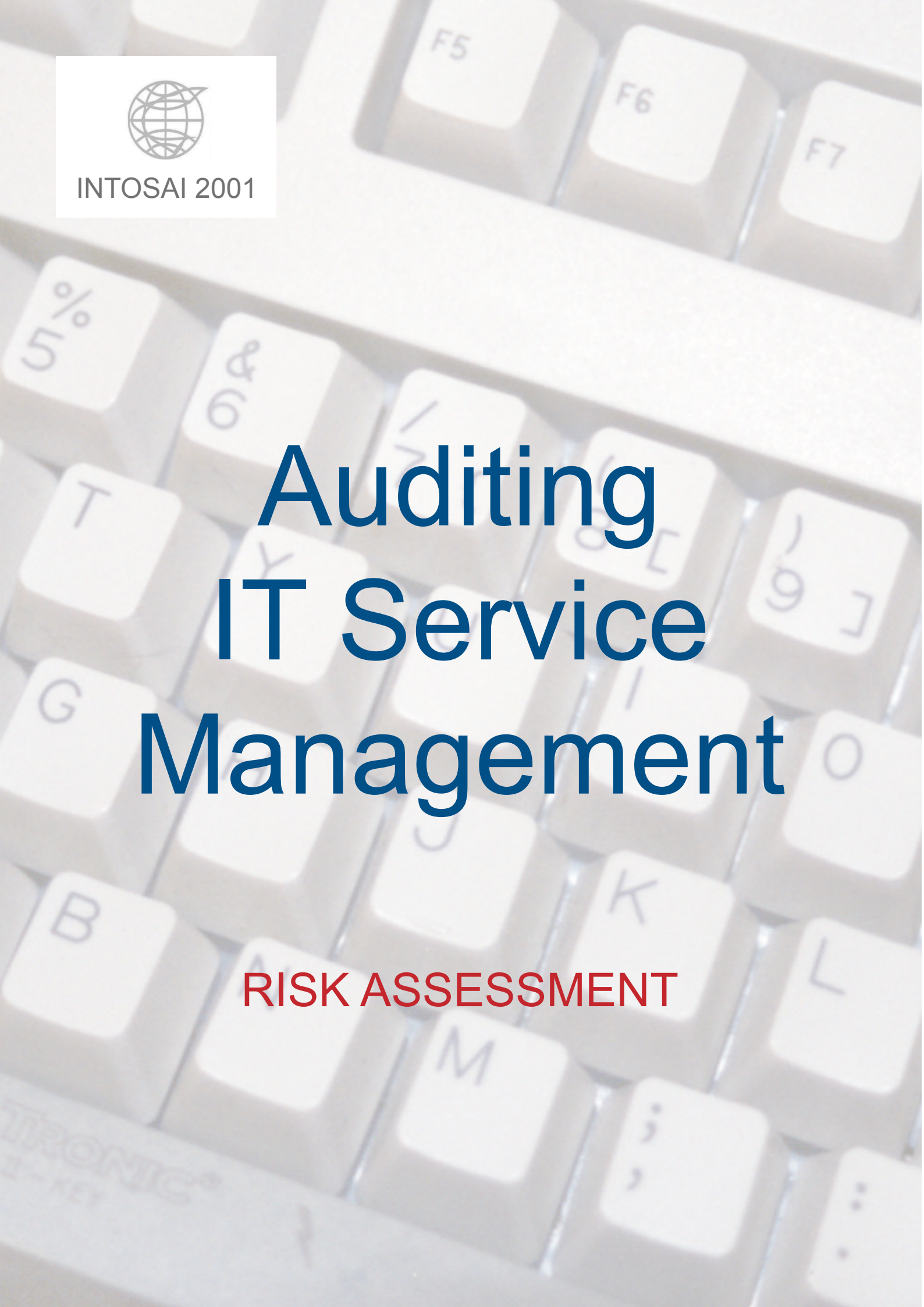


INTOSAI 2001

Auditing IT Service Management

RISK ASSESSMENT

Preface

The IT Infrastructure Management Project was initiated by INTOSAI Standing Committee on IT Audit at its 8th meeting in October 1999. The committee stated a need for an audit tool focusing on the overall management of IT infrastructure in public administrations. The project have been co-ordinated by the Office of the Auditor General of Norway with the SAIs of the United Kingdom, Sweden, Japan, Canada and Russia as project members.

The main objective of the project, as in the project charter has been to provide an efficient and effective process for auditing IT infrastructure management, with an aim to be useful at several levels of IT infrastructures. To comply with this objective the project group has found it suitable for this purpose to make guidelines built on a model concerning the audit of IT service management, including IT infrastructure management.

On behalf of the project group we hope you will find the guidelines userfriendly.

Office of the Auditor General of Norway, October 2001

Auditing IT Service Management

Table of contents

I
Introduction

Electronic business

Both private and public sector organisations are increasingly exploiting data networks to provide more efficient and customer-focused means of transacting business. This applies not only to inter-business relationships, but also increasingly to business to customer relationships.

The term "electronic commerce" (e-commerce) generally applies to the use of a data network for buying and selling. "Electronic business" (e-business) has much wider meaning. It may be defined as….

> *using a data network to simplify and speed up all stages of the business process. These include, for example, design and manufacturing; buying, selling and delivering;* ***and transacting government business such as applying for a passport, registering a motor vehicle and submitting a tax return.***

The exploitation of e-business technologies can no longer be regarded as merely a means of gaining competitive edge; its effective use in business has become an imperative. The implications are clear. Organisations need to pay far greater attention than in the past to the provision and management of the IT services on which their businesses rely. Without IT services most organisations cannot function; without quality services they cannot function well.

About this guide

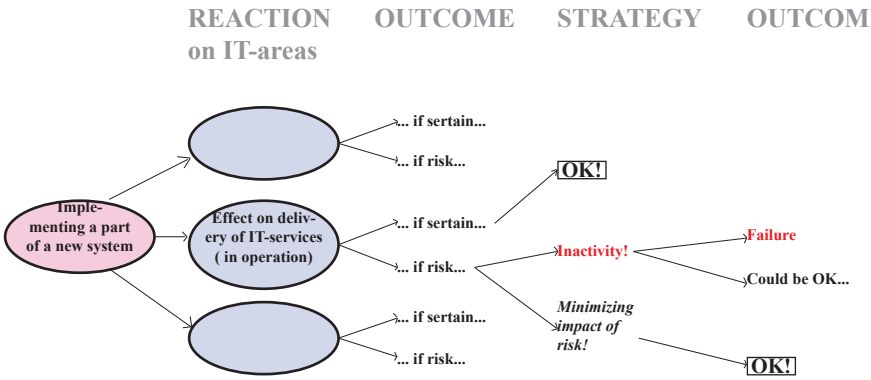
Information technology (IT) can significantly contribute to improvements in business effectiveness – *including the business of government* - but it is not always applied in the most appropriate or effective way. It is often difficult to determine which technologies are most relevant to business needs, whilst the full implications and risks associated with the various options may not always be clear. These problems can be made worse where there is a failure to communicate business needs effectively to technical advisors.

What is needed is a common understanding of business needs, of existing processes and the way technology supports them through the organisation together with a migration path designed to move the organisation forwards from where it is to where it wants to be (a "strategic plan"). Promoting a common understanding will involve consultation, defining policies and strategies to meet business needs, communicating them to relevant parties, monitoring their effectiveness and maintaining them in the light of experience and of business change.

This guide describes the policies, strategies and management frameworks that organizations should consider developing to support the delivery of quality IT services to their customers, regardless of whether these are internal or external (e.g. citizens) to the business. It also represents a tool for assisting in the audit of IT service management in public administrations based on risk assessment and risk management principles. *Several audits have attributed one of the main reasons for IT service failure to a lack of risk awareness*.

Example and basic terminology definitions

Where a new system is integrated into an existing network, the change could easily lead to unwanted impacts on IT service delivery. In this case, we assume impacts on the *"in operation"* area.



In order to comprehend the contents of this guide there are two keywords that need to be understood, **IT** and **RISK.**

INFORMATION TECHNOLOGY (IT)

IT is a term that encompasses all forms of technology that are used to create, store, exchange, and process information in its various forms. IT includes:

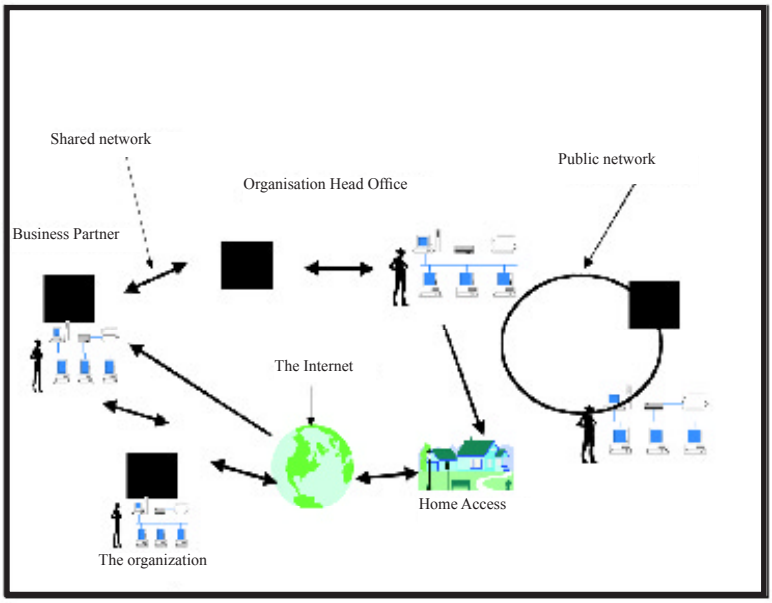
- Computer hardware (Processors, Input/Output devices etc.);
- Computer software (Operating systems etc.);
- Data;
- Storage devices; and….
- Networks.

IS (information systems) result from using IT to fulfill business needs. It is made up of the database, application programs, manual and machine procedures and encompasses the computer systems that do the processing.

IT Infrastructure is the computer hardware, software, storage devices, networks and environmental equipment (e.g. power supplies, air conditioning units) required to support the provision of IT services. This leads us to the term **IT Service Management**

IT Service Management. IT infrastructure exists to provide IT services that satisfy various business needs and customer requirements. These may range from providing access to a single application, such as a general ledger, to a complex set of facilities that include many applications as well as office automation. The service may be spread across a number of hardware, software, and communication systems. It may be provided internally or by an external organization under the terms of an outsourcing contract, or combination of both.

IT Service Management



***IT Service Management* is the totality of IT service provision, including management of the infrastructure and the environment**

IT service management covers a wide range of activities. This guide can only cover the subject to the extent necessary to explain the IT service delivery risks that are most likely to affect an organisation. The guide approaches the subject at a high level, and does not cover topics such as Information Security, the Internet and outsourcing in detail.

Security issues

Information security is a specialist subject, and a high level audit is unlikely to provide full assurance about its effective implementation. IT security audit needs to be addressed comprehensively, for example using the international *Code of Practice for Information Security Management* (ISO 17799) as an audit tool. Information security issues are covered in this guide to the extent necessary to cover IT service management risks, but not to the extent necessary to draw an overall conclusion on an organisation's implementation of information security.

Internet

In this guide Internet solutions are treated as one of several possible options for delivering electronic services. Adopting a technological solution is, however, intimated in the guide through focusing on external and internal user demands, security issues, evaluating possible consequences, etc, which together represent the management issues to be considered. The guide does not deal with questions concerning current Internet technology.

Outsourcing

Auditing the outsourcing of IT functions is a complex area that requires a separate risk audit guide. Public agencies often regard service delivery as a core business activity. Nevertheless, when services become electronic, some functions might be suitable for outsourcing, such as upgrading the network and computers, training, application development etc. This mainly affects activity area no 2 – "*In Operation*", and no 3 – "*Support"* in the IT Service Management Model. But even where services are outsourced, it is rarely possible to transfer all risks to the contractor. There will remain significant risks for the agency to manage, and these are covered in the risk assessments contained in this guide.

Acquisition

Auditing IT related acquisitions is a specialist subject that is outside the scope of this guide.

RISK

RISK is the potential for a given threat to exploit a vulnerability(s) of an asset or group of assets to cause loss or damage. It is usually measured by combining the probability of a threat occurring with its potential impact.

So risk consists of:
- *Possible* threats (e.g. fire, theft, software error, and hardware failure) and the probability of them occurring.
- The exposure of an asset or assets to a particular threat – generally referred to as the asset's "vulnerability".
- *The potential impact* of the defined threats.

Types of risk
- Financial.
- Legal (deriving from the establishment).
- Political embarrassment and loss of credibility.
- Physical danger to individuals.

Risk arises:
- In the course of system operation.
- As a result of internal strategies, system processes, procedures and information used by the organization.

Risk analysis is the study of potential threats, vulnerabilities and impacts in order to identify and assess the extent and potential severity of the risks to which the organization and its assets are exposed.

Risk Assessment is synonymous with **Risk analysis**.

Risk Management Reducing identified risks to acceptable levels by the application of various control strategies.

Investigating risk

In times of rapid change there is a need for quick and accurate assessments of the situation so that appropriate action can be taken. Managing change is easier if robust and responsive decision-making processes are in place, which include the analysis and management of risk.

Managers often need to make choices from a number of possible courses of action. In any situation there are potential benefits and risks associated each. It is necessary for the manager (or the strategy planners, programme or project board, etc.) to decide if an opportunity, in terms of its potential benefits, is sufficient to justify accepting the identified risks. Information is necessary to inform this decision:

- what could go wrong?
- what are the likely causes and possible impact?

- how likely is an identified risk to arise?
- what could be done to prevent it arising?
- how would I know if it did arise?
- what would I do (or be able to do) to recover from the impact?
- would alternative courses of action produce other risks? And if so, would they more or less severe?

Once these questions have been answered, the appropriate course of action can be selected and planned in detail before implementation. Finding the answers and being able to take appropriate action may not fall within an individual manager's control. However, the organisation needs to be able to make informed choices if it is to be successful.

Phases for the management of risk

The effective management of risk involves a two-phased approach.

During the "risk analysis" phase, risks are identified and described so that the associated impact and likelihood of occurrence can be estimated. The acceptability of each risk can then be evaluated. The risks should be placed in order of priority. This information is then passed on to the risk management phase.

The "risk management" phase is concerned with planning for, resourcing and controlling the adoption of a particular course of action to reduce risks to an acceptable level. The actions taken should then be monitored and their success assessed.

It is important for the auditor to know that there are a wide variety of different formal and informal approaches to Risk Assessment and Risk Management.

Although this guide discusses methods for minimizing risk, the terms "likelihood of occurrence" and "estimating" are not used in a precise, mathematical sense.

This guide introduces the risks that are most likely to affect IT service management. When analyzing them, the auditor should rank the identified risks in their *order of priority* in order to focus on those that require the most attention. This will help the auditor to plan the audit and allocate audit resources. The auditor may use statistical methods if this provides the best solution, but their use is outside the scope of this guide.

However, the auditor should not be too concerned about which approach is adopted. The aim should be to critically appraise the thought process that management has employed to identify and evaluate risks, and to take the management's thoughts into account when coming to a *decision about which risks to prioritize* in **Risk Assessment** (Part III of the guide).

(Annex 5 contains further information on Risk Management.)

II
How to use the guide

Audit plan

Having decided to audit IT service management, this guide may be used to help:

gain knowledge of electronic service delivery issues

gain knowledge of Risk Management in general

gain knowledge on IT service related risks likely to appear in public agencies

gain knowledge on how risks could impact on an organisation's activities

acquire typical risk management strategies

form audit questions

advise the client.

The guide aims to be generic, and applies regardless of an organisation's size. The risks described in the risk assessments are those likely to arise in any environment dealing with electronic service delivery. The auditor could perform a complete risk assessment, or a limited subset.

If choosing parts of the risk assessments, the auditor should be aware that the interface between the areas is not always distinct. It might be necessary to extend an investigation by moving into another area in order to get a sufficient overview of the situation.

The Risk Assessment tables

This guide provides a risk assessment for each area in the IT Service Management Model. These assessments share a similar structure, starting with a definition of the particular issue followed by management objectives to aim at in order to achieve stated business objectives.

A three-column table follows each of the management objectives. The table appears in part III of this guide.

The first column lists a number of high-level risks, which if not properly managed could affect the organisation's ability to achieve management objectives and, ultimately, its business objectives.

The second column lists the impacts most likely to occur. These provide a broad indication of the consequences that can arise where a particular risk is not managed effectively, or at all. In all cases it is possible that at least one of the following generic impacts will occur:

- ***financial impacts:*** These stem from the additional cost of remedial action and of wasted investment where the work undertaken cannot be repaired;
- ***damage to credebility:*** This includes loss of public confidence in the operators of an electronic service, but it can also affect an organisation`s staff morale in cases where services are poorly designed, difficult to operate, and are prone to error a nd/or failure;
- ***failure to meet strategic goals:*** This occurs where the outcome (as opposed to `output`) of a development project was not what was reguired to achive a strategic objective. Failure to deliver an operational service is one example of this, but a technically successful service that fails to satisfy business and/or end-user requirements may also result in an unsatisfactory outcome.

The impacts of risks therefore need to be considered against this general background. **The third column** describes typical strategies for managing the risk in question.

This structure will help the auditor to establish whether a particular management objective is achieved, which in turn will help the auditor reach an overall conclusion on whether the agency is managing their IT services effectively.

Top management's role and the "Entity Area"

An agency's top management tends to focus management tasks at two levels:

1) Responsibility of each activity area. An agency's business activities are often organised into 'units'. Middle managers undertake their responsibilities within divisions/ departments, but top management still retain an overall responsibility. For example, the manager of IS department is responsible for working out a long-range plan concerning the IS function. Top management's responsibility is to ensure that the departmental plan is in accordance with the corporate objectives.

2) The responsibility for managing the entity. Top management is responsible for co-ordinating activities across an organization and for making strategic decisions. This could mean that a decision regarded as beneficial for the agency might not appear so in the view of a particular department. For example, as a result of increasing social security fraud, top management decides to remove staff from the Casework department to an IT project developing a program for controlling information provided by social security clients. This could leave the Casework department with an increasing workload. In turn, failure to manage this risk could result in a significant level of unlawful social security disbursements.

This guide lists the risks connected to top management's responsibility for managing the entity in the Entity Area Risk Assessment, while the responsibilities for middle managers in any activity area are to be found in the relevant Activity Area Risk Assessment.

Communication and interaction

Effective communication is regarded to be essential for achieving stated IT service management objectives. All those involved in IT service management share a common responsibility, whilst top management have a special role in ensuring that procedures and reporting lines make effective communications possible. Poor communications are therefore considered to be an important risk in all areas of IT service management.

Overlap

The auditor may find that in some cases similar risks occur in different risk assessments. This is because some activities will inevitably cross several IT service management boundaries and may also occur at different management levels – assessing the risk of poor communications is such an example.

Annexes

The annexes to this guide provide the auditor with additional information. There is lot of specialist literature available on several of the issues dealt with in this guide. Where the guide does not cover a particular topic in sufficient detail, the auditor should refer to the relevant sources in the text and to the bibliography.

Focus

When auditing this topic, the auditor should focus on risk - in particular, on the likelihood of a risk occurring, and the strategy for managing it. Who's responsible for managing risks is of less importance (except for the entity area). This means that the auditor should "**focus on factors, not actors**".

Recommended competence

What competence the auditor should hold will depend on the scope. The auditor needs to be experienced, having the skills and knowledge necessary to perform the auditor's work. It might also be convenient having an IT auditor available for discussion or taking part in the audit, especially when auditing the area "In operation".