

# E-government – situation in Ukraine

Prepared by ISACA Kyiv Chapter

February 3, 2011



## Presenters from ISACA:

- Mykhaylo Lopatin, President
- Iryna Ivchenko, Vice-president Information Security
- Alexey Yankovski, Vice-president IT Governance

# Agenda

1. About ISACA
2. Definitions
3. Baseline requirements
4. Situation in Ukraine - overall
5. Situation in Ukraine: Banking Sector
6. Reasons of the problems – what needs to be changed

# About ISACA

- ISACA is a non-profit international professional IT association that promotes mature IT Governance, IT Audit and IT Security
- Unites more than 86,000 members and professionals in more than 160 countries.
- ISACA offers education and professional certification (CISA, CISM, CGEIT) and in the areas of IT Governance, IT Audit, Information Security Management and IT Risk Management
- The goal of the Kyiv ISACA chapter is to become a major driver behind bringing the IT governance, security and assurance to the agenda of the Ukrainian society.
- ISACA in Ukraine is to become the first and the best trusted and reputable community of IT professionals. Ukraine still lacks such a community, while being the largest territory in Europe with population of over 46 million people. The IT groups as they exist nowadays are disparate and least focused on the matters of proper governance.
- ISACA Kyiv chapter is a body entirely independent from influence of any vendors, individuals or groups. We see chapter purely focused on growing maturity of IT governance, security and assurance across all sectors of business and social life, with the help of establishing the ground for professional communication and development, share of best practices and development of the legal framework.
- More information available at: [www.isaca.org](http://www.isaca.org), [www.isaca.org.ua](http://www.isaca.org.ua)

# From E-government to E-governance

## E-government

- Use of Information Technologies to facilitate operation of the government authorities
- E.g. informational web sites, internal electronic document flow, finance budgeting and planning systems
- No means for on-line interaction with the citizens

## E-governance

- E-government + use Information Technologies to achieve interaction with the citizens and their involvement in governance
- Country-wide electronic services: e-voting, e-public discussion of important matters, e-issue of certificates/licenses/resolutions from authorities, e-notary, e-social programmes, social card, e-health, e-education

E-governance is not equal to Smart-city which in addition to “smart-governance” includes various means to improve city operation using ICT (smart-homes, smart-grid, smart-mobility, etc.)

# Baseline requirements to enable e-governance

- High bandwidth network channels
- Proximity to citizens, including affordable internet access
- Computer literacy
- Protected bearer of citizens' personal info, his digital ID and certificate for communication with the government authorities, medical info for emergency help ("digital ID", "social card")
- Availability of standards for: electronic communications, char set encoding, digital signature, digitally signed messages
- Availability of country-wide Public Key Infrastructure for management of citizens' certificates
- Availability of the standard of intuitive and user-friendly navigation of the government web sites

## World examples:

- Special free of charge public internet centres in Italy
- Smart-card issued to every child born includes all info
- Possibility to file state and federal taxes, obtain driver's licenses and pay all the bills via Internet - US
- Educational programs on TV "PC/internet for dummies"
- National Broadband Plan in the US
- Public Information Portal - a one stop access to online information and electronic services of central and local government for citizens and businesses – Czech Republic

## Situation in Ukraine (1/2)

- Relatively reliable communications channels and network infrastructure, including wireless (3G-modems, emerging 4G in Kyiv)
- Big number of Internet Service Providers. Access to internet is possible from almost any village in Ukraine
- Numerous internet-café's
- Yet, lack of high-speed access from home. Networks in the cities are primarily low quality, developed by small operators. 2G-technologies in the village areas. Need at least 10 MBPS per household
- Low level of computer literacy, low internet penetration
- State and municipal authorities created own web sites (mostly static), which are not always up-to-date neither contain information which is of interest to citizens
- Non-intuitive navigation
- Almost no on-line services for citizens
- Insufficient security – numerous cases of compromise by hackers

## Situation in Ukraine (2/2)

- State laws on digital signature and electronic document flow exist
- Lack of state-wide programme and standards for national digital card for identification, secure communication with the government authorities, digital signature, store of information about citizens' benefits and medial record
- A few authorities accept documents in electronic form. However “old mentality” of the authorities leads to the fact that internal processes must to be supported by the paper-based ones
- Citizens and businesses have to purchase different digital keys for use with different govt. authorities (up to 8 different keys)
- Lack of a single set of standards for messages, char encoding, digitally signed messages, structure for application of the digital signature – signed messages are not recognized by different applications
- National standard for the digital signature exists, yet it is different from the internationally-accepted ones which will result in difficulties in secure cross-bordered communication
- Existing PKI infrastructure (13 Ukrainian CAs) are not fully interoperable (CAs do not recognize certificates issued by each other) due to the lack of standards. Users have to certify their keys in different CAs



## Situation in Ukraine – Banking Sector

- 1994 – national System of Electronic Payments (SEP) launched
- 1996 – SEP is protected with the digital signature (each payment is signed by the crypto-program developed by NBU based on the RSA)
- 1997 – 1998 – protected data exchange between NBU and other state authorities (tax authority, customs service, etc.) using crypto means developed by the NBU
- 2002 – “SEP Online”
- 2006 – new generation of SEP - centralized architecture
- 2009 – NBU starts development of the PKI infrastructure for the banking sector, based on the international standards. This will allow digital signature of one bank to be recognized and accepted by the others
- 2010 - PKI governance requirements adopted for banks. NBU requires all the Bank to implement ISO-27001/27002 international information security management standards
- Overall assessment – level of IT maturity is one of the highest in the banking sector

## Reasons of the problems – what needs to be changed

- Despite availability of the specialized State Authority - State Committee on Science, Innovations and Informatization, there is generally lack of steering and direction for implementation of Information Technologies at the state level
- A high-level “Concept for Development of Electronic Governance in Ukraine up to 2015” was approved by the Cabinet of Ministers in Dec. 2010. Yet, specific programme of its implementation yet to be developed
- Lack of expertise for implementation and management of large-scale systems in the country
- Insufficient number of professionals in the area of IT Management and Governance
- Requirements in the area of information security, which are mandatory for state authorities are based on the outdated principles and do not take into account capabilities of the modern information technologies
- Insufficient level of education in the areas of modern information technologies, security and IT governance
- Insufficient level of reliance of the state on the international professional certification for IT and institutes of independent IT auditors to provide independent assurance for IT

## ISACA's contribution (1)

- **European Union (EU) Commission selected COBIT as an Information Systems Security Standard for Paying Agencies,** together with ISO Standard 17799 (currently BS27001) or the Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutzhandbuch/IT Baseline Protection Manual (BSI).
- The Superintendencia Financiera de Colombia, the entity that regulates the banks in Colombia, has adopted COBIT as a reference model for its evaluations, particularly of the entities they supervise, ensuring that these entities, banks and all other financial bodies also use COBIT
- Turkey passed legislation requiring all banks operating in Turkey to adopt COBIT's best practices when managing IT-related processes. Article 30 of the legislation specifically required all banks to comply with auditing requirements based on COBIT's control objectives. As the Banking Regulatory and Supervision Agency noted in the legislation, COBIT was selected as the framework with which to comply because its control objectives are internationally recognized and considered to be effective at controlling IT-related processes.

## ISACA's contribution (2)

- Bahrain Civil Agency prepared maturity model and applied COBIT controls to eliminate weak points after analysing existing internal controls using the COBIT framework.
- Also Central Banks in countries such as Argentina, Armenia, Bulgaria, Uruguay have adopted COBIT.
- The Thai Securities and Exchange Commission (SEC) adopted COBIT when implementing an IT governance program. COBIT helps minimize gaps in the external auditing process and acts as a basis for creating regulations regarding IT Risk Management.
- The standard applied across many governmentally owned businesses.
- CISA and CISM certifications are de facto and de jure standard in many countries.

# ISACA Kyiv Chapter

<http://www.isaca.org.ua>  
[office@isaca.org.ua](mailto:office@isaca.org.ua)

