ReSPA

Regional School
of Public Administration

7th meeting of eGovernment working group

Follow up Meeting to ReSPA Comparative Study on "Abuse of Information Technology (IT) for Corruption

27-28 April 2015, Belgrade (Serbia)

Background

For several years, ReSPA has supported well established and running networks/working groups, both on Ethics and Integrity and on e-Government. In 2014, ReSPA brought together the expertise of both working groups. The combined efforts resulted in the comparative ReSPA-Study on "Abuse of Information Technology (IT) for Corruption" (2014).[1] The Study was presented at the 7th meeting of the Ethics and Integrity Working Group, and the 6th meeting of the eGovernment Working Group, in Tirana on 26-27 November 2014. As a practical follow-up to the Study, ReSPA developed a draft "**Checklist** for Assessment of Risks for **Abuse of IT** for Corruption". The final draft was sent to one institution of each working group member, where it is currently applied in a pilot activity for reviewing the security of IT against abuse for corruption.

The previous work of the eGovernment working group has included:

- 2012-13: Comparative eGovernment study
- January 2014: seminar on eGovernment and mGovernment and Strategic Planning in the public administration
- February 2014: ReSPA study visit to OECD
- July 2014: seminar on Strategic Planning and Implementation of eGovernment Project
- November 2014: study on Anti-Corruption and eGovernment, jointly with the Ethics and Integrity Working Group, plus a short meeting of the eGovernment working group to discuss its work in 2015 which provides a basis for 7th Meeting of the eGovernment working group.

Objectives

The objective of the meeting on the first day is to allow for the exchange of experiences on the practical application of the checklist during its pilot phase, and to identify possible follow-ups.

The objectives of the second day are to build upon the results of the 'Abuse of IT for corruption' in 2014 to develop trust and collaboration and achieving impact through a seminar on Open Governance and Open Government Data (OGD).

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

Target group

The meeting is intended for primarily network/working group members who participated in previous meetings of the eGovernment working group (2 participants per ReSPA Member and Kosovo*), who have at least 5 years of relevant work experience in the topic of the working group who possess a clear and demonstrated interest in the topic and are motivated to participate in discussions and exchange of opinions/best practices with other colleagues from the Western Balkan. It is of crucial importance that the participants fulfill the necessary requirements and contribute to the results of the working group meeting with their professional skills, knowledge and active participation. The meeting is also intended for one additional participant, the person who directly worked on the piloting of the Checklist on risks of IT-corruption.

1st DAY – Checklist on risks of IT-corruption

The objective of the meeting on the first day is to review the experiences with the checklist from piloting them in different countries in institutions:

- Did the checklist correspond to all risks and aspects arising in practice?
- Are any points missing?
- Which questions are unclear or could be expanded?
- Are there sector-specific aspects, which should be considered?
- Which points are the easiest to assess, which are the most difficult?
- Is more guidance needed to properly implement the checklist?
- On which points can ReSPA members learn from each other?

The meeting will also look into possible implications for policy and legislation:

- Is there any need to revise the legislation in order to continue or facilitate assessments of IT-corruption?
- Should the assessment of IT-corruption be reflected in national or institutional strategies or integrity plans?
- How should ReSPA and its working groups accompany future reform processes in this direction?

2nd DAY - eGovernment

The 6th Meeting of the eGovernment Working Group in Tirana on 27 November 2014 agreed to link the on-going work of the working group to the issues of trust, collaboration and open governance. These issues lay the basis both for more user-centric services and better government-user relationships, as well as for improved public sector performance and greater impact on societal development. In this context, it was agreed to focus specifically on open government data (OGD) which, in the context of ReSPA, has two aspects:

1. Publishing data about public sector activities and performance, except where clearly of a confidential nature, such as budgets, human and other resources and assets, contracting, public policies, etc. The purpose is both to elicit public engagement and participation in the work of government, as well as to enable the scrutiny of what the public sector does and how it does it. The latter is also an important component of the anti-corruption work of the Ethics and Integrity Working Group.

2. Publishing public sector data sets, covering all aspects of the responsibilities of the public sector ranging from health, education, transport, utilities, employment, crime, weather, land use, planning, etc. It is suggested that in principle OGD should be 'open by default', i.e. data sets should be made publically available unless there is good reason not to do so which normally requires a legal or regulatory provision. In addition, all OGD should be subject to the standard provisions of data publishing in terms of formats, access, licensing and use, etc. It was also noted that work on OGD could also be linked to the Open Government Partnership (www.opengovpartnership.org).

Short Resumes of the Experts

Jeremy Millard is Associate Research Fellow at Brunel University, UK, and Chief Policy Advisor at the Danish Technological Institute, Denmark. He has forty years' global experience working with governments, development agencies, and private and civil sectors, focusing on how new technical and organisational innovations transform government and the public sector. (jeremy.millard@3mg.org)

Dr. Tilman Hoppe has worked as a judge, as an executive in the financial sector, and as a legal expert for the German Parliament. For several years he has advised the Council of Europe and other international organizations on governance reforms, and is currently implementing an anti-corruption project in Eastern Europe. (info@tilman-hoppe.de)

Agenda

DAY I, 27 April 2015 (Monday)

09:30 – 09:45 **Welcome**
Mr. Dusan Stojanovic, Director of the Directory for eGovernment
Mr. Goran Pastrovic, ReSPA Programme Manager

09:45 – 10:15 **Presentation of Checklist** (*Tilman Hoppe, Jeremy Millard and Goran Pastrovic*)

10:15 – 11:15 **Country presentations of results of pilot assessments** (*moderated by Tilman Hoppe and Jeremy Millard*)

11:15 – 11:30 Coffee break

11:30 – 13:00 **Country presentations of results of pilot assessments (continued)**

13:00 – 14:30 Lunch

14:30 – 15:45 **Plenary discussion: How could the Checklist be improved?** (*moderated by Tilman Hoppe and Jeremy Millard*)

15:45 – 16:00 Coffee break

16.00 – 17:00 **Plenary discussion: What next in terms of strategies, legislation, and future activities?** (*moderated by Tilman Hoppe, Jeremy Millard and Goran Pastrovic*)

DAY 2, 28 April 2015 (Tuesday)

09:00 – 09:15 **Objectives of the 2nd day**

09:15 – 10:30 **Overview of global experience, standards, good practice and relevance for fighting corruption and building trust and confidence, and relevance to the Western Balkans** *(Jeremy Millard)*

10:30 – 11:15 **Tour de table: status quo of open governance and OGD in the Western Balkan countries** *(moderated by Jeremy Millard and Goran Pastrovic)*

11:15 – 11:30 Coffee break

11:30 – 12:00 **Tour de table: ideas for developing open governance and OGD in the Western Balkan countries for improving services, government performance and building trust and confidence** *(moderated by Jeremy Millard)*

12:00 – 12.30 **Review of topics for open governance and OGD and future work of the eGovernment Working Group** *(Jeremy Millard and Goran Pastrovic)*

12:30 – 13:30 Lunch

13.30 Departure of the participants

Enclosures:

- Checklist for Assessment of Risks for Abuse of IT for Corruption

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)[2] 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 by the ReSPA Ethics & Integrity Network in 2015. 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". Please provide always explanatory comments for all questions to explain or justify your "Partially" or "Yes" scores.

Country	Institution

Area	No	Part.	Yes	Comments (if answer is "partially" or "yes")
1. Availability of regulations/instructions				
1.1. Are there clear, written, and **updated instructions** for data and equipment access, use, destruction, recovery, outsourcing, de-commissioning, transfer, sale and supervision?				
1.2. Are instructions **updated regularly**?				
1.3. Are the rules **clear** and without ambiguity, or do they leave any unnecessary room for **discretionary** decision making?				

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

Area	No	Part.	Yes	Comments (if answer is “partially” or “yes”)
2. Access control				
2.1. 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?				
2.2. Is **antivirus** software installed and enabled on all computers?				
2.3. Is a procedure in place for **restricted internet** connection for computers storing confidential data?				
2.4. Is there a defined procedure for using **memory storage** devices (USB, CD, etc.) and for preventing illegal download of data on private storage devices?				
2.5. Is access to different levels of sensitive data tailored to the **appropriate level**?				
2.6. 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?				
2.7. 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”)
3. Recovery				
3.1. 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.				
3.2. Are **backup procedures** implemented with periodic full backup of all systems and data, including desktop and laptop computers and other user interface devices? Are backup copies stored physically offsite or in a hazard-secure place onsite?				
4. Documentation				
4.1. 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?				
4.2. Are **copies** of **log files** stored off site and/or are they separate from the application itself?				
4.3. Are log files **deleted** only when national data protection rules require so, but not before?				

Area	No	Part.	Yes	Comments (if answer is “partially” or “yes”)
4.4. 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)?				
4.5. Are **rejected logins** automatically registered (logged)?				
5. **Supervision and audits**				
5.1. 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)?				
5.2. **Separation of roles:** Is the staff member responsible for systems technology independent from the staff responsible for the content (users of the IT-system)?				
5.3. Do all significant operational decisions by users require approval by at least one more staff (“**many eyes**” principle), and are such “significant operational decisions” clearly defined?				
5.4. Are system **audits** performed by an expert who is not the IT administrator and who is independent from any other involvement with the system?				
5.5. IT-compliance tests: is it verifiable and routinely **verified** that IT-procedures comply with the instructions?				

Area	No	Part.	Yes	Comments (if answer is “partially” or “yes”)
6. External partners and outsourcing				
6.1. Whenever IT development, maintenance, or deployment[3] is **outsourced**: Does the public entity ensure itself that access to data is only possible for authorised external personnel?				
6.2. Are there **written agreements** with external partners on how confidential data should be treated and what security measures must be taken?				
6.3. Does the public entity update **security clearances** to work with data regularly?				
6.4. Is the implementation of agreements **followed-up** regularly?				
6.5. Does the public entity assess risks and does it monitor and audit data **security measures**?				
6.6. 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)?				

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

Area	No	Part.	Yes	Comments (if answer is “partially” or “yes”)
7. Relation between IT systems				
7.1. 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?				
7.2. 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)?				
7.3. **Base registries**[4] 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?				
8. Training, awareness and responsibility				
8.1. Are **heads** of public entities as well as public officials aware of the risks which IT can pose with regards to corruption?				

[4] 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”)
8.2. Are employees **aware** of the instructions?				
8.3. Have employees **received training** in how to comply with instructions?				
8.4. 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?				
8.5. Are staff responsible for IT-systems regularly **trained** on up-to-date standards of technical security?				
8.6. Do employees **know where** and how to report IT violations?				
8.7. 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?				
8.8. Has the organisation instituted a formal **code of conduct** that every staff member at every level must re-certify regularly as part of their contract and/or terms of employment? Is there clear placement of **responsibility** to named individuals/positions for all relevant actions on this check-list?				
9. **Civil society and transparency**				

Area	No	Part.	Yes	Comments (if answer is “partially” or “yes”)
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**?				
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) [5] to ensure data safety and integrity?				
10.2. Does the public entity keep itself informed on **foreign and international** developments on information security?				

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