

IT governance in the public sector: 'top-priority'

Thomas Wijsman, Paul Neelissen, Chris Wauters
The Netherlands Court of Audit

Abstract

Management tools at the operational and tactical levels can contribute to better control of IT by ministries. However, what is of crucial importance is that the senior management level governs IT as a strategic asset. IT governance comprises strategic planning and control, accountability and external supervision. Results from a descriptive study by the Netherlands Court of Audit show that at this point ministries occupy themselves mainly with strategic planning, paying relatively low attention to internal control and accountability. We strongly believe IT auditors and SAIs can play a key role in advancing IT governance. However, while IT governance is still in its infancy, taking an audit stance we risk auditing IT governance 'to death'. A descriptive, fostering approach may be more fruitful.

1 Introduction

Planning and control of IT is a major problem. IT represents a substantial cost factor, but not always fulfils its promises. Existing systems often perform poorly, are generally expensive in terms of costs of use and maintenance, and get out of date rapidly. Also, the acquisition of new systems — whether in-house build or procured externally — is complex and costly and more often than not suffers from considerable overspending, overdue delivery and/or deficient user functionality. Issues such as these are getting more intricate over time because information systems evermore are expected to interact with other, internal and external systems. The need to find adequate solutions to these problems is becoming evermore urgent because expectations about the value IT can add to the business processes are continually rising.

In this paper we first identify the deployment of IT as a strategic issue. Next, we give a rough sketch of the development of IT governance as part of a wider governance movement. After that, we present our conception of the term IT

DRAFT

governance. Then we proceed with an account of a descriptive study by the Netherlands Court of Audit in the area of IT governance. We conclude with reflections on the role of IT auditors and SAIs.

2 IT Governance

2.1 A strategic issue

The problem of how to deploy IT in such a way that it adds value to the business is far from new and has been a focal area for information managers for a number of years. The use of tools in the area of development and management of information systems, such as Prince2, CMM/CMMI, ASL and ITIL can contribute substantially to better control of IT. However, all these tools offer solutions only to partial problems at the *operational/tactical* level, while the root causes of structural problems in the IT area often lie at the level of *strategic planning and control* of IT. After all, IT has evolved from a purely support technology of marginal importance to an essential and integral part of all government's primary and secondary processes. In the past, IT was no more than a business tool that made the ministries' processes more effective and efficient. Today, it has grown into a strategic resource without which the government could not meet the needs of society. IT increases the government's flexibility and customer friendliness and improves its collaboration with partners in the policy chain. The smart use of IT lets the government work more efficiently and operate better. Therefore, a ministry's senior management cannot afford to be non-committal on IT. In other words, ministries must get to grips with IT.¹

Since the 1990s the NCA carries out audits of the use of IT by the government, aiming to contribute to improved information management within the national government. Our reports show that fairly often it is precisely at the strategic level that government is not at grips with IT. Let us give an example. In 2003 we reported on our audit of a complete renewal programme of the technical and application infrastructures of the police sector. It showed that major problems existed in the areas of goal setting, justification of selected solution directions, deciding on targets and intermediate goals, carrying out base-line measurements of IT performance, financial underpinning, time planning and project risk awareness. These kinds of problems call for structural solutions at the strategic

¹ We use the term *IT governance* rather than *ICT governance* because it is more commonly used.

D R A F T

level of government organizations. We did not use the term then, but this is what we would now call IT governance.

2.2 *Getting to grips with IT: IT-governance*

The awareness that IT is the responsibility of the top level of an organization has become evermore widespread since the 1990s. The rise of the governance body of thought (corporate governance, government governance) and the understanding that the deployment of IT has developed into a crucial link between business operations and the realization of an organization's mission has led to heightened attention for IT as part of governance. Consequently, we are witnessing a rapidly growing interest in IT-governance worldwide. What is new about IT governance when we already had information management, IT management, IT project management and IT project portfolio management? We believe the innovative aspect is threefold. First, to us the essence of IT governance is the integration of the IT aspect in the 'mainstream' of an organization's governance processes, rather than treating the governance of IT as a separated set of activities to be carried out by specialists. Second, in connection with the previous point, IT governance is primarily the responsibility of top management, not IT staff. Third, IT governance has a wide scope and encompasses strategic planning and control, accountability and external supervision. We will clarify these components below. It is generally acknowledged that governance is a key factor in the achievement of policy objectives. Within this governance movement, IT governance is gradually emerging as a discernible but integrated field because of the strategic contribution of information systems and IT to policy implementation. The purpose of IT governance is to ensure that the application infrastructure and the underlying technical infrastructure enable public authorities to operate effectively, aware of its position in the policy chain and to the best of its ability.

2.3 *From Governance to IT governance*

The concept of governance has been evolving since the 1990s and its IT component has steadily been growing in significance. At the root of this rising interest lies the need of stakeholders for *transparency* and *accountability* regarding the way organizations are being governed. This governance 'movement' originated in the business sector in the form of corporate governance. Major initiatives were taken by the Committee on Sponsoring Organizations of the Treadway Commission (COSO) in the USA and the Cadbury Committee on Corporate Governance in the UK. Another milestone was the introduction of the Sarbanes-Oxley Act of 2002,

D R A F T

which applies to all companies traded on US stock exchanges. The application of the corporate governance concept to public authorities resulted in the emergence of *government governance*. Important documents in this area were published by the Chartered Institute of Public Finance and Accountancy (CIPFA) and the International Federation of Accountants (IFAC). The Guidelines for Internal Control Standards for the Public Sector (INTOSAI, 2004) should also be mentioned here. These standards can be considered as an interpretation of the COSO internal control standards for the public sector. In the Netherlands, the Ministry of Finance took the lead in turning corporate governance principles into government governance principles. The ministry defines government governance as safeguarding the interrelationship between management, control and supervision by government organizations and by organizations set up by government authorities, aimed at realising policy objectives efficiently and effectively, as well as communicating openly thereon and providing an account thereof for the benefit of the stakeholders.

The increased consideration of IT and its importance to operational management has led to the application of the body of thought on governance on the area of IT resulting in the emergence of *IT governance*.

Among the major international organizations that are engaged in IT-governance are the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI). ISACA is the international organization of IT auditors, which has developed the leading framework of Control Objectives for Information and related Technology (CobiT), maintained as well as supported by supplementary documents by ITGI. Also consultancy firms that provide advice in the area of information management in relation to organizational issues are active in this field. For instance, the Gartner consultancy was among the firms that were involved in IT governance at an early stage. Their publications include *Designing effective IT governance* (Gartner, 2003b), *Creating an effective IT governance process* (Gartner, 2003a) and *Tailor IT governance to your enterprise* (Gartner, 2003c).

In *the Netherlands*, NOREA, the association of IT auditors, is in the vanguard of IT governance. It published an explorative study which takes stock of the definitions and models of IT governance, looks at a number of practical applications and considers the significance and consequences of IT governance for the IT audit profession.

DRAFT

2.4 A definition of IT governance

There are plenty of definitions on IT governance. Typical examples are those given by Gartner and by the IT Governance Institute (ITGI):

- Gartner: IT governance specifies the decision rights and accountability framework to encourage desirable behaviour in the use of IT.
- ITGI: IT governance is the responsibility of executives and the board of directors, and consists of the leadership, organizational structures and processes that ensure that the enterprise's IT sustains and extends the organization's strategies and objectives.

What we learn from the various definitions is twofold. First, IT governance is the responsibility of top management of an organization, i.e. the person or group of people who direct and control an organization at the highest level. Second, The result of IT governance should be that IT is being deployed in a controlled manner, in line with the organization's mission.

In fact, this is precisely what IT governance is about. However, definitions at such a general level give us no clue about how we as auditors can obtain evidence of the existence of IT governance processes. Admittedly, it is true that ITGI's definition is linked to the CobiT framework. However, we see CobiT primarily as a management framework, rather than as a governance framework. It is true that CobiT can be used (and actually is often being used) to implement IT governance, but implementing CobiT per se is not identical with IT governance. Organizations that have implemented CobiT still need to explain how they use the framework to implement IT governance. For SAIs to be able to observe IT governance in practical situations we need a definition of the concept of IT governance at a more concrete level. We found a basis for such a definition in the definition of government as provided by the Netherlands Ministry of Finance (see above). We expanded the definition by adding a component that reflects the (partial) responsibility that ministers bear for non-departmental public bodies (NDPBs)².

We define IT governance as the joint responsibility of the executive management level of an organization and its supervisor(s) for (1) *strategic planning* and (2) *internal control* of the organization's deployment of IT and for (3) *external accountability* and (4) *external supervision* of the organization's deployment of IT. This definition, comprised of two internal and two external components has a

² The official term for Non-departmental public bodies (NDPB's), translated into English, is 'legal bodies with statutory tasks'. The NCA does not use the more common term 'autonomous public bodies' because public tasks may also be performed by *private* (non-departmental) bodies.

D R A F T

general scope and applies to both the private sector and government. Applied to the (national) government, still another component is relevant because external entities often play a substantial role in realizing a ministry's objectives. This fifth component is (5) *setting and supervision activities concerning the deployment of IT by NDPB's*.

2.5 Components of IT governance

We consider the five components of IT governance in more detail below.

Strategic planning

Strategic planning is the process of steering an organization so that it achieves its policy objectives. It '*sets the course*' for the deployment of IT. Strategic planning includes such activities as planning and organizing the information infrastructure and the underlying IT, designing the concern architecture (the information architecture for the organization as a whole) and IT processes and drafting internal procedures, rules and instructions.

Internal control

Internal control is the process of introducing and effecting a system of measures and procedures to determine whether the organization's activities are and remain consistent with the approved plans. Where necessary corrective measures are taken so that the policy objectives can be achieved. Internal control keeps the IT system '*on course*'. This component includes risk management, compliance with internal procedures and instructions and with external legislation and regulations, periodic and ad hoc management reports, progress checks and revision of plans and audits, evaluations and monitoring.

External accountability

External accountability entails reporting to external stakeholders. It includes progress reports (on large IT projects only)³ and the statement on operational management in the ministry's annual report. In the statement on operational management, the ministers state whether they are 'in control' of their operational management (is there good governance?). This would be a logical place to consider IT governance. The minister could use the statement on operational management to account for the information systems and IT policy and the policy achievements. External stakeholders would then be able to see whether the ministry was in control of its information systems.

³ The Netherlands House of Representatives monitors certain bigger and/or risky projects with extra attention. These projects are designated as 'large projects'.

DRAFT

External supervision

An external supervisor must check that an organization's processes satisfy the applicable requirements and intervene where necessary. In IT governance, the supervisor must monitor the IT policy conducted and the policy achievements. Activities included in this component include information collection, evaluation and intervention.

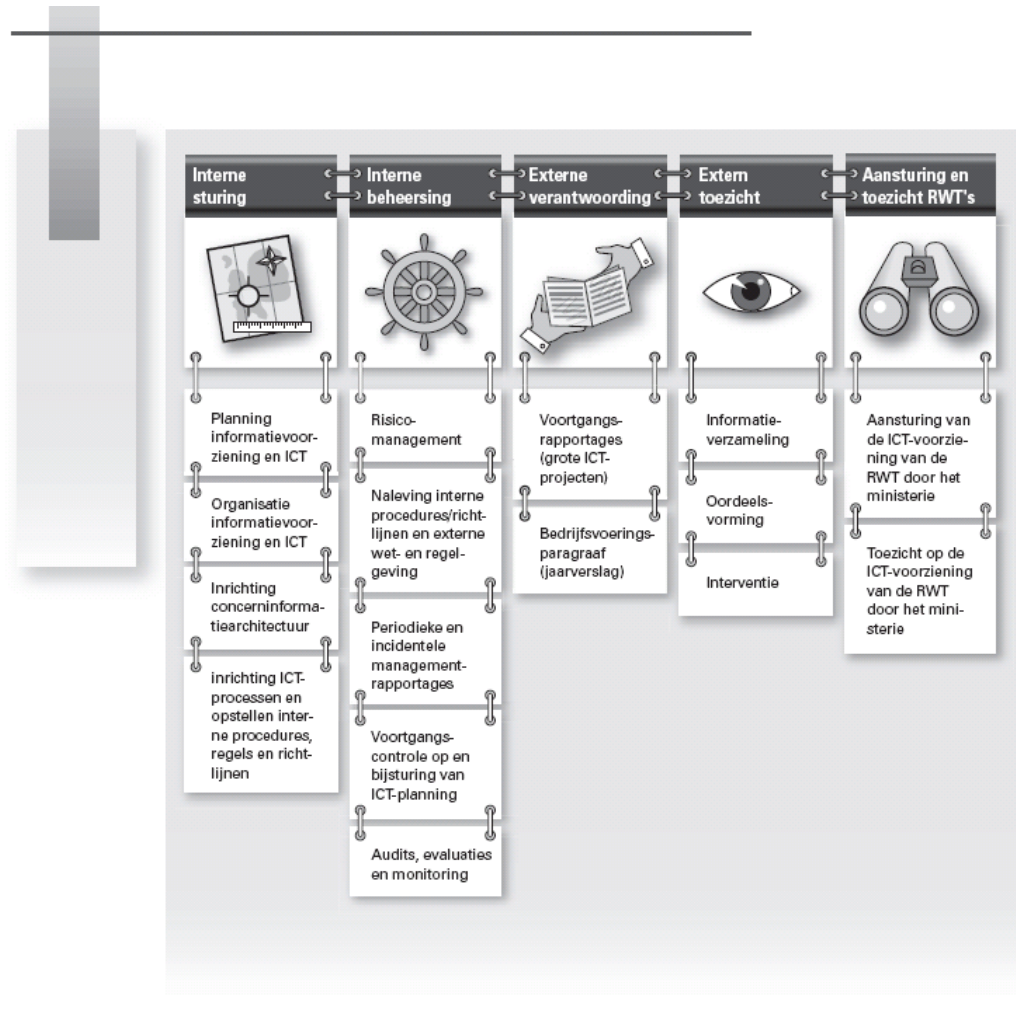
Objective setting and supervision of NDPBs

A ministry sets objectives for, and supervises NDPBs. It also determines whether the NDPBs have complied with applicable agreements and intervenes if they have not. Objective setting and supervision regarding the IT deployment of NDPBs is only included in a ministry's governance insofar NDPBs play an important part in achieving the ministry's policy goals and their work relies on IT systems. Objective setting and supervision are an integral part of the statutory management and accountability arrangements between ministers and 'their' NDPBs.

The figure below summarises the components of IT governance and their components.

D R A F T

Figuur 1



The five components should not be considered in isolation. Our definition of IT governance is based not only on the individual components but also on their relationship with each other. Internal management (setting the course) and internal control (keeping the course) are a 'duality'. There is a continuous interplay between these two components in the plan-control-revise cycle. External accountability is based on the outcome of internal control. External accountability is concerned with the course set and pursued and thus with strategic planning and internal control. External supervision utilizes external accountability information. External accountability information must therefore be keenly tuned to the external supervisor's information needs. The fifth component is closely related to the ministry's strategic planning and internal control. The ministry helps steer the strategic planning and control of its own policy processes by means of NDPBs in the sectors for which the minister is responsible.

DRAFT

To illustrate the model we clarify the component of internal control (see textbox).

Internal control: keeping IT 'on course'

One of our sources of inspiration being COSO, we have worked out the Internal Control component into the following five activities.

- *Risk management.* First: identifying risks and risk analysis regarding the existing application and technical infrastructures. Next: the continual management of risks, for instance using risk sections in yearly plans and periodic risk judgement by senior management.

- *Compliance with internal procedures, rules and directives, and external laws and regulations.*

Examples of the former category are internal directives pertaining to information security, project management, management of IT processes, software development, test management, contracting out and agreements between the user organization and the supplier of IT services. Regarding the latter category of external laws and regulations one can think of privacy protection and information security.

- *Periodical management reporting.* This reporting relates to both the regular, ongoing IT processes and IT projects. For instance: management reporting on ongoing activities comprises cost of IT operations, performance (e.g. compared to performance indicators as specified in a Service Level Agreement or SLA), risks, quality of service, user complaints and service disturbances.

Examples of incidental management reporting areas are major service disruptions and calamities.

- *Progress checks and adjusting IT planning.* This cluster of activities comprises three steps. The first one is to evaluate realized results and costs against the information plan and/or IT strategy, annual plans, project plans and budgets regarding the aspects time, quality and money. The second step is intervention in case of major differences between planning and realization, substantial shortcomings and/or serious risks. The third step is verifying that the intervention resulted in the desired improvement.

- *Audits, evaluations and monitoring.* The major methods that can be used to evaluate if the information processes and the underlying IT is functioning properly are internal or external IT audits, internal or external evaluations, third-party reports, quality assurance procedures, staff satisfaction measurement and measurement of the use of IT services.

IT governance is not a question of 'all or nothing'; IT governance must grow. The maturity of the individual components determines the maturity of IT governance as a whole. Growth models such as the CobiT maturity model can help determine the level of maturity.

Control Objectives for Information and Related Technology (CobIT)

CobIT is without doubt the most commonly applied IT management tool. It defines IT governance as:

'IT governance is the responsibility of the board of directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives.'

The CobIT model can be used by both management (design of IT management) and auditors (review of IT management).

CobIT includes a maturity model that describes the following six stages in the development process for IT governance:

- Non-existent
- Initial / Ad hoc
- Repeatable but Intuitive
- Defined Process
- Managed and Measurable
- Optimised

Other publications by the ITGI include *Board briefing on IT governance* (ITGI, 2003a), *IT governance implementation guide* (ITGI, 2003c), *IT control objectives for Sarbanes-Oxley* (ITGI, 2003b) and several publications as part of their 'Val IT' initiative⁴.

3 A descriptive study on IT governance

3.1 Approach

The conception of IT governance outlined in the previous sections was developed in preparation of an intended audit of IT governance. When working out the most promising approach for the Netherlands Court of Audit to enter the area of IT governance we considered that there did not yet exist an indisputable set of standards against which to audit the IT governance practice of our ministries. Because we also had indications that IT governance at the ministries was still in its infancy we decided against an audit-based approach and choose for a fostering strategy instead. Our aim was to start a discussion on IT governance with the

⁴ Val IT complements COBIT from a business and financial perspective. While CobIT is a best practices framework for the management and delivery of high-quality information technology-based services, VAL IT is a best practices framework aimed at measuring, monitoring and optimizing the realization of business value from investment in IT.

D R A F T

ministries with the aim to try and develop a common understanding about the concept and the way forward to further improve the government's IT governance. To be constructive this discussion should be based on evidence because a purely theoretical discussion would put the government in a noncommittal role. We therefore developed a descriptive framework taking our IT governance definition, as presented in section 2 as a starting point. Based on our experiences from previous audits we concretized the concept by specifying the observables we consider signs of the components of our governance framework being in place. While being interchangeable to a certain extent with those others may make, our choices are not arbitrary. They are based on our experiences about what the major measures are which contribute significantly to strategic planning and control and to accountability of the deployment of IT. Our elaboration of the component of internal control is given in the textbox in section 2.5; please consult the report for the complete framework (available in English via our website: www.rekenkamer.nl). The framework was used to carry out a descriptive study on IT governance in practice at two ministries, namely the Ministry of Economic Affairs and the Ministry of Social Affairs and Employment.

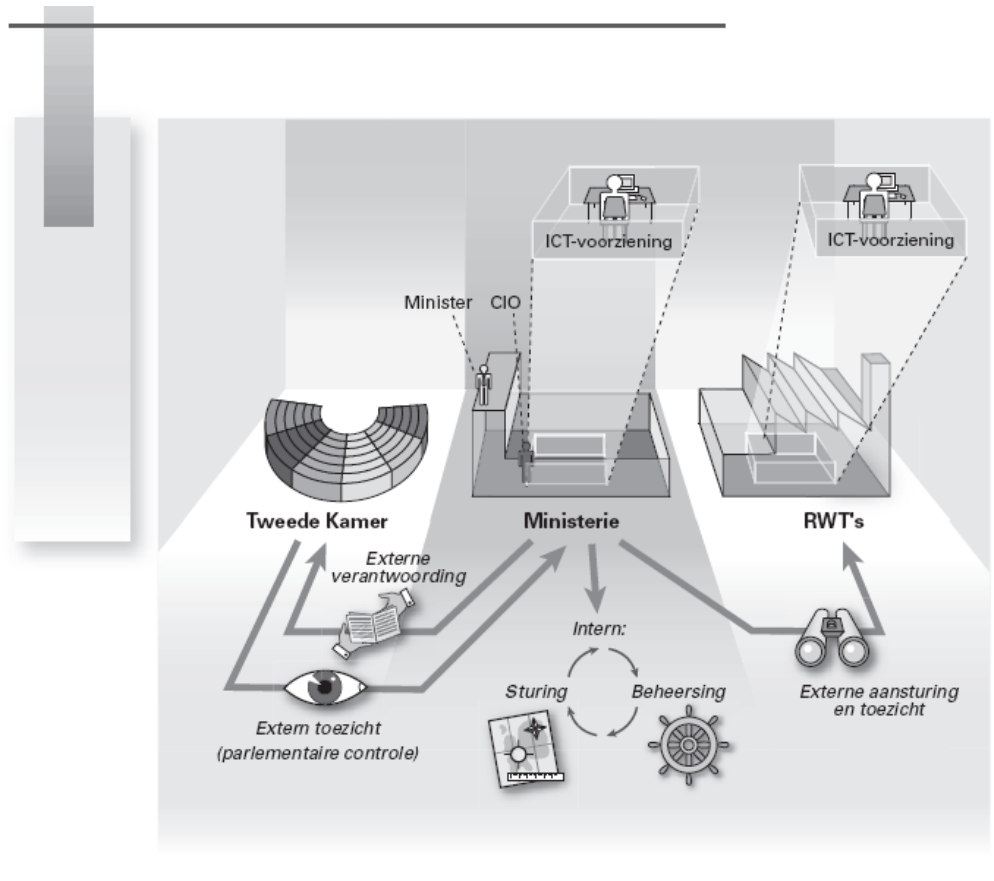
3.2 Key players

Responsibility for IT governance in government is shared by several players: the ministry, the House of Representatives and NDPBs where applicable (see figure 2).

Within the ministry, the chief information officer (CIO) is responsible for IT governance. At ministries, the deputy secretary-general usually exercises this function. As well as the CIO, the following players are involved in IT governance at a ministry: the central information management department, the policy departments, the central IT department, the local IT divisions, the financial and economic affairs department and the internal audit department. While in some cases there may also be other external supervisors, there is at least one external supervisor: the House of Representatives. Constitutionally, the House of Representatives *monitors* government. This term is used in this report where we refer specifically to the House of Representatives. In more general references, we use the term *supervision*. Supervision (monitoring by the House of Representatives) requires information and thus external accountability by the minister. Finally, NDPBs can play a role. If the IT element in an NDPB's primary process is essential to achieve the ministry's policy objectives, the ministry should be involved in objective setting and supervision of the NDPB's deployment of IT. Figure 2 shows the players involved in IT governance

D R A F T

Figuur 2



3.3 Findings

It appeared that both ministries are working hard on the design and implementation of their IT governance. Although there are some differences in their approaches, the number of similarities is remarkably high:

- definition of clear internal and external customer/supplier roles and relations;
- professionalization of the customer role;
- design of an IT coordination function;
- professionalization of the Chief Information Officer (CIO) function;
- a standardised IT architecture based on a view that considers the ministry as a 'concern';
- no structural consideration is given to evaluating and updating the IT strategy;
- first consideration of external accountability in the statement on operational management;

D R A F T

- absence of systematic monitoring by the parliament or other form of external supervision.

The consideration being given to the governance of information processes and the underlying IT is visibly increasing throughout government. There is a clear movement towards further cooperation and the accumulation of knowledge. The deputy secretaries-general, who are also the CIOs, are leading the way.

A notable finding was that there is definitely room for improvement. The ministries as yet chiefly focus on *strategic planning*. For instance, both ministries are seeking more central coordination of the organization of information processes and the design of support by IT. They pay less attention to internal control. To give an example, the two ministries systematically check the progress made with their projects and the implementation of their annual work plan but they do not pay systematic attention to evaluating and updating the IT strategy. Adapting the IT strategy is usually event-driven, for example when environmental developments make change unavoidable.

Case in point: redesign of the IT function

Ministry of Economic Affairs

A redesign programme was set up to streamline the IT function. It seeks solutions in the form of management agreements and joint decision-making on strategic IT choices. These agreements support the organisational objectives of the ministry at the 'concern' level and also those of its individual units. To this end the programme focuses on five aspects of IT:

1. IT management and decision-making;
2. joint IT strategy;
3. joint IT architecture;
4. joint IT sourcing policy;*
5. clear and transparent IT costs.

Ministry of Social Affairs and Employment

At the request of the deputy secretary-general, a study of the organisation of the ministry's IT function began at the end of 2003. It led to the adoption of a redesign programme for the IT function in 2004. The programme's objective is to improve the quality, organisation and working methods of the IT function. The programme was launched in response to dissatisfaction among both the internal customers and suppliers of IT services. The programme focuses on the following five points:

1. vision of the future;
2. transparent decision-making and financing;

D R A F T

3. clearly defined IT function within the ministry;
4. specific opinions on standards and guidelines;
5. a smoothly operating (new) IT Services department.

* Sourcing: contracting out, internal supply or a combination of the two.

3.4 Recommendations

We had not carried out the descriptive study with the intention of unveiling possible inadequate practices and to make recommendations to remedy identified shortcomings as we usually do. Rather, we took our description as a base-line measurement of existing IT governance practice and used this information to give impetus to the further development of IT governance in our national government. Hence, instead of recommendations we presented an overview of the issues we consider of critical importance. These were based on a mix of good practises that we had observed during our study and practices that, according to our experience, are vital features of (good) IT governance. The critical issues are:

- Avoid 'blind spots'.
- Environmental awareness.
- Alignment of policy, organizational strategy and information strategy.
- 'Concern' approach.
- Standardised 'concern' information architecture.
- Organisation of supply and demand for IT services.
- IT governance as a growth path towards a permanent process.
- Leadership and central coordination

See the Appendix for an explanation of these issues..

3.5 Follow-up

We have undertaken a number of follow-up activities and there are more to follow. Our main activities are presentations and discussion sessions with various ministries, writing papers and initiating a government-wide discussion and experience-sharing session.

DRAFT

4 Concluding remarks

As indicated by the title of this paper we consider IT-governance as a 'top priority'. It is top priority in the double sense of, first, attention from the top management level and, second, with the highest priority. We strongly believe that we, IT auditors, can play a key role here. To start with, we can stimulate senior managers to assume responsibility for major topics regarding IT. Also, we can support them from our experience with issues regarding planning and control, business alignment, risk management and budget management. We are also well positioned to link strategic IT governance concerns with issues in the area of management of IT processes. Most importantly perhaps, we can induce a change of mindset of executive managers. All too often, they consider IT merely as a technical support function. It is crucial however for top managers to shift towards treating IT as a strategic asset in the overall planning and control cycle and, consequently plan and control IT with a view to 'value delivery' in terms of better performance and higher efficiency of government.

How about auditing IT governance? If the discussions within the INTOSAI Standing Committee on IT audit and the timing of its seminar on this topic are anything to go by, IT governance is an emerging concern for the government, not only in the Netherlands but in many countries. Most likely, IT government will be better developed in some countries than others. We believe it is wise for SAIs to tailor their approach of the subject to the level of development of IT governance in the case at hand. Taking an audit stance when IT governance is still in its infancy and about the concrete meaning of the concept has not yet been reached brings the risk of Auditing IT governance 'to death'. In cases such as these a descriptive, fostering approach as outlined in section 3 may be more fruitful. We hope our experiences may be of use to sister SAIs that find themselves in a comparable situation.

D R A F T

Appendix: Critical issues in IT governance

Avoid 'blind spots'

The design of IT governance is complex and there is a risk of certain elements being overlooked. It is important to check that critical aspects are not missed. The descriptive framework used in the audit can be helpful in this (see appendix 1). We would stress that the descriptive framework is not a checklist. The correct design of IT governance is not only about *whether* the elements are in place but also about *how* they are implemented. The framework is intended principally to analyse IT governance and so detect 'blind spots'.

Environmental awareness

IT governance is impossible without environmental awareness. Many of the government's policy objectives cannot be achieved unless there is cooperation among organizations. Ministries participate in and are responsible for policy chains. They cannot operate in isolation. Furthermore, it is often more efficient for ministries to work with each other. Cooperation entails the need to exchange information. A ministry must be aware of this when it takes a decision on its information systems: the chain partners rely on each other for their information systems.

Alignment of policy, organizational strategy and information strategy

Cooperation with other ministries and chain partners has consequences at strategic ministerial level. Government-wide policy and administrative agreements with chain partners must be turned into internal organizational objectives and an associated information strategy. The information strategy is the framework that guides and clarifies the long-term organizational objectives, the information systems that are necessary to achieve those objectives and how IT can best be deployed. Coordinating the organizational objectives and the information strategy is known as business – IT alignment.

'Concern' approach

Compartmentments within the ministry must be removed through the introduction of a 'concern' approach, which considers the ministry as one entity. The information systems of individual organizational units should not be stand-alone systems but part of a coherent, integrated information system used by the entire ministry. This means that ministry-wide portfolio management must replace ad hoc decision-

DRAFT

making on individual projects. It also means that all Director-Generals⁵ must share responsibility for the quality of the group information system. Cooperation generates efficiency benefits and prevents everyone reinventing the wheel.

Standardised group information architecture

The group approach also calls for a standardised group information architecture: a coherent vision of tasks, processes, information system and IT services that is rolled out across the entire ministry and applies to all the organizational units. Such an architecture means decisions have to be taken. The challenge to the organization is to arrive at a future-proof information architecture that meets the longer-term needs of the organization and its chain partners.

Organisation of supply and demand for IT services

IT governance begins with a series of fundamental decisions on the desired business model. One is the decision to work with a customer/supplier model. Demand from the organization and supply by the IT service provider must be closely matched to each other. If not, there is a danger of service provision being driven by technology or, if the service is provided by an external party, by commercial considerations. In consequence, the IT services might not be of the quality required to optimise the information system or they might be unnecessarily expensive. Every organization faces the challenge of breaking down the established role patterns and effectively implementing and matching the supply and demand roles. The demand side is particularly difficult to implement. In practice, it is not always easy to be a good client. A good client knows what he wants, makes concrete and realistic demands regarding the required outputs and makes sure the outputs are actually delivered.

IT governance as a growth path towards a permanent process

IT governance cannot be implemented overnight. It has to grow. This is a difficult process of seeking new organizational structures and working methods. The entire organization must work on cultural change and professionalisation. Such a growth path can be structured by using a model such as the CobiT maturity model (see section 2.2.3). Ultimately, IT governance must be designed as part of the ministry's overall governance. It should not be treated as a one-off activity but embedded as a permanent process in the normal planning and control cycle.

⁵ Director-Generals are the senior managers, responsible for one or more policy areas, reporting to the Secretary-General of a ministry.

DRAFT

Leadership and central coordination

Governance is not possible without leadership. IT governance is no exception, especially because it is still on a growth path. Good leadership is essential on the path towards IT governance, where new organizational structures and working methods are being sought. Clear leadership based on a single vision of information systems and central coordination is necessary if an organization is to operate as a single group. Here lies an important role for the CIO at the top of a ministry.