FOLKETINGET
STATSREVISORERNE

FOLKETINGET
RIGSREVISIONEN

December 2020
– 7/2020

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

Steps taken to prevent fraud in the public-sector

1. Introduction and conclusion

1.1. Purpose and conclusion

1. This report concerns the steps taken by Danish ministries to prevent fraud committed internally by people employed in the public sector. Fraud committed internally by individuals employed in the public sector covers a wide spectrum of activities, including abusing public funds for private purchases or transferring money into private accounts. In recent years, we have seen several cases, where public-sector employees have committed fraud or been involved in fraudulent activities. Examples include procurement fraud in the Estate Agency under the Danish Ministry of Defence, social grants fraud and dividend reclaim tax fraud.

Definition of fraud
An intentional act by one or more individuals among management, those charged with governance, employees, or third parties, involving the use of deception to obtain an unjust or illegal advantage.

Definition as per ISA 240.

In the annual report on the audit of the Danish public accounts, Rigsrevisionen has, for many years, assured the Danish Public Accounts Committee that the overall accounting management of public funds is sound and reliable. However, Rigsrevisionen has also detected errors, uncertainties and weaknesses in internal controls and highlighted cases involving a risk of error or fraud.

It is not the auditors' responsibility to detect fraud that does not materially affect the financial statements, but they are required to act, if they become aware of fraudulent activities. The management of the individual ministries and government bodies is responsible for preventing and detecting fraud, and therefore also responsible for establishing appropriate business processes and internal controls. An important aspect of this work is ensuring separation of duties (also referred to as the Two-man rule or the Four-eyes principle), which means that, for instance, the person signing for the receipt of a purchase cannot also authorise payment of the purchase. Observing this principle is essential for the prevention of internal fraud in the public sector.

Business processes and internal controls
Business processes are processes and guidelines that describe how the administration has been organised and how internal controls and supervision of these should be conducted.

Internal controls cover the measures implemented by the management to avoid errors and fraud.

Rigsrevisionen initiated the study in April 2020 at the request of the Danish Public Accounts Committee. The members of the committee requested a study that covered grants, procurement and payroll fraud. In connection with Rigsrevisionen's presentation of how the study could be conducted, the members of the committee expanded the study to include also public-sector employees' use of credit cards. In the report, we highlight areas of public administration in which unsatisfactory business processes and controls entail a risk of internal public-sector fraud. Because fraud can involve large as well as small amounts, we report on all our findings irrespective of the amount involved and irrespective of whether a potential incident of fraud would affect the correctness of the overall accounts.

Management framework
An appropriate management framework sets out the rules and procedures that make it difficult for the individual employees to circumvent the rules. For instance, by defining settings for authorizing and paying invoices that require application of the Four-eyes principle.

Rules and procedures can be determined locally in instructions issued by the ministry, government bodies and in accounting regulations, or, at an overall level, in the government accounting regulations.

2. The purpose of the study is to assess whether the business processes and internal controls established in the ministries are appropriate to mitigate the risk of fraud committed by public-sector employees. The report answers the following questions:

- Did the ministries in 2019 have an appropriate management framework in place for mitigating the risk of grant, procurement and payroll fraud committed by public-sector employees?
- Did the ministries have satisfactory system support for separation of duties in shared government IT-systems in 2019?
- Had the ministries in 2019 in practice established appropriate internal controls to mitigate the risk of procurement and payroll fraud committed by public-sector employees?
- Did the ministries' grant systems have appropriate, IT-supported controls in 2019?

Main conclusion

It is Rigsrevisionen's assessment that, overall, the business processes and internal controls set up by the ministries in order to mitigate the risk of fraud committed by public-sector employees were not satisfactory in 2019. Rigsrevisionen has not detected any specific incidents of grant, procurement or payroll fraud, but has noted weaknesses in controls that would have made it possible for public-sector employees to commit fraud without being detected. The consequence of Rigsrevisionen's findings is that it would have been possible for employees in the public sector to authorise illegal payments in connection with the administration of grants, procurement and payroll in 2019 – and in principle – several years back.

The management frameworks of most ministries were inadequate for the purposes of preventing fraud committed by public-sector employees concerning procurement and payments of grants and salary

The study shows that the ministries have management frameworks that support the presentation of the accounts based on materiality and risk. However, the ministries' monitoring of internal controls in the government bodies is not supporting the top management in obtaining an adequate overview of the effectiveness of the grant, procurement and payroll controls in relation to preventing fraud by public-sector employees. Additionally, the majority of the ministries have neither in 2019 nor in 2020 updated the ministerial instructions with descriptions of the key elements of their respective internal controls and risk management requirements. This in spite of the fact that this annual update has been included in the government accounting regulations as a requirement since 2018. All the ministries make it clear that they have established fundamental controls such as separation of duties and logging of user activities across their remit, but 50% of the departments indicate that they have only partially or not at all in 2019 checked whether the implemented separation of duties functioned as intended.

At the same time, however, Rigsrevisionen notes that, after the detection of fraud in the public sector in 2018 and 2019, several ministries have reassessed and strengthened controls.

The system-supported separation of duties could be circumvented via adjustments and allocation of access rights implemented locally in the government bodies

The study found that the default setting of the shared IT government systems *IndFak, RejsUd* and *SLS* supports separation of duties. But the study also shows that it is possible to set up IndFak and RejsUd locally in a way that allows the employees to make transactions without appropriate separation of duties. Generally, case processing in the SLS system is subject to manual controls, because unauthorised salary payments are not automatically blocked in the payroll system.

IndFak, RejsUd and SLS

IndFak is the Ministry of Finance's shared procurement and invoice management system.

RejsUd is the Ministry of Finance's shared travel expense management system.

SLS is the government payroll management system.

Most of the ministries had not in practice established satisfactory internal controls to mitigate the risk of procurement and/or payroll fraud by public-sector employees

Samples drawn show that 13 out of the 15 ministries that mainly used the shared IT government systems in 2019 had, in some cases, not established adequate separation of duties in the systems RejsUd and/or IndFak, due to local adjustments in the procurement systems. Moreover, the ministries had not adequately supervised and monitored controls.

Overall, the study shows that access rights concerning the shared IT government systems IndFak and RejsUd are often inadequately managed, and the ministries fail to apply compensating controls.

The study also found specific examples of government credit cards that had been used contrary to current rules by employees in the Ministry of Defence, the Ministry of Justice and the Ministry of Climate, Energy and Utilities, and in the Ministry of Defence, fuel cards had been misused.

Rigsrevisionen recommends that the ministries should examine whether existing business processes and internal controls concerning use of credit cards and fuel cards are sufficient to mitigate the risk of fraud.

In regard to payroll fraud, the study shows weaknesses in several of the ministries' payroll controls and management of access rights in the SLS system.

Despite the fact that the study has not found any evidence of fraud, unlawful transactions may have taken place, and several of the ministries have in the wake of Rigsrevisionen's study taken steps to tighten up processes and counter the risk of payroll and procurement fraud.

Selected ministries that used the grant management system TAS in the period examined:

- The Ministry of Climate, Energy and Utilities
- The Ministry of Environment and Food
- The Ministry of Employment
- The Ministry of Social Affairs and the Interior
- The Ministry of Culture (is also using a tailored system).

Four out of five selected ministries used IT systems to manage grants in a way that did not adequately ensure that controls concerning management of access rights and monitoring of user activities in the grant system supported appropriate separation of duties.

The five ministries use a system called TAS for managing grants. The study found examples of unsatisfactory management of access rights. None of the five ministries had in 2019 established an adequate process for logging and control of privileged users' activities in the system. The study also found an example of missing separation of duties and inadequate management of access rights in a minor IT-system that involved a risk of internal fraud. The system is used by the Ministry of Culture for managing one specific grant.

The study has shed light on the fact that the ministries and government bodies have different practices concerning the administration of grants, procurement and payroll. Generally, the ministries can improve existing business processes and internal control through more knowledge-sharing on the mitigation of the risk of fraud not only across their particular remit, but also across the government departments.