ReSPA

Regional School
of Public Administration

Launching of the ReSPA Regional Comparative Study “Abuse of IT for corruption“ and

6th meeting of eGovernment Network

26-27 November 2014, Tirana, Albania

Discussion paper and provisional programme

Background

For several years, ReSPA has well established and running networks, both on ethics and integrity and on e-Government. During the fifth meeting of the eGovernment network (3-4 February 2014, Paris), ReSPA supported the idea of the network members for development of the comparative study on “Abuse of IT for corruption” and for merging both Networks in this regard. The idea was presented and approved at the fifth Ethics and Integrity Network meeting on 26-27 March 2014 in Danilovgrad. Furthermore, participants of the sixth meeting of the Ethics and Integrity Network (8-9 July 2014, Vilnius) adopted an international standard on asset declarations and a draft template for international data exchange, as well as identified conflicts of interest as the next issue to be reviewed through a comparative study.

Objective

The objective of the meeting on the first day is to allow for the launching of the Comparative Study on “Abuse of IT for corruption offences”. The event will also be an opportunity for regional and cross-disciplinary exchange on the findings and recommendations of the Study. It will furthermore provide a forum for identifying next steps in translating the recommendations into concrete in-country actions. On the second day the meeting will contribute to identifying regional reform steps related to IT-corruption, and to reviewing of the general network planning.

1st day – Launching of the Comparative Study on IT-corruption

The Study comes to conclusions/recommendations relevant both for the Ethics and Integrity and for the eGovernment Network, which can be summarised as follows:

Any stakeholder working on **corruption prevention** needs to accept ICTs, not only as a tool for fighting corruption, but also as a risk for committing corruption. To this end, anti-corruption experts need to cooperate closely with IT experts on identifying and preventing corruption risks from abuse of ICTs. This entails risk assessments, awareness and training measures, statistical monitoring of offences and trends, as well as inclusion of ICT risks in anti-corruption policies.

Any stakeholder working on **ICT** should ensure an information security management system that prevents abuse of IT-systems for corruption, in particular through asset, access and human resource security; operations management and business application controls; documentation and script sufficiency and security; physical and online security; business continuity; record keeping and compliance.

The meeting will try to address and answer the following questions:

- On which points can ReSPA members learn from each other?
- How can ReSPA members translate these recommendations into in-country reforms?
- Should there be additional recommendations?
- Where is further potential for a cross-disciplinary exchange between ethics and integrity and e-government as disciplines?
- Should ReSPA and other organisations and donors follow-up on this Study with more activities and if so, what kind?

2nd day

1st session - Comparative Study on IT-corruption

As the public event on 26 November will focus on an exchange of opinions and ideas about the Study with international organisations, local stakeholders, and the public at large, the Network Meeting following the launching of the Comparative Study is a non-public setting, will allow discussion and identification of concrete actions for each ReSPA member in an internal, closed atmosphere of country representatives and experts. Concrete actions are expected to come from this Network Meeting. The possible role of and support by ReSPA in these future actions will be one particular point of interest.

2nd session – Planning of next steps

The 2nd session on the last day will be dedicated to planning the next steps and activities of the e-Government Network. This includes activities related to the Study on IT-corruption, but also other activities of interest to participants. Possible items on the agenda are:

- Overall discussion
- Short roundtable on safeguards against abuse of IT for corruption offences in light of public administration reform process in the countries of the Western Balkan
- How to ensure practical utilisation of the Comparative study on IT-Corruption
- How ReSPA could contribute to improvement of fight against corruption in the domain of ICT
- Possible future cooperation with OECD on Digital agenda development, e-procurement, or overall eGovernment strategy design and/or upgrade

Short Resumes of the Experts

Louise Thomasen is an independent consultant, eGovernment, and technology expert. She has 25 years experience working with IT in the cross field of technology and society both nationally and internationally. (louise@cothomasen.dk)

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)

Vera Devine has been working on anti-corruption issues since 2001, when she joined the Anti-corruption Division of the OECD after having spent almost four years in post-war Bosnia and Herzegovina. Vera continues to work for a number of international organisations, mainly on corruption in the Western Balkans and the former Soviet Union. (veradevine@yahoo.com)

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)

Draft Provisional Agenda

DAY I, 26 November 2014, (Wednesday), Tirana International Hotel, Tirana

09:30 – 10:00 **Welcome**
- Mr. Suad Musić (ReSPA Director)
- Mr. Goran Pastrovic (ReSPA Training manager)

10:00 – 10:15 **Presentation of Study: rationale and methodology (*Dr. Tilman Hoppe*)**

10:15 – 11:00 **Presentation of Study: conclusions on information technology (*Louise Thomasen*)**

11:00 – 11:15 **Presentation of Study: conclusions on integrity (*Vera Devine*)**

11:15 – 11:30 Coffee break

11:30 – 12:00 **Plenary – questions and answers on the conclusions**
(moderated by expert Dr. Tilman Hoppe)

12:00 – 13:00 **Tour de table and plenary discussion: Regional exchange – each country delegation summarises challenges described in the Study**
(moderated by expert Louise Thomasen)

13:00 – 14:30 Lunch

14:30 – 15:45 **Plenary discussion: How could findings and recommendations of the study translate into country actions?**
(moderated by expert Vera Devine)

15:45 – 16:00 Coffee break

16.00 – 17:00 **Presentation of results and conclusions**
(*moderated by expert Dr. Tilman Hoppe*)

19.00 Social event and Joint dinner

DAY 2, 27 November 2014, (Thursday), Tirana International Hotel, Tirana

09.00 - 09.10 Objective of 2nd day (training manager Goran Pastrovic)

09.10 - 10.10 How could ReSPA follow up on the ICT Study with supporting reforms in the region? (moderated by experts Louise Thomasen, Jeremy Millard, Vera Devine and Dr. Tilman Hoppe)

10.10 - 10.30 Coffee break

10.30 - 12.30 Separate meetings on next steps of both Networks

- eGovernment Network (moderated by experts Jeremy Millard and Louise Thomasen)
- Ethics and Integrity Network: (moderated by experts Vera Devine and Dr. Tilman Hoppe

12.30 - 13.30 Lunch

13.30 Departure of the participants

Annex 1: Recommendations in the Comparative Study on IT-corruption

Part 1 – recommendations addressed at anti-corruption experts

Any stakeholder working on corruption prevention needs to accept ICTs not only as a tool for fighting corruption, but also as a risk for committing corruption. To this end, the following measures are necessary for **anti-corruption** experts:

- Anti-corruption experts need to **cooperate** closely on identifying and preventing corruption risks from abuse of ICTs.
- Corruption prevention bodies need to include the possibility of abusing ICTs for corruption into their catalogue of standard corruption risks. **Risk assessments** in public administration need to include the safety of IT against corruption risks. Risk assessments need to review any of the IT features listed below (Part 2 of the recommendations).
- Heads of public entities as well as public officials need to be made **aware** of the risks which ICTs can pose with regards to corruption. Corruption prevention bodies need to actively offer advice on closing safety gaps in the IT of public administration.
- Corruption prevention bodies and vocational training centres need to offer **training** on corruption risks connected to ICTs; such training should include IT experts.
- National anti-corruption **strategies** and action plans should include a section on preventing corruption related to abuse of ICTs. If other strategies (such as on e-government or public administration reform) already deal comprehensively with enhancing IT against abuse, the anti-corruption policy should at least contain a reference to the other strategies and ensure coordination between anti-corruption and IT experts on reform measures.
- Law enforcement bodies and corruption prevention bodies should collect **statistical** data on IT corruption, analyse patterns, and adopt reform measures accordingly.

Part 2 – recommendations addressed at by eGovernment experts

- Access to all proprietary data and systems has to be safeguarded with **access control** using individual private user IDs and passwords.
- In each public body it is a management responsibility to ensure that access to data is at the **appropriate level**. Access to proprietary data should be granted only when required for the immediate work tasks.
- **Physical access** to facilities which store data or physical copies of data should be restricted to authorised personnel whose access is both logged and monitored.
- Public organisations must implement **information security standards** such as ISO 27001 to ensure data safety and integrity.

ReSPA Activities are
Financed by the EU

- **Disaster recovery and continuity plans** in case of security incidents should be developed for each public organisation. 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.
- All public organisations should implement **backup procedures** with periodic full backup of all systems and data. This includes desktop and laptop computers. Backup copies should be physically stored offsite.
- **Log files** are a part of an organisation's monitoring and supervision structure. They also constitute an important auditing tool. Copies of log files should also be stored off site and/or separate from the application itself. Personnel responsible for altering content (data) should not be (technical) administrators of log files.
- Public bodies must ensure that all their processes, regardless of their being physical or electronic, are not vulnerable to corruption abuse**. A compromised process or step in a process will influence all other** processes it interacts with. ICT systems that rely on input from other systems or processes are as safe from corruption as the systems and processes they interact with.
- **Base registries** require special and heightened security measures as they are essential building blocks for coherent interoperable eGovernment.
- **Outsourcing** IT development, maintenance, or deployment requires enhanced diligence by the public organisation that outsources. Responsibility can never be outsourced. When outsourcing, ensure that access to data is only possible for authorised assigned personnel, and that they are monitored and audited.
- There should be a **separation of roles** between personnel responsible for data (content) and personnel responsible for systems (technology).
- System **audits** and audit trails must never be monitored and administrated by the same IT administrator.
- Supervision and applying the '**many eyes**' principle should be an integral part, not just in system design and development, but also in daily work.
- **Open government data** and citizen participation in scrutinising public sector data can provide both 'reality checks' and improve data quality, as well as reveal irregularities and abuse. Also important in this context is providing the public with channels to give feedback to government and the public sector. In case of corruption/irregularities, ethics offices whom citizens can report civil servants unethical behaviour to can be such a channel.
- It should be ensured that **training** on and raising **awareness** of ethics and integrity also includes personnel responsible for ICTs.