FOLKETINGET
STATSREVISORERNE

FOLKETINGET
RIGSREVISIONEN

December 2023
– 5/2023

Extract from Rigsrevisionen's report submitted to the Public Accounts Committee

The cyber security resilience of the Danish public sector II

1. Introduction and conclusion

In this report, the names of public authorities and systems are anonymised

The report presents assessments of security procedures in relation to government IT systems that are part of the critical IT infrastructure in Denmark. Some of the authorities and all the systems examined are anonymised because information about the authorities' cyber security resilience is considered confidential, cf section 27 of the Danish Public Administration Act and section 152 of the Danish Criminal Code. Rigsrevisionen has found no reason not to acknowledge this assessment. Due to the anonymisation, four authorities in the study are referred to by number (1, 2, 3 and 4), and the IT systems are referred to as system 'A' to 'L' in the report.

1.1. Purpose and conclusion

1. This report concerns the cyber security resilience of selected critical IT systems.

Public authorities depend on IT to deliver their services. Major IT breakdowns and loss of data relating to critical IT systems can have far-reaching consequences for the government, citizens and companies. It is, therefore, important that the authorities have developed appropriate IT contingency plans and can continue operations and mitigate the consequences of system breakdowns or data losses in the event of a major IT breakdown.

2. Approximately 90 of the government’s IT systems are assessed to be critical by the departments. In November 2022, Rigsrevisionen submitted a report to the Danish Public Accounts Committee concerning the contingency plans of 13 of these critical IT systems. The quality of the contingency plans for the 13 systems was not satisfactory, and it had not been tested if the majority of the systems could be recovered, in the event of a major IT incident. Rigsrevisionen’s follow-up on the report in October 2023 showed that the cybersecurity resilience of the 13 examined IT systems had been strengthened.

In this new report, Rigsrevisionen looks at the cybersecurity resilience of another 12 critical IT systems.

Critical IT systems
Interrupting the operation of such systems has severe consequences for the society at large, such as:

- Economic losses for the government, citizens or companies;
- Long-term breakdown of critical infrastructure;
- Threats to national security.

3. Figure 1 shows the authorities and number of IT systems in the report.

Figure 1

Authorities and number of IT systems included in Rigsrevisionen's study

The Ministry of the Interior and Health	The Danish Business Authority	Authority no 1	Authority no 2	Authority no 3	Authority no 4	The Danish Maritime Authority
System A	System B	System C	System E	System F	System H	System J
		System D		System G	System I	System K
						System L

Response to major IT incidents

Contingency plans must be developed to manage major IT incidents, including incidents that make IT systems inaccessible due to hacker attacks, damage to data centres, or server errors.

If data cannot be recovered from a backup system, for instance, after a system breakdown or hacker attack, major IT incidents may also result in data losses.

Types of IT contingency plans

- **Crisis management plans** outlines the authorities' internal crisis management and their communication with external parties.
- **Emergency plans** set out how the authorities can maintain critical tasks in the event of a system breakdown.
- **Disaster recovery plans** describe the recovery of IT systems after a system breakdown.

4. The purpose of the study is to assess whether the government has adequate contingency plans for 12 selected critical IT systems to ensure that the public sector can sustain critical public services in the event of major IT incidents. The report answers the following questions:

- Does the government have an adequate basis for developing contingency plans for the selected critical IT systems?
- Has the government developed satisfactory crisis management plans for the selected critical IT systems?
- Has the government developed satisfactory emergency plans for the selected critical IT systems?
- Has the government ensured that satisfactory disaster recovery plans have been developed for the selected critical IT systems?

In sections 3, 4 and 5 of the report, we have examined whether these three types of contingency plans have been developed and tested.

Rigsrevisionen initiated the study in February 2023. It covers the period from January 2020 up to and including March 2023.

Main conclusion

The contingency plans developed by the Ministry of the Interior and Health for its critical IT system are generally satisfactory. Although affected by shortcomings, the quality of parts of the contingency plans developed by the Danish Business Authority is mainly satisfactory, as are the contingency plans for the Danish Maritime Authority's three critical IT systems. The contingency plans for the remaining seven critical IT systems are not satisfactory. Five IT systems (systems C, D, E, F and G) are particularly inadequate. Shortcomings and inadequacies in contingency plans entail a risk of system breakdowns and data losses that may make it impossible for the government or severely disrupt its ability to perform tasks critical to society.

The authorities have established a sufficient basis for contingency planning for half of the IT systems in the form of risk assessments and overviews of the underlying IT systems that the selected systems depend upon to function.

The authorities have developed contingency plans for the majority of the IT systems, but the quality of the plans varies significantly. A few plans are satisfactory, whereas others, particularly the disaster recovery plans, are affected by significant shortcomings. For example, descriptions of the technical recovery of IT systems after a major IT breakdown were missing in more than half of the plans. A few of the IT systems are without contingency plans.

Rigsrevisionen finds it unsatisfactory that only a few of the contingency plans have been tested. It means that the authorities have not tested the effectiveness of the plans and do not know if the plans have the desired effect. As an example, it has not for the majority of the IT systems been tested whether they would be recoverable after a major IT incident.

The majority of the ministries have supervised the IT contingency planning. Despite this, the study found significant shortcomings in the authorities' contingency plans and testing of the plans.