Information Security Audit in e-business applications

Floarea NĂSTASE, Pavel NĂSTASE, Robert ŞOVA
Academy of Economic Studies, Bucharest

Electronic business (e-business) are different than other business because it involves any commercial or business activity that takes place by means of electronic facilities (buy and selling online), 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. These e-business related risks should not be considered in isolation but rather as part of the overall internal control framework of an entity. It is essential to identify and assess the risks associated with an e-business environment and management should develop an e-business strategy that identifies and addresses risks. The e-business Information Systems (IS) audit is a critical component of the e-business plan. This paper tries to present a risk analysis for e-business applications in order to establish the IS audit particularities in this field.

Keywords: *e-business, risk analysis, IS audit, confidentiality, reliability, integrity, availability.*

1 Introduction

In the competitive world of business, the survival of a company depends on how fast they are able to recognize changing business dynamics and challenges, and respond correctly and quickly. Companies must also anticipate trends, identify new opportunities, transform their strategy, and reorient resources to stay ahead of the competition. The key to succeeding is **information**.

In today's economy, information is the second most important asset apart from human resources. In the knowledge-based economy information is key both as input and output. At first glance, it appears we have a situation that presents tremendous opportunity for e-business: a global communication infrastructure that is very conducive for low cost transmission of information and a global economy that is tending to be highly information-based. However, the potential e-business scenario cannot be realized without a reliable supporting information security framework.

Business intelligence helps a company create knowledge from that information to enable better decision making and to convert those decisions into action. Web services are a key advance that has significantly impacted applications. The word Web in Web services means that all operations are performed using the technology and infrastructure of the World Wide Web. More recently, however, Web services increasingly make use of XML-based protocols and standards, and it is better to think in terms of XML Web services. ebXML is a set of specifications that together enable a modular electronic business framework. The vision of ebXML is to create a single global electronic marketplace where enterprises of any size and in any geographical location can meet and conduct business with each other through the exchange of XML based messages. The direct sponsors of ebXML are OASIS (Organization for the Advancement of Structured Information Standards) and UN/CEFACT (United Nations Centre for Trade Facilitation and Electronic Business). But lots of standards bodies have a finger in the pie, including NIST (National Institute of Standards and Technology) and W3C (World Wide Web Consortium).

Compared to the classical informatics applications, **the e-business applications need further security measures which imply audit methods and IS specific tools**.

Corporate USA scandals, including Enron and Parmalot, have resulted many changes in the **corporate governance** over the last years. The post-Enron business environment is very cleary quite different for IS audit than before. The passage of Sarbanes-Oxley Act of 2002 has focused a lot of attention on the IS audit function and the need for IS auditors in the processes that lead to audit opinions on financial statements. For companies that meet the criteria, the Sarbanes-Oxley regulation requires management to evaluate and monitor the effectiveness of internal control over the financial reporting process. In Europe, the Basle II Committee on Banking Supervision recommends conditions that should be fulfilled, besides the size of capital, to support credit exposures, which improve the management of credit risk, operational risk and the management of information systems through clearly defined requirements. Working through Information System and Control Associations (ISACA), the IT Governance Institute (ITGI) provide an IT governance and control framework incorporating good IT management practices-Control Objectives for Information and related Technology (COBIT).

2. Information security in e-business applications

"The only system which is truly secure is one which is switched off and unplugged, locked in a titanium lined safe, buried in a concrete bunker, and is surrounded by nerve gas and very highly paid armed guards. Even then, I wouldn't stake my life on it....” said Gene Spafford; Director, Computer Operations, Audit, and Security Technology (COAST), Purdue University. Information security is about minimizing the business impact of the unauthorized disclosure, modification, or loss of information assets. In short, total information security is just impossible.

Information assets for e-business applications can be: organization-specific secrets, IT and infrastructure, financial data, personnel and stakeholder details. Security is the confidence that systems are operating as expected and is commonly viewed as the security CIA triad, as in **C**onfidentiality, **I**ntegrity, and **A**vailability.

Analyzing the e-business applications, we can find many types of the security risks. One of them is disruption to the outside world’s view of your organization: web page vandalism, denial of service attacks, reputation damage with trading or research partners, brand damage. From point of view of your internal operations, we can find: viruses and malicious code and violation of data integrity. The second it’s a breach of contractual or regulatory responsibilities, such as: failure to meet contract commitments, unauthorized disclosure of confidential personal details. Also, we can find many thefts and frauds and the loss of competitive information, intellectual capital and corporate secrets.

The attack is coming from corporate internet connections, including: Internet gateways, email gateways, connections managed by 3rd parties, remote dial-in connections, trading portals or Extranets, Wireless networks. In general, the web-based applications are less secure than the network on which they sit and the attacks cannot be prevented by traditional controls such as firewalls.

Information security governance can be defined as the process of establishing and maintaining a framework and supporting management structure and processes to provide assurance that information security strategies are aligned with and support business objectives, are consistent with applicable laws and regulations through adherence to policies and internal controls, and provide assignment of responsibility, all in an effort to manage risk.

The key activities that facilitate such integration are strategic planning, organizational design and development, establishment of roles and responsibilities, integration with the enterprise architecture, and documentation of security objectives in policies and guidance (Figure 1). There are two models of information security governance structures: centralized and decentralized. Completely centralized or decentralized information security governance implementations are quite rare. In reality, the variety of implemented information security governance structures spans the continuum from a centralized structure at one end to a decentralized structure at the other.

Information security policy is an aggregate of directives, rules, and practices that pre-

scribes how an organization manages, protects, and distributes information. Information security policy is an essential component of information security governance and based on a combination of appropriate legislation, and standards, such as NIST Federal Information Processing Standards (FIPS) and guidance; and internal e-busıness requirements. Information security policy should address the fundamentals of information security governance structure, including:

- Information security roles and responsibilities;
- Statement of security controls baseline and rules for exceeding the baseline; and
- Rules of behavior that users are expected to follow and minimum repercussions for noncompliance.

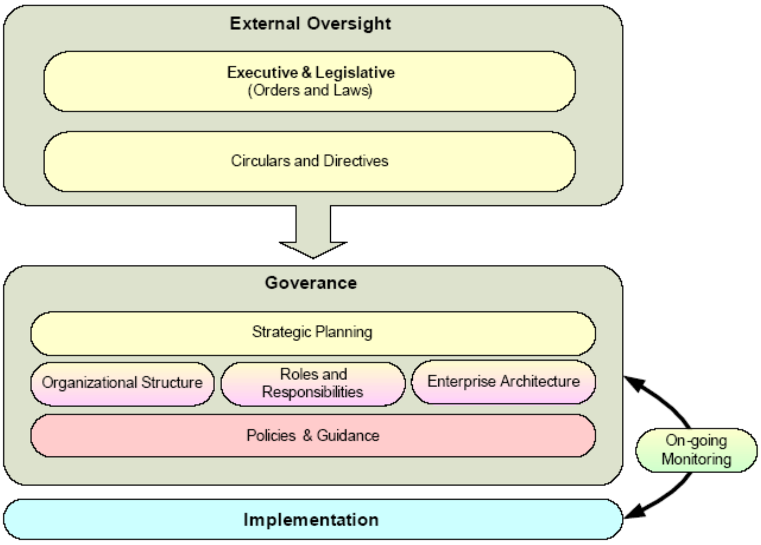

Fig.1. Information Security Governance Components (Source [1])

Thereby, the process of designing and deploying an information security infrastructure is a continuous process of analysis, design, monitoring, and adaptation to changing needs. All security architectures start with defining the business context, that being the balance of business drivers and acceptable risk. This business context is the result of decisions made from the analysis of internal and external factors. Security policies are the guidelines for this business context. The resulting architecture is a functional combination of process and technology to achieve the business goal within boundaries of the business context. The architecture must fit this business context for the enterprise to achieve security, and to provide legal and regulatory complian. The method for architecting secure solutions methodology was designed after careful evaluation of security standards, such as BS7799 and the Common Criteria. These standards represent internationally accepted "best practices" for design and measurement of security, but do not specify specific technologies or products.

Common Criteria provide a taxonomy for evaluating security functionality through a set of functional and assurance requirements. The Common Criteria include 11 functional classes of requirements: security audit, communication, cryptographic support, user data protection, identification and authentication, management of security functions, privacy, protection of security functions, resource utilization, component access and trusted path or channel.

3. Risk Assessment for e-business applications

National Institute of Standards and Technology (NIST) defines risk as, "a function of the likelihood of a given threat-source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization." The goal of the risk assessment process is to identify and assess the risks to a given environment. To meet the goal of the risk assessment, a six-step process is defined in NIST SP 800-30 (Figure 2).

The *system characterization* describes the following individual system components: hardware, software, external interfaces to other systems, data, system functional requirements, organizational security policy and architecture, system network topology, information flows throughout the system, security controls (management, operational, and technical), physical and environmental security mechanisms.

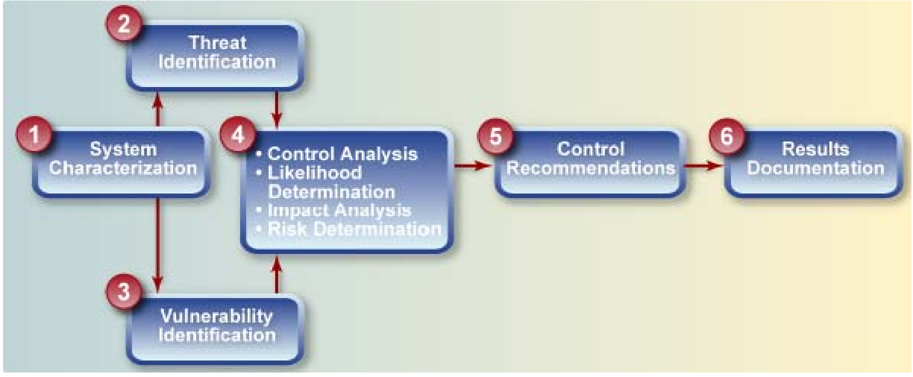

Figure 2. Risk Assessment Process (Source [1])

Threat identification consists of identifying threat sources with the potential to exploit weaknesses in the system. There are common threat sources that typically apply, regardless of the system, that should be evaluated and can be categorized into three areas: natural threats (e.g., floods, earthquakes, tornadoes, landslides, avalanches, electrical storms), human threats (intentional or unintentional), and environmental threats (e.g., power failure).

NIST SP 800-30 defines *vulnerability* as “a flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system’s security policy.” Vulnerabilities can be identified using a combination of a number of techniques and sources.

The *risk analysis* is a determination (or estimation) of risk to the system, an analysis that requires the consideration of closely interwoven factors, such as the security controls in place for the system under review, the likelihood that those controls will be either insufficient or ineffective protection of the system, and the impact of that failure. Risk analysis involves assessing what could go wrong, how likely it is to occur, and what damage results from that event. Elements to analyze include:

- *Threats*: The events, forces or persons that pose the risk. This could be an event to exploit a vulnerability;
- *Probability*: The likelihood this threat would occur;
- *Damage*: The impact of the threat being exploited. This includes loss of service, revenue, potential revenue, and image among and other business specific elements;
- *Trade-offs*: Evaluating two competing business drivers and evaluating the advantages and disadvantages of each to reach a compromise solution. A common technique to analyze these trade offs is a business impact analysis.

The level of risk to the system and the organization can be derived by multiplying the ratings assigned for threat likelihood (e.g., probability) and threat impact. Table 1 shows how to calculate an overall risk rating using inputs from the threat likelihood and impact categories. Many techniques exist for identifying and analyzing risks and determining mitigation. Guidance is needed as to the areas to consider when working towards a security policy. This guidance is often found in the British Standard 7799 (BS7799). Although there might be other ways of addressing enterprise security, we take a closer look at BS7799 to present the enormous scope of this task. The British Standard 7799 is the most widely recognized security standard in the world.

Table 1. Risk Level Matrix

	Impact		
Thread Likelihood	**Low (10)**	**Moderate (50)**	**High (100)**
High (1.0)	10 x 1.0 = 10	50 x 1.0 = 50	100 x 1.0 = 100
Moderate (0.5)	10 x 0.5 = 5	50 x 0.5 = 25	100 x 0.5 = 50
Low (0.1)	10 x 0.1 = 1	50 x 0.1 = 5	100 x 0.1 = 10
Risk Scale: High (>50 to 100) Moderate(>10 to 50) Low (1 to 10)			

The goal of the *control recommendations* is to reduce the level of risk to the information system and its data to a level the organization deems acceptable. These recommendations are essential input for the risk mitigation process, during which the recommended procedural and technical security controls are evaluated, prioritized, and implemented.

The selection and employment of appropriate security controls for an information system is an important task that can have major implications on the operations and assets of an organization. There are three general classes of security controls: management, operational and technical. Each family contains security controls related to the security function of the family. Table 2 summarizes the classes and families in the security control.

Table 2. Security Control Classes and Families

Class	Family
Management	Risk Assessment
	Planning
	System and Services Acquisition
	Certification, Accreditation, and Security Assessments
Operational	Personnel Security
	Physical and Environmental
	Contingency Planning
	Configuration Management
	Maintenance
	System and Information Integrity
	Media Protection
	Incident Response
	Awareness and Training
Technical	Identification and Authentication
	Access Control
	Audit and Accountability
	System and Communications Protection

Security services fall into one of three categories (Table 3):

- *Management Services*: Techniques and concerns normally addressed by management in the organization’s computer security program. They focus on managing the computer security program and the risk within the organization.
- *Operational Services*: Services focused on controls implemented and executed by people (as opposed to systems). They often require technical or specialized expertise and rely on management activities and technical controls.
- *Technical Services*: Technical services focused on security controls a computer system

executes. These services are dependent on the proper function of the system for effectiveness.

Table 3. Security services by category

Category	Security Service
Management	Security Program
	Security Policy
	Risk Management
	Security Architecture
	Certification and Accreditation
	Security Evaluation of IT Products
Operational	Contingency Planning
	Incident Handling
	Testing
	Training
Technical	Firewalls
	Intrusion Detection
	Public Key Infrastructure

For an e-business application the risks can be:

- *Business environment risks* (e.g. competitors, regulatory issues, stakeholder and user expectations)
- *Operational risks* (e.g. brand, HR, process realignment, fulfilment, provision of service to users)
- *Financial risks* (e.g. settlement, tax, currency, cost, return on investment)
- *Technology risks* (e.g. design, performance, availability, and security)

4. Auditing e-business security

The IS audit is performed on the basis of the general framework assured by the Information Systems and Control Associations (ISACA), which consist of a set of standards, guidelines and procedures and in conformity with the ISACA Code of Professional Ethics.

There are 3 key areas for auditing e-business security:

- Development of new e-business operations which consist in:
  - Assurance over effective identification and management of risks;
  - Timely reviews of proposed security architecture;
  - Pre-release penetration testing.
- e-business in service which consist in:
  - Assurance over development and change management controls;
  - Reviews of monitoring controls and escalation procedures;
  - Ongoing vulnerability reviews and penetration tests.
- Outsourced operations depending on right of audit over outsourced providers, e.g. hosting organisations.

IS auditors often evaluate IT functions and systems from different perspectives, such as security (confidentiality, integrity and availability) quality (effectiveness, efficiency), fiduciary (compliance, reliability), service and capacity. More organizations are moving to **a risk-based audit approach** that is usually adapted to develop and improve the continuous audit process. In this audit approach, IS auditors are not just relying on risk; they also are relying on internal and operational controls as well as on knowledge of the company's business.

The most important controls for auditing e-business security are the following:

Access control policy and procedures: which develops, disseminates, and periodically reviews/updates: a formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

Account management: which manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts.

Separation of duties: the information system enforces separation of duties through assigned access authorizations. The organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals. There is access control software on the information system that prevents users from having all of the necessary authority or information access to perform fraudulent activity without collusion.

Least privilege: the information system enforces the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.

Unsuccessful login attempts: the information system enforces a limit of consecutive invalid access attempts by a user during a time period. The information system automatically delays next login prompt when the maximum number of unsuccessful attempts is exceeded.

System use notification: the information system displays an approved, system use notification message before granting system access informing potential users: that the user is accessing a information system; that system usage may be monitored, recorded, and subject to audit; that unauthorized use of the system is prohibited and subject to criminal and civil penalties; and that use of the system indicates consent to monitoring and recording.

Previous logon notification: the information system notifies the user, upon successful logon, of the date and time of the last logon, and the number of unsuccessful logon attempts since the last successful logon.

Session lock: the information system prevents further access to the system by initiating a session lock that remains in effect until the user reestablishes access using appropriate identification and authentication procedures.

Supervision and review - access control: which supervises and reviews the activities of users with respect to the enforcement and usage of information system access controls.

Remote access: which documents, monitors, and controls all methods of remote access (e.g., dial-up, broadband, Internet) to the information system. Appropriate organization officials authorize each remote access method for the information system and authorize only the necessary users for each access method.

Wireless access restrictions/Access control for portable and mobile devices: which establishes usage restrictions and implementation guidance for wireless technologies/ portable and mobile devices; and documents, monitors, and controls wireless access/device access to the information system.

Audit and accountability policy and procedures: which develops, disseminates, and periodically reviews/updates: a formal, documented, audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.

Auditable events: the information system generates audit records for the events defined by each organization.

Content of audit records: audit records produced by or associated with the information system captures contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.

Audit storage capacity: the organization allocates sufficient audit record storage capacity and configures auditing to prevent such capacity being exceeded.

Audit monitoring, analysis, and reporting: the organization regularly reviews/analyzes information system audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.

Non-repudiation: the information system provides the capability to determine whether a given individual took a particular action.

Contingency plan: the organization develops and implements a contingency plan for the information system addressing contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the system after a disruption or failure. Designated officials within the organization review and approve the contingency plan and distribute copies of the plan to key contingency personnel.

Contingency plan testing: the organization tests the contingency plan for the information system using tests and exercises to determine the plan’s effectiveness and the organization’s readiness to execute the plan.

Alternate storage sites: the organization identifies an alternate storage site and initiates necessary agreements to permit the storage of information system backup.

Alternate processing sites: the organization identifies an alternate processing site and initiates necessary agreements to permit the resumption of information system operations for critical mission/business functions when the primary processing capabilities are unavailable.

Information system backup: the organization conducts backups of user-level and system-level information (including system state information) contained in the information system and protects backup information while in transit and at the storage location.

Information system recovery and reconstitution: the organization employs mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to a known secure state after a disruption or failure.

User identification and authentication: the information system uniquely identifies and authenticates users (or processes acting on behalf of users).

Incident response policy and procedures: the organization develops, disseminates, and periodically reviews/updates: a formal, documented, incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.

Incident handling: the organization implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.

Incident monitoring: the organization tracks and documents information system security incidents on an ongoing basis.

Incident reporting: the organization promptly reports incident information to appropriate authorities.

Application partitioning: the information system separates user functionality (including user interface services) from information system management functionality.

Transmission integrity: the information system protects the integrity of transmitted information.

Transmission confidentiality: the information system protects the confidentiality of transmitted information.

Cryptographic key establishment and management: the information system employs automated mechanisms with supporting procedures or manual procedures for cryptographic key establishment and key management.

Public access protections: for publicly available information and applications, the information system protects the integrity and availability of the information and applications.

Public key infrastructure certificates: the organization develops and implements a certificate policy and certification practice statement for the issuance of public key certificates used in the information system.

Information system monitoring tools and techniques: the organization employs tools and techniques to monitor events on the information system, detect attacks, and provide identification of unauthorized use of the system.

There are several different types of security testing: network scanning, vulnerability scanning, password cracking, log review, integrity checkers, virus detection, war dialing, war driving (802.11 or wireless LAN testing), and penetration testing often.

By example, *penetration testing* is security testing in which evaluators attempt to circumvent the security features of a system based on their understanding of the system design and implementation. The purpose of penetration testing is to identify methods of gaining access to a system by using common tools and techniques used by attackers. Penetration testing should be performed after careful consideration, notification, and planning.

5. Conclusions

In order to minimize the e-business impact of the security risk we can perform the following steps:

- *Understand the risk* using security risk assessment, establish the importance for each type of information asset, set-up differing levels of security are likely to be appropriate for different assets and what would the impact be of disclosure, modification or loss;
- *Promote security awareness* beginning with the executive management at the top of the organization;
- *Implement effective security strategy and policies*: management statement of importance of information and computer security, assignment of roles for: management, the ICT department, users and guests, assignment of responsibilities for: data ownership, education, monitoring, incident response/enforcement, maintenance. In the end must have a good documentation and communication of security administration procedures, standards and guidelines;
- *Define and implement a security architecture* which provides a common basis for agreement on design, development and implementation of the technical and management aspects of information security by all suppliers and users of information resources.

To summarize:

- e-business has dramatically increased the threat to key information assets;
- The incidence of security breaches appears to be increasing, indicating many organizations are not managing the issues effectively;
- New ways of breaching e-business security are arising every day;
- Regularly test for vulnerabilities;
- Internal Risk Management/Internal Audit has a critical role to play in all of these areas;
- Public key cryptography can play an important role in helping provide the needed security services including confidentiality, authentication, digital signatures, and integrity.

References

1. Pauline Bowen, Joan Hash, Mark Wilson, Nadya Bartol, Gina Jamaldinian, Information **Security Handbook: A Guide for Managers**, NIST, 2006

2. Năstase Floarea, Năstase Pavel, **ebXML: a global framework for e-business**, The 3rd International Workshop IE&SI, Editura Mirton, Timişoara, pag. 256-263, ISBN (10) 973-661-870-6 ; ISBN (13) 978-973-661-870-3, 2006

3. Chuck Ballard, Daniel M. Farrell, Amit Gupta, Carlos Mazuela, Stanislav Vohnik, **Dimensional Modeling: In a Business Intelligence Environment**, IBM, 2006

4. Axel Buecker, Juliana Medeiros Destro, Michael Ferrell, Guilherme Monteiro, Erik Wilson, **Enterprise Security Architecture** - *Using IBM Tivoli Security Solutions*, IBM, 2006

5. Ron Ross, Stu Katzke, Arnold Johnson, Marianne Swanson, George Rogers, **Recommended Security Controls for Federal Information Systems**, NIST, Draft 2006

6. Năstase Floarea, 2005, **Web Services Security**, The Impact of European Integration on the National Economy – Business Information Systems, Cluj-Napoca, Editura Risoprint, pag. 387-393, ISBN 373-651-007-0

7. Năstase Floarea, **Information Security in the Digital Age**, Information & Knowledge Age – The Seventh International Conference on Informatics in Economy, Bucharest, Ed. Inforec, pag. 926-932, ISSN 973-8360-014-8, 2005

8. David Hughes, **Electronic Insecurity**, Deloitte, September 2004

9. Tim Grance, Joan Hash, Marc Stevens, Kristofor O'Neal, Nadya Bartol, **Guide to Information Technology Security Services (800-35)**, NIST, 2003

10. http://www.isaca.org - The official ISACA web site

11. http://www.ebxml.org/ - The official ebXML web site

12. http://www.w3.org/Signature/ - XML Signature Working Group

13. http://www.w3.org/Encryption/2001/ - XML Encryption Working Group

14. http://www.oasis-open.org/ - OASIS Web Services Security page