Proceedings of the Federated Conference on Computer Science and Information Systems pp. 1309–1316
DOI: 10.15439/2016F72
ACSIS, Vol. 8. ISSN 2300-5963

An Information Security Framework for Ubiquitous Services in e-Government Structures: A Peruvian Local Government Experience

Manuel Tupia
Pontificia Universidad Católica del Perú. Engineering Department. Av. Universitaria 1801 San Miguel, Lima, Perú. Email: tupia.mf@pucp.edu.pe

Mariuxi Bruzza
Pontificia Universidad Católica del Perú. Engineering Department. Av. Universitaria 1801 San Miguel, Lima, Perú. Email: a20146472@pucp.pe

Flavio Rodriguez
Pontificia Universidad Católica del Perú. Engineering Department. Av. Universitaria 1801 San Miguel, Lima, Perú. Email: flavio.rodriguez@pucp.edu.pe

***Abstract*—This paper describes a framework designed to establish vital conditions of information security for *ubiquitous* services (U-Government) both in district and province municipalities (departments' capitals) within the Peruvian electronic (e-government) government structures. The framework contains current regulations concerning information security, data privacy, business continuity, and natural disasters management based on good international practices, including but not limited, ISO 27001, ISO 27002, ISO 22301 standards. The aim is to help implement security controls in the use of mobile services which are part of the e-government services catalogue. The framework structure is closely related to the COBIT 5.0 process model.**

I. Introduction

At present, electronic government structures include a solid component of services oriented to the use of devices and mobile solutions [1]. These services are intended to take advantage of the widespread use of this type of devices by citizens and their knowledge of mobile applications [2]. Most local (municipalities) electronic government initiatives in Peru are focused on this type of services rather than web services as displayed in Figure 1:

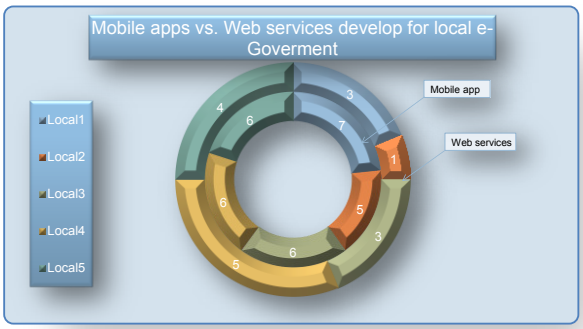

Fig. 1 Comparative table taken from http://www.movil.softwarepublico.gob.pe/ (2015)[1]

New technological developments and innovations are setting the stage for a higher demand of U-government services. This will lead, in turn, to new services for the government which will be forced to increase their number and take into account pertinent restrictions, e.g., information security for regulatory compliance [3], [4], [5], [23].

As there are doubts about the information security in the mobile applications (apps) and due to the huge amount of information to be protected by governmental institutions rendering services through them [6], [22], it is mandatory to develop a framework that facilitates the implementation of controls and the follow-up of good international practices on information security both in the implementation projects of U-Services (ubiquitous services) in Peruvian local governments and the assurance of the already existing apps. The proposed framework must comply with current domestic regulatory framework.

This paper discusses the general structure of a security framework based on COBIT 5.0 and above all its process reference model (PRM) [7] in ISO 27001, ISO 27002 and ISO 31000 standards.

Likewise, the current Peruvian regulations including the Personal Information Protection Law[2] and Peruvian Technical Standards on security will be referred to[3].

II. Ubiquitous Government

A. Ubiquitous computing

Ubiquitous technology (ubicomp, English acronym ubiquitous computing) is an extension of mobile informatics based on access technologies through mobile or handheld devices [8]. It consists of re-orienting ITs to propose mobile technology-based solutions for access, consumption and exploitation of information in an effort to render services as a support to business processes; thus paving the road on which companies and organizations would modify their strategies to meet the needs of clients and stakeholders.

[1] Local label represents a Peruvian public institution

[2] Personal Data Protection Law N°29733

[3] NTP ISO/IEC 17799 and NTP ISO/IEC 27001

B. U-Government

Ubiquitous computing has been closely linked to the electronic government on the premise that it will assure availability and multichannel connections to electronic services offered by the government to the citizen by means of mobile or web-based solutions. Ubiquitous government or u-government mirrors the new manner of interaction and transaction between the government and citizens and other stakeholders in such a way that access to these services is available through entry points (multi-purpose single windows) anywhere and anytime, from different types of mobile electronic devices [9], [13]. Precisely, the main concern of U-services implementation relates to security around the involved transactions and sending of information.

C. Information Security requirements in U-services

Most e-government implementations entail the design of web pages and services offered to citizens from these portals [10]. There are three types of said services: statics information, data consultation (mild interaction that may not imply personal data entry) and transactions (advanced interaction encompassing business transactions such as payments and personal data entry) [11], [20].

Below are the chief considerations on the security related regulatory compliance [14], [21]:

- Is there personal data involved in the service?
- Are digital signatures and certificates being used to authenticate the citizens for transactions?
- Are transactions encrypted? [12]
- Are there VPN infrastructures between local government (Website) and citizens to conduct the transactions involved in the services?
- Do services require the intervention of a payment gateway?
- Do services require the intervention of external payment methods (e.g. PayPal)?

D.Regulatory Requirements of Peruvian Local Governments

Peruvian local governments (province and district municipalities) set forth the following regulations with respect to information security, e-government, and data privacy:

- Mandatory use of the Peruvian Technical Standard "ISO NTP/IEC 27001:2014 Information Technology. Security Techniques. Information Security Management Systems. Requirements 2nd Edition",
- Open Government Action Plan (Open Data Plan AGA) 2015-2016
- Compliance of the Electronic Government Domestic Politics 2013 – 2017
- Personal Data Protection Law N° 29733
- Digital Signatures and Certificates Law N° 27269
- Law N° 29985 of Electronic Money as a financial inclusion tool

Local governments are bound by the current regulations to:

- Formulate the electronic government plan
- Establish the e-government structures needed to render U-services
- Implement the controls needed for U-services that require digital signatures and certificates for citizen authentication.
- Identify personal data sources held and managed by local governments, and comply with data privacy regulations.
- Set up an information security management system (ISMS) in accordance with ISO 27001 and ISO 27002 standards.

E. Applications involved in U-government in Peru

The nature of mobile applications involved in local government U-services in Peru is basically intended to load and report tax information, property tax, and information about traffic offenses. Only a few are focused on *payment transaction* of taxes, local duties, traffic offenses and the like. However, there exist regulations aimed at gradually increasing transactions by using, for example, electronic money in which mobile devices will serve as payment wallets for these procedures.

All these mobile services imply use, storage, handling and traffic of data of a personal nature, all of them regulated in Peru since 2013. Personal data-handling organizations are responsible for implementing – and stating their status as such – a series of ISO 27002 security controls, whereas governmental organizations must establish ISMS based on ISO 27001.

Nevertheless, the methodological gap identified shows lack of a suitable implementation guide for controls and good information security practices required for said cases [15], [16].

The proposed framework intends to fill this gap for U-services, which are part of more complex e-government organizational structures.

III. PROPOSED FRAMEWORK

A. Framework's General Structure

The framework has been divided into four parts:

- Stakeholders' needs
- Alignment matrix between business goals and information security goals for U-services supporting business goals.
- Information Security Process reference model (ISPRM) containing the relevant information security domains for the applications included in the U-services, and for the respective compliance, in light of the previous regulations.

- Current process implementation guide in the ISPRM.

The following paragraphs detail each of these components.

B. Stakeholders' Needs

In this case, by making an analogy with the COBIT 5.0 presentation, we can establish up to five related business objectives:

i. Optimize investments
ii. Optimize risks
iii. Comply with current and competent regulations
iv. Optimize resources
v. Satisfy citizens

Corporate and information security goals will be added to the above objectives in the following alignment matrix.

C. Alignment Matrix

The alignment matrix is introduced in two tables whose dimensions are those of the Balance Score Card. Table 1 shows the framework's corporate goals, whereas Table 2 lists the information security goals regarding development and delivery of U-services, which are in line with the business objectives. Letters P and S within the cells containing objectives mean that the goal is directly related to such objective.

Table I provides the 11 corporate goals related to e-Government and, intrinsically, to delivery of U-services. These goals have been adapted from [7]:

1. Value for stakeholders from the investments in e-Government
2. Portfolio of U-services
3. Risks of managed business
4. Compliance of laws and external rules with regard to e-Government
5. Orientation towards citizens
6. Continuity of U-services
7. Optimization of costs in delivery of U-services
8. Optimization of business processes involved in delivery of e-Government services
9. Compliance of internal policies and procedures related to delivery of e-Government services
10. Trained and motivated staff
11. Innovation culture in e-Government services, especially in the U-services

On the other hand, Table II shows the 12 proposed security goals, which have been adapted from [17]:

1. Alignment of the information security towards the business.
2. Contribution of information security to the compliance of e-government related regulations
3. Business risks regarding information security and compliance managed.
4. Top Management's commitment to decision-making related to information security of U-services.
5. Delivery of secure U-services according to business requirements
6. Adequate use of applications and information and other technologies for U-services development.
7. Design of appropriate U-services to citizens' needs
8. Optimization in the use of information, resources and capabilities of ITs in e-government services, especially U-services.
9. Adequate delivery of U-services to meet citizens' needs and compliance of the business requirements.
10. Compliance of security policies and current regulations in U-services
11. Skilled and motivated staff responsible for information security.
12. Knowledge, awareness and training in information security as part of the innovation process in delivery of e-government services.

The *so-called goals cascade* proposed by COBIT in order to conduct the respective alignment between business and security [18] will depend on each particular company and on their services provided as a part of its e-government. The goal cascade is not included in our research for an organization, however we do recommend it.

D. Information Security Process reference model (ISPRM)

As the next component, our research has put forward a series of processes both for government and information security management specific for development, acquisition, and maintenance of U-services.

After a first division by government processes and management processes, four domains of security management have been determined: planning and organization, acquisition and implementation of U-government, delivery of U-services and monitoring of U-services. Below are the definitive processes listed in Table II.

Government Processes:

1. Establish and maintain over time government structures for information security
2. Make sure risk optimization includes information security risks in e-government services
3. Secure resources optimization needed for establishing the information security government and its continuity over time

Management processes of U-Services' information security:

Planning and organization domain:

4. Manage and maintain the information security management framework
5. Prepare and maintain the information security strategy
6. Define the Ubiquitous architecture for services corresponding to e-government.

TABLE I.
CORPORATE GOALS IN EUFRAME-SECURITY

Balance Score Card Dim.	Corporate Goal	Obj i.	Obj ii.	Obj iii.	Obj iv.	Obj v.
Financial	1. Value for stakeholders from e-Government Investments	P			P	
	2 . U-services portfolio	S			P	P
	3. Managed risks		P	S	S	
	4. Compliance with laws and regulations related to external e-Government			P		
Client	5. Citizen orientation			S		P
	6. U-services continuity	S		P	P	S
	7. Cost optimization providing U-services	P		S	P	S
Internal	8. Optimization of business processes involved in provision of e-Government			S	P	S
	9. Compliance with internal policies and procedures related to provision of e-Government			P	S	S
Learning and knowledge	10. Personal prepared and motivated		P	S	P	
	11. Culture of innovation in e-Government services and in particular in the U-services		P	S	P	S

TABLE II
GOALS RELATED TO INFORMATION SECURITY IN EUFRAME-SECURITY

Balance Score Card Dim.	Information Security Goal	Obj i.	Obj ii.	Obj iii.	Obj iv.	Obj v.
Financial	1. Alignment of the information security towards the business	P			P	
	2. Contribution of information security to the compliance of e-government related regulations		S	P	S	
	3. Business risks regarding information security and compliance managed		P	P	S	
	4. Top Management commitment to decision-making related to information security of U-services	S			P	S
Client	5. Delivery of secure U-services according to business requirements		S	S	P	P
	6. Adequate use of applications and information and other technologies for U-services development		S	S	P	P
Internal	7. Design of appropriate U-services to citizens' needs		S	S	P	P
	8. Optimization in the use of information, resources, and capabilities of ITs in e-government services, especially U-services.	S			P	S
	9. Adequate delivery of U-services to meet citizens' needs and compliance of business requirements.			S	P	P
	10. Compliance of security policies and current regulations in U-services		S	P	S	
Learning and knowledge	11. Skilled and motivated staff responsible for information security		P	S	P	
	12. Knowledge, awareness and training in information security as part of the innovation process in delivery of e-government services		P	S	P	S

7. Manage U-services portfolio
8. Manage service level agreements (SLA) of U-services
9. Manage information security risks in U-services
10. Manage risks of non-compliance in U-services
11. Manage information security in the process of designing, developing, acquiring, and maintaining U-services within the e-government.

services based on this type of aplications. The list of procedures is as follows:

Governance procedures for the implementation of government processes[4].

- Define information security policies
- Determine the people responsible for the information security across all the organization

TABLE III
INFORMATION SECURITY PROCESS REFERENCE MODEL (ISPRM)

Government	1. Alignment of the information security towards the business	Monitoring U-services
	2. Contribution of the information security to the compliance of the e-government related regulations	19. Assess performance of U-services
	3. Business risks regarding information security and compliance managed	20. Assess compliance of information security regulations of U-services
Planning and Organization	4. Manage and maintain the information security management framework	Acquisition and implementation of U-government
	5. Prepare and maintain the information security strategy	12. Manage U-services implementation projects
	6. Define the Ubiquitous architecture for the services corresponding to the e-government	13. Define information security requirements at e-government structure level with emphasis on U-services
	7. Manage U-services portfolio	14. Manage availability and capacity of U-services
	8. Manage service level agreements (SLA) of U-services	15. Manage information assets taking part in U-services
	9. Manage information security risks in U-services	Delivery de los U-services
	10. Manage risks of non-compliance in U-services	16. Manage appropriate operation of U-services
	11. Manage information security in the process of designing, developing, acquiring, and maintaining U-services within the e-government	17. Manage problems and incidents of security with U-services
18. Manage continuity of U-services operations		

Acquisition and implementation of U-government domain:
12. Manage U-services implementation projects
13. Define information security requirements at e-government structure level with emphasis on U-services
14. Manage availability and capacity of U-services
15. Manage information assets taking part in U-services

Delivery of U-services Domain:
16. Manage appropriate operation of U-services
17. Manage problems and incidents of security with U-services
18. Manage continuity of U-services operations

Monitoring of U-services Domain
19. Assess performance of U-services
20. Assess compliance of information security regulations of U-services.

E. Implementacion Guide

The guide provides a series of procedures to implement the above listed processes. Our proposal focuses on transaction mobile applications dealing with information of a personal nature (Personally identifiable information – PII o Sensitive Personal Information - SPI), that is why proposed procedures lay emphasis on security and compliance of

- Conduct a risk management methodology at an organizational level, including information security risks.
- Determine the people in charge of conducting the risk analysis including information security risk analysis.
- Incorporate the resources deemed necessary into the budget to establish and maintain the information security government
- Prepare the electronic government plan
- Define e-government structures necessary for delivery of U-services
- Adjust e-government structures to comply with the Peruvian National Police of the 2013 – 2017 Electronic Government.

Below are the procedures for management processes within the security Planning and Organization domain:

- Define a framework for the information security management within the e-government structures.
- In the business strategy and information technology plans define information security

[4] Each procedure may include a series of related projects to be executed and in doing so achieve a complete related process(s)

strategies for e-government structures and services.
- Define U-services as a part of the e-government plan.
- Set up a management mechanism for IT services including U-services.
- Conduct the risk analysis including information security risks of U-services.
- Define Peru's Open Government Action Plan (Open Data Plan AGA) for 2015-2016
- Design an information security management system (ISMS) in accordance with ISO 27001 and ISO 27002 standards in order to comply with the mandatory use of the Peruvian Technical Standard "ISO NTP/IEC 27001:2014 Information Technology. Security Techniques. Information Security Management Systems. Requirements 2nd Edition"

Below are the procedures for management processes within the Acquisition and Implementation of U-government domain:
- Define a framework for projects management of acquisition, implementation, and deployment of U-services.
- Define information security requirements for outsourcing, which supply service assets of U-services or complete delivery.
- Identify personal data sources held and managed, and comply with data privacy regulations.
- Define security requirements and those responsible for compliance of Personal Data Protection Law N° 29733.
- Implement security controls needed for U-services requiring use of signatures and digital certificates for citizen's authentication.
- Define security requirements and those responsible for compliance of Digital Signatures and Certificates Law N° 27269.
- Define security requirements and those responsible for compliance of Law N° 29985 of Electronic Money as a financial inclusion tool.
- Maintain service level related to availability and capacity of U-services.
- Mantain service assets involved in delivery of U-services.

Below are the following procedures for management processes within the Delivery of U-services domain:
- Deliver U-services.
- Set up a help desk for incidents and problems management of the information security of e-government services, including U-services.
- In the business continuity plans and information technologies continuity plans include procedures to maintain continuity of U-services deemed critical.

Finally, below are the procedures for management processes within the domain Monitor U-services,:
- Set up and maintain an internal control system.
- Define metrics and performance indicators of U-services.
- Define metrics and satisfaction indicators of citizens in the use of U-services.
- Conduct measurements of all metrics and indicators of U-services.
- Identify non-compliance of information security within U-services.

F. Good Practices in the Implementation Guide

The guide is based on a series of good practices in which ISO 27000 standards are the most important ones. Table 4 shows the mapping among the above proposed procedures for each domain in line with clauses of the ISO 27002 standard [19].

IV. CONCLUSIONS

The lack of frameworks for the implementation of information security governments results in non-compliance of relevant regulations by local and municipal governments, above all in data privacy matters.

The proposed eUframe-security framework provides a basic guide for consolidating the information security government, thus filling the procedural gap to address the U-government needs.

Next step (which is part of the future work of this paper) is to establish a testing mechanism to validate the model.

Table IV
Mapping ISPRM procedures versus ISO 27002

Domains	Implementación Guide Procedures	Clauses ISO 27002
Government	· Define information security policies.	**5**
	· Determine the people responsible for the information security across all the organization.	**6**
	· Conduct a risk management methodology at an organizational level, including information security risks.	**6**
	· Define the people in charge of conducting the risk analysis including information security risk analysis.	**6**
	· Incorporate the resources deemed necessary into the budget to establish and maintain the information security government	**6, 7, 8**
	· Prepare the electronic government plan	**6**
	· Define e-government structures necessary for delivery of U-services	**6**

	· Adjust e-government structures to comply with the Peruvian National Police of the 2013 – 2017 Electronic Government.	**6**
Planning and Organization	· Define a framework for information security management within e-government structures.	**5, 6**
	· In the business strategy and information technology plans define the information security strategies for e-government structures and services.	**6**
	· Define U-services as a part of the e-government plan.	**6**
	· Set up a management mechanism for IT services including U-services.	**6**
	· Conduct the risk analysis including information security risks of U-services.	**6**
	· Define Peru's Open Government Action Plan (Open Data Plan AGA) for 2015-2016	**6**
	. Design an information security management system (ISMS) in accordance with ISO 27001 and ISO 27002 standards in order to comply with the mandatory use of the Peruvian Technical Standard "ISO NTP/IEC 27001:2014"	**5-18**
Acquisition and implementation	· Define a framework for projects management of acquisition, implementation and deployment of U-services.	**8, 14, 15**
	· Define information security requirements for outsourcing which supply service assets of U-services or complete delivery.	**7, 14, 15**
	· Identify personal data sources held and managed, and comply with the data privacy regulations.	**8, 9, 10**
	· Define security requirements and those responsible for compliance of Personal Data Protection Law N° 29733.	**18**
	· Implement security controls needed for U-services requiring use of signatures and digital certificates for the citizen's authentication.	**18**
	· Define security requirements and those responsible for the compliance of Digital Signatures and Certificates Law N° 27269.	**18**
	· Define security requirements and those responsible for compliance of Law N° 29985 of Electronic Money as a financial inclusion tool.	**18**
	· Maintain service level related to availability and capacity of U-services.	**12**
	. Maintain service assets involved in delivery of U-services.	**8, 12**
Delivery	**· Deliver U-services.**	**12**
	· Set up a help desk for incidents and problems management of the information security of e-government services, including the U-services.	**12, 16**
	. In the business continuity plans and information technologies continuity plans include the procedures to maintain continuity of the U-services deemed critical.	**17**
Monitoring	**· Set up and maintain an internal control system.**	**18**
	· Define metrics and performance indicators of U-services.	**18**
	· Define metrics and satisfaction indicators of citizens in the use of U-services.	**18**
	· Conduct measurements of all metrics and indicators of U-services.	**18**
	. Identify non-compliance of information security within U-services.	**18**

REFERENCES

[1] H. Ranaweera, "Perspective of trust towards e-government initiatives in Sri Lanka", *SpringerPlus*., vol. 5, no 22, pp. 1-11, 2016. http://dx.doi.org/10.1186/s40064-015-1650-y

[2] J. Batlle-Montserrat, J. Blat, and E. Abadal, "Local e-government Benchlearning: Impact analysis and applicability to smart cities benchmarking," *Information Polity*., vol. 21, pp. 43-59, 2016. http://dx.doi.org/10.3233/IP-150366

[3] P. Pitchay Muthu Chelliah, R. Thurasamy, A. I. Alzahrani, O. Alfarraj, and N. Alalwan, "E-Government service delivery by a local government agency: The case of E-Licensing Telematics and Informatics", vol. 33, pp. 925-935, 2016. http://dx.doi.org/10.1016/j.tele.2016.02.003

[4] A. Ramtohul, and K. M. S. Soyjaudah, "Information security governance for e-services in southern African developing countries e-Government projects", *Journal of Science and Technology Policy Management*., vol. 7, pp. 26-42, 2016. http://dx.doi.org/10.1108/JSTPM-04-2014-0014

[5] R. Kennedy and H. J. Scholl, "E-regulation and the rule of law: Smart government, institutional information infrastructures, and fundamental values", *Information Polity*., vol. 21, pp. 77-98, 2016. http://dx.doi.org/10.3233/IP-150368

[6] L. G. Anthopoulos and C. G. Reddick, "Understanding electronic government research and smart city: A framework and empirical evidence", *Information Polity*., vol. 21, pp. 99-117, 2016. http://dx.doi.org/10.3233/IP-150371

[7] ISACA, COBIT 5.0 *For Information Security*. ISACA Publishing, USA, 2012.

[8] J. Krumm, *Ubiquitous Computing Fundamentals*. Chapman and Hall/CRC, USA, 2009.

[9] A. Anttiroiko, "Towards Citizen-Centered Local e-Government – The Case of the City of Tampere", *Idea Group Publishing*, vol. 6, pp. 370–372, 2004. http://dx.doi.org/10.4018/978-1-59140-259-6.ch021

[10] J. Joo and A. Hovav, "The influence of information security on the adoption of web-based integrated information systems: an e-government study in Peru", *Information Technology for Development*, vol. 22, pp. 94-116, 2016. http://dx.doi.org/10.1080/02681102.2014.979393

[11] B. W. Wirtz and O. T. Kurtz. "Determinants of Citizen Usage Intentions in e-Government: An Empirical Analysis", *Public Organization Review*, pp. 1-20, 2016. http://dx.doi.org/10.1007/s11115-015-0338-7

[12] G. Sangeetha and L. Manjunatha Rao, "Modelling of E-governance framework for mining knowledge from massive grievance redressal data", *International Journal of Electrical and Computer Engineering*, vol. 6, pp. 367-374, 2016. http://dx.doi.org/10.11591/ijece.v6i1.9019

[13] A. Djeddi and I. Djilali, "A user centered ubiquitous government design framework", *ACM International Conference Proceeding Series*, 2015. http://dx.doi.org/10.13140/RG.2.1.4890.6000

[14] B. Schneir, "Ubiquitous Surveillance and Security [Keynote]", IEEE Technology and Society Magazine, vol. 34, no. 7270448, pp. 39-40, 2015. http://dx.doi.org/10.1109/MTS.2015.2461232

[15] A. Asquer. "E-government, M-government, L-government: Exploring future ICT applications in public administration", Public Affairs and Administration: Concepts, Methodologies, Tools, and Applications, 2015, vol. 4, pp. 2155-2168. http://dx.doi.org/10.4018/978-1-4666-8358-7.ch11

[16] K. Malladi, S. Sridharan and L. T. Jayprakash, "Architecting a large-scale ubiquitous e-voting solution for conducting government elections", International Conference on Advances in Electronics, Computers and Communications, ICAECC 2014, no. 7002445, 2015. http://dx.doi.org/10.1109/ICAECC.2014.7002445

[17] E. Mello and J. Souza Neto, "A Governance and Management Model for the Public Sector Shared Services Center Based on COBIT 5". COBIT Focus, ISACA Publishing, no. 3, on site http://www.isaca.org/COBIT/focus/Pages/a-governance-and-management-model-for-the-public-sector-shared-services-center-based-on-cobit5.aspx?utm_campaign=ISACA+Main&cid=sm_1202172&utm_content=1460055833&utm_source=facebook&utm_medium=social&appeal=sm, 2016.

[18] K. Maes, P. De Bruyn, G. Oorts and P. Huysmans, "On the Imperative Solicitude for Evolvability Evaluation in Value Management", International Journal of IT/Business Alignment and Governance (IJITBAG), vol. 5, pp. 70-87, 2014. http://dx.doi.org/10.4018/ijitbag. 2014070104

[19] nternational Organization for Standardization, ISO/IEC 27002:2013, Information technology – Security techniques – Code of practice for information security management, Switzerland, 2013.

[20] S. Alghamdi, N. Beloff, "Exploring Determinants of Adoption and Higher Utilisation for E-Government: A Study from Business Sector Perspective in Saudi Arabia", 10th Conference on Information Systems Management, ISM 2015, vol. 5, pp. 1469 – 1479, 2015. http://dx.doi.org/10.15439/2015F257.

[21] P. Chatzoglou, D. Chatzoudes, S. Symeonidis, "Factors affecting the intention to use e-Government services", 10th Conference on Information Systems Management, ISM 2015, vol. 5, pp. 1489–1498, 2015. http://dx.doi.org/10.15439/2015F171

[22] S. Alghamdi, N. Beloff, "Towards a Comprehensive Model for E-Government Adoption and Utilisation Analysis: The Case of Saudi Arabia", 9th Conference on Information Systems Management, ISM 2014, vol. 2, pp. 1217–1225, 2014. http://dx.doi.org/10.15439/2014F146

[23] G. Wangen, E. A. Snekkenes, "A Comparison between Business Process Management and Information Security Management", 1st Workshop on Emerging Aspects in Information Security, EAIS 2014, vol. 2, pp. 901 – 910, 2014. http://dx.doi.org/10.15439/2014F77