

# **E-government in an audit perspective**

## **(REPORT)**

**November 2004**



## TABLE OF CONTENTS

<b>1.</b>	<b>INTRODUCTION .....</b>	<b>1</b>
<b>2.</b>	<b>TRENDS IN E-GOVERNMENT .....</b>	<b>3</b>
2.1.	INTRODUCTION .....	3
2.2.	E-GOVERNMENT: WHAT IS IT? .....	3
2.3.	EXAMPLES OF E-GOVERNMENT APPLICATIONS .....	5
2.4.	POTENTIAL BENEFITS .....	7
2.5.	WHAT IS SPECIAL ABOUT E-GOVERNMENT? .....	8
2.6.	DEVELOPMENTAL ASPECTS .....	12
2.7.	CONCLUDING REMARKS .....	13
	<b>APPENDIX 1 .....</b>	<b>15</b>
<b>3.</b>	<b>RISK .....</b>	<b>17</b>
3.1.	INTRODUCTION .....	17
3.2.	RISKS INVOLVED IN THE PLANNING, DEVELOPMENT AND INTRODUCTION OF E- GOVERNMENT SERVICES .....	17
3.3.	RISKS INVOLVED IN THE RUNNING OF E-GOVERNMENT SERVICES .....	21
3.4.	AUDIT OF RISKS OF E-GOVERNMENT SERVICE PROJECTS .....	24
3.5.	CONCLUDING REMARKS .....	27
<b>4.</b>	<b>AUDIT OF PROGRAMMES AND PROJECTS .....</b>	<b>29</b>
4.1.	INTRODUCTION .....	29
4.2.	CONCEPTUAL FRAMEWORK .....	29
4.3.	AUDIT METHODS .....	31
4.4.	MAPPING ON THE COBIT FRAMEWORK .....	38
4.5.	CONCLUDING REMARKS .....	39
	<b>APPENDIX 2 .....</b>	<b>41</b>
<b>5.</b>	<b>FINANCIAL AUDIT IN DIGITAL ('PAPERLESS') ENVIRONMENT.....</b>	<b>43</b>
5.1.	INTRODUCTION .....	43
5.2.	DIGITAL ENVIRONMENTS .....	43
5.3.	AUDIT OF DIGITAL ('PAPERLESS') ENVIRONMENTS .....	45
5.4.	CONCLUDING REMARKS .....	50
<b>6.</b>	<b>ORGANISATIONAL CONSEQUENCES .....</b>	<b>51</b>
6.1.	INTRODUCTION .....	51
6.2.	THE TRANSITION TO DIGITAL PROCEDURES .....	51
6.3.	METHODS .....	52
6.4.	QUALIFICATIONS .....	52
6.5.	RESOURCES .....	53
6.6.	CONCLUDING REMARKS .....	53
	<b>GLOSSARY .....</b>	<b>53</b>



## PREFACE

During its first meeting in September - October 2002 the EUROSAT IT Working Group agreed to establish a sub-group to develop an overview on E-government and e-procurement and a report about trends, definitions, risks, audit methods, experiences etc. The formed subgroup consists of Portugal (lead), Denmark, Germany, Poland, Russia, and The Netherlands.

At its kick-off meeting in February 2003 the sub-group decided on a scheme for the report. Next, the members worked out the various chapters, and you have the result of this in front of you. Although we all belong to European countries, we all have our own 'country colour' because our experiences differ according to the situation in our respective countries. To a certain extent this will be reflected in the various chapters of this document. But, although some examples are based on country-specific experiences, they are here presented in such a way that they are of interest to the general reader.

Linked to the report is the background document 'E-Procurement and its effect on future audit approach', which is based on Danish experience.

An exposure draft of this report was sent out, on the 25 November 2003, for comments to all (at that time) 24 members of the working group. Comment deadline was on the 15 December 2003. Next, the report was revised according to the comments received, although some issues raised were postponed for discussion during the second meeting of the Working Group, March 2004, in Bern, Switzerland. During that meeting decisions were made about the final modifications to the text, which resulted in this final version.



## 1. INTRODUCTION

Under the heading of 'e-government', most European States have committed themselves under various national and international action programmes and initiatives to make as many as possible of their public services available online via the Web within the foreseeable future (by 2005 in most cases).

These programmes are to be major steps towards achieving governments' policy objective of transforming Europe into an information society. Governments want to ensure that citizens, businesses, academia, and other government entities have simpler, quicker and more cost-effective access to public services. The purpose of these efforts is to enhance the citizens' satisfaction with government and the competitiveness of countries, business and families' locations.

Furthermore, the e-government programmes are to be an important component of a comprehensive modernisation of government. Consistent e-government programmes are to create the momentum for re-engineering business processes throughout the public administration in order to simplify the entire range of administrative structures and procedures.

In this situation failure or even delay in the realization of e-government programs or projects will lead to failure or delay of this modernization programme. Also, the need for consolidating budgets calls for the exploitation of all opportunities to cut costs without deteriorating public service delivery. E-government programmes may open up new avenues towards accomplishing this goal.

One of the consequences of e-government is that governments move from paper-based systems towards paperless systems, thus totally altering the control environments. This fact raises new challenges that must be addressed by management as well as auditors. The absence of paper documentation increases the need for strong IT controls – general IT controls and programmed controls in user systems – and strict manual controls around user systems. This tendency has significant consequences for the development and implementation of e-government projects, as well as for the management of operational IT systems.

As regards the consequences for auditors, one of the major challenges is to assess the validity and reliability of data. To be able to audit an e-government system, we need to adapt existing methods and techniques and develop new ones.

Moreover, because IT systems and business processes are becoming evermore intertwined, decisions about IT are in essence business decisions, not merely technical ones that require the involvement of senior management. Only the active participation of the higher management levels can ensure that the organization as a whole has sufficient control of IT-related risks – i.e. risks related to projects as well as daily operations. Implementing e-government is complex and requires not only vision, but also strong political leadership at the highest level.

All this calls for SAs to give special attention to the given e-government program. This report aims to offer SAs a helping hand in this area. Following a short introduction five topics are covered: the first, '*Trends in e-government*' after exploring some of the existing definitions in order to clarify what e-government is all about, points out some of its potential benefits and covers some developmental aspects. The second, '*Risk*' describes some of the

risks involved in the pre-implementation phases of planning and development of e-government services, risks arising during their introduction and risks involved in the running of e-government services. The third and fourth, '*Audit of Programmes and projects*' and '*Audit in digital ('paperless') environment*' develop audit approaches from a strategic and an operational viewpoint, respectively – whilst the first focuses the need of new audit methods to determine the government's progress in implementing e-government programmes and projects, the second provides an appraisal of auditing in digital environments and of the requirements for audit completion with regards to objective, content and scope. Finally, the fifth, '*Organisational consequences*' raises demands for individual SAIs, referring to the need of strategic initiatives to be taken in the IT area as a consequence of the transition to digital procedures and towards procedural development in order to complete SAI's mission more efficient and more effectively.

While we have ordered the chapters of this report in a way that seems the most logical to us, readers may choose to follow their own route, depending on their existing knowledge and specific interests. The structure of the report allows this, because each chapter can be read as a self-contained unit, covering a specific subtopic within the general theme of e-government in an audit perspective.



## 2. TRENDS IN E-GOVERNMENT

### 2.1. Introduction

In this chapter we clarify what e-government is all about. First, in section 2.2, we propose a definition of e-government after exploring some of the existing definitions. Next, in section 2.3 we present some examples of e-government to give an idea of the scope of the concept. In section 2.4 we touch upon the potential benefits of e-government. In section 2.5, we continue by identifying the typical characteristics of e-government. In section 2.6 we cover some developmental aspects. We finish this chapter with some concluding remarks in section 2.7.

### 2.2. E-government: what is it?

When looking for a useful working definition of the concept of e-government, let us start 'close to home'. The e-government project group of the INTOSAI IT Committee uses the following working definition:

- *E-Government is the online exchange of government information with, and the delivery of services to, citizens, businesses and other government agencies.*

While information provision and service delivery certainly are very relevant elements of e-government as we see the concept, we believe that this definition, tailored to the needs of the INTOSAI project group, is too narrow to serve *our* purposes well. The reason is that it is restricted to those activities that have an online nature and that are directly aimed at external parties. Chain management for instance, aimed, as in e-business, at the enhancement of efficiency and/or effectiveness, we see also as a relevant element of e-government. The reader can refer to the example of personal care provision in section 2.3.5 for an illustration of what is meant here. Chain management is not covered however by the INTOSAI definition.

Looking for other definitions we see a plethora of definitions, ranging in scope from rather restricted to very wide ones. To illustrate the range of definitions, we present here three definitions given in a reader, based on a conference that was held in the Netherlands in 2001.

- *Electronic government concerns providing or attainment of information, services or products through electronic means, by and from governmental agencies, at any given moment and place, offering an extra value for all participating parties.*
- *E-government consists of the following clusters: e-governance, on-line democracy, and electronic service delivery.*
- *The four perspectives of e-government are:*
  - (a) the addressee's perspective (interface with public administration);*
  - (b) the process perspective (re-organization of government processes);*
  - (c) the cooperation perspective (cooperation and collaborative efforts);*

*(d) the knowledge perspective (management of information and knowledge within the public administration).*

We do not consider it wise to confine ourselves beforehand by adopting too narrow a definition. Here are some other encompassing definitions.

The University of Applied Sciences (Berner Fachhochschule) in Bern, Switzerland, gives the following definition:

- *E-government comprises support for relations, processes, and political participation both within all levels (federal and/or state level, regional level, local levels, et cetera) of government agencies and between the agencies and all their stakeholders, including citizens, businesses and other organizations. It does so by providing the necessary means of interaction via electronic channels.*

Still another definition is the one given by the European Union<sup>1</sup>:

- *E-government is the use of information and communication technologies in public administrations combined with organisational change and new skills in order to improve public services and democratic processes and strengthen support to public policies.*

The USA's E-Government Act of 2002 presents a comprehensive yet concise definition:

- *Electronic Government means the use by the Government of web-based Internet applications and other information technologies, combined with processes that implement these technologies, to:*  
*(A) enhance the access to and delivery of Government information and services to the public, other agencies, and other Government entities; or*  
*(B) bring about improvements in Government operations that may include effectiveness, efficiency, service quality, or transformation*

Based on the definitions given, we define the concept as follows:

*With the term e-government we mean the use of information and communication technologies by the government with the aim to:*

- (a) improve information exchange with and/or service provision to citizens and businesses;*
- (b) improve government operations in terms of more effectiveness, and/or efficiency<sup>2</sup>;*
- (c) enhance political participation.*

---

<sup>1</sup> COM(2003) 567 final, 26.9.2003, 'The role of eGovernment for Europe's future'.

<sup>2</sup> This includes the information exchange and/or service provision between government agencies

According to this definition, there are other aspects to the concept of e-government besides electronic service delivery. However, this chapter will focus mainly on this aspect, because to citizens and businesses it is the most visible aspect.

When speaking about electronic service delivery, a distinction can be made between three categories, depending on the target group involved: citizens, businesses, or government. Some authors describe Government-to-employee services as a fourth category. Among other services this comprises knowledge management and career management. Nevertheless we will not explore this borderline category in this document. To give a rough idea, here follows a short description of the three main categories<sup>3</sup>:

- As regards government-to-citizen (G2C), easy to find one-stop shops for citizens are deployed, including single points of easy entry to access high quality government services;  
*Some examples are information provision, electronic tax filing, and convenient passing of tollgates<sup>4</sup>;*
- Government-to-business (G2B) e-government reduces the burden on businesses by using Internet protocols and consolidating the myriad of redundant reporting requirements;  
*Besides services comparable with G2C services, an example is electronic bidding systems.*
- The government-to-government (G2G) variety supports the exchange of information between organizations within the public administration and makes information management more efficient and less cumbersome for citizens and businesses.  
*An example is the establishment of an information broker that allows government agencies to collect data items from citizens or businesses only once. This gives the advantage that, if another authorized agency needs an already collected data item, it needs not annoy the person or business concerned with a redundant request.*

Apparently, as already laid down in the definition of e-government, an important objective is to use IT to the benefit of citizens and businesses, as well as to the benefit of government itself.

### **2.3. Examples of e-government applications**

This section presents some clarifying examples of e-government applications. It is meant to give an idea of the richness of the field of e-government, rather than to present an

---

<sup>3</sup> The first two definitions (not the examples, though) are based on a memorandum of the director of the USA Office of Management and Budget (OMB): M-01-28, Memorandum for the Heads of Executive Departments and Agencies (Mitchell E. Daniels, Jr.).

<sup>4</sup> One way of implementing the latter service is to install a small device (a 'tag') that identifies the owner of a vehicle. A tag reader at the tollgate passes on the tag information to an information system, and as a result the proper amount is deducted from the customer's prepaid account.

exhaustive list of e-government applications. For more examples see Appendix 1 at the end of this chapter that contains the list of e-government services that the EU considers as basic services.

### ***2.3.1 Government information***

Several governments provide on their websites information for citizens and businesses, for instance remote access to archives and databases, news service, legal information, white papers and policy dossiers.

### ***2.3.2 Electronic offices***

Electronic offices offer citizens and businesses possibilities for submitting or updating personal data, for applying for permits or subsidies, or for putting in an application for a vacancy.

### ***2.3.3 One-stop shops***

One step beyond electronic offices, one-stop shops offer joined-up services that are provided by a number of organizations in cooperation. Entrepreneurs for instance, may get access to zoning schemes, submit requests for building permits, sign up at the Chamber of Commerce, and pay taxes, et cetera, all via one single service point.

### ***2.3.4 E-procurement***

Some government procurement portals have been created, with the aim of establishing a gathering point for public procurers and their suppliers. Such portals make it easier for both parties to get an overview of offers, agreements, procurement and sales statistics et cetera. They also enable all parties involved to integrate the relevant procurement, sales and payment data with their financial systems. One of the resulting benefits is cost savings because laborious manual entries and checks and procedures for the correction of errors can be significantly reduced. The procurement process can also become substantially streamlined.

### ***2.3.5 Personalized care provision***

Various projects are under way to explore the opportunities that smart card technology offers to provide personalized care to clients, for instance medical care. The problem at hand is that all the data that may be relevant for the treatment of a particular patient is distributed over a whole network of organizations. This network includes general practitioners, hospitals, medical specialists, and pharmacies. All parties involved possess some bits and pieces of information about the patient, such as medical history, blood type, allergies, medications symptoms, diagnoses, tests, prescriptions, emergency contacts, insurance policy conditions, et cetera. Systems are being developed to disclose all this information to authorized medical and paramedical practitioners, via a smart card that is owned by the patient. All necessary information will then be available, regardless of where

or when the patient applies for medical care, even if the patient was found unconscious after an accident (provided he had the smart card on him).

### ***2.3.6 Infrastructure***

Telematics<sup>5</sup> applications have been established to enable swifter and safer handling of traffic. One can think of matrix signals on motorways conveying speed limits and congestion warnings. Two other examples are traffic monitoring systems and systems for congestion charging<sup>6</sup>.

### ***2.3.7 Electronic tax filing***

In some countries the tax department offers the possibility of sending in tax declarations via diskette, via a modem-to-modem connection or via the Internet.

### ***2.3.8 Information exchange within public management***

Traditionally, public management is organized in such a way that every single government agency deals with its clients separately. This partitioning ignores the fact that there is quite some overlap between their customer bases. To our knowledge, Belgium was the first country to realize the necessity of streamlining information management regarding the data that citizens and business are obliged to provide the government with. Some ten years ago, the 'Crossroads bank for social security' was established, and more recently a 'Crossroads bank for enterprises' followed. Crossroads banks perform the role of information brokers. They allow to implement the principle of collecting each data item only once and to put it at the disposal of every organization that is entitled to use it.

### ***2.3.9 Participation in policy making***

Websites are being used to trigger responses from citizens to certain policy issues. Sometimes even very elaborate electronic discussions that may extend over several months of time may be set up in preparation of policy decisions.

## ***2.4. Potential benefits***

Potential benefits of e-government to citizens and businesses include:

- convenience (availability of the government any time and any place; one-stop shop; swift responses);
- improved quality of customer service;
- access to more and higher quality information;
- specifically for businesses: lower cost of doing business.

---

<sup>5</sup> Telematics is a collection of technologies that combine telecommunications and computing.

<sup>6</sup> Charging motorists a fee for the right to drive during rush ours in certain areas that are prone to congestion.

Potential benefits to government agencies include:

- greater overall effectiveness because of:
  - seamless online government presence that provides more and better structured information so that it is easy to find and does not require an understanding of how the government works;
  - providing joined-up services;
  - better information about citizens and businesses.
- greater efficiency because of:
  - reduced cost of servicing;
  - improved business processes;
  - automating paper-intensive, error-prone tasks;
  - enabling more intelligent and faster exception resolution;
  - providing real-time insight into inefficient stages of service provision.

## **2.5. What is special about e-government?**

This section deals with the question of what characteristics let e-government stand out as something special among other IT related developments. These characteristics may have implications for the (mix of) methods to be used (see figure 6 in section 4.3.1).

### **2.5.1 Client orientation**

One common denominator of e-government initiatives is that they take the client's needs as a starting point, acknowledging the need of a shift away from the conventional orientation on the government's own speculations about what the client's needs could be (or on what the government is able to provide easily). This shift has far-reaching consequences because, most of the times, client's needs do not fit the traditional partitioning of public administration. If it comes to housing issues for instance, traditionally, citizens have to deal with various ministries, such as the Ministry of the Interior and the Ministry of Housing, and with the municipal administration.

If the government wants to deliver joined-up one-stop services, the partitions between the agencies and between the levels within public administration have to be pulled down. All organizations involved should seek (further) cooperation, and restructure their interrelations. They have to do so, both at a strategic level as at the level of daily operations. This amounts to no less than a revolution of public administration, hence governments have to rethink their strategies and develop and implement new business models.

### **2.5.2 Paperless environment**

If a student applies for a study loan or if an entrepreneur requests a permit to establish a business, and they do so via a website, no paper forms are being created. As a consequence, no entry is being made into any registers of letters. The organization therefore needs to devise other means to keep track of the incoming stream of applications.

In the initial stages of e-government this may be circumvented by systematically printing all incoming requests and deal with these via the traditional letter processing procedures, but in the case of full-blown e-government (see section 2.6), this rather cumbersome work-around will be cut off.

In the instances given, 'only' legal certainty is at stake: if people request to enjoy a right they are entitled to, their claim should be properly dealt with, in compliance with any statutory completion times. In other instances however, there are also financial consequences. One can think of electronic tax declarations or electronic bidding system for e-procurement. In such cases, also regularity issues arise.

Section 5.2 ('Digital environments') covers this topic in more detail.

### ***2.5.3 Real-time processing***

Evident examples of services of a real-time nature are emergency alert systems. Gartner for instance, points at the Emergency Telephone Alert System that is in use in several U.S. states by public safety, public health and environment protection agencies to quickly inform citizens about significant events, such as chemical spills, utility disruptions and criminal searches. This technology mainly uses fixed phones as the most-ubiquitous device, but may extend into e-government, when e-mail, web browsers and mobile devices are supported by such systems. Also, less dramatic, information about traffic congestion or about school closing is of a real-time nature.

The provision of real-time services implies that the providing organization should transform the necessary back-office processes from batch to real-time processing. If, for instance, a newsletter that was formerly distributed on paper is being transferred to the Internet, the organization in question cannot suffice with, let's say a monthly, or even weekly update. Information management should be restructured, so that relevant new information can be posted (almost) immediately on the website.

### ***2.5.4 Front office – Back office integration***

A website or any other channel that may be used for interaction, in itself, attractively designed and full featured as it may be, is merely an empty shell. To be useful as a counter for service provision, it has to be connected to the back office, where the actual work underlying the service is done. There are two challenges here. First, existing agencies have established procedures according to their own logic. Often, they are neither client-oriented, nor real-time based. As depicted before, radical shifts in these respects are imperative if the agencies are to meet the needs of e-government. The second issue is that existing organizations carry their own legacy in the form of old information systems and databases. The problem is that these systems and databases are often ill documented and difficult to maintain. Also, in many cases the IT staff members that knew all the ins and outs of the systems in question have left the organization. For these and other reasons, it is difficult to build the necessary interfaces between a front office web server and legacy systems and databases.

### **2.5.5 E-channels**

The Internet is currently the prevailing channel used for e-government in general, and for electronic servicing in particular. Seen from the perspective of take-up however, the approach of using the Internet as the sole channel could prove to be too narrow. After all, not all people are equally adept at using the computer. Also, some target groups are less inclined to use the computer for communication. Young people for instance, do communicate mainly via their cellular phones. While the technology to develop websites that are browsable on cellular phones already exists – it is based on 'WAP': the Wireless Application Protocol – the consumer costs coming with it are pretty high. Besides, one should also realize that building such a second website, in addition to the original one, implies that additional efforts are needed for maintenance. Another possibility would be using the messaging service of the mobile telephone networks: SMS<sup>7</sup>. An example of the latter is an Australian governmental initiative that allows motorists to locate the cheapest fuel prices in their area via a variety of communication channels, one of these being SMS. Still another channel is the smart card<sup>8</sup>. Bracknell Forest Council in the UK for instance developed a smart card solution to deliver a variety of services available via a single smart card, including access to libraries and swimming pools and meal payments in schools. In the Netherlands, pilots are under way to explore the possibilities for using smart card technology for services such as public transport and medical services.

### **2.5.6 E-decision making**

Traditionally, democratically elected representatives on behalf of their constituencies make policy decisions. Over the recent years, many countries have been facing a decline in interest of citizens in politics. E-government may be used to counter this trend because it opens up new opportunities for citizens' participation in policy formation. Decision-makers may, for instance, organize opinion polls or referenda regarding certain policy issues, such as infrastructure plans, proposed legislation etc. The outcome of such polls/referenda may play a role in the process of decision-making.

### **2.5.7 Automated processes**

E-government reduces human intervention to a great extent. One of the advantages of this is that the service process is less dependent on staff members' whims and is also less prone to human error. Also, if properly designed, IT systems are more flexible as regards workload. In principle, E-government is therefore better suited to deal with great fluctuations in demand for services. To be able to automate service processes, the agency needs to link its front office systems in a smart way to the relevant databases within, but if the case may be, also outside the own organization.

However, eliminating human intervention has not only advantages: a possible adverse effect is that without human supervision errors may go unnoticed.

---

<sup>7</sup> Short Message Service.

<sup>8</sup> A smart card is a credit-card sized plastic card containing a microprocessor and a certain amount of memory. It is a kind of microcomputer that communicates with information systems via special devices known as smart card readers.



### **2.5.8 *Dependency on IT***

E-government almost by definition relies highly on IT. This means that e-government programmes are vulnerable to threats if IT risks are insufficiently recognized and mitigated. The two major issues here are information security and project management.

In the area of information security, a clear security policy is indispensable. This policy should be in alignment with both the agency's e-government programmes and its overall business strategy. On the basis of the security policy, a security plan should be developed. Among other things, this means laying down a coherent set of controls that reduces the security risks to an acceptable level. Besides controls to be implemented in hardware and software, also organizational controls are required. The plan should, for instance, lay down the various responsibilities for IT, paying due attention to segregation of duties. A business continuity plan that is in line with the security policy is also needed, to be able to counter any contingencies. The security plan should be carefully implemented, and periodic auditing should produce the necessary assurance that the controls are actually in place and working.

If no clear information security policy has been established and implemented, one of the risks is that the actual security level is either insufficient or too high (and costly), given the threats to the objectives of the e-government project or to assets of the organization. On the other hand, it is possible that the security level is sufficient, but that the set of security measures as a whole is inefficient. In section 3.3, the risks involved in the running of e-government services are addressed.

As regards project management, interestingly, the OECD in 2001 issued a warning that e-government is in danger because most governments experience problems when implementing large IT projects<sup>9</sup>. They went so far as to make the statement that 'unless governments learn to manage the risks connected with large public IT projects, these e-dreams will turn into global nightmares' (e-dreams meaning the e-government policies of governments).

In their background study 'Why IT projects fail', the NAO presented the following recommendations, worthy of consideration, to improve Government IT projects:

- ensure that projects are set in the context of delivering business change and are viewed as business projects, not IT projects, through the development of business development skills;
- break large projects into smaller more manageable components;
- assume active and visible leadership at the top level, with responsibilities and accountabilities clearly stated;
- improve project management skills, with the relative difficulty of project assessed against the abilities of project managers, and improve the understanding of managing risk;

---

<sup>9</sup> 'The hidden threat to E-Government; Avoiding large government IT failures', PUMA Policy Brief No. 8, March 2001.

- identify core skills necessary and provide rapid ways of developing and acquiring what is missing;
- improve relationships with suppliers so that both parties have a shared and mutual understanding of requirements and risks;
- ensure that intended benefits are realised by including formal processes to track progress on realisation;
- spread knowledge, best practice and experience to ensure that new projects have the benefit of experience as they go ahead.

### **2.5.9 Finally ... what is not special at all about e-government?**

Focussing on distinctive characteristics may obscure the sight on issues that e-government shares with other major developments in public administration. From this point of view, the paramount characteristic is that switching to e-government is essentially business process redesign. At an OECD Symposium for senior e-government officials in June 2003<sup>10</sup>, participants aptly stressed that 'e-government is more about government than about 'e' ', and that at some point, leaders have to 'start taking the 'e' out of e-government'. Rather than focusing on technology in itself, participants recognised the substantial potential of using technology as a strategic tool to modernise the structures, processes and overall culture of public administrations. In a number of countries this shift is called 'modernizing government', a transformation that is embedded in national plans and reform strategies for government agencies and the relevant information systems.

## **2.6. Developmental aspects**

It is a country's senior political management responsibility to decide on the e-government strategy to be implemented. This strategy is to be implemented by all levels of public management.

Gartner distinguishes the following stages of e-government development:

- (Presence): websites, presenting information only,
- (Interaction): limited interactivity, basic search, linked sites,
- (Transaction): portals, e-procurement, self-service applications,
- (Transformation): CRM<sup>11</sup> applications, personalization, polling and voting.

The European Commission (The 'e-Europe' initiative) defines the following stages:

- (Information): online information about public services,
- (One-way interaction): downloading of forms,
- (Two-way interaction): processing of forms, including authentication,

<sup>10</sup> The symposium was convened in Washington, at the White House on 9 June 2003.

<sup>11</sup> Customer relation management.

- (Transaction): portals, e-procurement, self-service applications case handling, decision and delivery (payment).

Both in the Gartner and EC models, the higher developmental stages build on the lower ones.

Note that, while both models recognize four stages, the EC's stage 4 (Transaction) corresponds with Gartner's stages 3 (transaction) and 4 (Transformation) in combination.

Because the two models are comparable to a great extent, while also complementing each other, we propose to combine the two. We thus identify the following stages:

- Stage 1 (Presence): websites, available round-the-clock, presenting information-only about public services,
- Stage 2 (Simple interaction): basic search, linked sites; downloading of forms,
- Stage 3 (Smart interaction): processing of forms, including authentication,
- Stage 4 (Transaction): case handling; decision and delivery (payment), CRM applications, personalization, polling and voting, e-procurement.

According to various experts, it may take at least five years to implement all four stages. Thus, the ambition to grow towards full-blown e-government will demand continuous efforts of all parties involved. The aspiration to progress to the highest stage of e-government development is now typical for many European countries. As stage 4 is being explored and innovative procedures of interaction, both among government agencies and between government and citizens/business, will be devised new perspectives may emerge.

## **2.7. Concluding remarks**

Numerous agencies, in many different sectors, have now implemented e-government or are in the process of doing so. If properly implemented, e-government can bring benefits to citizens and businesses, such as convenience and better service. Not unimportantly, also the agencies themselves can benefit from e-government, notably in the form of greater effectiveness and more efficiency. On the other hand, e-government also enhances the agency's vulnerability, because e-government is heavily dependent on IT. Also, the agency has to deal with various organizational issues, such as realizing a client-oriented organization and integrating the Front office with the Back office.

To ensure that potential benefits can be actually yielded and that unnecessary risks, either to the agency or its customers, are minimized, good governance of IT is indispensable. Project management and information security require special attention. Also, because of its critical role in the realization of the agency's mission, IT should be well aligned with the agency's business strategy. For these reasons, the responsibility for e-government developments cannot be placed at the lower management levels or the IT department. Instead, senior management plays a major role here. A key to successful e-government is that this top level develops a vision on e-government that is both challenging and viable, and that it shows clear leadership with a view to getting that vision realized.



## APPENDIX 1

### EU Common list of basic public services

This list contains the e-government services that the EU considers as basic services. The list has been established in the context of the e-Europe action plan. It is being used by the EU to monitor the progress made within the EU in implementing basic e-government services.

Public Services for Citizens	
1	Income taxes: declaration, notification of assessment
2	Job search services by labour offices
3	Social security contributions (3 out of the following 4): <ul style="list-style-type: none"><li>• Unemployment benefits</li><li>• Child allowances</li><li>• Medical costs (reimbursement or direct settlement)</li><li>• Student grants</li></ul>
4	Personal documents (passport and driver's licence)
5	Car registration (new, used and imported cars)
6	Application for building permission
7	Declaration to the police (e.g in case of theft)
8	Public libraries (availability of catalogues, search tools)
9	Certificates (birth, marriage): request and delivery
10	Enrolment in higher education / university
11	Announcement of moving (change of address)
12	Health related services (e.g. interactive advice on the availability of services in different hospitals; appointments for hospitals.)
Public Services for Businesses	
1	Social contribution for employees
2	Corporation tax: declaration, notification
3	VAT: declaration, notification
4	Registration of a new public body
5	Submission of data to statistical offices
6	Customs declarations
7	Environment-related permits (incl. reporting)
8	Public procurement



### **3. RISK**

#### **3.1. Introduction**

This chapter describes some risks involved in the pre-implementation phases planning and development of e-government services, risks arising during their introduction and risks involved in the running of e-government services. The chapter will be completed by several remarks on the audit of e-government service projects and accompanying audit approaches.

#### **3.2. Risks involved in the planning, development and introduction of e-government services**

##### **3.2.1 Strategic planning, co-ordination and quality management**

Absence or inadequacy of a central body playing a strategic role at federal, central or local level bear the risk of uncoordinated planning and introduction of e-government services<sup>12</sup>. The risks include the absence of central coordination leading to structural disparity, overlapping functions, duplication of assets, etc. Measures to be taken include appropriate provisions of the National Development Plan, central funding, 'stick and carrot' policy, obligatory quality standards etc.

##### **3.2.2 User expectations / exploration of user profile/Quality assurance**

It is beyond question that, by now, the Web has become a widely used communication platform in all EU Member States, and the cost of access to it has plummeted since the mid-1990s. Many of the services provided by governments via the Web are scarcely frequented. In spite of this loose 'customer relationship' between government and citizen (G-2-C), departments and agencies usually take the attractiveness of their online services for granted or at least proceed upon this assumption (on the basis of proof adduced such as the positive response to the possibility of filing customs declarations via the Web as a G-2-B relationship).

---

<sup>12</sup>For instance, the German Federal Ministry of the Interior is to be in charge of central planning and co-ordination of all e-government projects throughout the federal public administration and to establish contacts or links to the systems of state and local governments (and other national governments). On the other hand, the German Federal Constitution provides that each Federal Minister conducts the business of his or her department autonomously and on his or her own responsibility (although within the scope of policy guidelines set by the Federal Chancellor). This implies that the responsibility for delivering IT services largely lies with the individual federal government departments. These and the agencies subordinated to them design and develop most of their own IT applications needed for their specific operations and, in most cases run their own computer centres.

In Poland a government strategy 'Gateway Poland' defines two major objectives to be reached in the area of public services by 2005: reaching EU average for basic public services available through electronic media and increase the effectiveness of public administrations by 40%. The strategy also provides for transferring all public procurement process to the internet by the end of 2004.

Inadequate acceptance measurement surveys bear the risk of inappropriate targeting potential users and misleading efforts to make government more efficient and effective by Internet access in general and access to e-government services in particular. A lack of explicit quality criteria can put at risk a department's or agency's Web presence compliance with the needs and wishes of the 'customers', legal provisions and other requirements concerning privacy and data security.

Implementing agencies ought to assure that existing structures and procedures that were created to deal in the traditional way with cases and transactions are reviewed and properly modified or replaced by new ones, whenever necessary to facilitate and accelerate the introduction and development of e-government.

In practice government structures and procedures, (including administrative structures, human resources profiles and management patterns) rarely reflect e-government needs. Thus the success of e-government programs depends heavily on an ability and effectiveness of the business transformation related to the services to be delivered on-line. Most of the structures and procedures usually may come out directly from high level regulations subject to lengthy democratic process. Financial planning may depend on budget structure that is not at all e-government oriented.

The measures to mitigate this risk must involve multiple means and mechanisms that attend and provide for an effective and secure electronic back office able to store and retrieve government records cheaper and quicker.

### **3.2.3 Cost-effectiveness**

Administrations need to assure that e-government services are not only functional but also introduced in a cost-effective way. Overall, vast expenditures have been budgeted for e-government initiatives. The largest portions of total expenditure have been scheduled to be incurred in the coming years. For instance, in Germany, 25 per cent of these expenditures are to be used for re-engineering government structures and the related business processes. The funding needs are to be met largely by savings and the reallocation of funds within and between departments and agencies.

While potential benefits such as economies on material and the speeding-up of business processes have been described, cost-benefit analyses in monetary terms and evaluations of the quality and priority of the various services in most cases have not yet been undertaken. This can lead to inadequate estimation of the savings effect resulting from information services via the Web. Any potential savings are likely to be considerably less than those generated by providing communication and transaction services.

Furthermore, the following fact must be taken into account when carrying out cost-benefit analyses:

For a long time, e-government services may require a duplicative infrastructure alongside a conventional infrastructure for public services delivered without the Web.

Inadequate estimations may put at risk the perception of the considerable future expenditure to be expected in connection with co-ordinating, steering, accounting and – where applicable – charging for these services.



By year-end 2005, almost all of the services to be included in the e-government programme are to be available online via the Web; in many EU countries, about 60 per cent of these services are to be available on the Web as early as year-end 2003.

Implementing agencies ought to properly define its objectives and targets using existing instruments (including national development plans, annual and multi-annual budgets, regional and municipal plans etc.) as well as new task-specific instruments if necessary. Those documents should be consistent and observe good practice. Also necessary actions need to be effected to meet the objectives and targets.

At this time there is often no transparency as to projects and target definitions, planned milestones and road mapping with respect to the individual services. Existing documents may lack specific elements including measurable objectives and targets that allow subsequent program evaluation against them. Such information should be widely published for perusal by all who are directly or indirectly concerned.

### ***3.2.4 Creation of the necessary legal and organisational framework.***

Administrations need to assure necessary legal and organizational framework fostering e-government. Crucial areas are access cost and transactional security.

While many provisions of civil and administrative law have by now been adapted to the requirements of electronic communication and transaction, the risk of lacking a sound legal framework for the ambitious action programmes of government reform will require further unabated efforts to adapt existing and enact new legislation.

Early decisions will have to be taken about the legal and organisational framework for delivering public services via the Web. The alternative options to choose from are the following:

- delivery of the entire range of e-government services through direct service organisations (also known as ‘trading funds’) within departments or agencies or
- let contracts for all or part of the work involved to the private sector (outsourcing of development, operation and/or IT infrastructure, application service provision, network provision).

### ***3.2.5 IT-standards and regulations***

A number of binding standards have been set for the implementation of IT projects and their assessment under the criterion of performance (value for money) <sup>13</sup>.

Implementing agencies ought to assure e-government systems’ conformity with standards such as ISO 17799, CobiT and applicable legislation governing electronic commerce. Mere existence of standards and regulations do not suffice in cases of complex, new, cost-intensive and stressful tasks performed partly by organizations in deep re-engineering process that usually is needed during transformation to a true e-government. There is a serious risk that administrations concentrate firstly on delivery issues and forget about standards and regulations.

---

<sup>13</sup> E.g. in Germany: <http://www.kbst.bund.de/Anlage300441/Band+52+komplett+%281%2c3+MB%29.pdf>

As e-government communications and transactions also involve the exchange of confidential data between government and citizens, adequate guidance on the planning and implementation of secure e-government applications should be issued.<sup>14</sup>

Various public IT systems solutions, especially those fundamental to IT security in high risk areas need to be assessed. In order to do so specific security standards need to be identified and sometimes developed, and IT systems audited against them. Many IT systems solutions will have to undergo a security certification process either to meet legal requirements or to meet conformity assurance levels.

In addition, it may be possible to obtain free of charge public service software already developed by other government entities.

Absence of methodological guidance and appropriate IT standards<sup>15</sup> can jeopardise the interoperability between different e-government applications, of both newly developed and existing ones.

In case infrastructure development (quality, internet access etc.) in some areas does not reach desired standards in due time, this may deeply affect the availability and functioning of even the best e-government services provided by the most powerful servers and centres.

There are a number of ways conformity can be assured. Self-evaluation procedures, internal audits, SAIs, specialized organizations and procedures co-exist in many countries and create a network of structures and mechanisms fostering conformity with good practice, professional standards and legal requirements related to e-government and its elements.

### ***3.2.6 Provision of technical infrastructure***

Inconsistency of planning can risk the availability and reliability of basic IT components and facilities (Web portal, content management system, forms server, basic services for transaction security) that should be at the disposal of the majority of government departments and agencies and their different types of online services.

### ***3.2.7 Dependence on IT-companies***

As a result of poor provision or insufficient normative and legal regulation companies providing IT to Government may win a special position in e-government systems. Consequences may include the following: preferring some of them, disturbance of free market competition and decreasing cost-effectiveness of the whole system. Administrations should avoid locking in specific technology owned by companies, which could use this dominance to apply unjust prices.

---

<sup>14</sup> Compare the programme 'ePolska' of March 2003, which places the responsibility of setting standards for secure government applications on government Departments or for the German Federal Government: [http://www.bsi.bund.de/fachthem/egov/3\\_en.htm](http://www.bsi.bund.de/fachthem/egov/3_en.htm).

<sup>15</sup> To ensure the interoperability between different e-government applications, both newly developed and existing ones, the methodological guidance 'Standards and Architectures in e-Government Applications' (SAGA) was adopted in Germany in early 2003.

While confronted with this risk we may use open source technology, use two or more alternative technologies competitive to each other on the market, thoroughly develop long term contracts that provide for price stability (or reduction with market prices), maintenance and future developments.

### ***3.2.8 Right to the Internet domain***

Inadequate legal provision risks the right to the Internet domain. To maintain a Web presence, each department or agency must have a Web address or 'Internet domain' registered with the appropriate authority. The name chosen should be one that Web users can associate by logic with the services offered by the department or agency. For instance, for Polish authority, the logic choice would be '[www.nameofauthority.gov.pl](http://www.nameofauthority.gov.pl)' and for any German authority '[www.nameofauthority.de](http://www.nameofauthority.de)' or '[www.descriptionofservice.de](http://www.descriptionofservice.de)'.

### ***3.2.9 Progress in information and communication technology***

In contrast to other spheres of life, information and communication technology (ICT) is subject to extremely rapid change. As in the past, the capacities of the platforms used for running IT systems will perhaps double every 18-24 months. Inadequate communication platforms chosen for e-government, namely the Internet and e-mail, risk being affected by rapid technological progress. E-government services will have to keep up closely with these developments in interaction with the 'customers'.

Substantial risks exist in the pace in which ICT develops within the e-government target population and geographical area. This combines multiple development aspects including infrastructure, service quality, affordability and education.

## ***3.3. Risks involved in the running of e-government services***

### ***3.3.1 Adequate technical and organisational IT security***

The introduction of e-government services frequently implies the purchase of new or the restructuring of existing ICT equipment and infrastructure.

Risk of error and fraud implicates a necessity to plan for and implement numerous controls virtually nonexistent in an IT free environment: segregation of duties, access controls, input controls, processing controls etc.

Absence of clear arrangements not only for the legal protection of privacy but also of arrangements for achieving data security bear in particular risk associated with the insecure use of e-mail and the Web as communication and transaction platforms in connection with e-government services.

The measures to be taken aim but are not limited to the following (cf. section 5.3.3 'Audit of IT application'):

#### ***– Integrity***

The requirement of integrity implies that steps must be taken to safeguard computer-held information and data against partial or total loss, destruction or tampering. Where electronic communication is concerned, this means that the data must be fully protected against change or tampering during their transmission.

– *Authenticity*

This concept requires adequate measures to be taken to make sure that the communication partner really is the person he or she claims to be and/or that the information received really originates from the indicated source.

There must be arrangements that ensure that the source of personal data can be identified at any time. In that context, a distinction has to be made between the proof of identity (communication partners prove their identity in a way that excludes any doubt) and the proof of origin (the sender proves that a communication has originated from him or her and has not been changed). Authentication procedures serve to detect and afford protection against any unauthorised access or tampering and to safeguard sensitive data during their transmission through networks. This requires procedures that enable all parties involved to identify their communication partners without any doubt.

– *Confidentiality*

Assurance must be provided that data and information can be accessed only by authorised persons and in authorised ways.

Where data are transmitted via the Internet without technical protection arrangements, third parties may peruse message contents and modify them without the knowledge of the sender or addressee. Suitable countermeasures must be taken to prevent the unauthorised and undetected perusal of and tampering with the contents of electronic messages.

– *Availability*

Arrangements must be made to ensure that information and services are available on a timely basis whenever needed by users. The need for timely and correct processing of data is particularly great where e-government services are involved. Best efforts must be made to avoid the loss of data and the hampering of hardware or software operations by technical defects. Strong backup and recovery plans are needed in the frame of broader 'Safety Policy'.

– *Binding character of electronic transactions and corroborative proof of receipt of messages*

Arrangements must be made to ensure that the sending and receipt of data and information cannot be denied (i.e. to enable corroborative proof to be given that a legally binding transaction has been entered into).

– *Capability of being audited*

Authorities that run e-government services are under the obligation to make technical and organisational arrangements allowing the ex post verification of electronic transactions enabling supervisors or auditors to find out who entered or conveyed which data at which time. The arrangements made must also be adequate to detect and investigate any unauthorised attempts to access or tamper with data.

Examples of risks and potential damage caused by non-compliance with these requirements are:

- introduction into IT networks of malicious software (e.g. viruses; Trojan horses; logical bombs or worms);
- tampering with/ damaging / destruction of operating systems or application software (incl. affected records);
- inadequate protection of remote maintenance access;
- tampering by 'internal offenders' (e.g. administrators or users);
- faulty or risky software;
- tampering with communication links;
- inadequate security-consciousness;
- inadequately skilled staff.

The damage caused by these factors may be classified in these different categories:

- material;
- financial [(down) time is (also) money];
- immaterial (may be more detrimental than financial damage ) and
- staff-related.

Logging has a preventive effect against unauthorised access and tampering because nobody can be sure that transgressions will go undetected.

Audit trails<sup>16</sup> can provide assurance that data have not been tampered with. Special attention to this issue is crucial because, to the extent that an e-government programme leads to the discontinuation of paper forms, the traditional audit trails also tend to disappear. The organization should therefore create new audit trails in the automated information systems, to ensure that transactions can always be audited. Nonexistent or inadequate audit trails bring the risk that unauthorized changes of data go unnoticed.

### **3.3.2 Transaction security**

In order to prevent insufficient transaction security with respect to customer communication and – specially – transaction services (G-2-C; G-2-B; G-2-G), administration should comply with the strict requirements of the Digital Signature Ordinance. Furthermore, care must be taken to ensure interoperability between the national and international digital signature solutions.

---

<sup>16</sup> An audit trail is a chronological set of records that collectively provide documentary evidence of processing, sufficient to enable reconstruction, review and examination of an activity (source: 'Information Systems Auditing; Glossary of Terms', INTOSAI IT Committee).

For public authorities to communicate safely and legally binding via the Web, they should also have a 'virtual postmaster', which should serve as largely automated central security gateway, performing the functions of authentication, verification and generation of digital signatures, decryption and encryption as well as performing other security checks. High-grade services may require strong authentication of the customer, and where certain types of communication must be in writing to be legally valid, authenticity must be accredited, which requires a valid digital signature.

### ***3.3.3 Payment transactions***

In future payments of fees, customs duties and taxes in the range of tens of billions of Euros each year are to be transacted via IT systems of the tax and customs authorities. Insufficient security requirements can risk the electronic collection of these charges even more than standards not met by the other e-government service systems.

By means of a funds transfer platform the authority concerned could and should provide an electronic service for the collection of such fees, taxes and duties, ensuring that the amounts due are actually received and that the receipts are duly passed on to the appropriate cash management unit for accounting or, if an electronic funds transfer should fail, such failure is reported immediately.

### ***3.3.4 Redundancy, media discontinuities and inadequate interoperability***

Redundant structures for the provision of services should be dismantled. In order to eliminate media discontinuities the entirety of each e-government service should be transacted by means of IT in the long-term. Where administrative services do not involve any discretionary decisions on individual cases, service delivery could be fully automated.

## ***3.4. Audit of risks of e-government service projects***

### ***3.4.1 Requirements for the auditor***

The wide variety and complexity of the following factors can serve as first clues to audit approaches:

- the numbers of departments and agencies participating in the programmes;
- the vast number of electronic services and projects;
- the linking of electronic services with each other (and among national, regional and local government entities) and
- in particular, the vast amount of funding required.

These factors demand high professional requirements on the auditor of e-government services:

- technical background knowledge needed to assess the technical specifications to be met by the e-government service in question;

- in-depth knowledge of the ICT platform on which the e-government service will be run;
- ability to analyse data; knowledge and skills to use techniques of electronic collection and analysis of audit evidence.

### **3.4.2 Ethics**

Quite often an auditor performing e-government audits finds himself in awkward situations which create a need to make ethical decisions. SAIs will need to assure that each auditor involved in such audits is ready to deal with these situations.

### **3.4.3 Audit approaches**

Initial audit experience has already been gained with some of the projects implemented under e-government initiatives. Owing to the fact that especially the rather risky transaction services will be launched only at a later time, it will yet take some years before SAIs will be able to develop conclusive audit findings and conclusions about the introduction and operation of complex e-government services.

Examples of specific audit approaches on risks at the stage of programme design, planning public expenditure, during the realization of the programme<sup>17</sup> and at the stage of the evaluation of efficiency can be:

- At the stage of programme design:
  - absence of due coordination of works on creation of the e-government at federal, regional and local levels of management, absence of a single concept and programme;
  - preparation of e-government project in conditions of absence or out of the framework of the general strategies (the plan, the programme) of social and economic development of the country and digitalisation of the society which, in turn, should envisage necessary transformations of interrelations between the public bodies and the society;
  - non-conformity of functionality or logic of information provision and other new electronic services with existing administrative structures and decision making algorithms;
  - inadequate estimation of 'digital inequality' existing in the country, as the most important condition of productivity of e-government programme;
  - lack of clear definition of the project in terms of purposes, tasks, time, arrangements and necessary financial resources (absence of the problem-oriented approach) as well as absence of indicators of efficiency (productivity) of financial expenses;

---

<sup>17</sup> Chapter 4 covers the topic 'Audit of Programmes and projects' in more detail.

- absence of the commonly accepted standards of data storage and supply while organizing information interaction within the bodies of state power, their interaction with commercial and public organizations;
  - insufficient normative and legal regulation in the sphere of exchange of information at the level of state bodies and institutions of local self-government as well as in the sphere of information interaction of state bodies with citizens and business sector.
- At the stage of planning public expenditure:
    - inadequate estimation of expenditures on financing of the project and capabilities of the state on allocation of necessary volumes of financial resources;
    - existing system of financing and culture of the state organization does not allow to create effective system of investment, including public funds, into complex projects of digitalisation;
    - the system of priorities for promotion of the project in conditions of the limited financing which has not been created yet;
    - budgetary classification is insufficiently detailed to provide transparency of planning of expenditures and their subsequent control;
    - assignment in federal budgets for the next fiscal year is made without taking into account achievement of the purposes of programme actions which leads to accumulation of the uncompleted programmes and stages, investment in hardware and the general software without development of special tasks of final services;
    - inconsistency of timing of financial allocation from various sources (the state budget, foreign loans and credits, means of non-state funds, etc.).



- During realization of the programme:
  - the programme management system does not allow to react operatively to revolting factors and new risks (financial, technological, social and others);
  - high degree of inertia of the modern bureaucracy and, as consequence, resistance to changes;
  - estimation indicators of realization course of the programme (phases, stages), creation of subsystems are absent or insufficiently advanced;
  - time disproportions in legislative, organizational and technological provision of solving programme elements;
  - slow change of stereotypes of social and political behaviour of the population, disappointment regarding rates of realization of the programme and expected utility for business sector and population, mistrust to measures for securing confidentiality of the data;
  - there are no standard forms of reports on organization of information interaction of government bodies, commercial and public organizations;
  - inconsistency of development of the e-government programme and departmental information systems of bodies of state power, of the e-government programme and others components of 'electronic society', which are beyond relations G2X (B2B, D2C, C2C).
- At the stage of evaluation of efficiency of realization of the programme
  - the purposes and parameters of the programme are not achieved;
  - expenditure of the programme have exceeded scheduled ones;
  - cost of introduction and the further operation is unacceptable both for the state, for business sector and citizens;
  - realization of the programme has not resulted in improvement of position of the state in the world electronic community.

### **3.5. Concluding remarks**

The size of e-government programmes, the amount of the relevant projects and the different phases such as planning and development, introduction and running of e-government services bear various risks, of which only some have been highlighted in this report. The heavy dependence of the agencies and their customers on IT and their vulnerability present a formidable challenge to public accountability. Therefore policy makers and managers need to focus their attention on a minimisation of the risks encountered as early as possible to prevent potential damage that is often of a considerable but unknown magnitude.



## 4. AUDIT OF PROGRAMMES AND PROJECTS

### 4.1. Introduction

E-government is a new area, and we find it difficult to imagine that we can audit, for instance, a government portal, using only the traditional methods (including methods of IT-audit). Hence we need new audit methods in addition to the existing ones. With these new methods we will be able to determine the government's progress in implementing e-government programmes and projects (see for instance the Russian example in Appendix 2 at the end of this chapter). The new methods should explicitly take the IT aspect into account, because e-government programmes depend heavily on IT. While e-government as such is a new phenomenon, IT and IT audit are not. We can therefore rely to a great extent on our existing experience. However, as indicated in section 2.5 ('What is special about E-government?'), e-government has some specific characteristics. New methods may therefore be needed to do justice to these characteristics.

To be effective, an audit of a programme should address primarily the early stages of the programme, covering control issues while the programme is still being designed or implemented. An audit after programme completion cannot be very effective because at that point it is too late for taking steps that would improve control of the audited programme.

In this chapter, by 'programme' we mean the programme, consisting of interrelated projects (including IT-projects), aimed at intermediate or ultimate goals of transition to the e-government, for example, the state federal / regional program. In this sense, we can also consider a programme as a 'basket' of IT project and other projects. A project in this basket is understood as one of the separate projects in the basket (IT or other).

### 4.2. Conceptual framework

#### 4.2.1 Basic categories of audit objects

E-government audits may focus on one or more of the following three types of objects, corresponding to three control levels:

- a *programme* as a collection ('basket') of projects (including IT-projects), aimed at intermediate or final goals;
- an (IT) *project* either as a separate project or as a project within the framework of the programme ('project');
- an *information system* ('IS') or *information resource* ('IR') created or used in the interests of e-government ('IS/IR').

Control issues at the three control levels are:

- *strategic level*: efficiency with which the carrying out of programmes is being organized, planned, managed and controlled;
- *operational level*: the carrying out of projects;

- *application level*: the use of existing or newly created information systems and information resources.

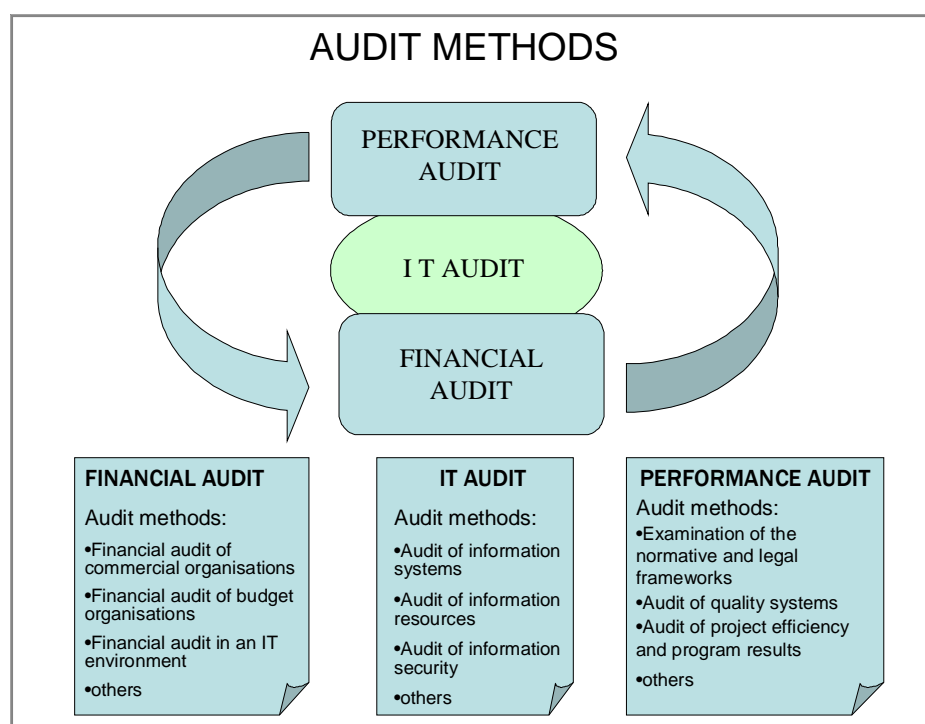
This chapter aims at the strategic level of control during the transition to e-government and its further development.

#### 4.2.2 General audit types

Standard classifications recognize the following general audit types:

- *financial audit*, i.e. audit of:
  - investments and expenditures;
  - accounting of funds;
  - organization of internal control and reporting, efficiency of expenditures.
- *IT-audit*: audit of IT governance;
- *performance audit*, i.e. assessment of:
  - systems for quality control;
  - efficiency and effectiveness;
  - efficiency of the decision-making process
  - service quality;
  - staffing policies; skills and knowledge of staff members.

**Figure 1 – Types and methods of general audit**



For each audit type we can rely partly on well-established audit methods and techniques. When applied to e-government issues, these need to be complemented by new approaches.

#### 4.2.3 Time perspective

According to accepted international practice of financial control institutions we can define three time frames for financial control:

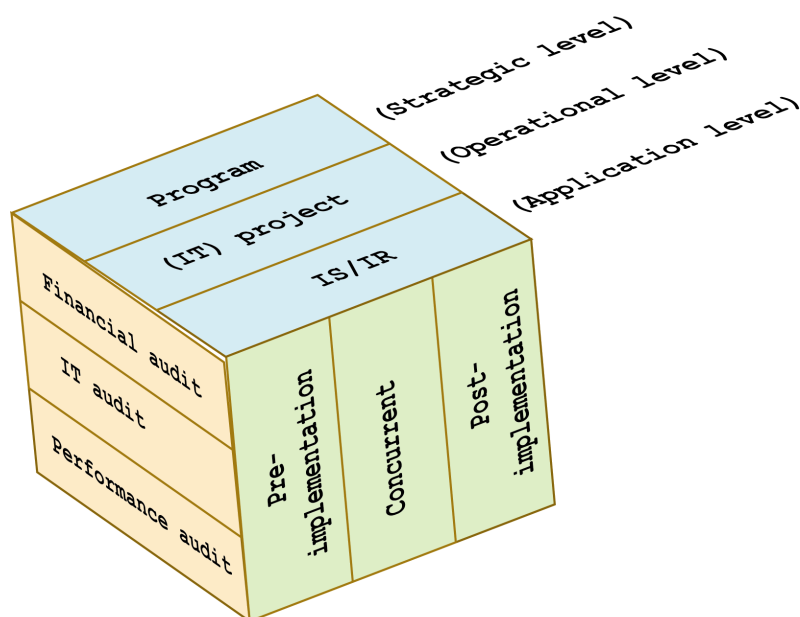
- *pre-implementation*: control during the process of policy decision making on budget and other law drafts or about other financial-control areas,
- *concurrent*: control of additional issues regarding budget execution that may arise while realizing programmes and projects,
- *post-implementation*: approval of the accountability reports on budget execution and on the effects (or 'outcome') of the programmes and projects.

### 4.3. Audit methods

#### 4.3.1 Applicability of existing audit types to the area of e-government

The three dimensional view covered in the previous sections builds a control space (fig. 2) where each element corresponds to a group of methods:  $M(i,j,k)$ . In this function the letters 'i', 'j' and 'k' represent the variables 'audit objects', 'audit types', and 'time perspective', respectively (fig. 3).

Figure 2 – Control space of e-government



**Figure 3 – Group of methods of audit of e-government**

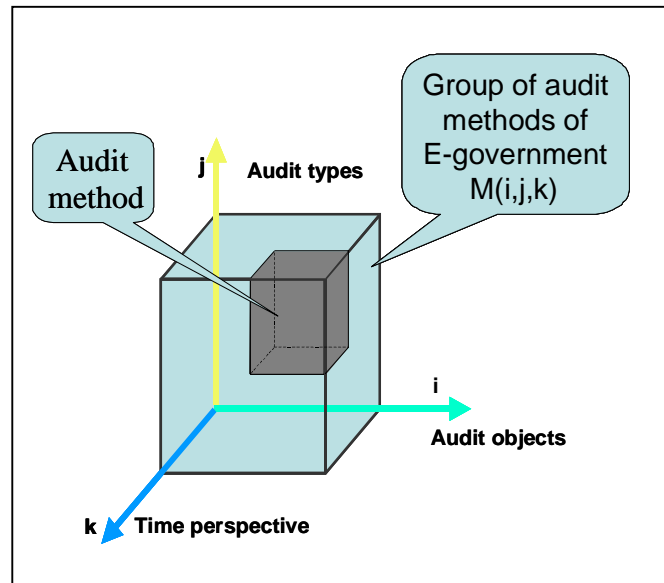


Figure 4 shows the suitability of the various groups of methods for auditing transition to e-government.

**Figure 4 – Applicability of existing methods of audit during transition to e-government**

Audit objects	Time perspective	Audit types		
		Financial audit	IT-audit	Performance audit
Programme	Pre-implementation	☑	New methods should be developed	☑
	Concurrent	☑	New methods should be developed	☑
	Post-implementation	☑	New methods should be developed	New methods should be developed
(IT) Project	Pre-implementation	☑	☑	☑
	Concurrent	☑	☑	☑
	Post-implementation	☑	New methods should be developed	New methods should be developed
IS/ IR	Pre-implementation	☑	☑	New methods should be developed
	Concurrent	☑	☑	☑
	Post-implementation	☑	☑	☑

When analysing the applicability of methods in more detail, it is useful to consider these from a life-cycle perspective.

For example, at a strategic level of control we recognize the following life cycle stages (see also figure 5).

- *strategic planning stage (I)*: political decision making; development of the programme with the definition of the objectives, requirements, tasks, and design criteria for a feasible programme;
- *design stage (II)*: creation of the programme's management body (development of the competitive documentation and realization of competition to choose entity responsible for the programme in question); formation of normative legal framework; decomposition of purposes and tasks of the programme; formation of basket of projects and budget of the programme etc.;
- *realization stage (III)*: development of the technical and economic basis of the project; competitive documentation on the projects of the programme; organization of competitions and conclusion of contracts pertaining to projects; formation of the portfolio of the investments and financing of the projects; control of stages and project results, finalizing / discontinuing / start of projects of the programme; updating of the programme etc.;
- *final stage (IV)*: Assessment of programme results; assessment of accounting and reporting quality; measurement of programme efficiency, etc.

**Figure 5 – Audit issues at the various life cycle stages.**

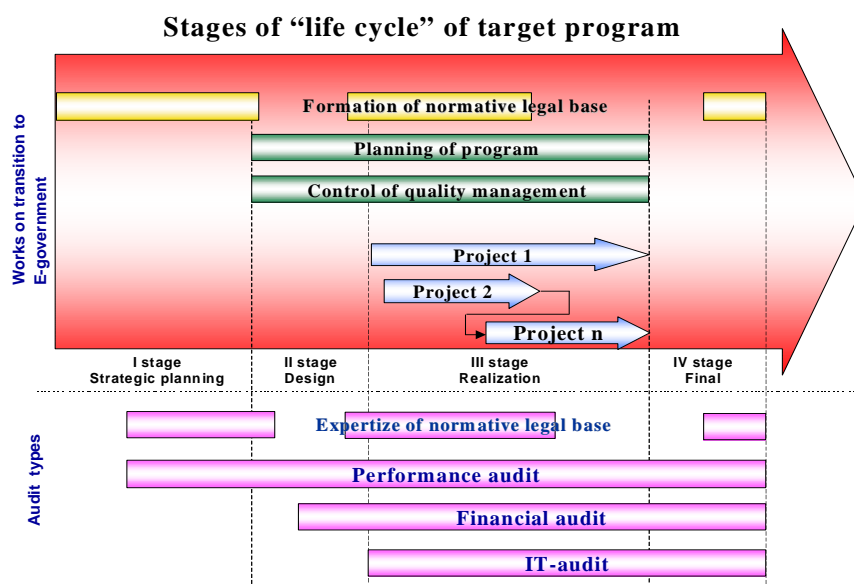


Figure 5 shows how various types of audit (financial, IT-audit and audit of efficiency) can be used at different stages of life cycle of the target program.

The appropriate methods to be used in the various life cycle stages are presented in the next table.

**Figure 6 – Audit methods appropriate in various programme stages**

Life cycle stages	Audit methods
(I) Strategic planning	1 Programme review from a normative (legal) perspective
	2 Evaluation of outcome forecasts
	3 Scrutiny of programme concept
(II) Design	4 Review of tender invitation for selection of responsible entity
	5 Audit of quality control system in use by responsible entity
	6 Review of projects from a normative (legal) perspective
	7 Audit of responsible entity's budget
(III) Realization	8 Financial audit of responsible entity's own budgeting system
	9 Financial audit of expenditures on programme realization
	10 Review of tender invitation for selection of project contractors
	11 Audit of organization and execution of tendering process
	12 Audit of logistic system of programme
	13 Performance audit
	14 Audit of programme risks
	15 Audit of information systems in use by responsible entity
(IV) Final	16 Financial audit of responsible entity's own budgeting system
	17 Financial audit of expenditures on programme realization
	18 Performance audit

Figure 6 gives information about the appropriateness of the audit methods at the various life cycle stages of the target program, based on the audit experience of the Accounts Chamber of the Russian Federation and accounting bodies of the Russian Federation.

The methods presented in the table will be explained in the next section.

#### **4.3.2 Explanation of methods**

Here follows an explanation of the methods presented in figure 6.



*(1) Programme review from a normative (legal) perspective*

Review projects from a normative (legal) perspective concerning political decision making on the:

- necessity of transition to e-government,
- forms, purposes and tasks of e-government,
- necessity of reorganization of public management,
- budget allocation and timing of targets.

*(2) Evaluation of outcome forecasts*

- check whether forecasts were made and if they are stated in terms of social and economic development,
- check whether these forecasts are based on correct and efficient methods and procedures

*(3) Scrutiny of programme concept*

- determine whether purposes and tasks of the programme are aligned with the strategic purposes and tasks with respect to the socio-economic development of the country,
- check whether correct and measurable criteria for the measurement of intermediate and final results of the programme have been laid down.

*(4) Review of tender invitation for selection of responsible entity*

Examine the:

- conformity of tender invitation with the existing legislation,
- realization of conditions for competition,
- results of competition.

*(5) Audit of quality control system in use by responsible entity*

- check whether the responsible entity has established a quality control system (if it is necessary),
- evaluate whether the quality control system is appropriate for the task of managing and coordinating the programme activities,
- check whether the programme will be managed by the appropriate authority,
- check whether the responsible entity conforms to the requirements of the quality control system.

*(6) Review of projects from a normative (legal) perspective*

Review the legal framework that applies for the responsible entity with respect to aspects such as:

- conformity to purposes and tasks of the programme,
- validity of cost calculations,
- validity of project planning (completion dates and sequencing),

- validity of termination of separate projects,
- specification or change of purposes and tasks of the projects.

*(7) Audit of responsible entity's budget*

- Audit the financial soundness of the responsible entity.

*(8,16) Financial audit of responsible entity's own budgeting system*

- examine the expenditures of the responsible entity in the course of programme realization,
- examine the financial and other statutory reporting documents.

*(9,17) Financial audit of expenditures on programme realization*

Audit the expenses of responsible entity with respect to:

- programme management,
- preparation, organization and realization of a competitive situation for the projects that belong to the programme,
- realization of centralized purchases of equipment and software for programme participants,
- regularity, timeliness and completeness of payments,
- correctness, completeness and timeliness of financial reports and other statutory reporting and accounting documents.

*(10) Review of tender invitation for selection of project contractors*

- verify whether the invitation to tender for the projects of the programme do conform to requirements of the existing legislation,
- verify whether conditions for competition have been fulfilled,
- examine the tender results and the choice of contractors that will realize the programme projects.

*(11) Audit of organization and execution of tendering process*

- examine the preparation and realization of the centralized purchases of equipment, software and services for the participants of the programme by the responsible or authorized entity,
- verify the regularity, timeliness and completeness of payments for purchases,
- verify whether the acquired equipment, software and services conform with established qualitative and technical requirements.

*(12) Audit of logistic system of programme*

Examine how:

- the purchase, storage and delivery of centrally acquired equipment and software for the programme participants is organized,

- the creation and presentation of design, accounting and financial documentation by the programme participants is organized.

*(13, 18) Performance audit*

Assess the results of programme realization from the point of view of:

- the timely and complete meeting of established targets,
- programme management efficiency,
- efficiency of the use of resources allocated to the programme.

*(14) Audit of programme risks*

These problems are considered in chapter 3.

*(15) Audit of information systems in use by responsible entity*

- Assess the extent to which the various quality aspects of information systems in use by the responsible entity conform to established norms, standards and requirements. This includes risk analysis and the review of corporate systems in use by the programme participants.

#### 4.4. Mapping on the CobiT framework

All audit methods of strategic, operational and application levels, stated in the given chapter, can be mapped on a CobiT<sup>18</sup> framework, as follows:

**Fig. 7 –Mapping of the three audit objects / control levels on CobiT processes.**

CobiT Domain	CobiT Domain Code	Process	Programme (Strategic)	Project (Operational)	IS/IR (Application)
Planning & Organization	PO1	Define a strategic IT plan	X		
	PO2	Define the information architecture		X	X
	PO3	Determine technological direction		X	X
	PO4	Define the IT organization and relationships		X	
	PO5	Manage the IT investment	X	X	X
	PO6	Communicate management aims and direction	X	X	
	PO7	Manage human resources		X	
	PO8	Ensure compliance with external requirements	X	X	
	PO9	Assess risks	X	X	X
	PO10	Manage projects		X	
	PO11	Manage quality		X	
Acquisition & Implementation	AI1	Identify automated solutions		X	
	AI2	Acquire and maintain application software		X	
	AI3	Acquire and maintain technology infrastructure		X	
	AI4	Develop and maintain procedures		X	
	AI5	Install and accredit systems		X	
	AI6	Manage changes		X	
Delivery & Support	DS1	Define and manage service levels			X
	DS2	Manage third-party services			X
	DS3	Manage performance and capacity			X
	DS4	Ensure continuous service			X
	DS5	Ensure systems security			X
	DS6	Identify and allocate costs			X
	DS7	Educate and train users			X
	DS8	Assist and advise customers			X
	DS9	Manage the configuration			X
	DS10	Manage problems and incidents			X
	DS11	Manage data			X
	DS12	Manage facilities			X
	DS13	Manage operations			X
Monitoring	M1	Monitor the processes	X	X	X
	M2	Assess internal control adequacy		X	X
	M3	Obtain independent assurance		X	X
	M4	Provide for independent audit		X	X

<sup>18</sup> CobiT- – Control Objectives for Information and Related Technology

This table reflects our idea that auditing e-government projects and programs should not be limited by any functional standard and can not be reduced to some domains or CobiT standard processes, such as PO10 (Project management) and PO11 (Quality management).

#### **4.5. Concluding remarks**

We would like to emphasize that the classification of audit types into separate categories (see section 4.2.2) was made for conceptual clarity. In actual practice, audit of programmes and projects typically combine financial-, IT- and/or performance audit approaches in a single programme or project.

Audit of all relevant aspects of programs and projects at transition to e-government, and of conditions for e-government, is not possible without the use of new methods. These methods should be created as e-government activities grow over time.

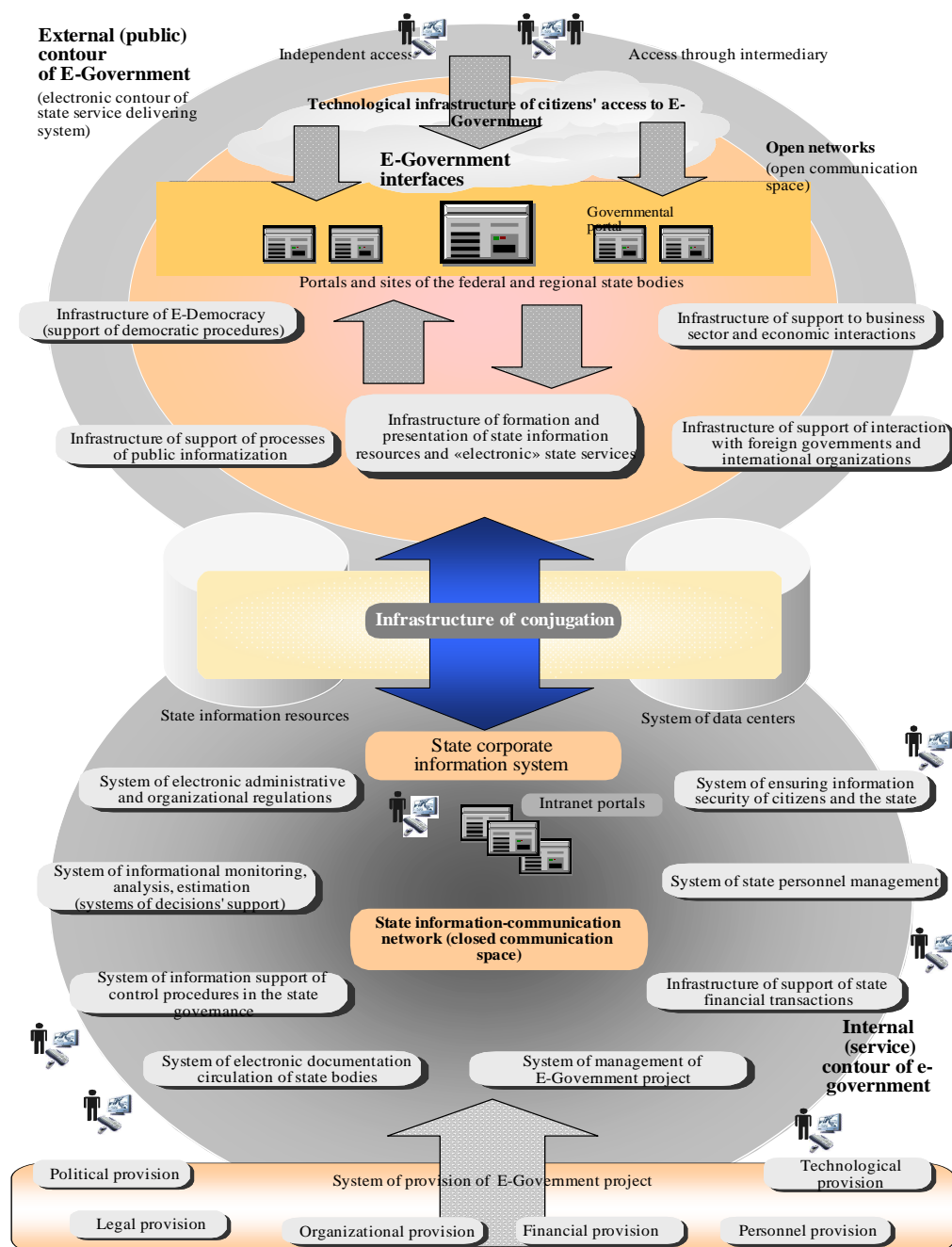
These new methods should cover such topics as:

- the quality of accounting systems of the organizations that are responsible for organizing and carrying out of e-government programmes;
- compliance of projects with functional standards such as the management of investments (ISO/IEC 15288:CD2);
- compliance with standards for the implementation and use of IT (CobiT);
- the existence of certified quality control systems at each stage of project realization.

It is also important to note that the best audit approach can differ from country to country, because there may be significant differences in the network of parties involved in an e-government programme and in the arrangement of the roles attributed to the various partners. For instance, system development may, but need not be contracted out.



**Russian experience of the creation of E-Government**  
**(Federal target program 'Electronic Russia for the years of 2002 - 2010')**







## **5. FINANCIAL AUDIT IN DIGITAL ('PAPERLESS') ENVIRONMENT**

### **5.1. Introduction**

The objective of this section is to focus on financial audit and to present a frame of reference for general audit requirements in digital environments with regard to objective, content and scope.

The presentation is mainly based on e-procurement experience. E-procurement is a further stage of e-government development, cf. section 2.6 (Developmental Aspects). However, it should be recognized that e-government is an open area, and that many other topics could have been chosen to demonstrate, how e-government is developing. As the target group primarily consists of decision-makers, emphasis has been allocated to the description of the main points in the audit of digital environments.

The digitalisation of the administrative and procurement functions of public sector bodies provides a number of advantages, for example, in the structuring of new and more efficient working procedures, as well as being able to communicate and co-operate in new ways. Traditional paper-based working procedures can be made more efficient, amended or dispensed with entirely when data and data-communication becomes electronic. As such, liberated resources can be transferred from administration to service.

However, digitalisation brings not only advantages with it. The risk factor changes radically in line with technical development, for example, when traditional paper-format documents are replaced by digital data that easily can be stolen (copied), changed and erased – in a second without trace and physical contact. In future, security surrounding digital systems will be assigned important priority in all fields of society. In section 3.3 the risks involved in the running of e-government services are addressed.

### **5.2. Digital environments**

#### **5.2.1. Characteristics**

IT constitutes the basis for a public body's knowledge, information and management, and is applied to an ever increasing extent in professional and administrative procedures. At the same time, the application of IT has received increasing strategic significance and has become decisive for the realisation of a public body's mission and vision. Therefore, an efficient and secure IT environment is essential to daily public body operations.

In paperless (digital) systems a public body's data does not exist in the form of traditional paper documents, but only in electronic or digital format.

Digital documents not only include documents that originate from paper media (e.g. letters) and which subsequently have been digitised, but also documents that only exist and are used in digital form throughout their entire 'life-span'.

The introduction of (paperless) digital systems and the hooking-up of internal systems to the Internet, for example in connection with electronic procurement, increases dependence on IT and heighten the demands on IT-resource accessibility and security.

When paper documents are not longer being used and have been replaced by electronic documents (data) as the only form of documentation for public body transactions, it places crucial demands on the public body's control environment in as much electronic documents must possess the same evidential value as paper-format documents.

In general, an established legal practice and methodology currently exists to assess the evidential value of paper documents. However, no equivalent practice exists for digital documents, meaning their evidential value often depends on the quality of the integrated controls in the digital systems and general operational environment<sup>19</sup>.

Consequently, security surrounding digital systems and the storage of digital data must be so stringent that internal control requirements and external legal requirements for documentation are satisfied.

With the transition from paper format to digital systems the control environment changes character further from essentially manual to essentially pre-programmed computer-based controls. These must function earlier on procedurally in order to be effective and preventative in relation to unforeseen or systematic faults in automated data-flows.

It is important to ensure that system, data and operational security, i.e. both IT security in general and security surrounding individual systems, is satisfactory and geared to public body activities and conditions in general.

### ***5.2.2. Risks of digital environments***

An inadequate control environment can allow for unauthorised access to systems and data – either via the Internet or an internal workstation. Thus, data can risk being changed, copied (stolen) or erased without being able to determine, when the changes have occurred or by whom.

Unauthorised access can pave the way for IT fraud. Examples of this have included attempts to change accounting data, set-up and transfer funds to fictitious suppliers, customers or employees, conceal fake or falsified transactions, theft of programmes and data, as well as hacking, sabotage, etc. This can lead to considerable damage to a public body's data assets – both economically and as operational data – and in certain cases potentially threaten a public body's operational ability or existential foundation.

---

<sup>19</sup> 'Auditing Paperless Systems, An internal guide to auditing electronic forms, imaging and messaging systems', The United Kingdom National Audit Office, April 1998.

### ***5.2.3. Managerial challenges***

In future, public body management must assess to a greater extent whether its digital systems meet its corporate strategy and are implemented in accordance with such. Likewise, it is the management's responsibility to ensure that the systems contain sufficient transaction and control-trace capabilities (known as audit trail), suitable preventative, detective/corrective controls (digital system controls), an adequate functional separation, and that the systems operate in an IT environment that is sufficiently safe.

Digital systems controls must often be activated earlier – be preventative instead of detective/corrective – due to the rapid electronic and automated information flow. It is important that not only master files (and corrections hereto) but also transaction files (and corrections hereto) are updated in a controlled manner and that computer-based controls be scheduled and maintained, as deficiencies in these will lead to the increased risk of financial loss.

The risk picture changes and becomes more dynamic. Both the technical and economical life span of hardware and software is shortened and must constantly be replaced by newer versions. Correspondingly, today's IT security systems may not be able to meet tomorrow's demands for security and must subsequently be replaced by new security systems or updated.

Therefore, IT security and policy in future should fill a regular slot on the agenda for public body management. IT security will no longer be an issue confined to a public body's IT departments.

Through IT security policy the management must decide on the desired level of security and how risks are to be countered. IT security policy should include both internal and external threats (risks) against the systems and data indispensable for a public body's mission and development.

## ***5.3. Audit of digital ('paperless') environments***

### ***5.3.1. Audit objective***

The financial audit's primary objective is to provide an informed opinion of the quality of the yearly accounts as submitted by the management in order for Supreme Auditing Institutions (SAIs) to be able to make an appraisal of this in an audit report. The audit objective is not affected by a public body having made the transition to a digital environment.

### ***5.3.2. System and substance audit***

An audit is arranged and performed on the basis of materiality and risk, based on the audit risk model – and carried out in accordance with proper, public sector auditing practices. SAIs must perform their audit in a financially expedient and efficient manner in order that relevant and sufficient audit proof is obtained at a reasonable price.

The audit is prepared as a system audit and combined with a substance audit to the necessary extent. The audit must establish proof of the system's audit trail. System audit involves both the audit of IT-based and manual procedures, including general IT controls supporting the IT-based user systems and internal controls. For example, substance audit can be accounts analytical auditing, voucher/receipt audit, possibly carried out with the support of CAAT (computer-assisted audit techniques) – based on an assessment of the reliability of the internal control body.

When a public body's administrative and financial procedures are digitised, a public body's IT and IT-related procedures gain significant importance for the planning and performance of the audit. Therefore, the SAI must investigate whether the internal supervisory body of the user systems, etc., functions so effectively that data integrity, reliability and completeness are assured, and whether the user systems function in the IT environment with satisfactory systems, data and operational reliability.

The following section describes how the audit of the application of IT can be structured.

### **5.3.3. Audit of IT application<sup>20</sup>**

The investigation of a public body's application of IT is divided most expediently into:

- a. initial assessment of the application of IT
- b. review of general IT controls
- c. review of controls in user systems
- d. outsourcing

#### **a. Initial assessment of the application of IT**

The objective of the SAI's initial assessment of the application of IT is to create an overview as a basis for the structuring of the audit and to gather information on the public body's IT organisation, hardware and software, method of management and important user systems and databases.

SAIs make an assessment – on the basis of materiality and risk – of the significance of the application of IT and whether the public body, in the event of failure or reduction of IT capacity, is at risk of significant financial loss, etc.

#### **b. Review of general IT controls**

The objective of the SAI's review of general IT controls is to assess whether systems, data and operational reliability are sufficient to form the basis for audit of the user systems. General IT controls are those controls that a public body management has decided should be implemented in the IT environment so that the outer perimeters for system, data and operational reliability become acceptable, according to the needs of the public body.

---

<sup>20</sup> Audit Committee, Association of State Authorized Public Accountants, Denmark, Statements of Auditing Standards nos. 14 (September 1995) and 17 (March 2000).

These controls are different in nature and can be organisational, physical, pre-programmed or manual, for example.

The audit of general IT controls is performed primarily by means of interview, observation and verification of the information obtained.

The review will normally comprise IT strategy and policy, organisational conditions, systems development and maintenance, operational execution, access controls, data-communication, physical security, backing-up and contingency plans.

The review includes e.g. an investigation of whether functional separation exists in and around the IT functions, around systems development and management and whether there are sufficient access controls.

Finally, the SAI must investigate whether relevant legislation concerning electronic data processing is being complied with.

The review of general IT controls is completed with the SAI's conclusion as to the quality of these, including to what extent the SAI can expand on these controls during the course of the further audit of the user systems.

### *c. Review of controls in user systems*

A user system is understood as being a system – an application – that involves some systematic, IT-based and manual administrative functions in a given area.

In a user system the internal controls are pre-programmed and supplemented to the necessary extent with manual controls.

Review of a user system normally comprises:

- the system's functions,
- the records used,
- processing of data input/output,
- pre-programmed and manual controls,
- transaction and control-tracking and
- compliance with relevant data legislation.

The objective of the SAI's review is to investigate whether the internal controls in the user system ensure a complete, exact and timely processing of approved transactions, and whether those internal controls prevent mistakes from occurring, or indeed ensure that mistakes are discovered and corrected. Finally, the review must account for the extent to which documentation exists on performed data processing in the user system and on the preventative, pre-programmed and manual controls.

In the event the internal controls in the user system function satisfactorily, then the audit can expand upon them to a considerable extent. If the controls do not function satisfactorily the SAI must assess whether the audit objective can be realised another way.

Should the SAI conclude that significant weaknesses exist in the internal controls in the user system or that there are discrepancies in the accounts or accounting procedures, then the

situation must be reported in the auditor's recommendations and possibly also in the audit report.

A user system, which provides the opportunity for sending, receiving and processing data electronically to/from the public body's trading partners, typically comprises the following primary components: an applications programme (e.g. finance system), a data communication method (e.g. a dial-up modem connection or link-up via a VANS<sup>21</sup> supplier), a shared standard for the exchange of data (e.g. XML-format) and possibly translation and/or conversion software (translation from a shared standard for the exchange of data to an internal record format).

System integration is possible because the systems are modularly constructed and have open interfaces both externally to the Internet and internally in the public body to other systems and in general are based on electronic approval of all transactions.

For the public body, the primary risk with such a system is whether the received input data is correct when it is downloaded into the user application, and whether the output data transmitted from the public body is also correct. Furthermore, it is important that a public body can ensure and secure documentation concerning the sending/receiving of transactions (non-repudiation), and that the content of those transactions are not affected during data transmission (integrity).

In order to validate that the input and output data is correct, it is important that the user system-controls validate the data using two controls, called Control 1 and 2, cf. figure 8<sup>22</sup>.

**Figure 8 – Dataflow and validation controls**

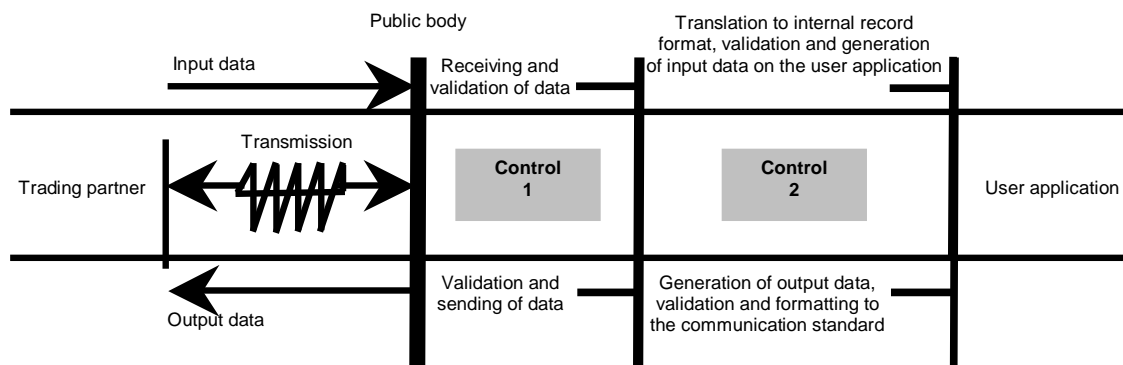


Figure 8 shows the electronic dataflow between the public body and its trading partners. In addition, it shows the validation of data received and sent at Control 1 and validation of input and output data at Control 2.

<sup>21</sup> Read Value Added Network Supplier (or Service)

<sup>22</sup> 'EDI in smaller business enterprises', Danish EDI-Counsel, 1998.

## Control 1

Control 1 is located in the user system's interface just after the receiving of and just prior to the sending of a transaction.

Control 1 must ensure that the electronic transaction complies with the following fundamental requirements of the data;

- **Authenticity** (the originator actually is who he/she/it claims to be).
- **Integrity** (data received is the same as the data sent).
- **Confidentiality** (data has not been accessed by unauthorised parties).
- **Non-repudiation** (sender/receiver cannot deny having sent/received the data).

In fully digitised systems the above-mentioned conditions are satisfied with both the sender and receiver.

When Control 1 has ensured that the received and/or sent data is authentic – that it has remained confidential and not been compromised during data transmission, that it has arrived at the recipient site and remains non-repudiated – then the received transaction can be transferred to the user application (finance system). This stage, however, is also open to a certain element of risk, which Control 2 aims at countering.

## Control 2

Control 2 is sited immediately before the application. Control 2 translates and forwards received transactions and transactions for sending to and from the underlying user application (finance system).

Control 2 must secure input and output data with regards to:

- **Completeness** (e.g. there is no break in completeness during translation from external to internal data format, that system failure does not cause loss of data or the such, or that faults with the sender of the transaction does not lead to the transaction not being received in its entirety. A manual control should ensure that potentially filtered faulty transactions are subsequently registered correctly in the application).
- **Accuracy** (e.g. the validation of received transaction data concerning, for example, product numbers, quantity, quality, prices, etc. The same control also applies to the transaction data sent by the public body).
- **Validity/approval** (e.g. validation to ensure that only transactions pertaining to the public body are transferred to the user application. It should be ensured that an approval procedure of collective received transactions is in place and that approval is performed by properly authorised personnel)
- **Timeliness** (ongoing operational updating cycles must ensure that the data processing of downloaded transactions takes place in a timely manner).

A precondition for the efficiency of the user system's controls is that sensible and efficient general IT controls are in place.

With the audit of controls in the user systems, the SAI should focus on controls being established on several different levels.

As outlined in the aforementioned, the first control must ensure a transaction's authenticity, confidentiality, integrity and non-repudiation.

The second control must ensure a transaction's completeness, accuracy, validity and timeliness.

#### ***d. Outsourcing***

Given that parts of a public body's IT application are outsourced to an external operative body, it will remain the responsibility of the public body's management to ensure that system, data and operational reliability surrounding the processes, as well as systems and access to data, is in accordance with the needs of the public body.

To ensure these conditions a written agreement must exist between the public body and the external operative body. Normally, such a written agreement should as a minimum also comprise a yearly declaration from the external operative body's accountant on system, data and operational reliability.

As part of the audit, the SAI must review the contract with the external body and in general be provided full access to collective procurement data held by the operative body pertaining to the public body in question.

### **5.4. Concluding remarks**

Although the primary objective of the financial audit is to provide the SAI with an informed opinion of the quality of the submitted annual accounts, the audit is prepared as a systems audit and combined with a substance audit to the necessary extent.

Systems audit comprises an audit of IT-based and manual procedures, including the general IT controls which support the IT-based user systems/procedures and internal controls.

The audit of digital systems is divided into an initial assessment of the application of IT, a review of general IT controls, a review of controls in user systems and an assessment of potential outsourcing agreement.

The audit of general IT controls reveals the extent to which system, data and operational security is adequate and can form the basis for an audit of the user systems.

Audit of the user system controls reveals whether there are suitable controls established that ensure a transaction's authenticity, confidentiality, integrity and non-repudiation, as well as its completeness, accuracy, validity and timeliness.



## **6. ORGANISATIONAL CONSEQUENCES**

### **6.1. Introduction**

Digitalisation of work procedures in public institutions raises similar demands for individual SAls to take strategic initiatives in this area. These initiatives must be targeted towards SAls making the transition to digital procedures and towards procedural development and continuing education in the IT skills area.

The basis for these initiatives is primarily the acknowledgement of the dependence on IT, and that IT constitutes a decisive factor for realisation of the SAI mission and vision.

The basis for the digital transition of SAls will be an interplay between organisational strategy and IT strategies. It is important that senior SAI management stipulates the formal framework for the application of IT and that primary responsibility for IT management and application, including security, rests with senior management.

The digitalisation of SAls requires adaptations in 4 important areas:

- the transition to digital procedures
- methods
- qualifications
- resources

### **6.2. The transition to digital procedures**

SAls, like any other public institutions, will experience the need to undertake an efficiency drive of working routines with the assistance of digitalisation. In order to adjust SAls to digital procedures and in order to better be able to process electronic documentation, this development will require:

- strengthening of IT organisation and technology,
- ensuring that IT security meets new demands, including back-up, firewall, etc, being able to cope with internal data only being available electronically,
- the implementation of a policy for new procedures and routines surrounding the receiving and sending of e-mails so that employees use, register and process e-mails professionally,
- the establishment of one or more official e-mail addresses at authority, institutional, departmental and/or employee level,
- communicating the transition process to employees in the organisation,
- communicating the institution's amended guidelines for digital communication to external partners.

As such, digitalisation will result in the demand for SAI knowledge of IT being strengthened in order to be able to implement and use new tools and methods. Similarly, digitalisation will demand that the internal IT function is strengthened, enabling the organisation to process

only digital information – i.e. mail servers, firewalls, security, etc, will assume a much more important role than before.

### **6.3. Methods**

Audit in a digital environment cannot be performed in the same manner as in one that is paper-based. One example of what these changes may imply is when a ferry public body has gone from a completely manual paper-based ticketing system to an electronic ticketing system which more or less functions without human intervention. The public body has installed a new, electronic sales/ticket/billing/payment system that can sell tickets via the Internet, receive payments via card systems via the Internet, register vehicle-boarding, perform accounting and print out invoices automatically, etc.

This development will give rise to the demand for auditing procedures and concepts to be amended, so auditing adequately reveals the new risks. Examples of necessary strategic initiatives include:

- development of new auditing methods and tools.
- the investigation of what new technologies can be used internally in new concepts, e.g. statistical random tests and specially developed applications (e.g. CAAT).

### **6.4. Qualifications**

Digitalisation of important functions in companies means that traditional paper-based procedures and internal controls will become obsolete and replaced by electronic data – with the exception of those elements of procedures concerning the physical flow of goods.

For SAIs this marks an important change in the control environment. One-off transactions that previously were documented with vouchers/receipts will now be replaced by digital information (data) accompanied by an electronic approval of transaction. The audit of general IT controls and IT-based user systems will in future constitute a much greater element of systems auditing and require more man-hours and personnel with both auditing and IT skills.

Examples of necessary strategic initiatives include:

- training in how a digital environment is audited, cf. Chap. V;
- training in use of the new tools (IDEA, CAAT, etc);
- ongoing continuing training as a result of technology – with the auditee and internally in the organisation – constantly evolving;
- course days for the whole organisation focussed on attitudes and understanding;
- strengthening internal IT so organisation and technology can cope with data only being available in digital format;
- organisational changes and restructuring in order to meet the new tasks.

## **6.5. Resources**

Primarily, the transition process entails the need for greater resources. The new concepts must be developed, just as it must be assumed that the auditing of the individual client will consume greater resources in a fully digitised environment. There are, however, two conditions that counter this tendency. Firstly, the development of new auditing methods and tools aims at improving efficiency. Secondly, development in some countries is heading towards ever larger IT service-centres.

One consequence of digitalisation is that the demand for close physical proximity to data and information will disappear. That is to say that functions that previously lay widely dispersed geographically can now be gathered together, for example, wages and recruitment, which are complex tasks and heavily taxing on resources.

On the one hand, it must be assumed that the auditing of the individual public body will consume greater resources, whilst on the other, the tendency is that there will be fewer companies to audit.

An uncertain picture is emerging on the resources front. Presumably the greater demand on resources will only last during a transitional period. One example of a necessary strategic initiative is:

- large-scale managerial awareness towards exploiting the opportunities for the improvements in efficiency with the structuring of the new auditing methods.

## **6.6. Concluding remarks**

For SAI's, digitalisation of the public sector will mean an important internal technical and organisational adjustment, demanding strategic initiatives consisting of:

- Transition to digital procedures
- Development of new auditing methods and tools
- Development of auditors' IT skills
- Exploitation of efficiency potential through improved structuring of new audit methods.

## **GLOSSARY**

<b>Accountability</b>	– In information security, a 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. This objective is defeated with the sharing of passwords.
<b>Accuracy</b>	– Property assured by a system's control sited immediately before the user application to validate received transaction data concerning, for example, product numbers, quantity, quality, prices, etc.
<b>Authenticity</b>	– In information security, the property that determines that the originator of a message, a file, etc., actually is who he/she/it claims to be.
<b>Availability</b>	– The ability to access and use a system, resource or file, when and where required.
<b>Back office system (or back end)</b>	– Computer infrastructure within an organisation, which supports core business process applications but has no external interface with costumers (unlike a Web site or portal)
<b>Certification authority</b>	– In cryptography, an authority trusted by all users to create and assign digital certificates This role is usually performed by public institutions, such as Post Office or clearing banks (e. g. Barclays).
<b>Controls in user systems</b>	– Internal pre-programmed controls supplemented to the necessary extent with manual controls.
<b>Completeness</b>	– Property assured by a system's control sited immediately before the user application, to ensure that there is no break during translation from external to internal data format or that system failure does not cause loss of data or that faults with the sender of the transaction does not lead to the transaction not being received in its entirety.
<b>Confidentiality</b>	– In information security, the property that information is not made available or disclosed to unauthorised individuals, entities or processes.
<b>Digital certificate</b>	– In cryptography, a message that guarantees the authenticity of the data contained within it. In public key cryptography to guarantee authentication a certificate should be issued by a Certification Authority trusted by all users. A certificate generally contains the public key owner's identity, the public key itself and its expiry date.

<b>Digital documents</b>	<ul style="list-style-type: none"> <li>– A public body's data that exists in electronic or digital format including not only documents that have been digitised from paper media (e.g. letters) but also those that only exist and are used in digital form throughout their entire 'life-span'.</li> </ul>
<b>Digital signature</b>	<ul style="list-style-type: none"> <li>– File decryption and encryption to authenticate certain type of communication in transaction services binding via the Web, that usually must be in writing to be legally valid, used by administration to communicate safely and legally with citizens, business or other public authorities(G-2-C; G-2-B; G-2-G).</li> </ul>
<b>Domain</b>	<ul style="list-style-type: none"> <li>– Part of the naming hierarchy of the internet. A domain name precisely locates an organisation or other entity on the internet, for instance: <a href="http://www.eurosai.org/">http://www.eurosai.org/</a> . An address of the form <a href="http://www.eurosai-it.org/">http://www.eurosai-it.org/</a> . is a sub-domain.</li> </ul>
<b>E-decision making</b>	<ul style="list-style-type: none"> <li>– Interaction between the public sector entities and how society organizes itself for collective decision through the use of electronic transparent mechanisms.</li> </ul>
<b>E-government</b>	<ul style="list-style-type: none"> <li>– The use of information and communication technologies by the government with the aim to: (a) provide more and/or better information and other services, externally to citizens and businesses, and internally to other government organisations; (b) improve government operations in terms of more effectiveness, and/or efficiency; (c) enhance political participation.</li> </ul>
<b>E-governance</b>	<ul style="list-style-type: none"> <li>– Signifies the development, deployment and enforcement of the policies, laws and regulations necessary to support the functioning of a digital society and economy. Governance issues blossom through all levels of e-government.</li> </ul>
<b>E-procurement</b>	<ul style="list-style-type: none"> <li>– The replacement of traditional trading documentation, for example purchase orders and invoices, by electronically transferred data.</li> </ul>
<b>Front office system (or front-end)</b>	<ul style="list-style-type: none"> <li>– Computer infrastructure in an organisation designed specifically as an interface for communicating with external costumers, such as Web sites or portals.</li> </ul>
<b>General IT controls</b>	<ul style="list-style-type: none"> <li>– In information security, controls implemented in the IT environment in order that the outer perimeters for system, data and operational reliability become acceptable, according to the needs of the public body. These controls are different in nature and can be organisational, physical, pre-programmed or manual, for example.</li> </ul>
<b>Integrity</b>	<ul style="list-style-type: none"> <li>– In information security, the property that signifies that data received is the same as the data sent.</li> </ul>

<b>Internal controls</b>	<ul style="list-style-type: none"> <li>– In information security, pre-programmed controls in the user system to ensure a complete, exact and timely processing of approved transactions; also meant to prevent mistakes from occurring, or indeed to ensure that mistakes are discovered and corrected.</li> </ul>
<b>Interoperability</b>	<ul style="list-style-type: none"> <li>– In information systems, the property that allows two operators networks to interconnect in order for services to interoperate across the interconnection boundary.</li> </ul>
<b>On-line democracy</b>	<ul style="list-style-type: none"> <li>– The carrying out of business with the citizens' participation in policy formation through processes running on the computer system, and specifically, on the Internet. Decision makers may, for instance, organize opinion polls or referenda regarding certain policy issues, such as infrastructure plans, proposed legislation etc. The outcome of such polls/referenda may play a role in the process of decision making.</li> </ul>
<b>Performance audit</b>	<ul style="list-style-type: none"> <li>– Performance audits are reviews designed to determine how efficiently and effectively an agency is carrying out its functions. Performance audits may review a government program, all or part of a government agency or consider particular issues which affect the whole public sector.</li> </ul>
<b>Procurement</b>	<ul style="list-style-type: none"> <li>– Every aspect of the process of determining the need for goods and services, and buying, delivering and storing them. Procurement is central to the management of any operation and is vital to get the necessary goods and services of the right quality, the right price and at the right time. is where aggregation of purchasing requirements enables significant value for money improvements to be made</li> </ul>
<b>Public-key certificate</b>	<ul style="list-style-type: none"> <li>– A statement, possibly on paper but more often transmitted electronically over an information network, which establishes the relationship between a named individual (or organisation) and a specified public key. In principle, it could (but need not) include other information such as mailing address, organisational affiliation and telephone number.</li> </ul>
<b>Non-repudiation</b>	<ul style="list-style-type: none"> <li>– In information security, the property that signifies that the sender/ receiver cannot deny to have sent/received the data.</li> </ul>
<b>Re-engineering business processes</b>	<ul style="list-style-type: none"> <li>– Innovation and transformation of structural and work processes in order to improve service quality and efficiency in public sector.</li> </ul>
<b>Reliability</b>	<ul style="list-style-type: none"> <li>– In information systems, the ability of a computer or an information or telecommunications system to perform consistently and according precisely to its specifications and design requirements and to do so with high confidence.</li> </ul>

<b>Security</b>	<ul style="list-style-type: none"> <li>– The collection of safeguards that ensures the confidentiality of information protects the system(s) or network(s) used to process it and controls access to it. Hence, security safeguards impose appropriate access rules for computer information.</li> </ul>
<b>Smart card</b>	<ul style="list-style-type: none"> <li>– Transactional electronic technology capable of storing and updating authentication or account information about the user</li> </ul>
<b>Substance audit</b>	<ul style="list-style-type: none"> <li>– The process of collecting and evaluating evidence to form an opinion on whether the internal control system is reliable.</li> </ul>
<b>System audit</b>	<ul style="list-style-type: none"> <li>– The process of collecting and evaluating evidence to form an opinion on whether an information system (user application) safeguards assets, maintain data integrity, allows organizational goals to be achieved and determine the efficient use of resources.</li> </ul>
<b>Technical audit</b>	<ul style="list-style-type: none"> <li>– The process of collecting and evaluating evidence to form an opinion on whether (components of) the IT infrastructure safeguards assets, maintain data integrity, allows organizational goals to be achieved and determine the efficient use of resources. IT infrastructure here means computer hardware, networks, operating systems and all other software that are not user applications (database management, security software, data center management systems, etc.).</li> </ul>
<b>Telematics</b>	Collection of technologies that combine telecommunications and computing.
<b>Timeliness</b>	<ul style="list-style-type: none"> <li>– In information security, a property assured by a system's control sited immediately before the user application to ensure that when operational updating cycles occurs the data processing of downloaded transactions takes place in a timely manner.</li> </ul>
<b>User system</b>	<ul style="list-style-type: none"> <li>– A system application that involves some systematic, IT-based and manual administrative functions in a given area.</li> </ul>
<b>Validity/approval</b>	<ul style="list-style-type: none"> <li>– In information security, a property assured by a system's control sited immediately before the user application to ensure that an approval procedure of collective received transactions is in place and that approval is performed by properly authorised personnel (e.g. validation to ensure that only transactions pertaining to the public body are transferred to the user application).</li> </ul>
<b>Vulnerability</b>	<ul style="list-style-type: none"> <li>– A weakness in a system that can be exploited to violate the system's intended behaviour. There may be security, integrity, availability and other vulnerabilities. The act of exploiting vulnerability represents a threat, which has an associated risk of being exploited.</li> </ul>

