

RiR 2006 24

## Audit of the Swedish Labour Market Administration's internal management and control of information security

### Summary

Almost one third of all public organisations in Sweden have been exposed to some kind of serious data trespass or virus attack. These attacks are becoming increasingly serious and more advanced. At the same time, government agencies are conducting more and more of their activity on the Internet in the form of electronic services and thus need to work to protect their information and the IT support for their activity. This work is both difficult and frequently makes heavy demands in terms of resources. It is against this background that the Swedish National Audit Office (SNAO) has increased its endeavour to audit information security within the public administration.

Responsibility for managing and controlling information security in the public administration is divided among the Riksdag, the Government, the Government-appointed supervisory and support agencies, and the management of the individual agencies. SNAO has chosen in this audit to focus on the way in which the agencies' management exercise their responsibility for information security.

In 2005–2006, SNAO audited information security at ten agencies. The focus of the present audit is the way in which the Swedish Labour Market Administration (AMV) has worked on its information security.

### What does information security mean?

Information security is about the right information being available, not being corrupted or destroyed and not being accessible for unauthorised persons. It shall also be possible to trace who has used the information and changed it.

SNAO has based its audit on an international standard, the LIS standard (SS-ISO/IEC 17799). The LIS standard describes how a well-functioning management system for information security should be designed.

The standard covers all the areas that security work should comprise: management, organisation and division of responsibilities, the purely technical protection system, and also influencing employees' behaviour.

### What are the potential consequences of inadequate information security?

The AMV's IT systems must be capable of handling very large cash flows and large volumes of integrity-sensitive data relating to a very large number of individuals, as well as data concerning enterprises and job vacancies.

In 2005, almost 720,000 individuals were registered as unemployed at any one time with AMV. Some 430,000 job vacancies were notified and about 415,000 placements in labour market programmes were carried out. The number of registered unemployed obtaining work has been about 630,000 per year in the last five years. The AMV's expenditure in the 2005 budget year amounted to approximately SEK 67 billion.

The Internet services offered by the AMV have been developed gradually. The number of unique visitors to the AMV's website has risen from approximately 700,000 in 2002 to fully 1.5 million in the first quarter of 2006 alone.

Stringent requirements must be satisfied to ensure that the information contained in the AMV's information system is protected: that the correctness,

accessibility, confidentiality and traceability of the information is protected. Wrong information in the AMV's records as a result of inadequate information security can have widespread consequences.

Some examples of the potential consequences of inadequacies in information security include:

- that confidential personal information is disclosed,
- that individuals may suffer financially if supporting information given to the unemployment insurance funds is incorrect and decisions are made on erroneous grounds,
- that statistical data and follow-ups to the Government and the Riksdag, among others, are misleading,
- that matching jobseekers with employers' job vacancies does not have the full effect because of the inadequate quality of records.

## Does the AMV have a well-functioning information security management system?

The audit shows that the management's information security work at the AMV has three serious inadequacies which impact on the management's ability to implement the security levels decided upon and to work to maintain them within the agency. These inadequacies relate to the management and control of the information security work, the work on an overall risk analysis, and the management's monitoring and further development of the information security management system.

More specifically, the following inadequacies can be mentioned. Several management decisions relating to the work on information security by staff responsible for operations have not been executed. There is no overall plan of action for the security work. No training in security work has been provided to the staff. The management have not taken the initiative to improve their work on information security but this need has been pointed out by staff within the organisation and by outsiders.

The inadequacies relate to significant points in the information security management system. All in all, SNAO takes the view that the AMV, on the basis of current standards, is not working fully systematically on its information security management system. The consequences of inadequate information security can be serious, as illustrated above.

## The recommendations of SNAO

In SNAO's opinion, a clear and coherent information security management system is essential in order for the AMV's management to ensure that the security levels decided upon are introduced and maintained within the entire agency. Among other things, this requires the system to comprise AMV in its entirety and to be integrated with other management systems. This should enable the AMV's management to have a general view of risks and differences in risks between different activities, the need for security measures, and the costs of security work in the various activities. It should also make plain the scope that exists for determining priorities between investments in security in different parts of the agency. In SNAO's opinion, the LIS standard employed in the audit contains the most important requirements that an information security management system should satisfy.

An important point of departure is that the AMV must be able to guarantee to citizens and enterprises that the information contained in the IT systems is being handled securely. The AMV's management should furthermore set requirements for their information security management system which take into account the serious consequences that can occur if the IT systems are not secure. The AMV has recently commenced important work to improve its information security management system.

SNAO recommends that the AMV should have regard for the following in the work done to improve the information security management system.

- The management should design the system so as to be sure that the security levels decided upon are introduced and maintained within the entire agency. This should also include specifying and establishing how the security work should be done and making clear the division of responsibilities, co-ordination, training programmes and reporting routes within the organisation.
- The AMV's information security management system should include a systematic process for the agency's risk analysis work. This process should enable the management to get a general view of the entire AMV, differences in risks between different activities, the need for security measures, and the costs of the security work in the various activities. It will also make plain the scope that exists for determining priorities between investments in security in different parts of the agency. These priorities should be collected in a plan of action. Using this plan, the management should follow up to ensure that the measures decided upon are introduced and that they function as intended. The plan should also be framed so that the resources devoted to security work can be described, followed and evaluated.
- The management should systematically monitor how well the information security management system is functioning, and whether the assumptions and requirements on which the management system is based are fulfilled and relevant. This should take place as part of a strategy for further development of the system.