5/2016

STATSREVISORERNE
RIGSREVISIONEN

Extract from Rigsrevisionen's report on

management of IT security in systems outsourced to external suppliers

submitted to the Public Accounts Committee

November 2016

1. Introduction and conclusion

1.1. PURPOSE AND CONCLUSION

1. This report concerns a number of government authorities' management of IT security in systems that have been outsourced to external suppliers. The report adopts a forward-looking perspective and makes recommendations for improving the authorities' management of IT security in outsourced systems. Rigsrevisionen took initiative to the study that is based on IT audits performed by Rigsrevisionen during the first six months of 2016.

2. We have examined the following five authorities and six IT systems: The Danish National Police (centralised passport service), the Danish Customs and Tax Administration (two self-service systems that allow individuals and businesses to manage their tax returns online), the Danish Agency for Labour Market and Recruitment (joint database providing historic and current data on citizens' employment), the Danish Agency for Digitisation (NemID – digital signature) and the Danish Maritime Authority (ship registration system).

- The Danish National Police is part of the Ministry of Justice.
- The Danish Customs and Tax Administration is part of the Ministry of Tax.
- The Danish Agency for Labour Market and Recruitment is part of the Ministry of Employment.
- The Danish Agency for Digitisation is part of the Ministry of Finance.
- The Danish Maritime Authority is part of the Ministry of Business and Growth.

3. Many government IT services have been outsourced to external suppliers. The benefits of outsourcing can include cost savings, enhanced quality and organisational improvements. However, in the course of the last couple of years, there have been examples of serious IT security incidents in the companies providing IT services to the government. For instance, in 2012, several of the Danish National Police's systems were compromised in a cyberattack on one of its external suppliers of IT services.

4. The authorities remain responsible for managing IT security, despite the fact that their IT systems have been outsourced to external suppliers. It is therefore important that the authorities conduct risk assessments, and based on their findings impose relevant requirements on and monitor the level of IT security in the outsourced systems. The risk assessments provide the basis for appropriate and well-founded management of IT security. Without active, risk-based management of IT security, the authorities will be unable to determine whether the level of IT security in the outsourced systems meets their requirements.

IT systems consist of various technical layers/components, which, together, make up the infrastructure of the systems. This is described in more detail in item 10. In principle, each of these layers could represent a potential risk. It is therefore essential that the risk assessments conducted by the authorities – often with the assistance of their external suppliers – take into consideration the risks associated with each of the layers of the IT infrastructure. Through this approach, the authorities can determine whether they need to impose requirements on and monitor the IT security in all technical layers.

5. The purpose of the report is to assess how the authorities have *managed* IT security in the systems that have been outsourced to external suppliers in selected areas and, based on the outcome of our assessment, make recommendations to the authorities as to how they can improve management in this area. More specifically, we have examined whether the authorities have conducted risk assessments as a basis for their management. Based on the results of this assessment, we have examined the extent to which the authorities have contractual claims regarding access to their suppliers' annual auditor's reports and access to audit the IT security level at their suppliers. We have also examined the extent to which the authorities have imposed requirements on the suppliers' access control and log management.

It should be emphasized that the report concerns the authorities' management of IT security in the examined systems, and not the actual IT security practices of the IT suppliers.

CONCLUSION

When IT processes are outsourced to external suppliers, the authorities no longer have direct control of the IT security, but remain responsible for managing the security of the IT. Authorities that fail to manage IT security actively based on risk assessments, and omit to monitor the implementation of these requirements, will not be able to determine if the level of IT security in the outsourced systems safeguards their systems and data.

Rigsrevisionen finds that the majority of the authorities examined need to improve their risk assessments, which should provide the basis for their management of IT security at their suppliers. It is also Rigsrevisionen's assessment that the majority of the authorities examined can refine their requirements for and follow-up on access control and logging practices.

With the exception of the Danish National Police, none of the authorities have conducted appropriate risk assessments of the examined IT systems. This is not considered satisfactory by Rigsrevisionen. The risk assessments conducted by the authorities were very general in their form and did not include all layers of the systems' IT infrastructure. Moreover, the authorities did not state their reasons for opting out controls in relation to access control and logging, and they were therefore unable to document how they had arrived at the conclusion that imposing requirements on and following up on access control and logging in all layers of the infrastructure would not be necessary. When the authorities fail to base their management of IT security on appropriate risk assessments, there is a risk that their management is not focused on the need to safeguard the confidentiality, integrity and availability of their systems and data.

Rigsrevisionen also finds that the majority of the examined authorities can refine their requirements for access control and logging. Either the authorities have failed to define access control and logging requirements altogether, defined only general and vague requirements or imposed requirements for only some of the layers in the IT infrastructure.

If requirements concerning the suppliers' obligations are either missing altogether, general or vaguely formulated – and thereby open to interpretation – there is a risk that the suppliers fail to establish the adequate and/or expected level of security.

Last, Rigsrevisionen finds that the majority of the authorities should improve monitoring of their suppliers' access control and logging, since they have either failed to monitor these or only monitored some layers of the IT infrastructure. The audit shows that some of the authorities need to acquaint themselves with the areas of IT security covered by their suppliers' auditor's reports.

The Danish Maritime Authority and the Danish Agency for Labour Market and Recruitment are both customers with the Agency for Governmental IT Services (agency under the Ministry of Finance); the audit shows that the distribution of responsibilities and tasks among the two agencies and the Ministry of Finance concerning supervision of the Agency for Governmental IT Services is unclear. The Danish Agency for Labour Market and Recruitment and the Ministry of Business and Growth, which includes the Danish Maritime Authority, have informed Rigsrevisionen that they were not aware of their obligations in relation to imposing requirements on and monitoring IT security in the examined IT systems, because it was their understanding that this would be covered by the supervision provided by the Ministry of Finance.

The Ministry of Finance has informed Rigsrevisionen that it will take steps to clarify the scope of its supervision of the Agency for Governmental IT Service.

Based on the audit findings, Rigsrevisionen recommends:

- that the authorities, based on their risk assessments, define clear requirements for the security level in their supplier contracts or in supplements, allonges or appendices to these contracts, and specify which layers of the IT infrastructure the requirements apply to;

- that the authorities monitor the suppliers' IT security and their compliance with the requirements in all layers of the IT infrastructure, unless the outcome of the authorities' risk assessments demonstrates that such monitoring is not necessary.

The authorities have been required to follow ISO 27001 since January 2014 and have it fully implemented early in 2016.