



**FOLKETINGET
STATSREVISORERNE**



**FOLKETINGET
RIGSREVISIONEN**

**September 2021
– 20/2020**

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

The Ministry of Taxation's IT contingency planning

1. Introduction and conclusion

1.1. Purpose and conclusion

1. This report concerns the Ministry of Taxation's IT contingency plans for critical business processes. The Ministry of Taxation depends on a vast number of IT systems to collect and enforce payment of taxes and duties, repay negative VAT and other transactions. The ministry carries out these tasks in so-called business processes that are supported by a number of integrated IT systems. This report has focus on the ministry's IT contingency planning covering business processes for personal taxes, VAT and corporate tax. Combined, these account for just under 80 per cent of the government's total tax revenue.

2. The number of IT incidents is increasing. In 2020, six out of 10 Danish companies experienced cyber security incidents, including hacker attacks, which is the highest level recorded in four years. According to the Danish Center for Cyber Security's risk assessment, all Danish public authorities, companies and citizens are exposed to a persistent threat of cybercrime. The authorities' contingency plans should enable the authorities to deal effectively with major IT incidents like, for instance, hacker attacks that could potentially lead to the breakdown of their IT systems or loss of data.

3. If the Ministry of Taxation's critical business processes and underlying IT systems are affected by major breakdowns and loss of data, the consequences for the government, citizens and companies can be dire. First, the Danish Tax Administration may be unable to collect taxes and duties. Second, the government may be unable to manage tax refunds, which could ultimately have a negative impact on the cashflow of companies that are waiting to receive, for instance, a VAT refund. Third, public authorities may be unable to manage payments of SU (Danish grants and loans scheme for students), social benefits, pension, etc., because the authorities depend on data from the Tax Administration's IT systems to be able to calculate payments to the citizens. Last, the Ministry of Taxation may be unable to recover data, or it may incur considerable costs to restore data from scratch, if data held by the Tax Administration are lost or affected by error.

Major IT incidents that require implementation of IT contingency plans

Major IT incidents include breakdown of IT systems due to, for instance, hacker attacks, damage to data centers, server errors or loss of data. Data can be lost, if it turns out to be impossible to restore data from a backup, following an IT breakdown or hacker attack, or if data affected by error have subsequently been copied to several IT systems or servers.

The Ministry of Taxation operates with three types of IT contingency plans

Business continuity plans

An emergency plan specifies how the Ministry of Taxation should handle and sustain the business processes that are affected in the event of a disaster.

Action plans

An action plan addresses internal crisis management of each individual IT system in the event of an unexpected major incident.

Disaster recovery plans

A disaster recovery plan deals with how you restore an IT system to working order following an IT incident.

4. It is therefore crucial that the ministry's contingency plans enable the ministry to respond quickly and effectively to major breakdowns and potential data losses. Contingency plans must be in place, before disaster strikes. The purpose of contingency plans is to ensure that the ministry will be able to implement alternative business processes in order to continue its operations during the time the IT systems are down. To achieve this, the ministry must have an overview of the IT systems that are included in the business processes, and it must have contingency plans in place that specify the actions that the ministry needs to take in an emergency situation. The contingency plans are intended to assist the ministry in restoring normal operations as soon as possible and minimize the consequences of major IT breakdowns and data losses. Like all other public authorities, the Ministry of Taxation is required to implement ISO27001, which prescribes the preparation and testing of IT contingency plans. The Ministry of Taxation has determined that its contingency plan should include three types of contingency plans: Emergency plans, action plans and disaster recovery plans.

5. The IT systems that support the Ministry of Taxation's critical business processes are interdependent. Data are transferred between the IT systems and some systems depend on other systems to be able to operate. To be able to put together an overall effective contingency plan, the ministry needs to coordinate contingency planning for the individual IT systems that support the business processes.

6. The purpose of the study is to assess whether the Ministry of Taxation has prepared satisfactory contingency plans for critical business processes. The report answers the following questions:

- Has the ministry's planning of information security continuity been established on an adequate basis?
- Has the Ministry of Taxation ensured the implementation of appropriate IT contingency plans?
- Has the Ministry of Taxation coordinated IT system contingency planning?

Rigsrevisionen initiated the study in June 2020.



Main conclusion

The Ministry of Taxation's IT contingency planning for critical business processes is not satisfactory. This entails a risk that the ministry will be unable to collect taxes and duties and repay amounts due to citizens and companies due to system breakdowns and loss of data.

The Ministry of Taxation's basis for preparing IT contingency plans is inadequate

The Ministry of Taxation has mapped the IT contingency plans for seven of the 45 IT systems that the ministry has characterized as being critical. The ministry has no overview of the IT contingency plans for the remaining 38 critical systems and the approx. 185 other IT systems in the remit of the ministry.

The Ministry of Taxation has worked out risk assessments of the critical IT systems, which do not consistently include assessments of risks relevant to IT contingency planning. The assessments are therefore not providing the ministry with an adequate basis for preparing appropriate contingency plans,

The Ministry of Taxation has not implemented emergency and action plans for critical business processes, but has generally ensured implementation of satisfactory disaster recovery plans

The Ministry of Taxation has only worked out one emergency plan, covering VAT, in the remit of the Tax Administration. However, the emergency plan is not satisfactory, since it addresses only critical failures in one of the five IT applications that perform specific administrative functions concerning VAT. The ministry has not worked out action plans for internal crisis management of eight of the nine examined IT systems that handle essential tasks in connection with personal tax, VAT and corporate tax. Neither the emergency plan for the VAT business process nor the one action plan prepared by the ministry has been tested by the ministry.

The Ministry of Taxation has ensured that disaster recovery plans have been worked out for eight of the nine examined IT systems that need to be recovered following a breakdown. This means that one of the critical IT systems is without a recovery plan. Six of the eight disaster recovery plans cover most of the essential elements that should be included in such a plan, and they are therefore generally found to be satisfactory. Several essential elements are, however, missing in two of the recovery plans. All eight disaster recovery plans have been tested. However, testing has been inadequate, since not all relevant key elements have been tested.

The Ministry of Taxation had difficulties procuring the existing IT contingency plans in the course of the study. It is crucial that the ministry in the event of an emergency can produce the relevant IT contingency plans without delay.

Business critical processes

The study looks into three critical business processes:

- Personal tax
- VAT
- Corporate tax.

The study looks at nine IT systems that support one or several of these three business processes.

IT applications

An IT application is a computer software package that has been developed for the users. It performs a specific function and is supported by underlying systems software (business support systems).

The Ministry of Taxation has not coordinated IT contingency planning for the IT systems that support critical business processes

The Ministry of Taxation has not systematically mapped the interdependence of the IT systems that support the business processes for personal tax, VAT and corporate tax. Nor has the ministry decided on, or agreed with the suppliers, the order in which the IT systems must be recovered, if all or several systems are down at the same time. This means that the ministry may find it difficult to minimize the impact of a major IT breakdown in the event of an emergency.

The Ministry of Taxation has not coordinated the Recovery Time Objective for each individual IT system, i.e. how long it must take before each IT system is recovered. Nor has the ministry coordinated the Recovery Point Objective for each individual IT system which is a measurement for the amount of data loss for each IT system. As a result, the ministry may experience a major data loss, and recovery of the systems may take longer than expected.

The Ministry of Taxation has yet to clarify which agency should be responsible for coordinating IT contingency planning across the IT systems. Coordination of contingency planning is essential for the ministry's effort to develop a satisfactory IT contingency plan.