

Audit of the National Government Employee Pensions Board's internal management and control of information security

The National Post and Telecom Agency incident centre, Sitic, notes that almost a third of all public organizations have been subject to some form of serious data encroachment or virus attack. The attacks are becoming increasingly "professional". At the same time authorities are presenting more and more of their business on the Internet in the form of electronic services. The authorities therefore need to work on the protection of their information and their activities. This is difficult and it also consumes resources. In these circumstances the National Audit Office has increased its efforts with regard to audit of information security within the state. This audit relates to the work of the National Government Employee Pension Board on security of information.

What is meant by security of information?

Information security is about the right information being available, not being corrupted or destroyed and not being accessible for unauthorised persons. It should also be possible to trace how information has been used and altered. In its audit the National Audit Office has proceeded from an international code of practice for information security management (SS-ISO/IEC 17799), known as the LIS¹ standard. This covers all the areas that the security work needs to include, both purely technical protection and the matter of influencing employee behaviour.

To what can failures of information security lead?

The National Government Employee Pension Board had a 2004 balance sheet of SEK 190 000 m. Payments of SEK 10 000 m were made in the form of 280 000 payments every month. Both the calculation of the pension and payment of the pension to the right person and also calculation of the authorities' premiums depend on the availability of accurate information. Error or manipulation leads to perceptible expense to both individuals and authorities as even small errors can add up to significant sums over the years.

Does the National Government Employee Pensions Board have an effective information security system?

Both yes and no. Our assessment is that the areas on which the Board needs to work and develop are those which are often problematical in connection with security work. There are control documents, but in combination with extensive delegation and high pressure to produce, areas such as interaction, follow-up and in-service training in the information security field do not receive priority. The great confidence that the Board places in its staff also means that risk analysis, and therefore safety precautions, are focused on external threats. There is also a lot of attention to confidentiality. Protection against, for example, internal threats then naturally receives a lower priority. Those parts of the information security management system that consist of control documents and also, to a large extent, technical protective measures are therefore largely in place. But those parts of information security management that concern security behaviour and interaction

¹ Swedish acronym for Information Security Management System

between persons need to be improved. This is crucial if information security management systems are to be of the desired usefulness. The conclusion is that the Board has not fully succeeded in creating the conditions for good information security which the effort and investment that have been put into the authority's information management security system have been intended to create.

The failings in information security management systems affect in turn the possibility of achieving and maintaining the desired information security. The answer to the question that the audit has been intended to answer is therefore that the Board is not working fully systematically on security of information on the basis of current norms.