ReSPA
Regional School
of Public Administration

ReSPA Activities are
Financed by the EU

Checklist
for Assessment of Risks for Abuse of IT for Corruption

Based on the findings and recommendations of the ReSPA-Study "Abuse of Information Technology (IT) for Corruption" (2014)[1] the following checklist is recommended for reviewing the security of IT against abuse for corruption during risk assessments or for any other review. It was adopted in 2015 by the ReSPA Networks on eGovernment and Ethics & Integrity. The checklist can be applied in different systems of corruption risk assessments used by different ReSPA member countries, or by any other country. Please answer each question by marking the appropriate cell: "No", "Partially", or "Yes". For "Partially" estimate the percentage of fulfilment. Please provide always explanatory comments for all questions to explain or justify your "Partially" or "Yes" scores. At the end of this checklist you will find further explanatory notes.

Country	Public sector entity

Area	No	Part.%	Yes	Comments (if answer is "partially" or "yes")
1. Access control				
1.1. Is access to all proprietary data and systems safeguarded with access control using inter alia individual private user **IDs** and **passwords**, or ideally even more secure methods such as **biometric** or **token/PIN** verification?				

[1] http://www.respaweb.eu/11/library#respa-publications-and-research-18.

Area	No	Part.%	Yes	Comments (if answer is “partially” or “yes”)
1.2. Is access control (i.e. passwords) **updated** and changed regularly?				
1.3. Is malware (e.g. antivirus) software installed and enabled on all computers?				
1.4. Is a procedure in place for **restricted internet** connection for computers storing or exchanging confidential and sensitive data?				
1.5. Is there a defined procedure for using **memory storage** devices (USB, CD, etc.) and for preventing illegal download of data on private storage devices?				
1.6. Is access to different levels of sensitive data tailored to the **appropriate staff**?				
1.7. Is access to different kinds of **data** granted only when required for the immediate work tasks and is this automatically logged in a tamper-proof way?				
1.8. Is **physical access** to facilities which store data or physical copies of data restricted to authorised personnel whose access is both automatically logged and monitored?				

Area	No	Part.%	Yes	Comments (if answer is “partially” or “yes”)
1.9. Is **remote access** to IT systems restricted to certain staff and cases? What are the security standards for remote access?				
1.10. Are there clear, written, and regularly **updated instructions** for access control?				
2. Recovery				
2.1. Are **disaster recovery and continuity plans** in case of security incidents in place? The plans must describe the procedures to follow in case of incidents, how to manage business continuity, and identify and agree on responsibilities for emergency arrangements.				
2.2. Are **backup procedures** implemented with periodic full backup of 1) central systems/workstations, 2) system software and platforms, 3) applications and databases, and 4) unstructured data? Are backup copies stored physically offsite or in a hazard-secure place onsite?				
2.3. Are there clear, written, and regularly **updated instructions** for recovery?				
3. Documentation				

Area	No	Part.%	Yes	Comments (if answer is “partially” or “yes”)
3.1. Are **log files** (i. e. a separate chronological record of IT activities, such as log-ins by users, access date and time, access to data, or downloads, which can be used as an audit trail) maintained **as** part of the organisation’s monitoring and supervision structure?				
3.2. Are log files made on **both application and database level**, so that logs on altering data by any user with any privileges is saved?				
3.3. Are **copies** of **log files** stored off site and/or are they separate from the application itself?				
3.4. Are log files **deleted** only when national data protection rules require so, but not before?				
3.5. Is the **administrator** of log files a staff member independent of the staff who can alter content/data and not him/herself engaged in data alteration (users and administrators of the IT system)?				
3.6. Are **rejected logins** to critical, sensitive and main systems automatically registered (logged), and does the system make it transparent from which computer it was unsuccessfully tried to login?				

Area	No	Part.%	Yes	Comments (if answer is “partially” or “yes”)
3.7. Are there **automatic restrictions** in place in case of repeated failed logins?				
3.8. Are there clear, written, and regularly **updated instructions** for documentation?				
4. **Supervision and audits**				
4.1. Are rejected logins **investigated**, if they are suspicious (depending on the frequency of rejection and the level of confidentiality of data targeted by the login)?				
4.2. **Separation of roles:** Is the staff member responsible for systems technology independent from the staff responsible for the content (users of the IT-system)?				
4.3. Are system **audits** performed by an expert who is not the IT administrator and who is independent from any other involvement with the system?				
4.4. IT-compliance tests: is it verifiable and routinely **verified** that IT-procedures comply with the instructions (e.g. through external audit) ?				
4.5. Are there clear, written, and regularly **updated instructions** for supervision and audit?				

Area	No	Part.%	Yes	Comments (if answer is “partially” or “yes”)
5. External partners and outsourcing				
5.1. Whenever IT development, maintenance, or deployment[2] is **outsourced**: Does the public entity ensure itself that access to data is only possible for authorised external personnel?				
5.2. Are there **written agreements** with external partners on how confidential and private data should be treated and what security measures must be taken?				
5.3. Does the public entity update **security clearances** to work with confidential or sensitive data regularly?				
5.4. Is the implementation of agreements **followed-up** regularly?				
5.5. Does the public entity assess risks and does it monitor and audit data **security measures**?				
5.6. Does the outsourcing agreement allow the public entity to draw appropriate consequences in **case of violations** (in particular notice, damages, immediate access to and withdrawal of external data at all times, right to information)?				

[2] http://en.wikipedia.org/wiki/Software_deployment.

Area	No	Part.%	Yes	Comments (if answer is “partially” or “yes”)
5.7. Are there clear, written, and regularly **updated instructions** for external services?				
6. Relation between IT systems				
6.1. Whenever the public entity interacts with **other IT-systems** or is part of a larger process: does the public entity ensure in particular awareness, training, and instructions for its employees on the possible risk of receiving compromised data or being part of a compromised IT-process?				
6.2. Are standard procedures in place in case an evidently **corrupted input** appears in this entity (such as an evident inconsistency of data received from another entity)?				
6.3. **Base registries**[3] are essential building blocks for coherent interoperable eGovernment: are special and heightened security measures in place for them, such as special logfiles chronicling which user inserted, changed, or deleted data, or such as secure back up?				
6.4. Are there clear, written, and regularly **updated instructions** for the relation between IT-systems?				
7. Training, awareness and responsibility				

[3] Reliable sources of basic information on items such as persons, companies, vehicles, licenses, buildings, locations and roads. Such registries are under the legal control of and maintained by a given public administration (see: http://ec.europa.eu/isa).

Area	No	Part.%	Yes	Comments (if answer is “partially” or “yes”)
7.1. Are **heads** of public entities as well as public officials aware of the risks which IT can pose with regards to corruption?				
7.2. Are employees **aware** of the instructions?				
7.3. Have employees **received training** in how to comply with instructions?				
7.4. Do heads of public entities know where to get advice/assistance for **closing safety gaps** in the IT of their public entity (corruption prevention bodies, IT-agencies, etc.) especially in emergency or acute situations?				
7.5. Is staff **qualified** to deal with technical security available?				
7.6. Are staff responsible for IT-systems regularly **trained** on up-to-date standards of technical security?				
7.7. Is there clear placement of **responsibility** to name individuals/positions for all relevant actions on this check-list?				
8. Proper conduct				

Area	No	Part.%	Yes	Comments (if answer is “partially” or “yes”)
8.1. Is there an overall, clear and proactive policy to build a culture of **ethics** and **compliance**, and are staff responsible for IT-systems trained in, and aware of, these principles?				
8.2. Has the organisation instituted a formal **code of conduct** that every staff member at every level must certify as part of their contract and/or terms of employment?				
8.3. Do employees **know where** and how to report cases of abuse of IT for corruption?				
8.4. Are there **Standard Operating Procedures** (SOP) in place to be followed in case of violations?				
9. **Civil society and transparency**				
9.1. Does the public entity provide **open government data** and citizen participation as much as possible, in order to allow for scrutinising public sector data and processes, as well as possible irregularities and abuses?				
9.2. Are channels provided to the public for giving **feedback** to the public entity and government in general?				
9.3. In case of abuse of IT for corruption and other irregularities, are channels provided for citizens to report **incidents**?				

Area	No	Part.%	Yes	Comments (if answer is “partially” or “yes”)
9.4. Does the Public Administration publish **lists of IT contractors and contracts**?				
10. International Standards and Cooperation				
10.1. Does the public entity implement **information security standards** (in particular ISO 27001)[4] to ensure data safety and integrity?				
10.2. Does the public entity keep itself informed on **foreign and international** developments on information security?				

[4] http://www.iso.org/iso/home/standards/management-standards/iso27001.htm.

Explanatory notes

The following are some explanations for each item of the checklist so users can understand the background and rationale of the questions. The explanations are not and cannot be a reference source for good practices on specific detailed implementation for several reasons: technical developments are fast in the area of ICT and any recommendation in the explanatory notes would soon be outdated. However, some international standards do offer good practices, in particular the ISO 27002 standard,[5] which provides some recommended practices for the implementation of the general principals outlined in ISO 27001. The explanatory notes will point out some indicative key points, but cannot be a comprehensive reference source for technical advice. Where relevant, these explanatory notes reference specific sub-parts of the ISO 27002 standard for further details. In addition, users will have to seek up to date advice from their national agencies on IT-security, or from private service providers, tailored to their situation.

1. Access control

1.1 **Is access to all proprietary data and systems safeguarded with access control using inter alia individual private user IDs and passwords, or ideally even more secure methods such as biometric or token/PIN verification?**

An access control policy should describe restrictions to data and system access, secure log-on procedures with a password management system ensuring quality password, and tight controls and restriction of utility programs capable of overriding system and application controls. Passwords are a common way to provide identification and authentication based on a secret that only the user knows. The same can also be achieved with cryptographic means and authentication protocols. The strength of user authentication should be appropriate for the classification of the information to be accessed. If passwords are transmitted in clear text during the log-on session over a network, they can be captured by a network "sniffer" program.

For implementation guidance, please see ISO/IEC 27002:2013 subchapters (security categories):

9.4 System and application access control
9.4.1 Information access restriction
9.4.2 Secure log-on procedures
9.4.3 Password management system
9.4.4 Use of privileged utility programs

1.2. **Is access control (i.e. passwords) updated and changed regularly?**

[5] ISO/IEC 27002:2013 http://www.iso.org/iso/catalogue_detail?csnumber=54533.

Passwords should be changed regularly (frequently) and always as soon as possible when a privileged user leaves or changes jobs. If a departing employee or external party user has known passwords for user IDs remaining active, these should be changed upon termination or change of employment, contract or agreement as well.

For implementation guidance, please see ISO/IEC 27002:2013 subchapters (security categories):

9.2.3 Management of privileged access rights
9.2.5 Review of user access rights
9.2.6 Removal or adjustment of access rights
9.3.1 Use of secret authentication information
9.4.2 Secure log-on procedures
9.4.3 Password management system

1.3. Is malware (antivirus) software installed and enabled on all computers?

The organisation should have some kind of policy describing the detection, prevention and recovery to protect against malware. Scanning for malware should include scanning any files received over networks or storage medium (e.g. USB sticks, flash memory cards, external hard disks, digital cameras, mobile phones, etc.); all mail attachments and downloads; and all web pages.

Scanning against malware includes implementing procedures and responsibilities to deal with malware attacks, and care should be taken to protect against the introduction of malware during maintenance and emergency procedures which may bypass normal malware protection controls.

For implementation guidance, please see ISO/IEC 27002:2013 subchapter (security category):

12.2 Protection from malware

1.4. Is a procedure in place for restricted internet connection for computers storing or exchanging confidential and sensitive data?

Confidential and sensitive data: State secrets should obviously be restricted from the internet; however, each organization will typically also handle confidential and sensitive data that can be abused for corruption. Confidential data refers to information not intended for disclosure outside the context of the organization responsible for that information (this includes person information). Sensitive data is information that could either harm the organization if disclosed, or provide an

undue advantage to others outside the organization upon disclosure (for the distinction of confidential and sensitive data, see also below under 1.6).

Restrictions could include physical or logical access measures for the isolation of sensitive applications, application data, or systems. Cryptographic measures should also ensure the integrity and authenticity of data, i.e. using digital signatures or message authentication codes to verify the authenticity or integrity of transmitted information.

For implementation guidance, please see ISO/IEC 27002:2013 subchapter (security category):

13.1 Network security management
13.1.1 Network controls
13.1.3 Segregation in networks

1.5. Is there a defined procedure for using memory storage devices (USB, CD, etc.) and for preventing illegal download of data on private storage devices?

Any memory storing device such as USB drives, external harddisks (SD-cards, micro-SD, CompactFlash, Solid State etc.), digital cameras, mobile phones, GPS navigators, iPods, MP3/4 players can become infected by malware, that can contaminate an organisations equipment and networks relatively easy. Anecdotal evidence even suggests that USB charged e-cigarettes are capable of infecting a computer with malware if plugged directly into a computer.[6] Essentially any device that can be connected through USB (including web-cams, keyboards and computer-mice) has the potential to infect.[7] If a lost or stolen USB drive contains sensitive personal information that is not encrypted or secure, it opens the door for identity theft and other cybercrimes. Organisations can implement solutions that discriminate between legitimate and illegitimate devices and use; solutions that monitor and record interactions between memory storage devices and computers and store it in a central database; and hardware encryption to automatically overwrite the contents if a wrong password is entered more than a certain number of times etc. Organisations should be aware of the vulnerabilities arising from using such devices and define appropriate procedures and policies for their use, as well as countermeasures for protection against misuse.

For implementation guidance, please see ISO/IEC 27002:2013 subchapter (security category):

8.3.1 Management of removable media

[6] http://www.theguardian.com/technology/2014/nov/21/e-cigarettes-malware-computers.
[7] As evidenced by the Stuxnet worm infecting Iranian nuclear operations, http://www.vanityfair.com/news/2011/04/stuxnet-201104.

8.3.2 Disposal of media

1.6 Is access to different levels of sensitive data tailored to the appropriate staff?

Normally, one needs to distinguish two different levels of restricted data: confidentiality under rules for state secrets, and confidentiality under rules for the protection of private data. Usually, each set of rules will (or should) define under what circumstances such data can be accessed and by whom. The technical means will have to reflect these requirements. For example, computers processing state secrets often are required to be permanently and physically disconnected from any internet access. As far as personal data is concerned, Article 17 para. 1 of Directive 95/46/EC[8] on personal data requires "that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing."

1.7. Is access to different kinds of data granted only when required for the immediate work tasks and is this automatically logged in a tamper-proof way?

Referring back to an access policy mentioned in question 1.1, the same considerations apply.

For implementation guidance, please see ISO/IEC 27002:2013 subchapter (security category):

9.4.1 Information access restriction
9.4.2 Secure log-on procedures

1.8. Is physical access to facilities which store data or physical copies of data restricted to authorised personnel whose access is both automatically logged and monitored?

To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities, secure areas should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access. This includes recording data and time of entry and departure of all visitors. Access can be restricted by access controls such as access card or secret PIN code. A log book or other audit trail should be

[8] http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046&from=en.

maintained and monitored. Access rights should be regularly reviewed and updated.

For implementation guidance, please see ISO/IEC 27002:2013 subchapter (security category):

11 Physical and environmental security
11.1 Secure areas
11.1.2 Physical entry controls

1.9. Is remote access to IT systems restricted to certain staff and cases? What are the security standards for remote access?

Remote access to systems can be the case both when using different physical locations (off-premises) and in cases of using mobile devices and teleworking. A policy and supporting security measures should be implemented to protect information accessed, processed or stored at teleworking sites, or just sites having some kind of mobile access to them. A mobile device policy accounting the risks of working with mobile devices in unprotected environments, and a teleworking policy to protect information accessed, processed and stored at teleworking sites are examples of security standards for remote access.

For implementation guidance, please see ISO/IEC 27002:2013 subchapter (security category):

6.2 Mobile devices and teleworking
6.2.1 Mobile device policy
6.2.2 Teleworking

1.10. Is access to data by other institutions limited to the competence of that institution?

When other public bodies request access to data or data exchange, are checks performed that ensures that such access is within the limits of the mission and field of each institution? Does the institution check that such access are within the law on data protection?

1.11. Are there written rules and instructions regulating access in case of termination or change of employment?

When an employee leaves a position (through dismissal or reassignment) he or she can be in possession of confidential/sensitive documents/information and may have made copies of such material. Are there written rules/instructions regulating this aspect, so that information security responsibilities and duties remain valid after

termination or change of employment? Are these duties defined and communicated to the employee or contractor. Are they enforced?
For implementation, guidance see e.g. ISO/IEC 27002:2013 – 7.3 – Termination and change of employment.

1.12. Are there clear, written, and regularly updated instructions for access control?

Answering this question should not require to consult a lawyer. The practice test for this question is, whether a (non-legal) practitioner has the impression that he/she finds sufficient guidance for the topic of this sub-chapter in the regulations, whether he/she can understand the guidance, and whether the guidance seems to be up to date.

For implementation guidance, please see ISO/IEC 27002:2013 subchapter (security category):

9.1.1 Access control policy

2. Recovery

For full implementation, guidance see e.g. ISO/IEC 27002:2013 - 12.3 Backup.

2.1. Are disaster recovery and continuity plans in case of security incidents in place? The plans must describe the procedures to follow in case of incidents, how to manage business continuity, and identify and agree on responsibilities for emergency arrangements.

Backup procedures should also include documented restoration procedures. Backup copies of information, software and system images should be taken and tested regularly in accordance with an agreed backup policy to ensure that they can be relied upon for emergency use when necessary.

2.2. Are backup procedures implemented with periodic full backup of 1) central systems/workstations, 2) system software and platforms, 3) applications and databases, and 4) unstructured data? Are backup copies stored physically offsite or in a hazard-secure place onsite?

The frequency of backups as well as full or differential backups depends on the individual organization's needs. Operational procedures should monitor the execution of backups and address failures of scheduled backups to ensure completeness of backups according to the backup policy.

For implementation, guidance see e.g. ISO/IEC 27002:2013 - 12.3 Backup.

2.3. Are there clear, written, and regularly updated instructions for recovery?

See above the explanatory notes to item 1.10.

3. Documentation

For implementation guidance of the management of audit-trail and system log information see. e.g. ISO/IEC 27002:2013 - 12.4 Logging and monitoring

3.1. Are log files (i. e. a separate chronological record of IT activities, such as log-ins by users, access date and time, access to data, or downloads, which can be used as an audit trail) maintained as part of the organization's monitoring and supervision structure?

Log files are event logging recording user activities, exceptions, faults and information security events. Remember that event logs can contain sensitive or person identifiable information, and wherever possible system administrators should not have permission to erase or de-activate logs of their own activities.

3.2. Are log files made on both application and database level, so that logs on altering data by any user with any privileges is saved?

Both applications (programs) and databases can create log files. It is harder to alter both sets of log files simultaneously. A user may have higher privileges in an application than in the database and vice versa. Tampering with data at one end might leave important clues in the log files at the other end, thus making forensic evidence available in the other end (see ISO/IEC 27002:2013 - 16.1.7 Collection of evidence).

3.3. Are copies of log files stored off site and/or are they separate from the application itself?

System logs need to be protected, because if the data can be modified or data in them deleted, their existence may create a false sense of security. Real-time copying of logs to a system outside the control of a system administrator or operator can be used to safeguard logs.

The organization should define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence (see ISO/IEC 27002:2013 - 16.1.7 Collection of evidence).

3.4. Are log files deleted only when national data protection rules require so, but not before?

National data protection rules usually set limits for how long personal data can be stored (e.g. a maximum number of years). Log files should be kept as long as such rules allow for it, so any abuse of IT for corruption can be properly investigated using such log files, even if conducted years after the incident.

3.5. Is the administrator of log files a staff member independent of the staff who can alter content/data and not him/herself engaged in data alteration (users and administrators of the IT system)?

Privileged user account holders may be able to manipulate the logs on information processing facilities under their direct control. Therefore, it is necessary to protect and review the logs to maintain accountability for the privileged users. An intrusion detection system managed outside of the control of system and network administrators can be used to monitor system and network administration activities for compliance.
(see ISO/IEC 27002:2013 - 12.4.3 Administrator and operator logs)

3.6. Are rejected logins to critical, sensitive and main systems automatically registered (logged), and does the system make it transparent from which computer it was unsuccessfully tried to login?

Depending on the technical setup, rejected logins should be registered and logged. In some technical setups, it is reasonable only to “flag” and act upon reject logins after a series of repeated failed logins (e.g. three consecutive failures raises a flag). In other technical setups, typically completed automated processes, even the first failure is worth flagging and investigating.

Event logs should include *who did something*, that is: users IDs, system activities, key events, and timings: network addresses and protocols, device identity or location if possible, and system identifier. Coupled with *what was done*, event logging should further include changes to system configuration; use of privileges; use of system utilities and applications; files accessed and kind of access; transactions executed by uses in applications; and finally alarms raised.

See e.g. ISO/IEC 27002:2013, sub-chapter 12.4.1 Event logging, for guidance on what event logging could include.

3.7. Are there automatic restrictions in place in case of repeated failed logins?

In case of repeated failed logins, the system should automatically perform some action (e.g. freeze the account) to safeguard against possible intrusion.

3.8. Are there clear, written, and regularly updated instructions for documentation?

See above the explanatory notes to item 1.10.

4. Supervision and audits

For implementation guidance see e.g. ISO/IEC 27002:2013, 16 Information security incident management.

4.1. Are rejected logins investigated, if they are suspicious (depending on the frequency of rejection and the level of confidentiality of data targeted by the login)?

For implementation guidance see e.g. ISO/IEC 27002:2013 - 16.1.5 Response to information security incidents

4.2. Separation of roles: Is the staff member responsible for systems technology independent from the staff responsible for the content (users of the IT-system)?

This requirement may be difficult for many organizations to comply to, but care should be taken that no single person can access, modify or use assets without authorization or detection. Whenever it is difficult to segregate, other means such as monitoring of activities, audit trails and management supervision should be considered.

Please see e.g. ISO/IEC 27002:2013:

6.1.1 Information security roles and responsibilities
6.1.2 Segregation of duties

4.3. Do all significant ICT related operational decisions by users require approval by at least one more staff ("many eyes" principle), and are such "significant operational decisions" clearly defined?

Formal management responsibilities and procedures should be in place to ensure satisfactory control of all changes. When changes are made, an audit log containing all relevant information should be retained. There should be a formal approval procedure for proposed changes with verification that information security requirements are met, and the changes should be communicated to all relevant persons.

Please see e.g. ISO/IEC 27002:2013:

12.1.2 Change management
12.4.3 Administrator and operator logs
12.6.1 Management of technical vulnerabilities

4.3. Are system audits performed by an expert who is not the IT administrator and who is independent from any other involvement with the system (e.g. through external audit)?

Please see e.g. ISO/IEC 27002:2013:

6.1.2 Segregation of duties
12.7 Information systems audit considerations
18.2.1 Independent review of information security

4.4. IT-compliance tests: is it verifiable and routinely verified that IT-procedures comply with the instructions?

Managers should regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements. Operating procedures should be documented and made available to all users who need them. Changes to the organization, business processes, information processing facilities and systems that affect information security should be controlled.

Please see e.g. ISO/IEC 27002:2013:

12.1.1 Documented operating procedures
12.1.2 Change management
18.2.2 Compliance with security policies and standards

4.5. Are there clear, written, and regularly updated instructions for supervision and audit?

See above the explanatory notes to item 1.10.

5. External partners and outsourcing

5.1. Whenever IT development, maintenance, or deployment is outsourced: Does the public entity ensure itself that access to data is only possible for authorised external personnel?

Supplier agreements should be established and documented to ensure that there is no misunderstanding between the organization and the supplier regarding both

parties' obligations to fulfill relevant information security requirements. Further, explicit list supplier personnel either authorized to access or receive the organization's information, or procedures, or conditions for authorization, and removal of the authorization, for access to or receipt of the organization's information by supplier personnel. Finally, care should be taken to include all relevant information security risks and requirements. Supplier agreements may also involve other parties (e.g. sub-suppliers).

Please see e.g. ISO/IEC 27002:2013:

15.1.2 Addressing security within supplier agreements

5.2. Are there written agreements with external partners on how confidential and private data should be treated and what security measures must be taken?

The written agreements with external partners on confidential and private data should reflect national regulations. If national sets of rules provide sufficient guidance, the contract could simply refer to such rules. It should be noted that Directive 95/46/EC[9] on personal data calls for respective agreements to "be in writing or in another equivalent form [...] for the purposes of keeping proof".

Please also see e.g. ISO/IEC 27002:2013:

15.1.1 Information security policy for supplier relationships 15.1.2 Addressing security within supplier agreements

5.3. Does the public entity update security clearances to work with confidential or sensitive data regularly?

Each individual organization will define security clearances necessary to work with specific data (confidential, sensitive, non-public, or person identifiable). However, as a general rule of thumb employees should only have access to data necessary for completing their immediate work tasks. IT staff and other cross-organizational staff functions may, due to the nature of their work, have access to a broad range of data across the organization and may be able to circumvent normal IT safeguards within technical systems. Depending on the access range, an organization may deem it necessary to apply higher security clearance requirement for such staff. Further, it is sensible to apply other types of safeguards, e.g. organizational and procedural safeguards such as such as the "many eyes" principle, for monitoring such employee access to data systems.

As with point 1.6, security clearances depend largely on the requirements under national rules for state secrets, and confidentiality under data protection rules.

[9] http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046&from=en.

5.4. Is the implementation of agreements followed-up regularly?

This requires designating a concrete staff with the task of monitoring implementation of the agreement and to sign off payments on the contract as well as any similar confirmation of actual performance of the contract. Fulfillment of contract obligations and the monitoring need to be documented in writing. Directive 95/46/EC[10] on personal data requires "that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures."

5.5. Does the public entity assess risks and does it monitor and audit data security measures?

A risk assessment can identify threats to the organizations assets; it will evaluate vulnerability to and likelihood of occurrence, and estimate potential impact.

A review should be carried out by individuals independent of the area under review, e.g. the internal audit function, an independent manager or an external party organization specializing in such reviews. Individuals carrying out these reviews should have the appropriate skills and experience. Managers should regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements. Information systems should be regularly reviewed for compliance with the organization's information security policies and standards.

Please see e.g. ISO/IEC 27002:2013:

18.2.1 Independent review of information security
18.2.2 Compliance with security policies and standards
18.2.3 Technical compliance review

Other standards:

ISO/IEC 27005[11] provides information security risk management guidance, including advice on risk assessment, risk treatment, risk acceptance, risk communication, risk monitoring and risk review.

ISO/IEC 27007[12], "Guidelines for information security management systems auditing" and ISO/IEC TR 27008[13], "Guidelines for auditors on information

[10] http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046&from=en.
[11] ISO/IEC 27005, Information technology — Security techniques — Information security risk management
[12] ISO/IEC 27007, Information technology — Security techniques — Guidelines for information security

security controls" also provide guidance for carrying out the independent review.

More information can be retrieved from the ENISA website – European Union Agency for Network and Information Security - Inventory of Risk Management / Risk Assessment Methods and Tools (https://www.enisa.europa.eu/activities/risk-management)

5.6. Does the outsourcing agreement allow the public entity to draw appropriate consequences in case of violations (in particular notice, damages, immediate access to and withdrawal of external data at all times, right to information)?

Depending on the advice by a national legal expert, the outsourcing agreement needs to grant the public entity the right to give regular notice without grounds, irregular notice in case of violation by the external service provider or in case of force majeure events, claim damages in case of breach of contract, immediate access to and withdrawal of external data at all times (as otherwise the service provider could blackmail the public entity), and the right to information about the performance of the contract (so the public entity can inform itself e.about the current technical specifications and security measures used, etc.). Directive 95/46/EC[14] on personal data states that "the processor [of the data] shall act only on instructions from the controller [the one primarily responsible for the data]".

5.7. Are there clear, written, and regularly updated instructions for external services?

See above the explanatory notes to item 1.10.

6. Relation between IT systems

6.1. Whenever the public entity interacts with other IT-systems or is part of a larger process: does the public entity ensure in particular awareness, training, and instructions for its employees on the possible risk of receiving compromised data or being part of a compromised IT-process?

Compromised means that a third party has had access to data with the intent of altering data or gaining an unfair advantage by knowing their contents. A compromised IT process or computer is one whose confidentially, integrity or availability has been adversely impacted by an untrustworthy source. Hacking, impersonating a legitimate user, brute-force attacks, exploiting loopholes in a

management systems auditing
[13] ISO/IEC TR 27008, Information technology — Security techniques — Guidelines for auditors on information security controls
[14] http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046&from=en.

computers configuration, can compromise not just an individual computer, but all data exchange taking place from that computer, thus compromising all IT processes the computer participates in. A compromised IT process is not necessarily limited to the organization itself if the computer or process exchange data across organizations.

The ISO/IEC 27002:2013 standard does not have specific guidance on this question, but it is worth being aware of the following sub-sections:

9.3 User responsibilities
13.2.1 Information transfer policies and procedures
13.2.2 Agreements on information transfer

6.2. Are standard procedures in place in case an evidently corrupted input appears in this entity (such as an evident inconsistency of data received from another entity)?

The following is an example of an evident inconsistency: A citizen applies for a pension, because she claims to have worked for 45 years as a teacher. The pension agency accesses the database of the ministry of education. The database shows that the citizen indeed worked 45 years as a teacher. However, the first and last entry of data was only two days before the application for a pension. This is obviously inconsistent, as there should have been many more entries during the last years when the applicant allegedly worked there. This raises the suspicion that the applicant possibly corrupted the data in the database of the ministry of education in order to falsely claim a pension without having actually worked there for 45 years or at all.

The standard procedure in such cases is simple: The staff should notify their superior in case of any evident inconsistency. It should then seek written confirmation and explanation from the entity responsible for the external database that the data is in fact correct and not corrupted (in our case one possible explanation could be that the applicant by mistake was not part of the database but only entered into two days ago).

6.3. Base registries are essential building blocks for coherent interoperable eGovernment: are special and heightened security measures in place for them, such as special logfiles chronicling which user inserted, changed, or deleted data, or such as secure back up?

See above the explanatory notes to item 6.1.

6.4. Are there clear, written, and regularly updated instructions for the relation between IT-systems?

See above the explanatory notes to item 1.10.

7. Training, awareness and responsibility

7.1. Are heads of public entities as well as public officials aware of the risks which IT can pose with regards to corruption?

Please consult the ReSPA-Study "Abuse of Information Technology (IT) for Corruption" (2014)[15] which highlighted risks IT can pose regarding corruption and outlined safeguards against such abuse.

7.2. Are employees aware of the instructions?

This could include, for instance, instructions on access control, making users accountable for safeguarding their authentication information as in ISO/IEC 27002:2013 - 9.3 User responsibilities.

7.3. Have employees received training in how to comply with instructions?

Such trainings could be online via e-learning, in class-rooms with a trainer, or in face-to-face sessions with a supervisor or other expert. It is recommended that the training sessions are rather interactive and do only consist to a smaller extent of lectures. The trainees should be motivated to actively reflect about risks and abuse patterns, as a mock-exercise should put themselves into the shoes of corrupt offenders and suggest ways of abusing the existing system (thus pointing to potential weaknesses), and discuss possible policies to address security risks.

7.4. Do heads of public entities know where to get advice/assistance for closing safety gaps in the IT of their public entity (corruption prevention bodies, IT-agencies, etc.) especially in emergency or acute situations?

This could include contacting national CSIRTs - a team of IT security experts whose main business is to respond to computer security incidents. It provides the necessary services to handle them and support their constituents to recover from breaches.[16]

[15] http://www.respaweb.eu/11/library#respa-publications-and-research-18.

[16] National CIRTs stands for Computer Security Incident Response Team, a term used predominately in Europe for the protected term CERT. Abbreviations used for the same sort of teams include:

- CERT or CERT/CC (Computer Emergency Response Team / Coordination Center)
- CSIRT (Computer Security Incident Response Team)
- IRT (Incident Response Team)
- CIRT (Computer Incident Response Team)
- SERT (Security Emergency Response Team)

In order to mitigate risks and minimize the number of required responses, most CSIRTs also provide preventative and educational services for their constituencies. They issue advisories on vulnerabilities in the soft and hardware in use, and also inform the users about exploits and viruses taking advantage of these flaws, so the constituents can quickly patch and update their systems.

More information can be retrieved from ENISA – European Union Agency for Network and Information Security (https://www.enisa.europa.eu/activities/cert)

7.5. Is staff qualified to deal with technical security available?

Qualifications relate to a sufficient understanding and expertise related to all points of this checklist.

7.6. Are staff responsible for IT-systems regularly trained on up-to-date standards of technical security?

Trainings should cover over time all issues of this checklist, in particular where security measures have been newly introduced.

7.7 Is there clear placement of responsibility to name individuals/positions for all relevant actions on this check-list?

For each item on this checklist, there should be a clearly defined employee in each organization. Ideally all or most of the items on this checklist will fall in the responsibility of one staff, but ultimately management *always* has the final responsibility.

8. Proper conduct

8.1. Is there an overall, clear and proactive policy to build a culture of ethics and compliance, and are staff responsible for IT-systems trained in, and aware of, these principles?

Code of conducts or ethics are nowadays a standard part of all public administrations, in particular in the executive sector. They are the cornerstone and main expression of ethics policies. Trainings on ethics complement such codes. Whenever such codes of conduct are updated, it is necessary to inform all employees of such changes. There are model codes of conduct, such as the Council of Europe Recommendation (2000)10E 11 May 2000 on Codes of Conduct for Public Officials.[17]

[17] http://www.coe.int/t/dghl/cooperation/economiccrime/corruption/Default_en.asp.

8.2. Has the organisation instituted a formal code of conduct that every staff member at every level must certify as part of their contract and/or terms of employment?

See above the explanatory notes to item 8.1.

8.3. Do employees know where and how to report cases of abuse of IT for corruption?

Codes of conduct or national anti-corruption laws normally provide employees with clear instructions and even obligations to report cases of corruption involving themselves or colleagues. The usual channels are superiors, internal anti-corruption focal points, or the national anti-corruption agency. Websites of the public organisations should contain easy access information on where to report cases of IT-corruption.

8.4. Are there Standard Operating Procedures (SOP) in place to be followed in case of violations?

Valuable time may be lost if the organisation does not know how to respond and what procedures should be followed in case of violations. Standard Operating Procedures (SOP) should include both establishing procedures and responsibilities, and communicating them adequately within the organisation. SOPs should also include reporting events and weaknesses; how to assess violation events; how to respond to violations; and how to secure evidence of the violation.

Please see ISO/IEC 27002:2013 – 16.1 Management of information security incidents and improvements.

9. Civil society and transparency

9.1. Does the public entity provide open government data and citizen participation as much as possible, in order to allow for scrutinising public sector data and processes, as well as possible irregularities and abuses?

Open government data is data produced or commissioned by government or government controlled entities and can be freely used, reused and redistributed by anyone. In a well-functioning democratic society, citizens need to know what their government is doing, and to ensure this, they must be able to freely access government data and information and to share that information with other citizens. Open government data can be any data(set), but a typical place to start is by publishing data on government spending (e.g. budgets), and common data produced by the entity. For it to be really open data, data must also be published in an open data format suitable for data analytics. For the purpose of this

questionnaire and for the purpose of true transparency, data on the investments and on the service output by the government entity is included.

9.2. Are channels provided to the public for giving feedback to the public entity and government in general?

Feedback channels include using social media, feedback/complaints/suggestion functionality on websites, open discussion forums etc.

9.3. In case of abuse of IT for corruption and other irregularities, are channels provided for citizens to report incidents?

Citizens will always have the possibility to report incidents – outside the public entity concerned - to the police, the court of auditors, to national anti-corruption agencies, or to the public entity itself. In this case, the entity should provide a clear contact point for such reports, such as an anti-corruption or integrity officer with contact details. It is important that anonymous channels should be available, either within the institution, or at least to external law enforcement bodies; Article 13 para. 2 of the United Nations Convention against Corruption (UNCAC)[18] calls for anonymous hotlines being available for reporting incidents of corruption.

9.4. Does the Public Administration publish lists of IT contractors and contracts?

Public procurement laws often require the public administration to publish to whom it awarded a contract.[19] Some countries go even further and publish the entire contract: In January 2011, Slovakia decided to have most of the public contracts published online, and that a contract not published is not in force.[20]

10. International Standards and Cooperation

10.1. Does the public entity implement information security standards (in particular ISO 27001) to ensure data safety and integrity?

For an overview of frameworks and standards for auditing security measures, please see the European Union Agency for Network and Information Security - ENISA (September 2013): “Auditing Security Measures”.[21]

[18] http://www.unodc.org/unodc/en/treaties/CAC/.

[19] See for example Article 51 para. 2 Directive 2014/24/EU on public procurement, http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014L0024&from=EN.

[20] Transparency International Slovakia, “Not in Force until Published Online – What the Radical Transparency Regime of Public Contracts achieved in Slovakia”, 2015, http://www.transparency.sk/wp-content/uploads/2015/05/Open-Contracts.pdf.

[21] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/schemes-for-auditing-security-measures-1.

10.2. Does the public entity keep itself informed on foreign and international developments on information security?

Some of the relevant platforms and sources are:

- International Organization for Standardization (ISO), www.iso.org
- Information Security Forum (ISF), www.securityforum.org
- SysAdmin, Networking and Security Institute (SANS), www.sans.org
- Information Systems Security Association (ISSA), www.issa.org
- Institute of Information Security Professionals (IISP), www.iisp.org
- European Union Agency for Network and Information Security (ENISA), www.enisa.europa.eu
- (United States) National Institute of Standards and Technology (NIST), Computer Security Division (CSRC), http://csrc.nist.gov