Algemene Rekenkamer

Government-wide operational audit performed as part of the 2011 audit into the state of central government accounts - Background document

Data security and positions with access to confidential information

Original title

Algemene Rekenkamer (May 2012). *Informatiebeveiliging en vertrouwensfuncties; Rijksbreed bedrijfs-voeringsonderzoek in het kader van het verantwoordingsonderzoek 2011 – Achtergronddocument.*

Contents

1 About this audit

In view of the importance of data security to the operation of central government, we decided to perform an audit on this topic at all Dutch ministries, as part of the 2011 audit into the state of central government accounts. Any breach of data security – whether in the form of a computer failure, the loss of data files or a situation in which unauthorised persons hack into data systems (to cite just a couple of examples) – can easily have serious consequences, not just for private citizens, but also for companies and government bodies. Society at large must be able to rely on government bodies taking good care of their data.

We performed audits at all the ministries and one departmental agency[1] into:

- the quality of the data protection policy;
- the way in which data systems are protected.

We also examined positions with access to confidential information, again at all the ministries. We looked both at the procedure for appointing staff to such positions and at the vetting of those appointed to the posts in question.

[1] The Ministry of General Affairs, the Ministry of Foreign Affairs and the Ministry of Finance do not have any departmental agencies that deal with sensitive data, which is why our audit did not include any departmental agencies at these ministries. In the case of the Ministry of Finance, in addition to auditing the ministry itself, we also audited the Tax and Customs Administration rather than a departmental agency, as this entity performs a vital social function in which data security is absolutely vital. In the case of the Ministry of Health, Welfare and Sport, we audited two departmental agencies, viz. the Medicines Evaluation Board and the National Institute for Public Health and the Environment, in the light of the shortcomings identified in our 2010 audit into the state of central government accounts.

We concluded in our audit report entitled *State of Central Government Accounts 2011*[2] that most ministries did not give sufficient priority to data security. We found a total of nine shortcomings at five ministries.[3]

The same applies to positions with access to confidential information, which is a subject that is not receiving sufficient attention at present. Not all the ministries and departmental agencies included in the audit keep full records; staff at a large number of ministries and departmental agencies are employed in positions with access to confidential information despite the fact that they have not been vetted. We identified two shortcomings in this respect: the list of positions with access to confidential information held by the Tax and Customs Administration is very out of date, and the Military Intelligence and Security Service has run up a huge backlog of security checks (i.e. repeat vetting) for the Ministry of Defence.

The shortcomings are described in detail in our audit reports on the annual reports in question. This government-wide audit report is intended to encourage ministries and departmental agencies to improve their data security and their management of positions with access to confidential information. We wish to point out not just *what* sort of improvements can be made, but also *how* these can be achieved, by listing various examples of good practice.

Methods

For the purpose of our audit of data security and positions with access to confidential information, we compared both policy and practice with the relevant legislation.[4] To this end, we compiled a questionnaire based on current legislation (see Appendix 1). We also compiled a questionnaire, based on specialist literature, to survey the type of access controls

[2] Netherlands Court of Audit (2012). *State of Central Government Accounts 2011*. House of Representatives, 2011-2012 session, 33 240 nr.2. The Hague: Sdu.

[3] We performed an extra audit at the Tax and Customs Administration (Ministry of Finance) into logical access controls. Taken together with the findings of the government-wide data security audit, this resulted in our identifying a shortcoming in relation to data security, alongside the nine shortcomings mentioned above.

[4] The relevant legislation consists of the Security Screening Act, the Personal Data Protection Act, the 2005 Civil Service Security Regulations, the 2007 Civil Service Data Information Security Decree and the Civil Service Information Security (Classified Information) Decree. We did not include the Personal Data Protection Act in this audit, as a body known as the Dutch Data Protection Authority is already responsible for monitoring compliance with this particular law.

currently used for regulating access to data systems (e.g. passwords and virus scans; see Appendix 2).[5]

[5] Among the sources used for compiling the questionnaire were the Data Security Code and the Control Objectives for Information and related Technology (COBIT).

2 Quality of data protection policy 4

We assessed the quality of data security policy with reference to the relevant legislation:

- the 2005 Civil Service Security Regulations;
- the 2007 Civil Service Data Information Security Decree;
- the Civil Service Information Security (Classified Information) Decree.

These regulations and decrees lay down ten requirements that data protection policy needs to meet. We sought to ascertain to what extent all the ministries and the departmental agencies included in our audit were in compliance with each of these requirements. The requirements, and the scores allotted to each department and agency, are listed in Appendix 3.[6]

Most ministries and departmental agencies score badly in the following two respects:

- It is not clear who is responsible for which data systems and data chains.[7]
- No regular reviews of data protection policy have been planned or performed.

The responsibility for data chains is particularly unclear. As long as it is unclear who is responsible for which systems in the chain, no arrangements can be made about the protection of these systems. This creates a risk that the desired level of security cannot be guaranteed.

Our auditors found that the following ministries and departmental agencies had taken effective action in terms of allocating responsibility for data chains:

- the Ministry of Foreign Affairs,
- the Ministry of Defence,
- the Ministry of Finance (i.e. the Tax and Customs Administration),
- the Ministry of Social Affairs and Employment,

[6] Appendix 5 contains a graph showing the weighted scores for both data protection policy and data system security.

[7] Chains of interdependent information systems.

- the Ministry of Security and Justice,
- IVENT (part of the Ministry of Defence),[8]
- DICTU (part of the Ministry of Economic Affairs, Agriculture and Innovation; see box),[9]
- the Directorate-General for Public Works and Water Management (part of the Ministry of Infrastructure and the Environment),
- the Social Affairs and Employment Agency,
- the Central Fines Collection Agency (part of the Ministry of Security and Justice).
-

Example of good practice in relation to data chains: DICTU (Ministry of Economic Affairs, Agriculture and Innovation)
DICTU manages all the data systems controlled by the Application Portfolio Management System (APM). The APM records which line manager 'owns' which data system. DICTU told us that the Chain Management Team has operational responsibility for 16 critical data chains.

The data protection policies adopted by virtually all the ministries and departmental agencies make provision for regular policy reviews. However, there are many ministries and departmental agencies where such reviews are either not performed or not performed as frequently as they should be. As a result, good opportunities for improving data protection policies go to waste. Such failures may also create certain risks in terms of both operational management and policy-making, as data protection policies are not adjusted to cater for organisational changes and the lessons learned from security incidents. Those ministries and departmental agencies that do carry out regular reviews of their data protection policies are:

- the Ministry of General Affairs (see box),
- the Ministry of Foreign Affairs,
- the Ministry of Defence,
- IVENT (part of the Ministry of Defence),
- DICTU (part of the Ministry of Economic Affairs, Agriculture and Innovation),
- the Tax and Customs Administration (part of the Ministry of Finance).

[8] The Communication and Information Technology Section (IVENT) at the Ministry of Defence supplies communication, IT and documentary information services.

[9] DICTU stands for IT Services Department.

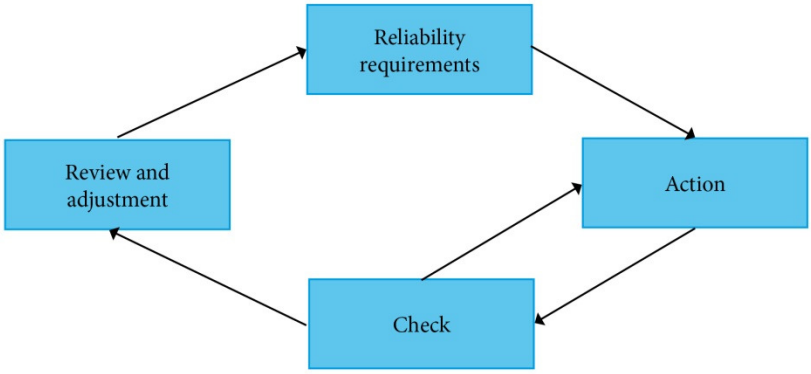
Example of good practice in relation to data protection policy reviews: the Ministry of General Affairs
Chapter 11 of the Data Protection Policy Document published by the Ministry of General Affairs explains that use is made of Deming's 'quality cycle'.[10] This also involves reviewing the findings of audits and regular checks. The Policy Document also states that the central data security officer is responsible for performing biennial data protection policy reviews. The Ministry said that the current data protection policy had been evaluated in the light of various recent developments, including an internal reorganisation and the adoption of the 'tactical guidelines for the Civil Service Digital Workplace'. The Ministry's data protection policy had been updated as a result.

[10] Otherwise known as the 'Plan-Do-Check-Act' cycle. See also Figure 1 on p. 7.

3 Protection of data systems

The purpose of a data protection policy is to help to protect data systems in practice. The ultimate aim is to devise a comprehensive package of security measures for every single data system so as to control the risks of hacking, abuse and data system failure.[11] Line managers[12] are responsible for the security of the data systems used for the operating processes for which they are responsible. The 2007 Civil Service Data Information Security Decree uses Deming's quality cycle (i.e. the 'Plan-Do-Check-Act' cycle shown in Figure 1) to manage data security.

Figure 1 The PDCA cycle for data security



Once a decision has been taken on what is needed (i.e. the *reliability requirements* have been set), *action* is taken. The next step is to *check* whether the action has had the desired effect. The results of this check may prompt the line manager to adjust the action. A *review* may also reveal a need for adjusting the overall package of requirements, actions and checks. If the steps in this quality cycle are followed carefully, the

[11] Data systems are defined as 'an interrelated collection of data sets together with the relevant staff, procedures, processes and software, plus the storage, processing and communication facilities designed for the system in question' (see article 1 (b) of the 2007 Civil Service Data Information Security Decree).

[12] The term 'line manager' is used here in the broadest possible sense. Depending on the situation, a department manager or the manager of a support department may also be regarded as a line manager.

result should be an adequate level of security at all times that meets the six requirements listed in the 2007 Civil Service Data Information Security Decree. We compared the way in which responsibilities are discharged with these six requirements (see Appendix 4), and also with a set of conventional access controls (see Appendix 2). The scores awarded to the various ministries and departmental agencies are set out in Appendix 4.[13]

A number of ministries and departmental agencies have incorporated effective data security measures in their operational management, by adopting the full quality cycle. These are the Ministry of Foreign Affairs, the Ministry of Defence and IVENT (which falls under the Ministry of Defence). Two departmental agencies, viz. Logius (part of the Ministry of the Interior and Kingdom Relations) and the Central Fines Collection Agency (part of the Ministry of Security and Justice) follow practically all the steps in the quality cycle: Logius does not perform a regular review of the full package of reliability requirements and security action and the Central Fines Collection Agency does not submit regular reports to line managers. Most of the ministries and departmental agencies included in our audit, however, either had failed to take effective action, or were unable to demonstrate that they had taken effective action, to protect their data systems against the risks of hacking, abuse and computer failure.

Poor scores were noted in the two following areas in particular:

- there is no clear picture of the security risks associated with data systems;
- the overall package of reliability requirements and security measures is not reviewed at regular intervals.

In order to obtain a clear picture of the risks, ministries and departmental agencies should perform risk assessments of their data systems. Many ministries and departmental agencies either do not do this or do not do so to an adequate degree. In some cases, no information is available about past risk assessments; in other cases, risk assessments are too old, are not fully documented or are performed only in relation to critical systems. Without the backing of a risk assessment, ministries do either too much or too little in terms of data security. As a result, ministries waste time or money, or else are exposed to an undesirable level of risk.

[13] Appendix 5 contains a graph showing the total scores for both data protection policies and data security in practice.

The following ministries and departmental agencies perform good risk assessments:

- the Ministry of General Affairs;
- the Ministry of Foreign Affairs;
- the Ministry of Defence;
- IVENT (part of the Ministry of Defence; see box);
- Logius (part of the Ministry of the Interior and Kingdom Relations);
- the Central Fines Collection Agency (part of the Ministry of Security and Justice).

Example of good practice in obtaining a clear picture of security risks: IVENT (Ministry of Defence
Explicit (and therefore verifiable) risk assessments have been performed of all key data systems, using an analytical method developed by the Ministry of Defence, based on the Civil Service Data Security Regulations on Efficient and Effective Analyses. A special department at IVENT staffed by certified personnel performs this special type of risk assessment for all Ministry of Defence data systems.

Given that organisations constantly change (in both organisational and technical terms) and because security incidents cannot be ruled out at any time, the overall package of reliability requirements and security measures needs to be reviewed at regular intervals. Regular reviews are also necessary to prevent ministries and departmental agencies from spending either too much or too little time and money on data security.

One of our findings was that most ministries do not do this, and that they either fail to take this final step in the quality cycle, i.e. perform the 'Act' part of the PDCA cycle, or are unable to demonstrate that they have taken it. Regular reviews are, however, performed by the following ministries and departmental agencies:

- the Ministry of Foreign Affairs;
- the Ministry of Defence (see box);
- the Ministry of Finance (i.e. the Tax and Customs Administration);
- IVENT (part of the Ministry of Defence);
- the Education Executive Agency (part of the Ministry of Education, Culture and Science);
- the Central Fines Collection Agency (part of the Ministry of Security and Justice).

Example of good practice in performing regular reviews of reliability requirements and security measures: Ministry of Defence
Risk assessments based on the Civil Service Data Security Regulations on Efficient and Effective Analyses are reviewed every three years. Accreditations and Interim Approvals to Operate (IATOs) are subject to time limits. An IATO is issued in cases where not all measures have been taken, but this does not pose a major risk. Once the time limit for the accreditation or IATO has passed, the accreditation process, including an Efficient and Effective Analysis in accordance with the Civil Service Data Security Regulations, has to recommence anew.

4 Positions with access to confidential information

Staff appointed to posts where they have access to confidential or sensitive information bear a special responsibility. We are referring to staff who have access to sensitive information or state secrets or who perform jobs that are of vital importance for the preservation of society or which involve high standards of ethical behaviour. In order to ensure that staff with access to confidential information are reliable, they need to be vetted by the General Intelligence and Security Service. Staff working for the Ministry of Defence have to be vetted by the Military Intelligence and Security Service. Under the Security Screening Act, ministries are obliged to maintain an up-to-date record of posts classified as 'providing access to confidential information'. Before appointing anyone to such a post, the ministry must ask the General Intelligence and Security Service to screen him or her. The person in question may start work only once the General Intelligence and Security Service has issued a security clearance. It is a criminal offence to appoint someone to a position with access to confidential information without the necessary security clearance.

We sought to ascertain whether the ministries comply with these obligations. With the exception of the Tax and Customs Administration, all ministries have classified certain posts as being 'positions with access to confidential information', in accordance with the terms of the Security Screening Act and in consultation with the General Intelligence and Security Service.

At most ministries, a number of posts classified as being 'positions with access to confidential information' are held by staff who have not been vetted in advance by the General Intelligence and Security Service. The lack of a complete set of records (see table overleaf) is the main reason for this.

Classification of posts as 'positions with access to confidential information' and screening of staff with access to confidential information, at ministries included in the audit 12

Ministry	Have posts been classified as 'positions with access to confidential information'?	Number of positions with access to confidential information	Number of staff holding positions with access to confidential information who have not been vetted*	Are full records kept?
General Affairs	Yes	144	5**	No
Interior and Kingdom Relations	Yes	635	22**	No
Foreign Affairs	Yes	448	5	Yes
Defence	Yes	4877	0	Yes
Economic Affairs, Agriculture and Innovation	Yes	467	47**	No
Finance	Yes	115	28**	No
Tax and Customs Administration (Ministry of Finance)	No	Unknown		Not applicable
Infrastructure and the Environment	Yes	532	130**	No
Education, Culture and Science	Yes	78	4	Yes
Social Affairs and Employment	Yes	388	3	Yes
Security and Justice	Yes	210	40**	No
Transport, Public Works and Water Management	Yes	214	34	No

* It is not possible to use these figures to calculate the percentage of unvetted staff, as in many cases posts with access to confidential information are held by more than one person.

** Estimate based on random sample.

The last time the Tax and Customs Administration formally classified certain posts as 'positions with access to confidential information' was in April 2005. A number of reorganisations have taken place since then necessitating the reclassification of these posts. The Tax and Customs Administration has not updated the listed of such posts yet, however. This means that the Tax and Customs Administration does not have a clear picture of the posts in relation to which staff need to be vetted prior to their appointment. We regard this omission as constituting a shortcoming in the Tax and Customs Administration's operational management.

The Military Intelligence and Security Service at the Ministry of Defence has run up a major backlog of vetting procedures. This is another area that we regard as forming a shortcoming. The Ministry of Defence nonetheless sets a good example: it has adopted an effective procedure for ensuring that security screening is carried out. This involves staff being alerted (by the staff records system) to new appointments to posts with access to confidential information. Although the staff records systems at other ministries also contain this type of warning facility, the routine reports sent to managers and controllers do not contain any information on appointments made to posts with access to confidential information. We recommend that the other ministries adjust the reporting feature in their staff records systems.

5 Response of Ministers and Court afterword

We presented this report to all the ministers on 13 April 2012. No specific responses were received from the Minister of the Interior and Kingdom Relations, the Minister of Foreign Affairs, the Minister of Infrastructure and the Environment, the Minister of Social Affairs and Employment, and the Minister of Health, Welfare and Sport.

The Minister of General Affairs wrote on 16 April 2012, welcoming the positive statements about his ministry. The Minister of Defence also stated (on 23 April, in an appendix to the response to our audit report on the Ministry of Defence's Annual Report) that he was delighted with the positive comments made about his ministry.

The Minister of Economic Affairs, Agriculture and Innovation and the Minister of Education, Culture and Science made clear that they accepted the findings and would be implementing the recommendations. This the former did in a letter dated 25 April, and the latter did on 26 April, in an appendix to the response to our audit report on the Annual Report of the Ministry of Education, Culture and Science.

The Minister of Finance and the Minister of Security and Justice responded to our audit findings on positions with access to confidential information (see chapter 4). The text of their responses is reproduced below *verbatim*, together with our own afterword.

We have posted the full (Dutch) text of all the responses on our website (www.rekenkamer.nl).

Response of the Minister of Finance

The Minister of Finance responded as follows to the web publication on 25 April:

"I already discussed the various points of concern, and the shortcoming identified, in my response to the regularity audit, to which I refer for the sake of convenience. I wish to make the following comments about positions with access to confidential information.

It is clear from the table that no full record is kept of security screening procedures. This is correct. The problem is now being rectified. The table also suggests that a large number of posts with access to confidential information are held by staff who have not been vetted. This finding prompted us to launch our own investigation. We found that, although the lack of a full set of records and fully documents procedures was capable of creating this impression, security clearances had in fact been issued for all staff actually appointed to positions with access to confidential information.

The Tax and Customs Administration began compiling a full list of positions with access to confidential information in the summer of 2011. The previous list had been found to be out of date. This process is now on the verge of completion and the aim is to produce a classification, in consultation with the General Intelligence and Security Service, by the end of the year."

Court afterword

We applaud the steps taken by the minister to update the records on positions with access to confidential information, and to compile a list of such positions at the Tax and Customs Administration. The minister writes that, in practice, all staff actually appointed to positions with access to confidential information have been given security clearances. Our auditors found that a number of staff with access to confidential information had been appointed pending security screening. This is not permitted under the Security Screening Act.

Response of the Minister of Security and Justice

The Minister of Security and Justice discussed the web publication in Appendix 4 to the response to our audit report on the 2011 Annual Report published by the Ministry of Security and Justice. He wrote as follows: "Your background document contains, on pages 8 and 9, a table listing the number of posts at each ministry in which staff have access to confidential information. It would appear that the ministries did not adopt a consistent approach in identifying the number of posts classified as being 'with access to confidential information'. My own ministry stated the actual number of posts classified as being 'with access to confidential information'. However, other ministries would appear to have converted the number of such posts into FTEs. This indicates a lack of consistency in the planning, and notably the execution, of the audit, and as a result creates a distorted picture of the situation at the various ministries. It would be a very good idea if all the ministries took the same approach and stated either the actual number of posts or the equivalent in FTEs."

Court afterword 16

The minister claims that our report paints a distorted picture. For the purposes of our audit, we used the designation order provided by the ministers to ascertain which posts have been classified as 'positions with access to confidential information'. We then sought to ascertain whether security clearances had been issued for staff appointed to these positions. We used two sources for this purpose: the records kept by the ministries, and a set of random samples taken at various ministries. Whether a post classified as being a 'position with access to confidential information' represents a full FTE or only half an FTE is not relevant.

Appendix 1 Questionnaire on data security and positions with access to confidential information

The following list of questions was used for the data security part of the audit. Part 1 of the list (Quality of the data protection policy) centres both on the planning of data security procedures and on the effects of the security measures taken, e.g. in questions 1.5 and 1.8. Part 2 (Security of data systems) focuses on the effectiveness of the data security measures. Although we were interested specifically in finding out whether certain data security measures[14] were useful in relation to critical data systems, we decided in the end, for the sake of enabling comparisons between the ministries, to look at the effectiveness of a number of conventional access controls in relation to a single critical data system. What we wanted to establish was not simply whether the entity in question had put such controls in place (and, where relevant, drawn up operating procedures and guidelines for their use), but also whether the entity was able to demonstrate that the procedures were followed in practice.

[14] These could take the form of measures included in the technical specifications of a given data system, such as integrity checks and measures relating to the availability of hardware, as well as contractually agreed security measures, i.e. agreed when the system in question was procured. Other measures relate to procedures that need to be followed by users of the data systems.

1. Quality of data protection policy		
1.1	Has a data protection policy been formulated, and adopted by the Secretary-General?	Article 3 of Civil Service Data Information Security Decree
1.2	Does this policy incorporate aspects included in statutory regulations?[15]	Civil Service Security Regulations; article 3 of Civil Service Data Information Security Decree and article 13 of Civil Service Information Security (Classified Information) Decree
1.3	Is there documentary evidence to show that the data protection policy meshes in with the ministry's overall security policy?[16]	Article 3 (a) of Civil Service Data Information Security Decree
1.4	Are there manuals or guidelines describing data security procedures,[17] including the relevant tasks, responsibilities and powers?	Article 3 (b) of Civil Service Data Information Security Decree
1.5	Has a procedure for security incidents been established? Is this procedure followed in practice?[18]	Article 3 (b) of Civil Service Data Information Security Decree
1.6	Is there an up-to-date record of all data systems and data chains, and have the relevant responsibilities in this connection been assigned to line managers?	Article 3 (c) of Civil Service Data Information Security Decree
1.7	Does the ministry work with a common set of reliability requirements (i.e. is there a shared data security baseline)?	Article 3 (d) of Civil Service Data Information Security Decree
1.8	Is there a programme for raising staff awareness of data security? Has the programme been implemented by the entities concerned?	Article 3 (f) of Civil Service Data Information Security Decree
1.9	Is there a written procedure for monitoring the implementation of the data protection policy?	Civil Service Security Regulations; article 3 (e) of Civil Service Data Information Security Decree and article 14 (3) of Civil Service Information Security (Classified Information) Decree
1.10	Is there a written procedure for evaluating the data protection policy (including for establishing whether action has been taken to implement the findings of past reviews), and is this procedure followed in practice?	Article 3 (e) of Civil Service Data Information Security Decree

[15] See the separate table listing the applicable laws and regulations.

[16] The ministry's overall security policy as referred in the 2005 Civil Service Security Regulations covers both data security and the security of equipment and staff.

[17] The term 'data security procedures' covers all relevant functions performed within an organisation and the associated tasks.

[18] This means that staff are familiar with the procedure and observe it in practice.

2. Security of data systems		
2.1	Has an explicit (and verifiable) risk assessment been performed for each data system?	Article 4 (a) of Civil Service Data Information Security Decree
2.2	Is the procedure for formulating the reliability requirements verifiable and documented? Is there a written record of these requirements?	Article 4 (a) of Civil Service Data Information Security Decree
2.3	Has a written record been made of the security measures (i.e. of their existence, nature and effect)? Have they been implemented in practice, and is there documentary evidence to show that this is the case?	Article 4 (b) of Civil Service Data Information Security Decree
2.4	Have monitoring tasks been allocated? Have steps been taken to ensure that monitoring is performed in practice, so as to guarantee that security measures have been put in place and are observed in practice?	Article 4 (c) of Civil Service Data Information Security Decree
2.5	Are regular reports submitted to and drawn up by line managers, on the implementation of the data protection policy?	Articles 4 (d) and 2 (3) of Civil Service Data Information Security Decree
2.6	Are regular reviews undertaken of the overall package of reliability requirements and security measures? Do the results of these reviews lead to adjustments being made where necessary?	Article 4 (d) of Civil Service Data Information Security Decree
3. Enforcement of Security Screening Act		
3.1	Has a list been drawn up of 'positions with access to confidential information'?	Article 3 (1) of Security Screening Act
3.2	Have security clearances been issued for all members of staff working in posts with access to confidential information?	Article 4 (3) of Security Screening Act

Appendix 2 Access controls

Checks performed in 2011 of data security measures		
	Measure	**Evidence**
1	**Regular checks (e.g. internal controls, penetration tests and special-purpose audits) are performed of the effectiveness of access controls**	**Documentation (last 2 or 3 reports)**
1.1	**Access controls: malevolent software**	
1.1.1	Every server and/or work station (i.e. PC, laptop, etc.) is checked for malevolent software and access by means of USB ports, CD ROMs, e-SATA, etc. is blocked	Printout of settings (network filter)
1.1.2	Security software is set so that downloads and emails (including attachments) are scanned for viruses.	Printout of settings of anti-virus software and/or firewall (access filter)
1.2	**Access controls: user passwords**	
1.2.1	Users issued with temporary passwords are required to change them straightaway.	Printout of settings of operating system or relevant application
1.2.2	The password system satisfies the following conditions as a minimum requirement: Minimum length, i.e. 8-10 characters for users, longer for system managers Frequent password changes (at least once every three months for users and at least once a month for system managers) Feature preventing the reuse of passwords (by keeping a record of at least 10 previous passwords) Passwords must meet various quality criteria, i.e. they may not be based on dates (years, months and days) or on names of organisational units, they may not consist solely of numerical or alphabetical characters, etc.	Printout of settings of operating system or relevant application
1.3	**Access controls: operating system and network**	
1.3.1	Users have only limited opportunities to connect with networks; any such facilities are consistent with the policy on access controls.	Printout of settings of operating system or relevant application
1.3.2	Users only have access to services they have specifically been authorised to use.	Printout of authorisation table + random sample of authorisation signatures
1.3.3	Users can access the network and their computers only by following a routine log-in procedure.	Demonstration
1.3.4	Only essential data input fields are displayed when users log-in (i.e. no help messages are displayed that unauthorised persons might be able to use).	Demonstration
1.3.5	All users (including computer engineers) are allocated a unique user ID, so that all activities can be traced to them (or: there are procedures for restricting the use that can be made of a universal system manager's ID).	Log use made of system manager's ID and log use made of system managers' personal IDs + procedure for use of

		system manager's ID
1.3.6	There is a screensaver that is programmed to start after 15 minutes at most.	Printout of settings of operating system or relevant application, plus on-site test
1.3.7	The screensaver can be disabled only by the user with the aid of his or her personal password.	Printout of settings of operating system or relevant application
1.4	**Access controls: Teleworking**	
1.4.1	Users wishing to use the teleworking facility can access the network only by using a two-factor or three-factor authentication process.	Demonstration
1.4.2	Are there any exceptions to the above authentication policy for teleworking (e.g. for system managers)?	Demonstration
2	**A log is kept of unsuccessful log-in attempts and all activities affecting critical systems that can be used for the preventive and repressive integrity policy (network and critical systems).**	**Demonstration (see below)**
2.1	Logs contain the following relevant data: user ID; server or work station ID; date, time and details of incidents, i.e. successful and unsuccessful log-in attempts: rights and authorisations granted; changes in the configuration; and use made of the following privileges: a, b and c	Demonstrate log settings + sample log for a day or week
2.2	The logs are used for the preventive and repressive integrity policy.	Demonstrate procedure and last check or last two checks

Appendix 3 Targets and scores for quality of data protection policy

Under the 2007 Civil Service Data Information Security Decree and the Civil Service Information Security (Classified Information) Decree, the data protection policy must meet the following requirements:

1. The policy must be adopted at senior management level; this means that senior management should be committed to the policy and should feel responsible for it.
2. The policy should be consistent with the latest legislative developments.
3. The data protection policy should form past of the general security policy.
4. It should be clear who is responsible for which aspect of data security and what powers ensue from these responsibilities.
5. The ministry must have adopted a routine procedure for responding to security incidents such as attempts to hack in to data systems.
6. It should be clear, in relation to all data systems and data chains, which organisational unit is responsible for data security.
7. The ministry should work with basic reliability requirements and reliability measures that apply to all systems.
8. Staff should be taught how to deal with data in a secure manner.
9. The ministry should check that the data protection policy is enforced and that staff deal with data in a secure manner.
10. The data protection policy should be reviewed at regular intervals.

The table shows that the ministries and departmental agencies score relatively badly on points 6 (allocation of responsibility for data systems and data chains to organisational units) and 10 (regular reviews of data protection policy).

Scores awarded to ministries and departmental agencies for their data protection policies

	1	2	3	4	5	6	7	8	9	10
Ministry of General Affairs										
Ministry of the Interior and Kingdom Relations										
Logius (part of the Ministry of the Interior and Kingdom Relations)										
Ministry of Foreign Affairs										
Ministry of Defence										
IVENT (part of the Ministry of Defence)										
Ministry of Economic Affairs, Agriculture and Innovation										
DICTU (part of the Ministry of Economic Affairs, Agriculture and Innovation)										
Ministry of Finance										
Tax and Customs Administration										
Ministry of Infrastructure and the Environment										
Directorate-General for Public Works and Water Management (part of the Ministry of Infrastructure and the Environment)										
Ministry of Education, Culture and Science										
Education Executive Agency (part of the Ministry of Education,										

Culture and Science)										
Ministry of Social Affairs and Employment										
Social Affairs and Employment Agency (part of the Ministry of Social Affairs and Employment)										
Ministry of Security and Justice										
Central Fines Collection Agency (part of the Ministry of Security and Justice)										
Ministry of Health, Welfare and Sport										
National Institute for Public Health and the Environment (part of the Ministry of Health, Welfare and Sport)										
Medicines Evaluation Board (part of the Ministry of Health, Welfare and Sport)										

Key Satisfactory Scope for improvement Lots of scope for improvement

The numbers at the head of the columns correspond with the ten data protection policy requirements listed above.

Appendix 4 Targets and scores for protection of data systems

Under the 2007 Civil Service Data Information Security Decree, the method used for protecting data is based on Deming's quality cycle (the 'Plan-Do-Check-Act cycle'). By completing all the stages of the cycle, organisations can ensure that data are properly protected and that the security system meets the following requirements:

1. the responsible organisational units have analysed the security risks associated with the data system (i.e. the 'Plan' part of the PDCA cycle);
2. as a result, they know where these systems are vulnerable and what level of reliability is required (i.e. the 'Plan' part of the PDCA cycle);
3. they are aware that the necessary conventional logical access controls are performed and also that they are effective (i.e. the 'Do' part of the PDCA cycle);
4. they are aware that the necessary, specific logical access controls are performed and also that they are effective (i.e. the 'Do' part of the PDCA cycle);
5. data protection procedures are reviewed at regular intervals (i.e. the 'Check' part of the PDCA cycle);
6. reviews are performed to ascertain when the security system is working properly and whether it needs to be adjusted (i.e. i.e. the 'Act' part of the PDCA cycle).

The table shows that the ministries and departmental agencies score relatively badly on points 1 (awareness of the security risks associated with data systems) and 6 (reviews of reliability requirements and the security of data systems).

Scores awarded to ministries and departmental agencies for their data security

	1	2	3	4	5	6
Ministry of General Affairs						
Ministry of the Interior and Kingdom Relations						
Logius (part of the Ministry of the Interior and Kingdom Relations)						
Ministry of Foreign Affairs						
Ministry of Defence						
IVENT (part of the Ministry of Defence)						
Ministry of Economic Affairs, Agriculture and Innovation						
DICTU (part of the Ministry of Economic Affairs, Agriculture and Innovation)						
Ministry of Finance						
Tax and Customs Administration						
Ministry of Infrastructure and the Environment						
Directorate-General for Public Works and Water Management (part of the Ministry of Infrastructure and the Environment)						
Ministry of Education, Culture and Science						
Education Executive Agency (part of the Ministry of Education, Culture and Science)						
Ministry of Social Affairs and Employment						
Social Affairs and Employment Agency (part of the Ministry of Social Affairs and Employment)						
Ministry of Security and Justice						
Central Fines Collection Agency (part of the Ministry of Security and Justice)						
Ministry of Health, Welfare and Sport						

National Institute for Public Health and the Environment (part of the Ministry of Health, Welfare and Sport)						
Medicines Evaluation Board (part of the Ministry of Health, Welfare and Sport)						

Key  Satisfactory  Scope for improvement  Lots of scope for improvement

The numbers at the head of the columns correspond with the ten data protection policy requirements listed above.

Appendix 5 Scores for data security (i.e. data protection policy and protection of data systems)