

## **Theme 1: “IT Governance and Audit Methodologies”**

Recent rapid development of new IT technologies was followed up by an instantaneous integration of them at the organizational level. The management of the enterprises faces a new challenge: structural redefinition of the IT segment in order to create plus value and to minimize IT risks through an efficient management of all IT resources of the organization. These changes have had a significant impact on the governance of the IT departments.

### **Scientific task:**

- (1) Examination of existing auditing methodologies for the IT Governance at the organizational level.
- (2) The evaluation of existing research references on the risks associated with IT Governance, as a key process in planning the audit mission that allows for the identification of the segments with increased risks.

### **Preliminary literature:**

1. Mirela GHEORGHE, “Audit Methodology for IT Governance”, *Informatica Economica*, Vol. 14 No. 1/2010, Issue Topic: Informatics Audit.  
<http://revistaie.ase.ro/53.html>
  2. G. Hardy, “The Role of the IT Auditor in IT Governance,” *Information Systems Control Journal*, 2009.
- 

## **Theme 2: “Service Oriented Architecture and Audit Techniques for its Services”**

The Service Oriented Architecture (SOA) approach enables development of flexible distributed services. Auditing such services implies several specific challenges related to interoperability, performance and security.

### **Scientific task:**

The recherché, analysis and systematization of scientific literature on:

- (1) Emphasizing the quality attributes and potential risks in SOA applications that an architect should be aware when designing a distributed system;
- (2) Identifying the key risk factors and models for risk evaluation;
- (3) The reasons for auditing SOA applications, as well as the most important standards;
- (4) The steps for a successful audit process.

### **Preliminary literature:**

1. Liviu COTFAS, Dragoş PALAGHIŢĂ, Bogdan VINTILĂ, “Audit Techniques for Service Oriented Architecture Applications”, *Informatica Economica*, Vol. 14 No. 1/2010, Issue Topic: Informatics Audit.  
<http://revistaie.ase.ro/53.html>
  2. Young-Gab Kim, Dongwon Jeong, Soo-Hyun Park, Jongin Lim, and Doo-Kwon Baik. 2007. Modeling and Simulation for Security Risk Propagation in Critical Information Systems. In *Computational Intelligence and Security*, Yuping Wang, Yiu-Ming Cheung, and Hailin Liu (Eds.). Lecture Notes In Artificial Intelligence, Vol. 4456. Springer-Verlag, Berlin, Heidelberg 858-868.
  3. S. Senft and F. Gallegos, *Information Technology Control and Audit*, 3rd ed., CRC Press, 2009.
- 

## **Theme 3: “eBusiness Services and Information Security Auditing”**

eBusiness is different than other business because it involves any commercial or business activities that takes place by means of electronic facilities, including on the Internet, proprietary networks and home banking, instead of through direct physical exchange or contact. This system creates an environment that operates at a much greater speed than traditional methods and involves much less

paper-based evidence of activities. However, the eBusiness related risks should not be considered in isolation but rather as a part of the overall internal control framework of an entity.

#### **Scientific task:**

The recherche, analysis and systematization of scientific literature on:

- (1) identifying and assessing the risks associated with an eBusiness environment;
- (2) managerial eBusiness strategies those identify and address risks;
- (3) eBusiness Information Systems (IS) audit as a critical component of the eBusiness plan;
- (4) risk analysis for eBusiness applications in order to establish the IS audit particularities in this field.

#### **Preliminary literature:**

1. Floarea NĂSTASE, Pavel NĂSTASE, Robert ȘOVA, "Information Security Audit in e-business applications", *Informatica Economica*, Vol. 11 No. 1/2007.  
<http://revistaie.ase.ro/41.html>
  2. Carlin and F. Gallegos. *IT Audit: A Critical Business Process*. IEEE Computer, 40(7):87–89, 2007.
- 

### **Theme 4: "Auditing Cloud Computing"**

The use of cloud computing is rapidly expanding all over the world at an amazing pace because of its tangible benefits in cost reduction of IT services by obtaining them over the Internet.

Possible advantages are quite obvious: ability to reduce capital expenditure, share the services ensuring massive, often seemingly unlimited scalability, the ability to dial up usage or pay as you use and when required, reduce IT related expenses and thereby enhance competitive advantage along with bottom line. In a typical cloud service model, External Service Provider (ESP) offers various IT services to the business, depending on the Service Level Agreement (SLA) and selection of services.

#### **Scientific task:**

Examination, evaluation and systematization of methodical literature on:

- 1) *Risk management* - Though cloud computing services have unique advantages, there are critical issues relating to confidentiality, data integrity, security, availability, disaster preparedness, tax implications and other risks. Most of these challenges arise out of loss of physical control over IT assets and services. Internal audit needs to evolve from its traditional passive role of looking at internal control and compliance issues to a proactive role of a strategic value advisor.
- 2) *Role of audit* – Information System Audit should help in planning and organizing, acquisition and implementation, delivery and support, monitoring and evaluation of technology selection, regulatory compliance, selection and performance of third party service providers and suppliers and contract compliance. Information system audit checks should be used to test confidentiality, data integrity, availability, security, authentication, reliability etc. It should take increasing responsibility and ensure value addition in key strategic domains such as brand protection, mergers and acquisitions, customer relations, cost reduction and revenue maximization, fraud detection, control and prevention, data governance and quality, keeping in pace with rapidly changing business environment and the way business is carried out in a cloud service environment. Audit should focus on value addition by supporting strategic initiatives, providing high quality business insights as an integral part of the process and should also actively involve in continuous monitoring, evaluation and improvement of control environment and regulatory compliance.
- 3) *Tech infrastructure* - Important audit concerns are focused on creation and maintenance of a technology infrastructure plan in alignment with IT strategic and tactical plans based on technology direction, contingency arrangement, and direction for acquisition of technology resources. Internal audit should also focus on critical business concerns while adopting a cloud computing strategy such as classification of data on the basis of sensitivity and criticality of business, security issues along with legal and privacy implications, formulation of appropriate cloud policies and procedures, retrieval of data, disaster management and identification of

services which can be depended on the cloud without serious business risk. In nutshell, auditing should evolve as a value adding, assurance providing, consulting activity, based on objective, independent evaluation of control environment, systems and procedures and continuously monitoring for improving governance process and risk management to help the organization accomplish its business objectives.

#### **Preliminary literature:**

1. Jeremy Rissi, Sean Sherman, Ben Halpert, "Cloud-Based IT Audit Process", book chapter, Ben Halpert book "Auditing Cloud Computing - A Security and Privacy Guide", John Wiley & Sons, 2011.
  2. S. Pearson, "Taking account of privacy when designing cloud computing services", Software Engineering Challenges of Cloud Computing (CLOUD'09), ICSE Workshop on, 23-23 May Vancouver, BC, 2009.
- 

#### **Theme 5: "eServices Security Audit"**

The eServices security audit target consists of complex applications that function as eBusiness systems. In general such applications are tested from the external perspective. Typical eServices security auditing in different areas:

- eBanking - The eBanking services audit is applied to typical online banking applications at the application layer. Included by default in the scope of auditing are PIN / TAN (including iTAN / mTAN), HBCI, BTX (also with newer interfaces), common web-based systems, mobile banking. The auditing is performed from all available perspectives (e.g. simulating that the potential attacker would be a client, another bank, employee, contractor, etc.). Applicable areas:
  - e-Banking Services Audit / Anonymous Perspective
  - e-Banking Services Audit / Anonymous & User Perspectives
  - Fake Services Audit for e-Banking
  - Client System Audit
- eTrading / eInsurance / eCommerce / Generic eBusiness - the selected auditing covers the particular aspects of the online trading, online insurance and eCommerce platforms. The audit must cover practically any possible type of online services both internal and external ones:
  - e-Business Services Audit / Anonymous Perspective
  - e-Business Services Audit / Anonymous & User Perspectives
  - Fake Services Audit for e-Business
- eGovernment - the same functional services as for other complex application environments, customized to fit the target selection, with the addition of structuring the procedures and reporting as required by governmental regulations (federal / local state legal and procedural requirements):
  - eGovernment Services Audit / Anonymous Perspective
  - eGovernment Services Audit / Anonymous & User Perspectives

#### **Scientific task:**

The recherché, analysis and systematization of scientific literature on the above areas of the eServices Security Audit.

---

#### **Theme 6: "Auditing IT Service Management"**

The Model comprising six sub-areas:

- policies and strategies;
- operation; support;
- external drivers;
- user interaction; and

- impacts on the external environment.

It can be applied in the areas of financial and performance auditing to support comparative evaluations of service management within or across several agencies.

**Scientific task:**

Provide a systematic presentation through the recherche and analysis of scientific literature on the above sub-areas, beginning with a review of the risk factors connected with senior management's roles and responsibilities, give examples of the risk factors associated with service management activities, and provide practical examples of potential risk factors and the impacts they might inflict. Typical risk reduction strategies are also need to be described.

-----

**Theme 7: “Auditing by the Delivery of eGovernment Services”**

Government information and services are increasingly being made available electronically to citizens and businesses via the Internet. This concept is termed eGovernment.

The eGovernment is a major strategic initiative of the government’s information technology (IT) plan. The government’s website, is the portal (single electronic access point) through which eServices can be accessed. The government’s primary method for developing and maintaining eServices is through a self-funded contract with a third party contractor. The contract focuses exclusively on the government market and has established eServices.

An eGovernment service is defined as an application, or series of applications, on the Internet that provides a specific service to a citizen or business. The application(s) are interactive and/or transaction based. This means information is collected or provided by the customer and a service is then delivered (a transaction is completed). The goal of an eService is to provide a start-to-finish solution to the customer. As an example, a citizen seeking a permit or license provides all necessary information, payment is collected, and the state delivers the service including all necessary information and documentation (in this case a permit or license) to the customer. Additional examples are:

- Web systems that allow customers to enter search criteria and then receive information from those systems;
- Filling out a tax form and paying taxes online;
- Purchasing goods and paying for them using an online shopping cart;
- Any service that accepts an electronic payment using the payment portal.

Thus, it is important to audit eGovernment services, also known as eServices, regularly.

**Scientific task:**

The audit work focuses on the government eServices. The auditing objectives are to:

- identify the methods used to provide eServices;
- determine the processes and criteria established to identify, evaluate, and prioritize the development and implementation of eServices;
- review the methodologies used to determine the fees to pay for the self-funded electronic government services.
- determine if controls are in place to measure the success of eServices.

Perform recherche, assessment and categorization of scientific literature on the above objectives/aspects of the eGovernment services auditing.

-----

**Theme 8: “IT auditing software”**

### Auditing Software

Specialized programs that perform a variety of audit functions, such as sampling databases and generating confirmation letters to customers and vendors. It can highlight exceptions to categories of data and alert the examiner to possible error. Audit software often includes a non-procedural language that lets the auditor describe the computer and data environment without detailed programming.

### EDP audit

An analysis of an organization's computer and information systems in order to evaluate the integrity of its production systems as well as potential security cracks.

### EDP auditor

A person who performs an EDP audit within an organization. Such individuals analyze the existing systems and procedures using audit software that samples databases and generates confirmation letters.

### **Scientific task:**

Perform recherche, assessment and categorization of existing or proposed by market auditing software.

### **Preliminary literature:**

<http://www.theiia.org/ITAuditArchive/index.cfm?act=ITAudit.reflibcategory&catid=7>

-----