SWEDISH NATIONAL AUDIT OFFICE

Summary

Date: 2023-11-23
Reference number: 2022/0652
RiR 2023:20

Information security at higher education institutions

– management of research data requiring protection

Summary

The objective of research policy is for Sweden to be one the world's foremost research and innovation countries and a leading knowledge nation. Internationalisation and open science are seen as a means to promote quality. At the same time, certain research needs to be protected so as not to harm, for example, the privacy of individuals, Sweden's competitiveness and the security of society. The number of cyber attacks has increased and intelligence activities against higher education institutions (HEIs) have intensified in recent years. The need for HEIs to work effectively on information security has thus increased.

The overall conclusion of the Swedish National Audit Office (Swedish NAO) is that the HEIs do not carry out effective information security measures to protect research data. Even though regulatory requirements have existed since 2008, and shortcomings have been known for a long time, essential elements of systematic information security are still missing. The measures taken to date by the Government, HEIs and other agencies concerned have not been sufficient.

The audit covers 24 higher education institutions that conduct research in natural sciences, engineering and technology.

Swedish National Audit Office / Riksrevisionen
S:t Eriksgatan 117
Box 6181, 102 33 Stockholm, Sweden
+46 8 5171 40 00
www.riksrevisionen.se

HEIs are not effective in identifying research data requiring protection

Few researchers classify their research data in accordance with the HEIs' models for information classification. Instead, it is common for external funding agencies or partners to demand that research data be classified, or researchers may make a less formal assessment that is not documented. HEIs' failure to systematically identify research data requiring protection means that they lack a sufficient basis to assess risks and determine which protective measures are appropriate. It can also lead to certain research data requiring protection not being identified at all. There are also cases of researchers and departments having their own IT solutions outside the IT structure provided by the HEI. This may entail that research data requiring protection does not receive appropriate protection.

HEIs have insufficient knowledge and expertise to assess what requires protection

There is a general lack of knowledge and expertise concerning issues related to information security among many employees at HEIs. This includes knowledge on how to protect their information in practice, as well as knowledge on how to classify their research data and how they relate to current regulations and external requirements. HEIs themselves request support to assess external threats and antagonists that may pose information security risks. The audit shows that HEIs make different assessments of what needs protecting, which can lead to research data requiring protection not being appropriately protected. The training sessions offered by HEIs reach a limited number of employees. HEIs also face challenges in recruiting and retaining staff in this field.

HEI managements have not managed and organised information security effectively

HEI managements have not ensured that adopted guidelines, procedures and working methods have been implemented throughout the organisation. There are ambiguities in the distribution of roles and responsibilities at various levels within the HEIs. For example, both heads of department and researchers are unsure what responsibility they have for information security and what this means in practice. The support provided by HEIs for managing research data has limited impact. The support is also not always coordinated with the information security functions at the HEI. Those who are appointed to coordinate and lead information security efforts often lack the framework to work strategically, in part due to their position in the organisational structure. They also do not report regularly to the vice-chancellor or to the board.

Government and agency measures to strengthen information security have been insufficient

Despite knowing that HEIs' work related to information security for a long time was inadequate, it was not until 2019 that the Government began following up their work more systematically through agency dialogue and various reporting requirements. The Swedish Civil Contingencies Agency's training initiatives, methodological support and tools for following up the systematic information security efforts have not had sufficient impact in the higher education sector. This also applies to the training initiatives of the Swedish Security Service and the Inspectorate of Strategic Products aimed at higher education.

Recommendations

To the Government

- Commission the Swedish Civil Contingencies Agency with carrying out skills enhancement initiatives for management at the HEIs. These initiatives should be adapted to the needs of the HEIs.
- Task HEIs, in cooperation, to establish a joint support function for information security. This should take place in consultation with the Swedish Civil Contingencies Agency and other relevant agencies. These agencies should continue to provide advice and support after the function has been established. The support function is to support HEIs with matters such as:
    - Advisory services to those leading and coordinating information security on matters such as the design of information security systems, analysis, security measures as well as interpretation and compliance with regulations on matters such as protective security and export control
    - tailored training sessions and courses on information security for all employees at HEIs
    - support to relevant functions at HEIs for analysing and assessing sector-wide risks and external threats.

It can be useful for the support function to benefit from knowledge and experiences from ongoing cooperation between HEIs and information security networks.

To the 24 higher education institutions included in the audit

- Ensure that roles and the distribution of responsibilities are clear from the management level to individual employees, so that each employee knows their responsibilities in terms of handling research data correctly.
- Ensure that those leading strategic information security efforts have a mandate to set requirements and review information security and that they regularly report to the HEI management and board.
- Ensure that working methods for information classification of research data are uniform.
- Ensure that there is competence in place to analyse information security risks linked to research data.
- Ensure that there is coordinated support for employees to manage research data correctly throughout its life cycle.