systems analysis, design and construction.

Casework department A department handling applications, complaints etc.

Certification authority In cryptography, an authority trusted by all users to create and assign digital certificates. The role is generally performed by large public institutions, such as the Post Office, BT and clearing banks (e.g. Barclays).

Change management The process of controlling and managing requests to change an IT Infrastructure or IT service, and then controlling and managing the implementation of the changes that are subsequently approved.

Channel In data communications, a path along which signals can be sent. The term may also refer to a mechanism by which the path is effected.

CI Configuration Item. In configuration management, a component associated with an IT infrastructure that is under the control of the Configuration Manager. CIs vary widely in complexity, size and type. They can range from an entire system (including all its hardware and documentation) to a single program module or a minor hardware component.

Ciphertext In cryptography, unintelligible text produced through the use of encryption.

Classification The process of formally identifying incidents, problems and known errors by origin, symptoms and cause.

Client (1) A computer that interacts with another computer, usually referred to as the server, using a client program. E-mail is an example - an e-mail client connects to an e-mail server to send and receive messages. (2) A term sometimes used by auditors to refer to an audited organisation.

Code Program instructions written by a programmer in a programming language.

Cold site In business continuity, a site that is suitable for the installation of computer equipment and its environmental and ancillary support.

Commit In databases, a command to update the physical database with the transactions input to the system and held in temporary storage (or buffer).

Confidentiality In information security, the property that information is not made available or disclosed to unauthorised individuals, entities or processes.

Configuration audit Verifying the completeness and correctness of CIs. This involves verifying that all items are present in their correct version and, where computer files are concerned, their integrity is sound; and that no extraneous items have been introduced (e.g. unauthorised equipment; unauthorised and/or unlicensed software).

Configuration Item See CI.

Configuration Management The process of identifying and defining the CIs in a system; recording and reporting their status; and verifying their completeness and correctness.

Controls In information security, policies, procedures and mechanisms designed to ensure that activities achieve their authorised objectives. Controls can be preventive (e.g. a 'no smoking' policy is enforced), detective (e.g. a smoke detector), corrective (e.g. a sprinkler system) or restorative in character (e.g. a disaster recovery plan).

CMDB Configuration Management Database – a database that contains details about the attributes and the history of each CI, and details of the important relationships between CIs.

CRAMM The CCTA Risk Analysis and Management Methodology. A software-supported method for identifying and justifying security measures for both current and future IT systems. The method provides assistance with risk assessment, and the identification of cost-effective controls (see risk management). The software package assists in recording review information, provides audit trails between recommended controls and related risks, and provides a "what if?" facility.

Cryptography The discipline that embodies principles, means and methods for the transformation of data in order to hide its information contents, prevent its undetected modification, and/or prevent its unauthorised use.

Customer The individual or organisation that buys a product or *service* (see *user*).

Cyberspace The virtual space created by the technology of computer systems enabling people to communicate with other users worldwide.

Data In computing, (1) a representation of facts, concepts, information, or instructions in a manner that is suitable for processing by an information system. (2) The building blocks of information.

Data dictionary In databases, a centralised repository of information about the stored data, providing details of its meaning, relationship (to other data), origin, usage and format.

Data file A file consisting of data in the form of text, numbers or graphics, as distinct from a program file containing commands and instructions. Data files may also be called documents or spreadsheets.

Database An extensive and comprehensive set of records collected and organised in a meaningful manner to serve a particular purpose.

UK Data Protection Act Legislation designed to protect the rights of individuals whose personal data are stored in either manual or computerised systems. Systems covered by the Act are those where (1) personal data is held (data relating to a living individual who can be identified from the data, or from the data and other information that the data user has access to. And (2), the files holding the data are structured in the same way. The Act contains a strict code of conduct, which includes an obligation to protect personal

data against loss, destruction, damage or disclosure. Both civil and criminal penalties can apply to contravention of the Act.

DBMS Database Management System. Software that handles database access requests from application processes. Essentially a DBMS handles storage, access, data sharing among multiple users, and database administration tasks (e.g. controlling what data an application user can view and update).

Decrypt In cryptography, to convert by use of the appropriate key, encrypted text (see ciphertext) into its equivalent plaintext.

Definitive Software Library DSL. A secure library where quality-controlled versions of all software CIs that have been accepted from the developer or supplier are held in their definitive form.

Device A generic term for printers, scanners, mice, keyboards, serial ports, video adapters, disk drives and other computer subsystems. Such devices frequently require their own controlling software, called device drivers.

Device driver A software component that permits the computer system to communicate with a device. Many devices, especially video adapters on microcomputers, will not work properly, if at all, without the correct device drivers installed in the operating system.

Digital certificate In cryptography, a message that guarantees the authenticity of the data contained within it. In public key cryptography it is important that anyone using a public_key can be sure about its authenticity. Such a guarantee may be issued by a Certification Authority trusted by the users, and based on assurances obtained from applicants for digital certificates. A certificate generally contains the public key owner's identity, the public key itself and its expiry date. A user supplies the certificate and the recipient decrypts it using the certification authority's public key (often performed automatically by the recipient's browser/e-mail software). The recipient gains assurance that a trusted authority has signed the user identity and corresponding public key.

Digital signature A data block appended to a file or message (or a complete encrypted file or message) such that the recipient can authenticate the file or message contents and/or prove that it could only have originated with the purported sender.

Document Information in readable form. The medium on which the document is held (e.g. paper, fiche, film and magnetic disk) is not important. See also record.

DSDM Dynamic Systems Development Methodology. A formal method for developing information systems quickly using RAD techniques.

Dump In computing, the act of copying raw data from one place to another with little or no formatting for readability. It usually refers to copying data from main memory to a display screen or a printer. Dumps are useful for diagnosing bugs. After a program fails, a dump can be used to analyse the contents of memory at the time of the failure.

EBCDIC Extended Binary Coded Decimal Interchange Code. Developed by IBM, and mostly used by mainframe systems, EBCDIC is a standard way of representing text symbols using binary numbers (see also ASCII).

E-business See electronic business.

E-commerce See electronic commerce.

E-government See electronic government.

EDI Electronic Data Interchange. In computing and communications, the transmission of documents from one computer to another over a network. Although EDI is sometimes carried out over direct links between trading partners (and increasingly the Internet), it is more usual to involve a value added supplier to operate an electronic mailbox through which documents are exchanged on a store and collect basis, similar to e-mail. The ability of communicating computer systems to exchange and process information in this way can significantly speed up processing and reduce manual transcription errors.

ESD Electronic Service Delivery. One or several systems that uses the network to provide information e.g. the e -mails system.

EFT Electronic Funds transfer. Systems designed to move funds between banks using electronic communications rather than paper media. Common EFT systems include BACS (Bankers' Automated Clearing Services) and CHAPS (Clearing House Payment System).

Electronic business Using an electronic network to simplify and speed up all stages of the business process including such as activities as design and manufacturing; buying, selling and delivering; and transacting government business.

Electronic commerce Using an electronic network to simplify and speed up the process of buying, selling and delivering.

Electronic government Using an electronic network to deliver government information to, and transact government business with other departments of state, citizens and businesses, and other governments.

Encryption (Also encipher). The process of transforming *information* into an unintelligible form in such a way that the original information cannot be obtained ("one-way" encryption) or cannot be obtained without using the inverse *decryption* process ("two-way" encryption).

Encryption algorithm A set of mathematically expressed rules implemented in either *firmware* or *software*, and used in conjunction with a *secret key* for *encrypting* plaintext and decrypting *ciphertext*.

End user computing Refers to the use of non-centralised (i.e. non-IT department) data processing using automated procedures developed by end-users, generally with the aid of *software packages* (e.g. spreadsheet and database) and enquiry *software*. End-user processes can be sophisticated and become an extremely important source of manage-

ment information. Whether they are adequately tested and documented may be questionable.

Error (1) In *IT Service Management*, a condition identified by successful diagnosis of the root cause of a *problem* when it is confirmed that a *CI* is at fault. (2) In *quality* management, any non-conformance between *software* and either its *specification*, design or implementation, or its behaviour as stated or implied by *users* and operations staff.
Error control In IT Service Management, the process of identifying, recording, classifying and progressing known errors. This includes the resolution phase until successful implementation of an amendment or replacement CI is confirmed.

ETHERNET A common LAN technology that employs CSMA/CD (carrier sense multiple access with collision detection) over either coaxial cable or twisted pair wiring. CSMA/CD allows computers to transmit when the network is free.

Facilities management In computing, the management, operation and support of an organisation's computers and/or networks by an external provider under a contract, and at agreed levels of service (see Service Level Agreement; outsource).

File A complete, named and collection of information. (1) In computing, a file can contain program code, data (e.g. transactions to be processed by a program), or user-created data (e.g. a word processor file). Most commonly, however, the term refers to data (numbers, words, or images) that a user has created and then saved for subsequent retrieval, editing or printing. (2) In information systems, a collection of documents. The medium on which the documents are stored (e.g. paper, fiche, microfilm, magnetic disks) is not important.

File server In a local area network (LAN), a computer that provides access to files for workstations that are connected to the network.

Firewall A security system used to prevent unauthorised access between networks (both internal/internal, and internal/external) by examining and filtering IP data packets. A firewall will allow only approved traffic in and/or out by filtering packets based on source/destination IP address, source/destination port. The firewall inspects the identification information associated with all communication attempts and compares it to a rule-set consistent with the organisation's security policy. Its decision to accept or deny the communication is then recorded in an electronic log.

Firmware Programming that is inserted into Programmable Read-Only Memory (PROM), thus becoming a permanent part of a computing device. Firmware is created and tested like other software. It can also be distributed like other software and installed in the PROM by the user. Firmware is sometimes distributed for printers, modems and other computer devices.

Fourth Generation Language (4GL). Any programming language that uses English terminology and allows rapid software development. With 4GLs the user specifies what is required and the programming language works out what actions are needed to carry out the required task. Structured Query Language (SQL) is a commonly used 4GL.

FTP File Transfer Protocol. In communications, a protocol that ensures the error-free transmission of program and data files via a data communications link.

Gateway A computer or other device that links two networks, routing and often converting protocols or messages from one network to the other. The term can also refer to a system capability that provides direct access to other remote networks or services.

Gigabyte (GB) 1,024 megabytes (2^{30} bytes). Often interpreted, though, as approximately one million bytes.

Hash total A figure obtained by some operations upon all the items in a collection of data and used for control purposes. A recalculation of the hash total, and comparison with a previously computed value, provides a check on the loss or corruption of the data.

Help Desk A focal point established for the purpose of providing first line incident support; help with using IT-based business systems; and management reporting on IT service quality. (Sometimes called a "service desk").

Host A computer connected to a network that offers services to one or more users.

Hot site In business continuity, a fully equipped computer installation designated for standby purposes. Data will need to be loaded; and software may need to be installed and configured.

HTML Hypertext Markup Language. The programming language used for web pages. It is called a "mark-up" language because it is used to describe the formatting to be used to display the document. The html file contains both the text and code (called tags). It is read by a web browser, which interprets the code and displays the web pages in the format specified by the HTML.

HTTP Hypertext Transfer Protocol is the set of rules for exchanging files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web. By comparison with the TCP/IP suite of protocols, which forms the basis of information exchange across the Internet, HTTP is an application protocol.

Hub A device that connects several devices (terminals, printers, etc.) to a network.

ICT Information and Communications Technology. The acquisition, processing, storage and dissemination of information using a combination of computer and telecommunications technologies.

Impact In information security, the damage to an organisation resulting from a threat exploiting a vulnerability. The business consequences may result from unauthorised disclosure of sensitive information; or modification or unavailability of information; or a combination of these impacts. Impact generally has financial implications, but depending on the circumstances and the nature of the information at risk, other consequences might be loss of credibility, contravention of the law, personal injury and/or loss of life (e.g. as in medical records, patient management and safety critical control systems).

Impact code A simple code assigned to incidents showing the extent of deterioration in normal user service levels. It is the major means of assigning priority for dealing with incidents.

Implement Install, utilise or bring into operation.

Incident An operational event that is not part of the normal operation of a system. It will have an impact on the system, although this may be slight or transparent to the users.

Incident control The process of identifying, recording, classifying and progressing incidents until affected services return to normal operation. Collection of data to identify causes of incidents is a secondary objective, although this may be necessary to effect incident resolution.

Information Knowledge that was unknown to the recipient prior to its receipt. Information is derived from data, which to be of value needs to be valid (e.g. not duplicated or fraudulent), complete, accurate, relevant and timely.

Information security The result of any system of policies and procedures for identifying, controlling and protecting information against unauthorised disclosure, manipulation, modification; unavailability and destruction. Unauthorised disclosure refers to information that is, for example, commercially sensitive, nationally classified or subject to data protection legislation. Manipulation is concerned with changing some attribute of the data, such as file ownership, security classification, destination, etc. Modification involves unauthorised alteration of the data itself, which can take place without leaving any trace. Unavailability refers to an inability to access and process the data (e.g. due to computer or communications failure). Data can be destroyed quickly and efficiently in electronic or magnetic storage devices (e.g. by degaussing, powering down volatile storage and overwriting).

Information security policy A formal statement that defines top management intentions on information security, and provides general direction for protecting the confidentiality, integrity and availability of corporate information.

Information system The means for organising, collecting, processing, transmitting, and disseminating information in accordance with defined policies and procedures, whether by automated or manual means.

Integrity In information security, the property that information is valid, complete and accurate.

Internet A worldwide system of linked computer networks that enables data communication services (based on TCP/IP) such as remote logon, file transfer, electronic mail, and newsgroups. The Internet is not a discrete computer network, but rather a way of connecting existing computer networks that greatly extends the reach of each participating system. It is not single service, has no real central hub, and is not owned by any one group.

Intranet A private network inside an organisation that uses the same kinds of software and protocols found on the Internet. Intranets may or may not be connected to the Internet.

Top-down-based audit approach A top-down approach is based on a general review - carried out in one organisation - which has no predefined audit objectives. The auditor often starts by interviewing top management to obtain a more specific understanding of organisation-related problems. The auditor then defines audit objectives based on this information.
This guide can be a useful help when accomplishing these specific audit goals. The auditor first defines the overall entity area, and then relates the identified problems to current activities.

IP Internet Protocol. A protocol that defines and routes data across the Internet. It uses packet switching and makes a best effort to deliver its packets (see also TCP/IP).

IP address Every computer on the Internet is assigned a unique number so it can be identified. IP addresses are 4 dot-separated numbers (for example, 205.243.76.2) that specify both the network the computer is connected to and the host.

ISDN Integrated Services Digital Network. A medium speed, digital connection. It provides up to 128kbps bandwidth over two channels. Like normal phone lines, it has a number that can be dialled into and it can dial out to any other ISDN number, unlike leased lines, which are strictly point-to-point. Like leased lines, ISDN provides a reliable digital service that is not normally affected by line noise and other ailments that modems can experience.

ISO International Standards Organisation. An agency of the United Nations concerned with international standardisation across a broad field of industrial products. An example of an ISO standard against which some audit clients (or their external providers) are formally certified is that governing quality management systems, ISO 9001.

IS Strategy An organisation's master plan for directing, developing, installing and operating the information systems necessary to satisfy its business needs. An IS strategy should be supported by a business case to provide purpose and economic justification for what is proposed. It should also include measurable performance targets and deadlines against which its success can be monitored. Due to the delay generally involved in bringing new IT infrastructure into operation, an IS strategy usually covers a three to five year planning period. It should, however, be monitored and updated frequently to ensure that it continues to represent an effective and workable plan. See IS Steering Committee.

IT infrastructure The hardware, software, computer-related communications, documentation and skills that are required to support the provision of IT services, together with the environmental infrastructure on which it is built.

IT infrastructure management The processes that are required to manage an IT infrastructure. They comprise processes covering service management, hardware and software release, incident and problem resolution, customer and supplier management, and overall control of assets (see change and configuration management).

IT service (1) In IT Service Management, an operational IT service comprises the IT infrastructure necessary to provide a designated group of users or customers with access

to one or more designated applications, generally within the terms of a service level agreement. (2) In computing, the provision of data processing facilities.

IT service management Sometimes shortened to "Service Management", is the totality of (a) IT service provision and (b) IT infrastructure management (the term is synonymous with "IT systems management" and "IT Service Delivery").

IT Steering committee An organization's senior management should appoint a planning or steering committee to oversee information systems department activities. The planning or steering committee membership should include representatives form senior management, the information systems department and user department management.

Java A programming language, similar to C++, created by Sun Microsystems for developing that are capable of running on any computer regardless of the operating system.

Key In cryptography, a symbol or sequence of symbols that controls the operations of encryption and decryption. It is essential that keys are protected against unauthorised disclosure.

Known error In IT Service Management, a condition identified by successful diagnosis of the root cause of a problem when it is confirmed that a CI is at fault.

LAN Local Area Network. A network that connects PCs and other computers within a limited geographic area by high-performance cables so that users can exchange information, share expensive peripherals, and draw on the resources of a massive secondary storage unit, call a file server. See also WAN.

Lights out operating Sometimes known as "darkroom" operating, is where the computer room is not staffed, but people are available to control the system via one or more terminals or consoles connected to the system, often as part of an Operations Bridge.

Log In computing, a record (or "journal") of a sequence of events (1) relating to the jobs run through a computer. Job logs generally contain chronologically listed information on when jobs start and end, the resources they access (and whether or not access was successful), together with any messages generated from within the applications that are running. (2) A chronological record of the activities performed (or attempted) by individuals when using a computer system.

Logical In computing, conceptual or virtual (i.e. within the computer; in cyberspace), as compared with physical or actual (i.e. outside the computer; real world).

Logical access The act of gaining access to computer data. Access may be limited to "read only", but more extensive access rights include the ability to amend data, create new records, and delete existing records (see also physical access).

Login The act of connecting to a computer and being authenticated as a legitimate user. The usual requirements are a valid user name (or user ID) and password, but in higher risk scenarios a user may also have to insert a physical token (e.g. a smartcard) and/or provide biometric proof of identity.

Mainframe A high-level computer designed for the most intensive computational tasks. Mainframe computers are often shared by multiple users connected to the computer by terminals.

Macro A macro is a list of actions to be performed that is saved under a short key code or name. Software can then carry out the macro's instructions whenever the user calls it by typing its short key code or specifying the macro name.

Media The physical material, such as paper, disc and tape, used for storing computer-based information.

Memory Memory generally refers to the fast semiconductor storage (Random Access memory, or RAM) directly connected to the processor that is dependent on electrical power for activation. Memory is often differentiated from computer storage (e.g., hard disks, floppy disks, CD-ROM disks) that is not dependent on electricity and is therefore a more permanent means for holding data.

Memory chip Or "chip", is an integrated circuit devoted to memory storage. The memory storage can be volatile and hold data temporarily, such as RAM, or non-volatile and hold data permanently, such as ROM, EPROM, EEPROM or PROM.

Message In data communications, an electronic communication containing one or more transactions or one or more items of related information.

Message header The additional information attached to e-mail messages that provides information about the e-mail; who sent it, where it came from, what path it took, when it happened.

Messaging Also called electronic messaging, is the creation, storage, exchange, and management of text, images, voice, telex, fax, e-mail, paging, and EDI over a communications network.

MICR Magnetic Ink Character Recognition. A technique for the identification of characters printed with ink that contains particles of a magnetic material. Used widely in the banking industry to capture sort codes and account numbers on cheques.

Microprocessor A central processing unit (CPU) on a single microchip. A microprocessor is designed to perform arithmetic and logic operations that make use of small number-holding areas called registers. Typical microprocessor operations include adding, subtracting, comparing two numbers, and moving numbers from one area to another. These operations are the result of a set of instructions that are part of the microprocessor design. A modern microprocessor can have more than one million transistors in an integrated-circuit package that is roughly one inch square. Microprocessors are at the heart of all computers, from mainframes down to smartcards.

Middleware Software that is neither part of the operating system, nor an application. It occupies a layer between the two, providing applications with an interface for receiving services. Common examples are communications programs and transaction processing monitors.

Modem A communications device that enables a computer to transmit information over a standard telephone line. Because a computer is digital (it works with discrete electrical signals representing binary numbers 1 and 0) and a telephone line is analogue (carries a signal that can have any of a large number of variations), modems are needed to convert digital to analogue and vice versa. The term is short for MOdulator/DEModulator.

Multiplexor Equipment that takes one or more data channels and combines the signals into one common channel for transmission. At the receiving end a demultiplexor extracts each of the original signals.

Network A computer-based communications and data exchange system created by physically connecting two or more computers. The smallest networks, called local area networks (LAN's), may connect just two or three computers so that they can share an expensive peripheral, such as a laser printer, but some LAN's connect hundreds of computers. Larger networks, call wide area networks (WANs), employ telephone lines or other long-distance communications media to link computers.

Network Control Terminal In computers, a terminal (sometimes qualified as a "dumb" terminal) is an end-use device (usually with display monitor and keyboard) with little or no software of its own that relies on a mainframe or another computer (such as a PC server) for its "intelligence." A network control terminal is an ordinary terminal but it is used for network controls.

Node In a LAN, a connection point that can create, receive, or repeat a message. Nodes include repeaters, file servers, and shared peripheral devices. In common usage the term node often relates to a workstation or terminal.

Object (1) In computer security, a passive entity that contains or receives information. For example, records, files, programs, printers, and nodes. (2) In object-oriented programming, an entity that encapsulates within itself both the data describing the object and the instructions for operating on those data.

Objective A desired goal, or end result.

OCR Optical Character Recognition. Techniques and equipment for reading printed, and possibly hand-written, characters on a document and converting them to digital code (e.g. ASCII) for input to a computer.

Off-the-shelf A packaged item ready for sale. The term can refer to hardware, software or both.

On-line Generally describes a computer that is connected to a network and is thereby ready for operation or interaction over the network. It may also refer to the ability to connect to the Internet by virtue of having an Internet account.

Operations bridge The combination in one physical location of computer operations, network control and the Help Desk.

Operating system In computing, a collection of software designed to directly control the hardware of a computer (e.g. input/output requests, resource allocation, data

management), and on which all other programs (including application programs) running on the computer generally depend.

Organisation See business.

Output controls Controls whose objectives are to ensure that computer outputs are complete and accurate, are securely held until distribution (they may include financial instruments), and are distributed to the intended recipient(s) in a timely manner.

Outsource The use of an external contractor to provide (1) both the IT systems and the personnel required to run them (see also facilities management). (2) support services, such as hardware maintenance.

Package release In IT Service management, a set of software that is CIs that are tested and introduced into the live environment together.

Packet (Sometimes referred to as a 'frame') in communications, a packet comprises a well-defined block of bytes consisting of 'header', 'data' and 'trailer'. Packets can be transmitted across networks or over telephone lines. The format of a packet depends on the protocol that created it. Various communications standards and protocols use special purpose packets to monitor and control a communications session. For example, the X.25 standard uses diagnostic, call clear and reset packets (among others), as well as data packets.

Packet switching A transmission method in which packets are sent across a shared medium from source to destination. The transmission may use any available path or circuit, and the circuit is available as soon as the packet has been sent. The next packet in the transmission may take a different path, and packets may not arrive at the destination in the order in which they were sent.

Password In Access Control, confidential authentication information, usually composed of a string of characters, that may be used to control access to physical areas and to data.

Patch A piece of programming code that is added to an existing program to repair a deficiency in the functionality of an existing routine or program. It is generally provided in response to an unforeseen need or set of circumstances. Patching is also a common means of adding a new feature or function to a program until the next major version of the software is released.

PD0005 A Code of Practice for IT Service Management. A guide published by the *BSI*, that is designed to provide advice and recommendations for *IT service management*. The subjects dealt with include managing incidents, *problems*, *system* configuration and system *change*.

PD0008 A Code of Practice for Legal Admissibility and Evidential Weight of Information Stored electronically. A BSI guide on the management of systems in which original paper documents are scanned to form electronic images. The object is to ensure that the images so formed may be regarded as authentic, for example in a court of law or by external regulators or auditors.

Phreaking In communications security, fraudulent use of a telephone system to make calls at the expense of another. Cases brought under English law are prosecuted under the Theft Act.

Physical access In Access Control, gaining access to physical areas and entities (see logical access).

Platform The computer hardware, and the associated operating systems software necessary for its operation, on which applications software is run.

Policy A formally stated course of action to be followed for achieving an objective (see strategy).

Post Implementation Review (PIR) Verification of the stated implementation objectives.

PRINCE 2 Prince (PRojects IN Controlled Environments) is a structured method for effective project management. It is a de facto standard used extensively by the UK Government and is widely recognised and used in the private sector, both in the UK and internationally. Prince, the method, is in the public domain, offering non-proprietorial best-practice guidance on project management. Prince® is, however, a registered trademark of CCTA.

Private key See secret key.

Problem In IT Service Management, a condition identified from multiple incidents that exhibits common symptoms. It can also arise from a single significant incident that suggests a single error for which the cause is unknown.

Problem control In IT Service Management, the process of identifying, recording, classifying and progressing problems through investigation and diagnosis until either known error status is achieved, or an alternative procedural reason for the problem is revealed.

Problem management In IT Service Management, a generic term used to identify the combined processes of incident, problem and error control, complemented by the utilisation of associated management information. The primary objective is to make sure that services are stable, timely and accurate.

Procedure A set of instructions for performing a task. Procedures should be consistent with policy requirements.

Process In IT Service Management, a sequence of operations that are intended to achieve a defined objective. Processes require policy, people, procedures and IT infrastructure.

Processing controls Controls whose objectives are to ensure that only valid data is processed, and that processing is both complete and accurate.

Program In computing, a series of instructions that conform to the syntax of a computer language, that when executed (or "run") on a computer will perform a given task.

Programme A group of projects. The projects that comprise a "programme" are selected and planned in a co-ordinated way so that, overall, they serve to implement a business strategy. Sometimes a large, complex project is described as a programme.

Project A temporary management environment, set up to deliver a specified business product in accordance with a defined business case.

Project Evaluation Review (PER) Project evaluation is a definite assessment of an on going or a finished project, program or policy, -aiming to be as systematic and objective as possible when it comes to design, implementation and results. The purpose is to judge the objective achievement, the efficiency, the level of influence in the organization and the sustainability. Project evaluation should communicate credible and useful information providing experience for both users and donors.

Project Support Office A central support unit that provides a planning and monitoring service to project boards and project managers.

Protocol A set of rules that must be followed for any data communications to be made. Protocols enable totally different platforms (e.g. computers connected to the Internet) to communicate with each other. For one computer to communicate with another, both must adhere to the same protocol(s).

Public key In cryptography, the key, in an asymmetric encryption system, of a user's key set that is known to other users.

Quality The attributes of a product or service that make it fit for its intended use. The term also embraces "value for money", which in turn implies a "satisfied customer".

Query In computing, a specific set of instructions for extracting particular data from a database.

RAD Rapid Application Development. An approach to system development that aims to speed up the development process. RAD focuses on core business requirements to the exclusion of inessential items (the 80/20 rule), and makes extensive use of the construction of models and prototype systems in place of formal system analysis and specification. It also makes extensive use of CASE (see also DSDM).

RAM Random Access Memory. Semiconductor-based memory that can be read and written by the central processing unit (CPU) or other hardware devices. The term is generally understood to refer to volatile memory that does not permanently hold data or programs.

RDBMS – Relational Database Mmanagement System. A relational database allows the definition of data structures, storage and retrieval operations and integrity constraints. In such a database the data and relations between them are organised in tables. A table is a collection of records and each record in a table contains the same fields. Certain fields may be designated as keys, which means that searches for specific values of that field will use indexing to speed them up.

Reciprocal agreements This is an agreement between two or more organizations with similar equipment or applications. Under the typical agreement, participants promise to provide computer time to each other when an emergency arises.

Record (1) In computing, a collection of related data treated as a unit. A record is the main unit of storage within a file. (2) In record management, anything that provides permanent evidence of, or information about past events. Although the term document includes records, records are particular types of document that are not subject to amendment, and for which there is often a legal or contractual requirement.

Redundant circuits Completely Connected (Mesh Configuration) can be an example of a redundant circuits network. A Mesh configuration is at network topology in which devices are connected with many redundant interconnections between network nodes (primarily used for backbone networks.)

Regression testing Testing undertaken to prove that a change introduced to a system does not affect the way in which the remainder of the system performs.

Relational database A type of database in which data is organised as a collection of two-dimensional tables. Microsoft Access and ORACLE are examples of widely used relational database systems.

Release In IT Service Management, a CI that is introduced into the test, and subsequently the live environment. In most cases a release will also include documentation and possibly hardware as well (see also updates and upgrades).

Release (Delta) A delta release does not replace all component CIs of a release unit, but rather includes only those CIs that have changed since the last version of the software.

Release (Full) A full release replaces all components of a release unit, regardless of whether or not they have changed since the last version of the software.

RFC Request For Change
(1) In IT Service Management, a form or screen, used to record details of an RFC to any component of an IT infrastructure or any aspect of an IT service. Generally forms the basis of authorisation for the change to take place and as such is an important audit trail item. Although rarely viewed as such, requests to introduce new users; alter the access permissions of existing users; and delete accounts are also examples.
(2) **Request For Comment** on a specification.

Risk In information security, the potential that exists for damage or unwanted consequences to arise from a threat exploiting a vulnerability to cause an impact. Risk management strategies aim to reduce risk to an acceptable level by implementing controls designed to reduce threat, vulnerability or impact, or a combination of these.

Risk assessment In information security, a study of the threats (and their likelihood), vulnerabilities and potential impact, and the theoretical effectiveness of controls. The results of risk assessment are used to develop security requirements and specifications.

Risk management In information security, the total process involved in reducing identified risks to a level that is acceptable to an organisation's top management.

Rollback In databases, a technique employed to protect a database against incorrect user action. The state of the database is preserved and subsequent transactions stored. If the user decides to implement the total set of transactions a commit command is issued. If the rollback command is employed the transactions are aborted and do not affect the database.

ROM Read-Only Memory. A semiconductor circuit into which code or data is permanently installed by the manufacturing process. ROM contains instructions or data that can be read or executed, but not modified.

Script A simple program consisting of a set of instructions that are designed to perform or automate a task or function.

Secret key In cryptography, the key of a user's key set in an asymmetric or public key cryptographic system, which may be known only to that user.

Server A computing unit or node in a network that provides specific services to network users, e.g. a printer server provides printing facilities to the network, and a file server stores users' files.

Service Performance of a specified function. See also IT service.

Service Level Agreement Or **SLA**, is a written agreement between a user and an IT service provider that documents the agreed service levels for an IT service (e.g. hours of operation, maximum downtimes, transaction throughput, terminal response times, security, contingency). An SLA is not normally a contract in itself, but it may form part of a contract.

Severity code In IT Service Management, a simple code assigned to problems and errors to indicate the seriousness of their effect on the quality of an IT service. It is the major means of assigning priority for resolution.

Smartcard A plastic card (of identical dimensions to a credit card) that has electronic logic embedded in it in the case of a stored data card, or a microprocessor in the case of cards with processing ability. Smartcards are commonly used to perform digital signatures, authenticate users for access control purposes, and encrypt or decrypt messages.

SMTP Simple Mail Transport Protocol. The protocol that is used to move e-mail and any attachments between mail servers.

Software Instructions for the computer. A series of instructions that performs a particular task is called a program. The two main types of software are system software (operating system), which controls the workings of the computer and application programs, which perform the tasks for which people use computers. A common misconception is that software is data. It is not. Software tells the hardware how to process the data. Software is "run" (or "executed"), whereas data is "processed."

Software package A software program or application sold to the public, ready to run, and containing all necessary components and documentation. Also called "shrink wrapped" or "off-the-shelf" software.

Software maintenance Any modification to a software product after delivery to correct faults, to improve performance or other attributes, or to adapt the product to a changed environment.

Specification A detailed description of the requirements for a product or service.

Spoofing In Information Security, (1) assuming the characteristics of another computer system for purposes of deception. (2) Malicious code that masquerades as the operating system, presenting a login screen and tricking the user into revealing their password.

SQL Structured Query Language, the traditional language for accessing data stored in a relational database.

Standard Agreed, and generally widely recognised criteria, against which a product or service may be evaluated. See ISO and BSI.

Strategy A detailed and systematic plan of action (see also IS strategy).

Superuser A user with unrestricted access to user files and system utilities. For reasons of security, this level of access should only be granted to the minimum number of staff necessary to perform system administration duties.

Symmetric encryption A form of data encryption algorithm that employs the same value of key for both encryption and decryption processes.

System Any collection of components that work together to perform a task. Examples are a hardware system consisting of a microprocessor, its allied chips and circuitry, input and output devices, and peripheral devices; an operating system consisting of a set of programs and data files; a database management system used to process specific kinds of information; or an application system used to perform a particular business function.

System Development Life Cycle (SDLC). is the process of developing information systems through investigation, analysis, design, implementation, and maintenance.

System Interoperability Framework Interoperability is the ability of a system or a product to work with other systems or products without special effort on the part of the customer. Interoperability becomes a quality of increasing importance for information technology products, as the concept that "The network is the computer" becomes a reality. For this reason, the term is widely used in product marketing descriptions. System Interoperability Framework is a tool in how to handle this interaction between different systems.

System Owner Management should ensure that all information assets (data and systems) have an appointed owner who makes decisions about classification and access rights. System owners typically delegate day-to-day custodianship to the systems delivery/ operations group and delegate security responsibilities to a security administrator.

Owners, however, remain accountable for the maintenance of appropriate security measures.

System software Software primarily concerned with co-ordinating and controlling hardware and communication resources, access to files and records, and the control and scheduling of applications (see also operating system).

TCB Trusted computing base. In Information Security, the totality of protection mechanisms within a computer system (including hardware, firmware and software) the combination of which is responsible for enforcing a security policy.

TCP/IP Transmission Control Protocol/Internet Protocol. A set of protocols that make Internet services (Telnet, FTP, e-mail, etc.) possible among computers that don't belong to the same network.

Telephone call centre See call centre.

Test environment A computer system or part of a computer system (made up of hardware and system software), which is used to run, and sometimes to build, software releases for acceptance testing.

Test data In computing, data prepared solely to test the accuracy of the programming and logic of a system. It is used to prove each branch and combination of branches (within feasible limits) of a system and should, therefore, be as comprehensive as possible.

Threat In Information Security, actions and events that may jeopardise a system's objectives (see vulnerability and impact).

Transaction A discrete activity within a computer system, such as an entry of a customer order or an update of an inventory item. Transactions are usually associated with applications.

Trapdoor A hidden hardware or software mechanism that permits access controls to be bypassed. Trapdoors often inserted by system developers as a convenient means of testing computer programs and diagnosing bugs.

Trojan Horse In Information Security, an apparently useful program that performs unauthorised functions by taking advantage of an innocent user's access rights in order to copy, misuse or destroy data. For example, a Trojan Horse hidden in a text editor might covertly copy sensitive information contained in a file being edited to another file that is accessible by the attacker (see also Virus and Worm).

Uninterruptible Power Supply (UPS) An uninterruptible power supply (UPS) is a device that allows your computer to keep running for at least a short time when the primary power source is lost. It also provides protection from power surges. An UPS contains a battery that "kicks in" when the device senses a loss of power from the primary source. If you are using the computer when the UPS notifies you of the power loss, you have time to save any data you are working on and exit gracefully before the secondary power source (the battery) runs out. When all power runs out, any data in your

computers Random Access Memory (RAM) is erased. When power surges occur, a UPS intercepts the surge so that it doesn't damage your computer.

UNIX A highly portable, general purpose, multi-user operating system, generally used on small and mid-range computers (versions are also available for PCs). There is many common features between the numerous commercial versions of UNIX. UNIX provides facilities for sharing resources (disc space, CPU time, etc.) and for protecting users' files. For each file users can allocate individual read, write and execute privileges to themselves, members of groups and all other users. The operating system is also multitasking, which allows users to relegate programs that require no interaction to background processing whilst working interactively on other tasks.

Update A new release of an existing software product. A software update usually adds relatively minor new features to a product or addresses issues found after the program was released. Updates can be indicated by small changes in the software version numbers, such as the change from version 4.0 to version 4.0b.

Upgrade The new or enhanced version of a software product that is considered to have major enhancements or improvement to its features or functionality. Software upgrades are typically indicated by a significant (integer) change in the version number, such as from version 4.0 to version 5.0.

URL Uniform Resource Locator. A uniform method where a host can be accessed at a specific address using a specific protocol. An example is http://www.nao.gov.uk/, the URL for the UK National Audit Office.

User The individual or organisation that puts an IT service to productive use (see also customer).

User profile In Information Security, a list of an individual's access rights, or of the access rights of a group of people who share common business needs. Access may be to physical areas, such as buildings or rooms within them, or to data held within a computer system (see also physical access and logical access).

Utility program Software designed to perform maintenance work on a system or on system components (e.g., backing up data; disk and file recovery; editing; sorting and merging; file and memory dumps).

Version A particular issue or *release* of a hardware or *software* product. Version numbers are generally represented by an integer (a whole number) combined with a decimal number (for example 3.2). Successive releases of a *program* are assigned increasingly higher numbers. Major releases are reflected with whole number increments; minor releases with decimal increments. When discussing software versions, an "x" is often used after the version integer to designate a range of minor releases. For example, Internet Explorer 5.x refers to all minor releases of Internet Explorer 5.

Virus A computer program designed to carry out unwanted and often damaging operations. It replicates itself by attaching to a host, which depending on the type of virus, may be a program, macro file or magnetic disc. In common with a human virus, the effects of a computer virus may not be detectable for a period of days or weeks during

which time the virus will attempt to spread to other systems by infecting files and discs. Eventually, the effects manifest themselves when a date or sequence of events triggers the virus. Impacts range from prank messages to erratic system software performance, even catastrophic erasure of all the information on a hard disc.

Virtual Private Network A VPN is a private data network, but one that uses the public telecommunication infrastructure, such as the Internet. It is similar in concept to a system of owned or leased lines, but provides comparable capabilities at much lower cost by using shared rather than private infrastructure. Using a virtual private network involves encrypting data before sending it through the public network and decrypting it at the receiving end. An additional level of security involves encrypting not only the data but also the originating and receiving network addresses. VPN software is typically installed as part of the organisation's firewall server.

Volatile In data storage, a term used to describe any device that needs to be powered on in order to function. Most microchip storage technologies are volatile, compared with optical and magnetic storage devices which are non-volatile (although considerably slower to access).

Vulnerability In Information Security, a weakness or flaw (in location, physical layout, organisation, management, procedures, personnel, hardware or software) that may be exploited by a threat to cause an impact.

Warm site In business continuity, a site that is fully equipped with environmental and ancillary equipment, and partly equipped with computer hardware (generally the less expensive components).

Web browser Or web client, is software designed to navigate the WWW, view its information resources and, when used interactively, exchange information. Netscape Navigator and Internet Explorer are widely used examples of web browsers.

Web server An Internet host computer that stores web pages and responds to requests to see them. Web servers talk to web browsers by using a language named HTTP.

Web site A location on the World Wide Web (WWW). It is synonymous with web page and web server.

Web page The basic building block of the World Wide Web (WWW). Information displayed on a web page can include highly sophisticated graphics, audio and video, the locus of contemporary creativity. Web pages are linked together to form the WWW.

Wide Area Network (WAN) - a telecommunications network that is dispersed over a wide geographic area – possible world wide - as distinct from a local area network (LAN) that is generally confined to a confined geographic area, such as a building. A wide area network may be privately owned or rented; either way it usually requires the use of public (shared user) networks (e.g. the Internet) and/or leased communication circuits. See also VPN.

Windows NT Often referred to as "NT", is the high-end member of a family of operating systems from Microsoft. It is a completely self-contained with a built-in graphical user interface. NT is a 32-bit, multitasking operating system that features networking, symmetric multiprocessing, multithreading and security. It is a portable operating system that can run on a variety of hardware platforms including those based on the Intel 80386, i486 and Pentium microprocessors and MIPS microprocessors; it can also run on multiprocessor computers. NT supports up to 4 gigabytes of virtual memory and can run MS-DOS, POSIX, and OS/2 (character-mode) applications. Authentication checks are made during the login process (which uses a secure communications channel) and also during network operations (e.g. when a user or process needs access to a service).

Workstation This term tends to have different meanings in different contexts. Generally it refers to a high-powered microcomputer, such as a SPARC workstation and other typically single-user but very powerful machines, often running the *UNIX operating system*.

Worm (1) In communications, a malicious program which, unlike a virus, is free-standing (i.e. it does not require a host). Worms replicate themselves across networks, cause both traffic congestion and can cause network failure. (2) In computing, Write Once Read Many **(WORM)**. A data storage device to which code or data can be written but not altered or erased. They are generally implemented on non-rewritable optical discs, although pseudo-WORM magnetic tape devices are becoming available.

WWW - World Wide Web. Refers to the information resources of the Internet that are accessible via web pages using a web browser. Technically speaking, the WWW refers to the abstract cyberspace of information whereas the Internet is the physical side of the network, i.e. the computers and communications that link computers throughout the World.

XML Extensible Markup Language, is a set of tags and declarations used as a complement to HTML in the construction of web pages.

X.25 A common communication standard for the transfer of information between terminals operating in the packet mode.

X.400 A communication standard for message handling systems (e.g. e-mail).

X.500 A standard for the storage and retrieval of directory information about hosts and users of distributed systems.

Reference Library

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

Information Systems Audit and Control Association, Norway and Den Norske Dataforening: *Anbefaling til God IT-skikk (Recommendations for Best practice on IT)1999*

Information Systems Audit and Control Foundation: *COBIT 3rd Edition*

Warren, Edelson, Parker: *Handbook of IT Auditing 1997 Edition.*

Weber, Ron : *Information Systems Control and Audit, 1999*

Laudon & Laudon: *Management Information Systems, 6th Edition*

Other Reference material:

The IS Management Handbook at http://www.ccta.gov.uk/ , See also http://www.ccta.gov.uk/itil/

British Computer Society – Information Systems Examination Board. – Certificate in IT Service Management

http://www.bcs.org.uk/iseb/index.htmlSNAO 1987: System Maintenance (Systemförvaltning)

Anderson, Bengt E. W.: *Samvärkande informastionssystem mellan aktörer i offentliga åtaganden - en teori om aktörsarenor i samverkan om utbyte av information. Linköpings Universitet FiF 25, 1998*

SNAO 1987: EDP Security (ADB-säkerhet)

SNAO 1991: EDP Systems in Co-operation (ADB i samverkan)

SNAO 1992: Wrong Data Costs! (Fel Data Kostar!)

SNAO 1993:34: Public Administration Agencies and IT (Myndigheterna och informationsteknologien)

SNAO 1994:31: Better Performed IT Projects (Bättre ADB-projekt)

SNAO 1995:59: Information Exchange and Use of IT in the Area of Environment Protection (Informationssamverkan och IT-användning inom miljöskyddet)

SNAO 1996:23: Public Administration Control over the Health Care (Statens tillsyn över hälso- och sjukvården)

SNAO 1997:19, 42: Register Based (Registerbaserad Folk- och bostadsräkning)

SNAO 1997: 51: Better Performed IT System Maintenance (Bättre systemförvaltning)

SNAO 1998: IT Projects in the Public Administration (IT-projekt i staten)

SNAO 1999: Auditing the Y2k Preparations in Public Administration

SNAO 2000: IT Projects in the Public Administration (IT-projekt i staten)

Working group and contact persons

The report draft is made by a working group with members from United Kingdom, Sweden and Norway. Among others the following persons have been involved:

Project coordinator Bernt Nordmark, Deputy Director General, Office of the Auditor General of Norway (OAG), e-mail: bernt.nordmark@riksrevisjonen.no

Beate Setnes, Audit Adviser, OAG, e-mail: beate.setnes@riksrevisjonen.no

Steve Doughty, IT Director, National Audit Office (NAO), United Kingdom, e-mail: Steve.DOUGHTY@nao.gsi.gov.uk

Bengt E W Andersson, Audit Director, Performance Audit Department, Swedish National Audit Office (RRV), e-mail: Bengt.Andersson@rrv.se