FOLKETINGET
STATSREVISORERNE

FOLKETINGET
RIGSREVISIONEN

November 2022
– 3/2022

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

The cyber security resilience of the public sector

1. Introduction

1. In October 2021, the Danish Public Accounts Committee asked Rigsrevisionen to look at cyber security resilience in the public sector. Rigsrevisionen completed the study and reported its findings in a confidential report to the Public Accounts Committee because the report included assessments of IT-security measures in relation to critical IT systems.

2. This brief report does not include any confidential information but is expected to contribute to ensuring that both the authorities referred to in the report, and other public bodies, direct more attention to building cyber and security resilience.

2. Background and main conclusions

Response to major IT incidents

Contingency plans should be implemented to manage major IT incidents, including incidents that make IT systems inaccessible due to, for instance, a hacker attack, damage to a data centre, or server errors.

Major IT incidents may also result in loss of data, when data cannot be recovered from a backup system, for instance following a system breakdown or hacker attack, or when data affected by error are copied to other servers or IT systems.

Types of contingency plans

- **Disaster recovery plans** describe the technical recovery of IT systems in emergencies.
- **Crisis management plans** outline the internal crisis management in the event of an unexpected major system breakdown.

3. 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 appropriate IT contingency plans in place to manage and mitigate the consequences of potential system breakdowns or loss of data.

4. The purpose of Rigsrevisionen's study is to assess whether the government has established adequate contingency plans for selected critical IT systems to ensure that the public sector can sustain critical services in the event of major IT incidents. We have also examined the guidance and support on the development of IT contingency plans provided by Digitaliseringsstyrelsen (Danish Agency for Digital Government). The study covers the years 2019 to 2021.

5. The Danish Agency for Digital Government estimates the total number of IT systems operated by public bodies at approx. 4,200. Rigsrevisionen has examined 13 critical IT systems that support delivery of essential services to society.

The study looks at the authorities' mapping of critical IT systems, risk assessments and two types of overall IT contingency plans that both specify a course of action in response to incidents:

- *Disaster recovery plans* for the recovery of IT systems in the event of loss of data or system breakdown
- *Crisis management plans* for the authorities' internal management of major IT incidents.

Main conclusions

The cyber security resilience of the 13 critical IT systems selected for this study is not satisfactory. The resilience of one of the authorities, where Rigsrevisionen examined several IT systems, is particularly unsatisfactory. The consequence of inadequate cyber security resilience is that critical services provided by the public sector risk being either seriously disrupted or impossible to deliver.

It should be noted that the level of cyber security resilience varies between the authorities in the study.

Our conclusion is based on the following findings:

Basis for the authorities' cyber security resilience

The authorities have mapped their critical IT systems. However, not all the authorities have an overview of the underlying systems which the systems examined depend upon to function. The authorities must have an overview of this interdependence because critical IT systems may cease to function if underlying support systems and platforms, for instance, are down.

The authorities have made risk assessments of ten out of the 13 IT systems in the study. It is essential for the cyber security resilience of the public sector that the authorities' risk assessments of critical IT systems can be operationalised and used in managing identified risks.

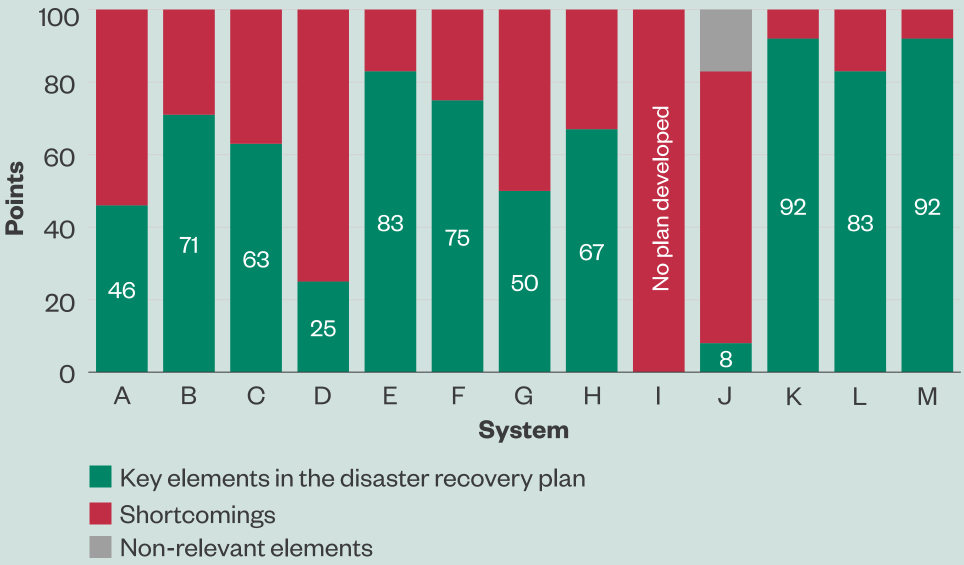
Disaster recovery plans

The authorities have not ensured that adequate disaster recovery plans have been developed for the 13 selected critical IT systems. The purpose of disaster recovery plans is to ensure that the authorities can resume normal operations as quickly as possible after a breakdown. To achieve that, the authorities must have disaster recovery plans that address key elements and are updated and tested.

Some disaster recovery plans are affected by a few shortcomings, but the majority are affected by several shortcomings, and one IT system was without a disaster recovery plan altogether. Figure 1 shows Rigsrevisionen's assessment of the disaster recovery plans for the 13 IT systems.

Figur1 1

Overall assessment of the disaster recovery plans developed for the 13 IT systems



Source: Rigsrevisionen based on information provided by the authorities in the study

None of the disaster recovery plans developed for the 13 IT systems have been sufficiently tested and five of the systems were not tested in the period from 2019 to 2021. This means that the authorities do not know whether it will be possible to recover the systems in the event of a complete breakdown, nor do they know how long it will take to get the systems up and running.

The study shows that the authorities' management of IT-systems outsourced to external suppliers is inadequate. For instance, under half of the contracts require the suppliers to test system recovery.

Crisis management plans

The crisis management plans developed by the authorities are generally adequate. The crisis management plans should, among other things, define response roles and responsibilities and how the authorities should communicate in the event of major IT incidents. These factors must be in place before a major incident occurs in order to minimize the potential impact of a major system breakdown or loss of data.

Most of the authorities' crisis management plans address all the key elements that should be included in such a plan. A few of the examined plans are, however, not entirely satisfactory.

With the exception of one, all the authorities have tested their crisis management plans in the period from 2019 to 2021. It is essential that the plans are tested regularly to ensure that they are up to date and support effective internal crisis management.

Digitaliseringsstyrelsen's guidance on the development of IT contingency plans

Digitaliseringsstyrelsen's guidance to public bodies on implementing their cyber resilience strategy has been satisfactory. However, Rigsrevisionen recommends that in the future Digitaliseringsstyrelsen should examine the authorities' need for guidance systematically to support their implementation of an adequate level of cyber resilience more effectively.