SWEDISH NATIONAL AUDIT OFFICE

REPORT NUMBER: RIR 2016:8
DATE: 26 MAY 2016

Summary:
Information security work at nine agencies

Summary and conclusions

In public administration much information is processed that requires protection. Information security entails ensuring that all information requiring protection is accessible, correct, confidential and traceable. Information security is a matter that concerns every member of an agency's staff. Creating high quality information security is important, since deficient information security may have serious consequences, such as the spread of sensitive information or inhibited payment of transfers.

In the previous Swedish NAO audit of information security in civil public administration of 2014, a number of threats and risks were dealt with. It is a matter of the dependence of many public services on information technology to be able to function. Additionally, various technical systems are often interdependent or technically linked, which constitutes a vulnerability in itself, in that disruptions may have consequences that are both difficult to predict and deal with. What constitutes a threat or a risk varies, for example from states, state-subsidised actors, terrorists and organised crime to errors and disruptions not caused by antagonists but due to software or hardware errors, process deficiencies, lack of quality control, carelessness, miscalculations or pure accident. Those affected can be anyone from private individuals to entire sectors of society. Examples of the consequences may be non-payment of transfers and disruptions to electricity or water supply.

Audit background

In 2005-2007 the Swedish NAO audited the work of information security at eleven public administration agencies. The audit showed several deficiencies. The Government had not followed up whether the agencies' internal control of information security was satisfactory, nor given the agencies sufficient conditions for effective information security work. In 2014 the Swedish NAO again audited information security with a focus on the Government and its expert agencies' governance and support. This audit showed that there were considerable deficiencies in the information security work and that the Government had not exercised effective management.

REPORT NUMBER: RIR 2016:8
DATE: 26 MAY 2016

Purpose of the audit

The purpose of this audit was to investigate how nine agencies work with their information security. These agencies conduct critical infrastructure activities, handle large amounts of money, are strongly IT-dependent and handle information that requires protection. The Swedish NAO has audited whether the agencies, based on current requirements and conditions, conduct information security work so as to achieve appropriate protection of their information assets. Another purpose was to examine whether the Government ensures that the agencies audited have effective internal control of their information security.

For information security to be effective, both for the respective agency and for public administration as a whole, it must be possible to weigh costs against benefits. Consequently, the Swedish NAO has made an investigation of the cost picture for information security work.

Audit findings

The Swedish NAO's conclusions

The overall conclusion drawn by the Swedish NAO is that the work of information security at the agencies audited is at a level that falls considerably short of being adequate. An important explanation for this is that understanding for the importance of sound information security is in general far too limited. The consequence of this is that information security work is not given high enough priority in relation to the risks that exist. This applies to both the Government, which should have been clearer in its directions to agencies on this matter, and to agency managements, which did not give priority to the work of information security to the extent required. Much indicates that it is difficult for many agencies to achieve an appropriate level of information security work. Consequently, the Swedish NAO has no reason to assume that the picture that emerges at the agencies audited would not also apply to most of the other agencies in the public administration.

The work of information security is not at an acceptable level at the agencies audited

Audit of the Public Employment Service, Social Insurance Agency and Migration Agency was particularly in depth. None of these agencies can be said to have systematic information security work in compliance with the requirements of the Civil Contingencies Agency's regulations on government agencies' information security. These

requirements stipulate that agencies must apply a management system that includes drawing up a policy for information security, classifying their information on the basis of correctness, accessibility and confidentiality as well as determining how to deal with risks on the basis of risk and vulnerability analyses and incidents that have taken place.

An important condition for paving the way to a good information security culture and creating understanding for information security is that the agency management shows commitment to the issue. The audit shows that agency managements have delegated responsibility for information security, without ensuring that those responsible have an adequate mandate to carry out their tasks and sufficient resources. The functions in charge of information security find it hard to contend with core activities that tend to see information security requirements as obstacles, which results in functionality requirements being put before security requirements. It is the IT or security functions that impose security requirements rather than the core organisation. The situation at the six other agencies audited – the National Grid, the Companies Registration Office, Lantmäteriet (National Land Survey), the Post and Telecom Agency, the Maritime Administration and the National Government Employee Pensions Board – varies, but is by and large the same as at the three agencies that were audited in particular depth.

Despite the fact that the agencies have drawn up policies, guidelines and manuals on information security, knowledge of the contents and purpose of these documents is low among many employees and managers. Security work is not implemented in the ordinary processes of the organisations. The core organisation does not perceive that it has any responsibility for information security, but that this lies somewhere else in the agency, such as the IT or security functions. There is a considerable lack of participation and responsibility that should permeate the entire agency, and there is a lack of understanding of the need for security investments without visible benefit.

Risk analyses are made in varying ways within and between the agencies audited and cover more than just information security. This is not in itself wrong, but within the agencies it contributes to overlaps and a risk of areas falling between different stools, as well as some areas not being highlighted. The agencies seldom amalgamate their various analyses into an overall analysis focusing on information security. Seen from an information security perspective this is a fragmented approach, which needs to be coordinated better.

It is difficult to gain a coherent picture of the information security situation at the agencies, which is linked to the fact that there is often no structured follow-up of the management system. The lack of follow-up makes it more difficult to work in way that is focused on improvement. The lack of a learning perspective is also apparent in incident

management, which is more focused on creating statistics than finding out the causes of incidents.

The Swedish NAO can note that the work of information security at the agencies audited is conducted in different ways, despite the fact that significant components of this work should be generic by nature. It can also be noted that the parts of information security work that cover IT security and physical external protection are generally better than the organisational parts, even if there is potential for improvement in IT security. Many of the components of the management system seem to exist because this is a requirement, rather than because they could be a powerful tool in the change process.

The Government has not ensured the necessary conditions

At first glance the conditions may seem adequate in that the Government has created certain requirements to enable agencies to work on internal control of information security. There is a structure in place, with different statutes intended to steer this work. Part of this is that the Government has decided that the management of a number of agencies must certify that internal control is satisfactory. In addition, each ministry conducts regular dialogues with agency managements. Nevertheless, the audit shows that there are serious deficiencies in the agencies' information security work.

The Swedish NAO considers that stronger governance is required from the Government in relation to the agencies, so that necessary security measures are actually implemented. Simply drawing up an overall regulatory framework is not sufficient to make security adequate. If the Government does not require information concerning the agencies' information security and does not highlight the importance of good information security, in the opinion of the Swedish NAO the agency managements will not make the matter a priority either.

The costs of information security are unknown

To be able to determine whether or not there are well-founded decisions on the measures that need to be taken to protect all the information in public administration that requires protection, a coherent status report on threats, risks and suitable measures is needed. In addition to this it is necessary to know the size of the annual amounts spent on information security. Only when these pictures have been presented is it possible to weigh up the costs in relation to the benefit of protective measures and thus achieve an optimum level of information security in central government as a whole.

At present there are no data, either individual or for public administration as a whole, on agencies' costs for information security. Hence it is not possible to express an opinion on

whether management of information security is cost effective. In the opinion of the Swedish NAO it is a clear deficiency that the Government does not request these data, particularly in relation to the fact that IT has been pointed out as a central tool for developing public administration.

Resources are probably not used effectively

Swedish public administration functions in a way that allows agencies to enjoy far-reaching independence in relation to organising their activities. From this follows that all agencies in public administration, regardless of size, are obliged to manage their own information security. This means that they must either do most of the work themselves, or engage consultants. The largest agencies are better equipped to build up and maintain good information security themselves, due to economies of scale. However, the situation of most agencies is not as favourable. This audit has shown that it is a heavy burden even for fairly large agencies to conduct successful information security work. The Civil Contingencies Agency contributes a good guide to how an agency is to work with information security. Nevertheless, for several of the agencies audited this is not enough, as they lack operative assistance, which the Civil Contingencies Agency does not currently provide. In the opinion of the Swedish NAO this means that it is probable that information security work at aggregate level is not cost-effective.

The Swedish National Audit Office's recommendations

The audit shows that the agencies' information security work has serious deficiencies. The Swedish NAO therefore makes the following recommendations to the Government.

- The agencies have not succeeded in establishing information security work that complies with the Civil Contingencies Agency's regulations and thus the standard on which the work is based (ISO 27000). To improve the conditions for meeting the requirements the Swedish NAO recommends that the Government increases the clarity of its agency governance, so that each of the agencies in public administration achieve a good level of information security within a reasonable period.
- There is a need to supplement the Civil Contingencies Agency's methodology support for risk analyses, to be better able to utilise the outcomes of the various processes and combine them into an overall unit, so that the greatest benefit can be gained from all the efforts put into risk management work. The Government should therefore consider instructing the Civil Contingencies Agency to prepare a model or methodology support to enable the agencies to effectively coordinate results and processes. This model should as far as possible support the work of the agencies on

risks and in combining them in a manageable way. It is also important that the Government, through its agency governance, ensures that the agencies also apply the model.

- In order to achieve effective protection of information assets in central government it is essential to be able to weigh up costs and benefits. This is not at present possible, since the costs of agencies' information security input are unknown. It would also be a matter of urgency to investigate how decisions on investments in information security are made in practice and the organisational factors that influence the view of investments in information security. The Government should therefore investigate the requirements for presenting all costs associated with information security for central government activities.
- Each of the agencies is obliged to proceed through trial and error to how they conduct their information security work. The Civil Contingencies Agency's guidelines are good, but the agencies lack operative support. The Swedish NAO therefore recommends that the Government considers investigating the need to establish a central function tasked with providing operative support to the agencies.