SWEDEN

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

This article describes experiences from 19 audits of the Government's and the public administration senior managers' IT governance. Our main conclusions are that there is an urgent need for stronger IT governance at both the levels of the Government and senior 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. Since the audits were conducted actions have been taken at both levels to strengthen IT governance.

In Sweden, according to the Government, government agencies should become proficient information technology (IT) users, especially in 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 within these areas, performing 19 audits, from 2002 to 2007[1]. The IT Governance audits can be classified in three audit areas:

1. Effective IT-Based Investment in Business Change – Focus on Agency senior managers
2. Effective Web Sites and Good e-Services – Focus on the IT Governance of the Government and Agency senior managers
3. Effective Security for Information Assets and especially for e-Services – Focus on the IT security governance of the Government and Agency senior managers

They are described below, together with some lessons to be learned.

Audit area 1: Effective IT-Based Investment in Business Change – Focus on Agency senior managers

In this area, we audited the IT governance of senior managers in 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 senior managers took to assure 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 the IT investment management model (ITIM) of the U.S. Government Accountability Office (GAO), supplemented by Swedish legal requirements and adapted to the Swedish administrative environment. This adaptation was key in making it easy for senior managers at different levels in the agency to understand the audits. During the audits, we noted that senior 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[2].
- Assess proposals: (1) Investment proposals include proposed development programmes (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 programmes (so-called "investment portfolios"), so as to guarantee links to the (1) investment strategy and (2) evidence trail for tracking decisions.

[1] 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).

[2] An innovation system consists of a network of groups, organizations, people, and rules in which new processes and methods are created.

- Manage implementation: (1) Programmes 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 audit area we used these methods: asked the senior managers to answer a questionnaire with self-evaluation questions, asked for relevant documents showing the agencies' activities for each strategy in our audit norm, analysed the answers on the self-evaluation questionnaire and the norm-related documents, interviewed 15 to 25 staff, 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 senior managers of our findings and recommendations.

Audit Findings

We found that the five agencies, despite their long experience with IT investment, had considerable shortcomings in the governance of IT investment (see IntoIT issue 18 Better managed investment in IT-based business development). These agencies lacked:

- sufficiently well-developed processes to elicit good ideas as to how IT can be effectively managed;
- periodic, systematic reviews of their investment processes, enabling them to identify where change is needed;
- 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. In addition, 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 organisation. 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) rather 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 utilised 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 utilised 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 Government should exert better governance of government agencies that are concerned with IT investment.

Audit area 2: Developing Effective Web Sites and Good E-Services – Focus on the IT Governance of the Government and Agency senior managers

In audit area 2, we audited the development of e-services, asking detailed questions concerning the development of effective Web sites and good e-services. As part of this audit area, 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[3]:

- 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 project A: How effective are agency Web sites in meeting the needs and requirements of the individual user?
For project B: How effective are the Government and government agencies in developing good e-services?

Methods Used

For project 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.

For project B, we investigated all levels of the government: the demands, requirements, e-policies and strategies from the Parliament and the Government. We performed interviews focusing on the interaction between the Government and agency senior managers concerning the direction of the development of e-government, and the agency Senior

[3] We have not analysed risks from the Swedish Parliament's point of view, for example, risks related to democracy.

Manager's strategic analysis and actions based on direction of Government. 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 project 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 project B, we found that the governance of the Government for investing in good e-services, including the types of e-services to which the agencies should give priority, was limited. Instead, the Government chose to exert governance mainly through its own support agencies and by means of rules, which were inadequate. In addition, the Government'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 Government, 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 modernisation efforts, including the establishment of clearer rules and guidelines, so as to enable e-government for government agencies' handling of e-mail.

Audit area 3: Effective Security for Information Assets and especially for e-Services – Focus on the IT Security Governance of the Government and Agency senior managers

In audit area 3, we audited IT governance of e-services security. As part of this audit area, in 2005-06, we initiated audit project C. In particular, we looked at whether senior managers systematically used internationally accepted standards for information and IT security. In 2007, we initiated audit project D, an analysis of the Government's governance of the public administration's field of actions in the area of information and IT security.

In audit project C, we audited senior managers' governance of information and IT security. The information and IT 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 used.

This security is especially important now that e-government is opening up agencies to threats from the outside world. For this reason, we carried out audits in 2005 and 2006 of IT security at 10 major government agencies with significant information assets.

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

This means that we studied senior 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.

In audit project D, we audited the Government's governance of information and IT security within the public administration. The audit was carried out in the light of the problems that have emerged in the SNAO's audits of ten public agencies' performance of their responsibilities for information security (audit area C).

Audit Questions

For project C: Considering the prevailing standards for information security management systems, is the government agencies' IT security governance effective?

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

For project D: Is the Government taking its responsibility for making requirements of and following up the work of their agencies (the public administration) with respect to security of information and IT, and for taking the initiative for measures aimed at improving the conditions for the work of the public administration within this area?

Methods Used

For project C, 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 organisation 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 senior 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 senior 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 senior agency management's internal control and monitoring of information assets and IT security.

For project D, we used several methods: we analysed the findings from the 10 audit projects in order to ask the Government if the common pattern of problems among the 10 audits was known or not, we gathered information concerning our pattern of problems from four agencies being expert and used by Government in the area of information and IT security, we analysed the Government's written statements in official documents to the Parliament concerning the status of information security and what actions the Government had promised to take, we performed in-depth interviews (based on questionnaires) in the Government focusing on the information gathering and organising of matters concerning information and IT security. We also made a special analysis of shortcomings in the legislation in the area.

Audit Findings

In project C, we found that government agencies were not working effectively because important parts of the information security management systems were missing or defective:

- Control environment—organisation of security work, policies, and reporting Senior managers' attitudes (1) were not always favourable 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, senior 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 organised.
- Cost: No one senior manager had a clear picture of the costs of IT security.
- Senior 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 senior managers make decisions, was missing. This made it hard for senior 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!

In project D, we stated that the problems on agency level described above were serious and that they imply a risk of significant negative consequences for government commitments such as electronic government and national emergency management. In the light of the above, the SNAO considers that the Government's control of information security is of great importance. The SNAO's overall assessment is that the Government has not followed up to ensure that the internal management and control of information security in the public administration is satisfactory. The Government has not taken sufficient initiative to improve the conditions for the administration's work on information security.

The SNAO has established that the Government has taken measures with respect to the technical conditions for agencies' information security work, such as e-signatures, e-identification, secure Internet, etc. On the other hand, no measures have at the time of the audit been taken to support the agencies' internal management and control of information security.
The SNAO takes the view that an overhaul of the regulations is urgently needed, particularly against the background of the investment in e-government.
The Government has not given the expert agencies a sufficiently explicit mandate, which has meant that they have had difficulties in giving the Government a complete picture of the information security problems at the agencies.
An explicit mandate is also needed in order for the expert agencies to provide appropriate regulations detailing the Government's requirements for the agencies' work on information security.

The audit shows that over the past ten years the Government has been broadly aware of certain management problems in the sphere of information security, but the picture has been unclear with respect to central government agencies and the Government has been unable to present any complete picture of the problems affecting the public administration.

According to the SNAO, the Government's organisation of the work done by the Government Offices on information security issues and the management of the expert agencies is together insufficient to handle the agencies' problems with their information security.

Recommendations

For project C: Senior managers' control in the field of IT security should be strengthened. This could be done using the standard SS-ISO/IEC 27001/17799 Information Security Management. One key activity is the risk analysis. This activity needs to be strengthened since it is the base for information security measures.

For project D: The Government should focus more clearly on information security issues. Give the expert agencies an explicit mandate to follow up and report on the agencies' work on information security. Give the agencies better conditions - set more explicit requirements for information security work.

Lessons Learned

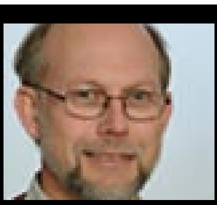
As a result of the Government's investment in electronic government, growing numbers of agency services are becoming available on the Internet, agencies are joining together to create co-ordinated e-services and there is a general increase in IT-based development work. In order for this reform of the public administration to succeed, citizens and businesses must have confidence in the e-services provided on the Internet. There is a risk of a lessening of confidence in the agencies' e-services if the information cannot be protected. It may be a case of unauthorised persons gaining access to sensitive information or changing data or in some other way acting so that the services cannot be used. If that happens, there is a considerable risk of the entire investment in e-government being jeopardised.

In the transition to e-government, in our opinion, there is an urgent need for stronger IT governance at both the levels of the Government and senior 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.

Since the audit projects been finalised in spring 2007 we have made some follow-ups. At the agency level we noticed some improvements of IT governance of information security in form of plan of actions, reviewing important documents, implementing information security standard and educating the staff. During autumn 2007 an expert agency published regulations stating that government agencies should implement an information security management system. At the Government level a plan of action to improve e-government recently (February 2008) has been taken. In this plan of action the need for stronger IT Governance is stated to ensure that good, secure IT service will be conceived. Several actions will be performed 2008 – 2009 in order to fulfil the Government's goals. ○

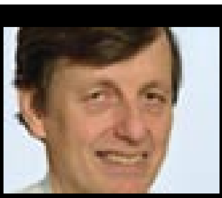
References

1. SNAO. IT i verksamhetsutvecklingen: RRV 2002:30
2. SNAO. Webben 1: 2003.
3. SNAO. Vem styr den elektroniska förvaltningen: 2004:19.
4. SNAO. Project Auditing Information Security (ten different audit reports): 2005– 2006.
5. SNAO. Government control of information security work within the public administration: 2007:10
6. Undall, Bjorn, and Bengt E W Andersson. "Better managed investment in IT-based business development," IntoIT, no. 18 (June 2003).



Bengt E. W. Andersson

Bengt E W Andersson specialises in auditing the use of IT and information exchange between Public Administration bodies. Within the office he has also been involved in quality assurance and IT support. He holds a Licentiate of Philosophy in Information Systems.



Bjorn Undall

Björn Undall's main audit responsibility is the effective use of IT in Public Administration. Recently he has specialised in auditing Information Security issues. He holds an MBA from the University of Lund, and has (alas!) unfinished doctoral studies.