

# Conclusions of the National Audit Office

## State of cybersecurity management in the central government

The audit focused on the state of cybersecurity management in the central government. The aim of the audit was to provide an up-to-date overview of the situation. The relevance of the audit stemmed from the EU's cybersecurity directive (NIS2), the transposition of which into national legislation was still ongoing at the time of the audit's information-gathering phase. Another key basis for the audit was Finland's Cyber Security Strategy, the update of which was completed in October 2024. In the audit, the National Audit Office examined particularly the central government's readiness to implement both the new legislation and the cybersecurity strategy.

## The cybersecurity strategy provides guidance for development, but there are insufficient conditions for its effective implementation

Finland has for a long time had a national cybersecurity strategy, which the EU also requires its Member States to draw up and maintain. However, the implementation of the strategy has been fragmented. The strategy updated in 2019 was implemented in four separate programmes or projects, and the implementation was not monitored or assessed as a whole. Monitoring information on the different programmes has also been fragmented and partly incomplete.

Finland's Cyber Security Strategy was revised in 2024. The new strategy is intended to be implemented through a joint implementation plan, which is a clear improvement compared with the previous strategy. The monitoring of the implementation is also coordinated, and there is a jointly agreed model for it, but the monitoring indicators need to be specified. The implementation plan seems to be quite comprehensive, which was seen in the audit in that many of the areas of improvement identified in the audit are already included in the plan. Therefore, the National Audit Office does not raise any individual points included in the implementation plan in its recommendations but considers it to be important overall that the plan is implemented.

Although the strategic-level coordination has improved, the challenge for the implementation of the strategy continues to be that the implementation plan does not include a budget or allocated resources, but each administrative sector responsible for the different measures is responsible for its own resources and submits its own proposals related to them. This does not enable cross-administrative prioritisation of measures according to the overall interests of the state and society, and no single entity holds overall responsibility for the implementation of the strategy. The resource situation also limits the

development in individual organisations, which underlines the importance of prioritisation.

Based on the audit, the development of cybersecurity in the central government can be considered at least partly long-term and systematic. However, in practice, the long-term nature of the implementation can be seen, for example, in that previously identified or launched measures are carried over from one plan to the next.

## The cybersecurity management model requires cooperation

The management of cybersecurity in Finland is based on the division of responsibilities among competent authorities, which in turn is based on the operating model of comprehensive security. The model requires inter-agency cooperation and coordination, which, according to the audit's overall findings, has improved in recent years.

As a counterbalance to the decentralised operating model, certain functions have also been centralised. The National Cyber Security Director's Office, placed at the Ministry of Transport and Communications, is responsible for the national coordination of cybersecurity. However, the Office has no specific competence or performance and development responsibility for the national cybersecurity. Another very important centralised actor is the National Cyber Security Centre of the Finnish Transport and Communications Agency Traficom. It brings together expert functions and services that support the management of cybersecurity. According to the audit findings, the role of the National Cyber Security Centre is generally considered to be well established and very important.

The National Cyber Security Centre collects and maintains a situational picture of cybersecurity, mainly based on the reports it receives from different actors. It publishes situational picture products on a daily, weekly and monthly basis and, based on the audit, there is general satisfaction with them. However, the analyses mainly relate to past events, and more forward-looking situational pictures have been identified as a development target.

The national legislation implementing the NIS2 Directive entered into force in April 2025. The supervisory roles under the Directive are distributed among authorities overseeing different sectors. Most of these supervisory bodies consider the resources available for the oversight to be very limited in relation to the scope and importance of the task.

## The overall state of cybersecurity management at different authorities is reasonably good

In a survey conducted by the National Audit Office, the central government authorities and wellbeing services counties considered their cybersecurity management processes and practices to be reasonably good. Based on the overall picture obtained in the audit, an increasing number of organisations have started

to pay attention to cyber and information security in recent years, which has led to an overall improvement in maturity.

Based on the survey conducted in the audit, approximately half of the central government actors and wellbeing services counties estimated that the NIS2 Directive sets additional requirements for their organisation. As a rule, the respondents assessed that their readiness to meet the requirements was at a good level.

Most central government organisations report that they utilise different standards and criteria in the development of their operations. There are also common assessment models available for improving cybersecurity, but for the time being, they do not provide a comprehensive overview of the state of cybersecurity management processes in the central government or in general government as a whole. The guidelines on cybersecurity and information security are fragmented, although efforts have been made to bring them together in one place.

The authorities have recognised that incident response exercises are very important in cybersecurity management. The Taisto and KYHA exercises form the foundation for exercise activities in the central government, but in addition to them, the different administrative sectors and organisations also carry out other exercises to varying degrees.

## Recommendations of the National Audit Office

1. The Ministry of Transport and Communications should actively monitor the implementation of the cybersecurity strategy and, if necessary, update the implementation plan together with the administrative sectors and authorities that are responsible for the measures.
2. The Ministry of Transport and Communications and the Ministry of Finance should strive to ensure that the development targets in cybersecurity are prioritised, where necessary, across administrative boundaries and that the measures assessed to be the most important are allocated the resources required for their implementation.
3. The Ministry of Transport and Communications and the Finnish Transport and Communications Agency Traficom should monitor and support the readiness of the authorities responsible for the supervision under the NIS2 Directive to carry out high-quality supervisory work.