Summary

Information security in the civil public administration (RiR 2014:23)

SWEDISH NATIONAL
AUDIT OFFICE

DATE: 10-11-2014

Information security in the civil public administration

We now live in a society where larger amounts of information than ever are processed, stored, communicated and reproduced. Greater use of information entails significant opportunities and benefits. At the same time, the greater development of IT entails that society is exposed to major risks which we are probably not currently aware of. Shortcomings in the handling and security of the information risks having extensive consequences, both for society at large and for individuals. Shortcomings can also result in lower confidence in public and private actors who provide important services. In this manner information security covers the entire society and is a concern for everyone.

Background of the performance audit

This audit is based on the ever-increasing use of information in society and public administration and on the shortcomings which were identified through the previous audits of information security by the Swedish National Audit Office (NAO).

Between 2005–2007 the Swedish NAO audited eleven agencies and their work on information security. A more detailed audit was conducted for six of these agencies. This series of audits was concluded by an audit which related to the Government's management of the information security work of agencies. The overall assessment of the Swedish NAO was that there were shortcomings in the work of agencies on information security and that the Government had not monitored whether the internal management and control of information security was satisfactory. The Government had neither taken adequate initiatives to improve the prerequisites for the public administration's work on information security.

The aim of the audit

This audit aimed to investigate whether the work on information security in the civil public administration is appropriate based on increasing threats. Thus, the audit neither covers the management nor level of information security in society at large. In the audit we have focused on the knowledge and information which is collected about which threats are realised and about threats and risks on a systematic and overall level for the civil public administration. The audit also aims to assess whether the Government and agencies in charge of support and supervision have adequate knowledge of the security measures which have been taken by agencies within the civil public administration.

DATE: 10-11-2014

The audit answers two questions:

- Is the Government's management of information security in the civil public administration efficient?
- Have the Government's support and supervision agencies taken adequate measures to inform themselves and the Government about which threats exist against the civil public administration, to what extent they are realised and which security measures are taken?

How individual agencies work with information security is not included in the audit. Neither has the audit sought to prove the scope of specific shortcomings in the information security.

The audit relates to the Government (through the Ministry of Defence, Ministry of Justice and Ministry of Enterprise, Energy and Communications) and the support and supervision agencies the Swedish Civil Contingencies Agency (MSB), National Defence Radio Establishment (FRA), Swedish Security Service and Swedish Post and Telecom Authority (PTS). The audit refers to the civil part of public administration and therefore does not cover how the Swedish Armed Forces manage the work on information security within their operational area.

Results of the audit

The overall conclusion of this audit of the Swedish NAO is that the work on information security is not appropriate in terms of the threats and risks which exist. The technical development has accelerated and the risks an organisation is exposed to are increasing and can be expected to increase in the future. As the supporting material of the audit reveals, some risks have been realised and the consequences have been serious. This emphasises the importance of good awareness of preparedness to prevent and handle similar and other incidents. A risk-based approach in the work on information security is a prerequisite to evaluate the probability of different incidents occurring and the resulting consequences in a coordinated manner. There are several risk areas within public administration in terms of information security, for example, lack of competence, procurement, supervision/monitoring/providing feedback as well as management/re-regulation/coordination.

A large share of the information which is created and stored in society is both important and sensitive. There may be serious consequences if the information is lost, stolen, manipulated or disseminated to unauthorised persons. The consequences range from affecting entire social functions to affecting individuals. The audit has revealed extensive shortcomings in the public administration. The supporting material of the audit reveals that 84 per cent of the agencies which administer their IT systems themselves state that they have an information security policy. At the same time, it is clear that 38 per cent of the agencies assess that competence, mandates or resources are inadequate to perform the information security work in a satisfactory manner. Furthermore, 42 per cent of the agencies state that rules are missing for what a risk analysis, which should be done in systematic information security work, should cover or when it should take place.

Finally, 65 per cent of the agencies state that they are lacking a continuity plan. Therefore, the Swedish NAO assesses that a large share of agencies do not have central parts of systematic information security work in place.

The Government does not have any overall situation awareness which includes threats, to what extent and against who the threats are realised and which security measures the agencies are taking. The Government's support and supervision agencies do not either have any such situation awareness. This means that the overall capacity to be able to handle the consequences which can arise from a serious incident are largely unknown. Due to this it is necessary that the Government and these agencies take measures, so that it is possible to attain overall awareness of the situation and based on this adapt the requirements for security to the needs which exist.

The audit of the Swedish NAO has shown that

- the Government has not exercised efficient management of information security in the civil public administration and
- the Government's support and supervision agencies have only partially taken necessary measures to inform themselves and the Government about which threats exist against the civil public administration, to what extent they are realised and which security measures are taken.

The Swedish NAO draws this conclusion based on the following reasons. As a part of the audit, the Swedish NAO has commissioned MSB, FRA and the Security Service to analyse information about the situation of information security in the public administration. The reporting of these assignments entails essential, new information about the situation. Furthermore, each statement of the agencies clearly points in the same direction.

The regulatory system for information security practically looks the same as it did in 2007 when the Swedish NAO most recently audited the area. The shortcomings which were identified then largely still remain, which entails shortcomings in the Government's management. Clear and well-adapted regulations are a prerequisite for attaining efficiency in the work on information security. Therefore, the Swedish NAO draws the conclusion that the regulations which control the work of agencies on information security may need to be better adapted to different types of state operations to attain the desired targets.

Overall balancing for the State for the amount of resources which need to be invested in security measures in terms of the existing risks is lacking. Overall risk evaluation is currently lacking; instead there is uncertainty on how strong the protection is, which incidents have taken place and how the threats are developing. If there was overall situation awareness it would have provided prerequisites for overall evaluation of the risks and probability that the threats are realised. This could in turn be balanced against how extensive the support needs to be. Occurred incidents have shown that the costs can be significant, partly to handle the incident and partly for subsequent rectification. The risks for information security can thus potentially result in extensive damage, not least in the form of extra costs and reduced confidence in public administration. Therefore it is important that measures are taken and prioritised to control these risks.

Now each agency has personal responsibility for its entire operations in both normal situations and crises, which is naturally completely necessary for efficient management of the operations. However, this is probably not sufficient; most agencies find it difficult to recruit and maintain the competence which is required to meet the requirements for safe information handling. The support agencies identified by the Government have limited resources and lack opportunities to provide operational support to individual agencies to any large extent. Thus there is a need for better extended support which focuses on the entire public administration, and which supplements the competence of individual agencies. If this was the case, it could result in better security in total in the public administration while the total cost of information security ought to be significantly lower than if each agency sticks to specialist competence.

Recommendations of the Swedish NAO

To the Government

The audit has revealed a significant knowledge deficit in terms of the situation of information security in public administration. The supervision which takes place largely only covers the operations most worthy of protection – the majority of the civil public administration is left without supervision. Measures are not always taken after conducted inspections. Systematic and compulsory reporting of incidents is also missing. All this results in it being impossible to capture the real image of the state of information security. From this it follows that there is not sufficient decision data to take necessary measures to meet the threats and risks.

Therefore, in order to improve the State's information security, the Swedish NAO recommends the following to the Government:

- Extend the supervision of information security in the civil public administration, so that it covers significantly more than only the areas most worthy of protection.
- Investigate whether the regulations which control the work on information security are appropriate with their existing structure and whether responsibility to exercise supervision of information security in the civil public administration can be collected and coordinated in a better manner than at present. The Swedish NAO already identified these shortcomings in 2007, and as the shortcomings have still not been rectified, speedy handling is important.
- Consider allowing the supervision agency to receive a mandate to issue sanctions against agencies which do not take necessary measures after supervision which has revealed shortcomings.

DATE: 10-11-2014

- Immediately introduce compulsory incident reporting for all agencies. Commission one agency to handle this reporting.

There is no coordinated central function in the Government Offices with responsibility for preparing issues on information security in the public administration. Cases concerning information security are currently handled in several departments depending on the nature of the case (internal management and control, administrative policy, crisis management, infrastructure, etc.). The Swedish NAO believes that information security is an important strategic issue for the entire public administration, that force is required in the management for the protection to be raised to an appropriate level. Therefore, the Swedish NAO recommends the following in order to create better prerequisites for efficient management in information security:

- Ensure that there is a function and a process in the Government Offices with the aim of handling information security in a coordinated manner. This function and process should be able to prepare all the cases the Government needs to decide on in order to increase information security in the public administration. The function should also serve as recipient of MSB's information on overall situation awareness and other necessary information on the situation of information security in the public administration.

To the Government´s support and supervision agencies

In this audit the Swedish NAO has been able to show that the support and supervision agencies appointed by the Government within the current mandate should be able to do more, both by increasing knowledge of the security situation and providing support to the rest of the public administration to increase the protection. It is naturally an issue of what should be prioritised both within these agencies and within the public administration as a whole. Therefore, in order to improve the State's information security, the Swedish NAO recommends the following:

- MSB should continue and also intensify its work on seeking to create shared situation awareness of information security in the public administration.
- In accordance with the Emergency Management and Heightened Alert Ordinance (2006:942), MSB has the opportunity to request that more agencies than currently provide a report on their risk and vulnerability analysis to the Government Offices and MSB. MSB should utilise this opportunity to thereby increase the coordinated knowledge of the information security situation and thereby be able to contribute to an improvement.
- MSB should provide the agencies which do not fulfil the requirements in the provisions on state agencies' information security (MSBFS 2009:10) the support which is necessary, so that they attain adherence within a reasonable time.
- Both the Security Service and FRA generate important knowledge on the security situation within the area of public administration most worthy of protection. Therefore, the Security Service and FRA should respectively systematically submit aggregated reports on the security situation to the Government Offices and MSB.