

# DRAFT

## Effective IT Governance: How to Get Good, Secure IT- Services

Mr. Bjorn Undall and Mr. Bengt E. W. Andersson

Department of Performance Audit  
The Swedish National Audit Office

Nybrogatan 55  
S-114 90 Stockholm  
Sweden

30<sup>th</sup> of March 2007

{bjorn.undall@riksrevisionen.se bengt.andersson@riksrevisionen.se

***Abstract.** This country paper describes experiences from auditing the Cabinet and the public administration Top Manager IT governance. Our main conclusions are that there is an urgent need for stronger IT governance at both the levels of the Cabinet and top managers. Only such governance can ensure that good, secure IT services will be conceived, developed, and implemented, as well as meet all significant requirements for IT security.*

In Sweden, according to the Cabinet, government agencies should become proficient information technology (IT) users, especially in these two areas: (1) good e-services, as part of e-government, and (2) security of these services, that is, the protection of the confidentiality, integrity, availability, and traceability of data, as well as the protection of IT systems. The Swedish National Audit Office (SNAO) audited the performance of government agencies in these areas, using 18 audit studies, from 2002 to 2007.<sup>1</sup>

---

<sup>1</sup> Until June 30, 2003, there were two public audit offices in Sweden: Riksrevisionsverket (RRV) and Riksdagens revisorer (the Parliamentary Auditors). On July 1, 2003, these two offices were amalgamated to form Riksrevisionen (RiR). The RRV and the RiR have the same English name: Swedish National Audit Office (SNAO).

## **Case Study 1: Guaranteeing Effective IT-Based Investment in Business Change -- Focus on Agency Top Managers**

In case study 1, we audited the IT governance of the top managers at the five agencies heavily dependent on IT: the National Labour Market Administration, the National Land Survey, the National Road Administration, Statistics Sweden, and the Swedish Meteorological and Hydrological Institute. In particular, we looked at IT governance in terms of the steps top managers took to guarantee good investment in IT business change.

### Audit Question

Did the agencies manage investment in IT-based business change so as to achieve efficiency?

### Methods Used

Our audits were based on our own audit norm. We derived this norm using the IT-investment management model of the U.S. Government Accountability Office (GAO), as supplemented by Swedish legal requirements and as adapted to the Swedish administrative environment. This adaptation was key in making it easy for top managers at different levels in the agency to understand the audits. During the audits, we noted that top managers did not have any problem relating their work to our norm. The norm includes agencies' operational activities, such as strategies, with the requirements for each:

- Develop proposals: An innovation system, built on activities that are well managed and developed, which produces good investment proposals, including those for IT support.<sup>2</sup>
- Assess proposals: (1) Investment proposals include proposed development programs (for example, for IT support) and (2) assessments based on an agency's available IT resources (including a database).
- Select proposals for implementation: New proposals are related to earlier, ongoing and approved development programs (so-called "investment portfolios"), so as to guarantee links to the (1) investment strategy and (2) evidence trail for tracking decisions.
- Manage implementation: (1) Programs are given realistic conditions for success, (2) project risks are assessed and managed, (3) standards are used consistently, and (3) completed projects are monitored.
- Knowledge management: Good use made of the experience acquired to continuously improve the investment process.
- Create and maintain the investment process: Sufficient oversight of the investment process, identifying strengths, weaknesses, and possibilities for improvement.

For each case study, after the introduction at the agency to be audited, we used these methods: asked the top managers to answer a questionnaire with self- evaluation questions, asked for relevant documents showing the agencies' activities for each

---

<sup>2</sup> An innovation system consists of a network of groups, organizations, people, and rules in which new processes and methods are created.

strategy in our audit norm, analyzed the answers on the self-evaluation questionnaire and the norm-related documents, interviewed 15 to 25 personnel, drafted an audit report and asked for agency comments, gathered agency representatives to a special seminar in which both the identified problems and possible solutions were discussed, and informed top managers of our findings and recommendations.

### Audit Findings

We found that the five agencies, despite their large experience with IT investment, had considerable shortcomings in the governance of IT investment (these findings were published earlier in *IntoIT*). These agencies **lacked**

- sufficiently well-developed processes to elicit good ideas as to how IT can be effectively managed;
- periodic, systematic reviews--enabling them to identify where change is needed--of their investment processes;
- adequate articulation of their investment strategies, making it difficult to justify and select among competing proposals;
- obtaining a clear and comprehensive understanding of an investment proposal;
- business management driven projects in combination with well-established methods and models for managing and undertaking investment project; and
- achieve the anticipated benefits of IT investments in an agency's operations.

Shortcomings in investment strategies created problems when translating the assessment of IT-investment proposals into approved decisions. Because the investment proposals did not link well with the operational strategies, the risk increased that the

proposals would not lead to the investments sought by each agency. And investment decisions were not always based on clear descriptions of the proposal's expected business benefits and implementation risks. Furthermore, proposals setting out the comparative costs, risks, and effects of alternative approaches to IT-investment projects were not adequately dealt with, nor were proposals clearly linked to each other. These combined factors prevented decision-makers from obtaining a clear and comprehensive understanding of an investment proposal.

Moreover, IT projects were inadequately integrated into (1) previously approved investment projects and (2) the IT systems—the environment—in which they were intended to operate or which they were intended to support. An IT investment alone rarely achieves the anticipated benefits in an agency's operations. It is often necessary to change working methods, staff development, and staff organization. In addition, governance of the IT projects was carried out at too low a management level. This meant that the governance of individual business projects was more geared to reacting to problems that arose (reactive management) than to systematic risk assessment (proactive management). With systematic risk assessment, an environment is created and maintained in which risks are not allowed to develop into problems.

Finally, well-established methods and models for managing and undertaking investment projects--such as those identified in the IT investment management model--were not used consistently. Experience and knowledge of different components of the investment process were not utilized in a systematic way, which all the agencies in our audits acknowledged to be an area for improvement. In addition, we found it difficult to (1) obtain an overview of the knowledge that exists and (2) gain access to the knowledge

when needed. In particular, only one of the agencies had utilized lessons from past investment projects for new ones.

### Recommendations

In general, all five agencies should improve each step in the IT-investment process. In addition, the Cabinet should exert better governance of government agencies that are concerned with IT investment.

### **Case Study 2: Developing Effective Web Sites and Good E-Services--Focus on the IT Governance of the Cabinet and Agency Top Managers**

In case study 2, we audited the development of e-services, asking detailed questions concerning how to develop effective Web sites and good e-services. As part of this case study, in 2002-03, we initiated audit project A. Two risks were defined in a pre-study: (1) the digital divide and (2) poor usability of Web sites and other services, which were squeezed out by investment in e-services. In 2003, we initiated audit project B, a materiality and risk analysis of the government's IT governance of the transition to e-government—that is, 24-hour, 7-day government agencies. We found eight main risk areas:<sup>3</sup>

- overall governance of government agencies' work on e-government,
- agencies' implementation of e-government,
- administration and operation of the infrastructure for different types of services;
- use of e-services,

- the effects of investments in e-government,
- the support for the work on e-government,
- the sources—what are they?—and purpose of the current fashion of investing in e-government, and
- technical advances as a foundation (that is, the development of components for Internet applications) for e-services.

### Audit Questions

For audit A: How effective are agency Web sites in meeting the needs and requirements of the individual user?

For audit B: How effective are the Cabinet and government agencies in developing good e-services?

### Methods Used

For audit A, we used several methods: a Web questionnaire sent to 92 government bodies, in-depth interviews with immigrants and elderly people, and a test of 92 Web sites using national and international accessibility standards and our own criteria for special categories of users.

---

<sup>3</sup> We have not analyzed risks from the Swedish Parliament's point of view, for example, risks related to democracy.

For audit B, we investigated all levels of the government: the demands, requirements, e-policies, and strategies from the Parliament and the Cabinet. We performed interviews focusing on the interaction between the Cabinet and agency Top Managers concerning the direction of the development of e-government, and the agency Top Manager's strategic analysis and actions based on direction of Cabinet. We did 10 case studies, divided among government agencies and related government departments. These case studies included in-depth study of Web sites (for incoming e-mail, information quality, and initiatives for new e-services).

### Audit Findings

For audit A, we found that the agencies' Web sites and the e-services offered there did not promote an efficient dialogue between users and agencies. In particular, the Web sites failed to meet certain accessibility requirements for the disabled, immigrants, and the elderly.

For audit B, we found that the governance of the Cabinet for investing in good e-services, including the types of e-services to which the agencies should give priority, was limited. Instead, the Cabinet chose to exert governance mainly through its own support agencies and by means of rules, which were inadequate. In addition, the Cabinet's reports to the Swedish Parliament contained no information about the effects of e-government, including e-services.

We also found that government agencies had difficulty in developing good e-services because they lacked government support. As a result, e-services have not been developed; do not meet user requirements; and are at risk of citizens' mistrust, given that the agencies, as well as the Cabinet, can not guarantee security, especially for e-

mail to the agencies. In addition, at the agencies, narrow reasoning was allowed to govern investment. Agencies had to finance such investment entirely from their own resources. This created poor incentives to build e-services in collaboration with other agencies.

Finally, certain legislation made it difficult to achieve an effective use of e-mail and Web sites. We found e-mail--a basic service of e-government and the most important route for citizens wishing to contact their government—a particular problem. Citizens demand to be able to use e-mails as a means of formal communication, but agencies are not legally bound to answer e-mail or attend to e-mail enclosures.

### Recommendations

The government should improve interagency collaboration, which requires more elaborate governance of communication among agencies. The government should also appreciably improve its control of agency modernization efforts, including the establishment of clearer rules and guidelines, so as to enable e-government for government agencies' handling of e-mail.

### **Case Study 3: Developing Effective IT Governance--Focus on Security for Information Assets and especially for e-Services**

In case study 3, we audited agency top managers' IT governance of e-services security. In particular, we looked at whether top managers systematically used internationally accepted standards for security. In addition, we audited top managers' IT governance of security. This security is concerned with

- protecting information assets against manipulation and destruction,

- preserving information assets availability,
- preserving information assets confidentiality,
- and preserving an audit trail concerning information assets use,

This security is especially important now that e-government is opening up agencies to threats from the outside world. To address these threats, auditors--both performance and financial--have identified the need for systematic audit. For this reason, we carried out audits in 2005 and 2006 of IT security at 10 major government agencies with significant information assets, which need to be protected. These agencies must follow laws, regulations, and international standards that impose requirements for IT security.

In the audits, we focused on top managers and their governance of IT security.

This means that we studied top managers' IT governance of security, including

- control environment;
- risk analysis;
- control functions and individual security measures;
- information and training; and
- follow-up, evaluation, and further development and administration.

### Audit Question

Considering the prevailing standards of the information security management systems, is the government's IT governance effective, including having requirements for IT security in place?

Given the audit question, there were two possible areas to be audited: (1) actual security and (2) top managers' IT governance of security. We chose to focus our case study on (2).

### Methods Used

We used several audit techniques: (1) a Web questionnaire to get agencies' opinions about their IT security; (2) a request for formal documents showing the agencies' security activities at all organization levels (we received 50 to 100 different documents from each agency); (3) follow-up concerning the documents; (4) study of the questionnaire answers and the documents; and (5) 10 to 15 interviews, focusing on top managers (interview questions were based on a special questionnaire, related to the COSO-structure). Finally, we drafted an audit report, letting each agency comment on the draft and informing the top managers about our findings and recommendations.

We took as our starting point an international standard (ISO 17799), and added components from Swedish legislation, as well as international experience. We then transferred the requirements for IT security to a COSO perspective which means that we examined top agency management's internal control and monitoring of information assets and IT security

## Audit Findings

Government agencies were not working effectively because important parts of the information security management systems were missing or defective:

- Control environment—organization of security work, policies, and reporting: Top managers' attitudes (1) were not always favorable towards security investments, (2) did not show a keen understanding of today's threats, and (3) did not always formulate clear security objectives.
- Risk analysis: Often patchy, seldom comprehensive. Following the implementation of investments in security measures, top managers often did not demand an overview of important and residual risks. Responsibility often unclear, and methods for analysis not selected and decided.
- Training for skills: Priority was given to technical measures rather than training. Education seldom systematic, including that for staff who need refresher knowledge about (1) their responsibilities and (2) how, if there are problems, troubleshooting should be carried out.
- Chain of command: Reporting upwards was not well organized.
- Cost: No one top manager had a clear picture of the costs of IT security.
- Top managers' responsibilities: Inadequate follow-up on the implementation and operation of security measures that had been decided earlier.

Finally, the information security management systems are not comprehensive—that is, responsibilities, reporting, and follow-up are not integrated. Important objective data,

with which top managers make decisions, were missing. This made it hard for top managers to exert effective IT governance of security. Therefore, the potential for investment in IT security is not well exploited. The amount of resources invested and the costs were most often not even known!

### Recommendations

Top managers' control in the field of IT security should be strengthened.

### **Lessons Learned**

In the transition to e-government, there is an urgent need for stronger IT governance at both the levels of the Cabinet and top managers. Only such governance can ensure that good, secure IT services will be conceived, developed, and implemented, as well as meet all significant requirements for IT security.



## References

1. SNAO. *Webben 1*: 2003. xxp.
2. SNAO. *Vem styr den elektroniska förvaltningen*: 2004:19. xxp.
3. SNAO. *IT I verksamhetsutvecklingen*: RRV 2002:30
4. SNAO. *Ongoing project Information Security (ten different audit reports)*: 2005–2006.
5. Undall, Bjorn, and Bengt E W Andersson. "Better managed investment in IT-based business development," *IntoIT*, no. 18 (June 2003).