

Audit of the Swedish Maritime Administration'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 Swedish Maritime Administration 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 Maritime Administration is responsible for shipping infrastructure in the form of fairways, icebreakers, and networks for communication with shipping. In addition important services such as pilotage, maritime traffic information, inspection and rescue are provided. Information from the Administration's IT system is crucial to many of these services. Failings in the security of information of the Maritime Administration may have consequences for both Swedish shipping and shipping in Sweden. These consequences may in turn have implications for the wider community. Industry and commerce may be affected by transport delays and loss of safety at sea. The safety of the country could also be affected when the Maritime Administration handles secret information. Implications for the Swedish Maritime Administration may be loss of confidence from the world around, reduced internal efficiency and lower revenues.

Does the Swedish Maritime Administration have an effective information security system?

Both yes and no. The Administration has several of the components that according to the standard together constitute an information security management system. However certain parts are less well developed – functions that create a general view, reporting, risk analysis, training and monitoring, and administration of the system. These links in the chain that the management system ought to form are missing or they are too weak. These inadequacies mean that the Maritime Administration's information security management system is not a fully appropriate and functional totality. In practice the failings mean that the possibility of the Administration

¹ Swedish acronym for Information Security Management System

systematically discovering and learning from experience in information security work and use of the management system is reduced. This in turn reduces the possibility of carrying out effective improvements to the information security management system in stages. The inadequacies of the system in turn affect the possibility of achieving and maintaining the desired security of information. The answer to the question that the audit was intended to ask is therefore that the Swedish Maritime Administration is not working fully systematically on security of information on the basis of current norms.