



USAID
FROM THE AMERICAN PEOPLE



INFORMATION TECHNOLOGY (IT) ASSESSMENT GUIDE

FOR

THE EGYPTIAN INSURANCE SUPERVISORY AUTHORITIES

March 1, 2008

This publication was produced for review by the United States Agency for International Development. It was prepared by Ron Bergeron

INFORMATION TECHNOLOGY (IT) ASSESSMENT GUIDE

FOR

THE EGYPTIAN INSURANCE SUPERVISORY AUTHORITIES

TECHNICAL ASSISTANCE FOR POLICY REFORM II

CONTRACT NUMBER: 263-C-00-05-00063-00

BEARINGPOINT, INC.

USAID/EGYPT POLICY AND PRIVATE SECTOR OFFICE

MARCH 1, 2008

RON BERGERON

DELIVERABLE COMPONENT: B

DISCLAIMER:

The author's views expressed in this publication do not necessarily reflect the views of the United States Agency for International Development or the United States Government.

CONTENTS

	Page
Introduction.....	2
Guidelines Establishing Information Security Standards.....	3
Part 1 – Risk Assessment.....	5
Part 2 – Operations Security and Risk Management.....	6
Part 3 – Audit / Independent Review Program.....	9
Part 4 – Disaster Recovery and Business Continuity Management....	11
Part 5 – Vendor Management and Service Provider Oversight.....	12

A Guide to Conducting an Information Technology (IT) Assessment During On-Site Examination¹

Introduction

This document contains questions covering significant areas of a company's information technology (IT) function. The responses to these questions will help provide insight into the composition of the company's IT operations, information security program, and IT governance processes; and will be relied upon to form conclusions as to the condition of the company's IT functions and to the residual risk related to this activity. Examiners will need to review IT supporting documentation (i.e. policies, procedures and plans) to assess the quality and content of the company's IT operations and information security, and IT governance programs.

While the majority of the questions require only a "Yes" or "No" response, **you are strongly encouraged to expand or clarify any response as needed directly below each question.** Copy of supporting documentation e.g. reports to the Board of Directors should be attached to this section note. In addition, additional comments can be included in this document near the end under the heading "Clarifying or Additional Comments." For any question deemed non-applicable to the company's institution or if the answer is "None," please respond accordingly ("NA" or "None"). Please do not leave blank responses.

¹ Most of the material contained in this document was extracted from the USA - FDIC Examination Manual re. **Instructions for Completing the Information Technology Officer's Questionnaire**, revised and transformed into a guideline for EISA supervisors to assess a company's IT infrastructure and process while doing on-site examination work.

Guidelines Establishing Information Security Standards

I. Standards for Information Security

- A. Information Security Program. A company should implement a comprehensive **written** information security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the company and the nature and scope of its activities. While all parts of the company are not required to implement a uniform set of policies, all elements of the information security program should be considered.
- B. Objectives. A company's information security program should be designed to:
1. Ensure the security and confidentiality of customer information;
 2. Protect against any anticipated threats or hazards to the security or integrity of such information;
 3. Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer; and
 4. Ensure the proper disposal of customer information and consumer information.

II. Development and Implementation of Information Security Program

- A. Involve the **Board of Directors**. The Board of Directors or an appropriate committee of the Board of a company should:
1. Approve the company's written information security program; and
 2. Oversee the development, implementation, and maintenance of the company's information security program, including assigning specific responsibility for its implementation and reviewing reports from management.
- B. Assess Risk.
A company should:
1. Identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems.
 2. Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information.
 3. Assess the sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks.
- C. Manage and Control Risk. A company should:
1. Design its information security program to control the identified risks, commensurate with the sensitivity of the information as well as the complexity and scope of the company's activities. A company should consider whether the following security measures are appropriate for the company and, if so, adopt those measures the company concludes are appropriate:
 - a. Access controls on customer information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing customer information to unauthorized individuals who may seek to obtain this information through fraudulent means.
 - b. Access restrictions at physical locations containing customer information, such as buildings, computer facilities, and records storage facilities to permit access only to authorized individuals;
 - c. Encryption of electronic customer information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access;

d. Procedures designed to ensure that customer information system <u>modifications</u> are consistent with the company's information security program;
e. <u>Dual control</u> procedures, <u>segregation of duties</u> , and <u>employee background checks</u> for employees with responsibilities for or access to customer information;
f. Monitoring systems and procedures to <u>detect</u> actual and attempted <u>attacks</u> on or <u>intrusions</u> into customer information systems;
g. <u>Response programs</u> that specify actions to be taken when the company suspects or detects that unauthorized individuals have gained access to customer information systems, including appropriate reports to regulatory and law enforcement agencies; and
h. Measures to protect against <u>destruction, loss, or damage</u> of customer information due to potential <u>environmental hazards</u> , such as fire and water damage or technological failures.
2. <u>Train staff</u> to implement the company's information security program.
3. Regularly <u>test the key controls</u> , systems and procedures of the information security program. The frequency and nature of such tests should be determined by the company's risk assessment. Tests should be conducted or reviewed by <u>independent</u> third parties or staff independent of those that develop or maintain the security programs.
4. Develop, implement, and maintain, as part of its information security program, appropriate <u>measures to properly dispose</u> of customer information and consumer information in accordance with each of the requirements of this paragraph.
D. Oversee Service Provider Arrangements. A company should: <ol style="list-style-type: none"> 1. Exercise appropriate due diligence in selecting its service providers; 2. Require its service providers by contract to implement appropriate measures designed to meet the objectives of these Guidelines; and 3. Where indicated by the company's risk assessment, monitor its service providers to confirm that they have satisfied their obligations as required by paragraph D.2. As part of this monitoring, a company should review audits, summaries of test results, or other equivalent evaluations of its service providers.
E. <u>Adjust the Program</u> . A company should monitor, evaluate, and adjust, as appropriate, the information security program in light of any relevant changes in technology, the sensitivity of its customer information, internal or external threats to information, and the company's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to customer information systems.
F. Report to the Board . A company should report to its board or an appropriate committee of the Board at least <u>annually</u> . This report should describe the overall <u>status</u> of the information security program. The report, which will vary depending upon the complexity of a company's program should discuss material matters related to its program, addressing issues such as: <u>risk assessment</u> ; <u>risk management</u> and <u>control decisions</u> ; <u>service provider arrangements</u> ; <u>results of testing</u> ; <u>security breaches or violations</u> , and <u>management's responses</u> ; and recommendations for changes in the information security program.

PART 1 – RISK ASSESSMENT

An IT risk assessment is a multi-step process of identifying and quantifying threats to information and IT infrastructure in an effort to determine cost effective risk management solutions. The following is a series of questions that should be raised with the IT manager:

- a. Name and title of individual(s) responsible for managing the IT risk assessment process:
- b. Names and titles of individuals, committees, departments or others participating in the risk assessment process. If third-party assistance was utilized during this process, please identify the name and address of the firm providing the assistance and a brief description of the services provided:
- c. Does the company have a written information security program? Does the company's written information security program include a risk assessment (Y/N)? Get a copy of the information security program.
- d. Does the company have an adequate level of knowledge, expertise and qualification to manage and safeguard the IT infrastructure, information and data (Y/N)?
- e. Is the IT budget adequate given the nature, complexity, scope and risk profile of the company (Y/N)?
- f. Does the scope of the company's risk assessment include an enterprise-wide analysis of internal and external threats and vulnerabilities to confidential customer and consumer information; the likelihood and impact of identified threats and vulnerabilities; and the sufficiency of policies, procedures, and customer information systems to control risks (Y/N)?
- g. Does the company have procedures for maintaining asset inventories (i.e. software and hardware) and identifying customer information at the company, in transit, and at service providers (Y/N)?
- h. Do risk assessment findings clearly identify the assets requiring risk reduction strategies (Y/N)?
- i. Do written information security policies and procedures reflect risk reduction strategies for the assets identified in "g" above (Y/N)?
- j. Were changes in technology (e.g. service provider relationships, software applications, and/or service offerings) implemented since the previous examination reflected in the company's risk assessment (Y/N)?

If “No,” what technology changes were excluded?

- i. Is the company’s risk assessment *program* formally approved by the Board of Directors at least annually (Y/N)?

If “Yes,” please provide the date that the risk assessment program was last approved by the Board of Directors (check Board minutes).

- j. Has a report of risk assessment *findings* been presented to the Board of Directors for review and acceptance (Y/N)?

If “Yes,” please provide the date that the risk assessment findings were last approved by the Board of Directors (check Board minutes).

- k. Is the company planning to deploy new technology within the next 12 months (Y/N)?

If “Yes,” were the risks associated with this new technology reviewed during the company’s most recent risk assessment (Y/N)?

PART 2 – OPERATIONS SECURITY AND RISK MANAGEMENT

To help assess how the company manages risk through its information security program, the following questions should be addressed. If any of the following questions are not applicable to the environment, simply answer “N/A.”

- a. Does the company have a written information security program designed to manage and control risk (Y/N)?

If “Yes,” please provide the date that the written information security program was last approved by the Board of Directors (check Board minutes).

- b. Does the company’s information security program contain written policies, procedures, and guidelines for securing, maintaining, and monitoring the following systems or platforms:
 - 1. Core company system (Y/N)?
 - 2. Imaging (Y/N)?

3. Payment systems (including wire transfer for premiums collection) (Y/N)?
 4. Voice over IP telephony (Y/N)?
 5. Instant messaging (Y/N)?
 6. Virtual private networking (Y/N)?
 7. Wireless networking - LAN or WAN(Y/N)?
 8. Local area networking (Y/N)?
 9. Wide area networking (Y/N)?
 10. Routers (Y/N)?
 11. Modems or modem pools (Y/N)?
 12. Security devices such as firewall(s) and proxy devices. (Y/N)?
 13. Other remote access connectivity such as GoToMyPC, PcAnyWhere, etc. (Y/N)?
 14. Portable devices such as PDAs, laptops, cell phones, etc. (Y/N)?
 15. Other – please list:
- c. Does the company employ access controls on customer information systems (Y/N)?
- d. Does the company have a physical security program which defines and restricts access to information assets as well as protects against destruction, loss, or damage of customer information (Y/N)?
- e. Does the company encrypt customer information (Y/N)?

If “Yes,” describe where encryption has been implemented.

- f. Does the company’s information security program incorporate dual control procedures, segregation of duties, and employee background checks for employees with responsibilities for, or access to, customer information (Y/N)?
- g. Does the company have formal logging/monitoring requirements for platforms identified in “b” above (Y/N)?
- h. Does the company have a formal intrusion detection program, other than basic logging, for monitoring host and/or network activity (Y/N)?
- i. Does the company have an incident response plan defining responsibilities and duties for containing damage and minimizing risks to itself and customers (Y/N)?

If “Yes,” does the plan include customer notification procedures (Y/N)?

- j. Provide the names and titles and/or committee members charged with formally overseeing and implementing the information security program.

- k. Does the company maintain topologies, diagrams, or schematics depicting the company's physical and logical operating environment(s) (Y/N)?
- l. Does the company have a process in place to monitor and adjust, as appropriate, the information security program (Y/N)?
- m. Does the company have an employee security awareness training program (Y/N)?

If "Yes," please indicate the last date training was provided.

- n. Does the company report the overall status of the information security program and compliance with internal guidelines to the Board or designated committee (Y/N)?

If "Yes," please provide the date that the findings were most recently approved by the Board of Directors. Get a copy of the report.

- o. Does the company's strategic planning process incorporate information security (Y/N)?
- p. Do you have policies/procedures for the proper disposal of customer and consumer information (Y/N)?
- q. Is a formal process in place to address changes to, or new issuance of, laws/regulations and regulatory guidelines (Y/N)?
- r. Has the company experienced any material security incidents (internal or external) affecting the company or company customers since the prior examination (Y/N)?
- s. Are project management techniques and system development life cycle processes used to guide efforts at acquiring and implementing technology (Y/N)?

PART 3 – AUDIT / INDEPENDENT REVIEW PROGRAM

In order to assess how the company monitors operations and compliance with its written information security program, the following questions should be addressed:

- a. Provide the name and title of the IT auditor or employee performing internal IT audit functions (this may include outsourced internal control audits). Include who this person reports to, and a brief description of their education and experience conducting IT audits:

- b. Does the company have a written IT audit/independent review program that is based on the results of a risk analysis (Y/N)?

- c. Provide the following information regarding the company’s most recent IT audits/independent reviews:

	Audit Date	Entity Conducting Audit	Written Audit Report (Y/N)	Audit Committee/Board Review Date
Information Security Program				
IT General Controls Review				
Vulnerability Testing				
Penetration Testing				
Other:				

Get a copy of the audit reports.

- d. Does audit coverage include a comparison of actual system configurations to documented/baseline configuration standards (Y/N)?

- e. Does audit coverage include assessing compliance with the information security program requirements (Y/N)?

- f. Does audit coverage include assessing users and system services access rights (Y/N)?

- g. Are the results of the company's audits/independent reviews used to adjust the company's risk assessment findings/results (Y/N)?
- h. Briefly describe any known conflicts or concentrations of duties:
- i. Does the company have a system for tracking audit and regulatory exceptions to final resolution (Y/N)?

PART 4 - DISASTER RECOVERY AND BUSINESS CONTINUITY MANAGEMENT

To help assess the preparedness for responding to and recovering from an unexpected event, the following questions should be addressed:

- a. Does the company have an organization-wide disaster recovery and business continuity plan (Y/N)?

If “Yes,” please provide the name of the company’s coordinator and get a copy of the disaster recovery plan.

- b. Are disaster recovery and business continuity programs based upon a business impact analysis (Y/N)?

If “Yes,” do the plans identify recovery and processing priorities (Y/N)?

- c. Does the company have formal agreements for an alternate processing site and equipment should the need arise to relocate operations (Y/N)?

- d. Does the company business continuity plans address procedures and priorities for returning to permanent and normal operations (Y/N)?

- e. Does the company maintain offsite backups of critical information (Y/N)?

If “Yes,” is the process formally documented and audited (Y/N)?

- f. Does the company have procedures for testing backup media at an offsite location (Y/N)?

- g. Have disaster recovery/business continuity plans been tested (Y/N)?

If “Yes,” please identify the system(s) tested, the corresponding test date, and the date reported to the Board. Get a copy of the report sent to the Board.

PART 5 – VENDOR MANAGEMENT AND SERVICE PROVIDER OVERSIGHT

Given the increased reliance on outside firms for technology-related products and services, the following questions should be addressed to help assess the effectiveness of the company vendor management and service provider oversight programs:

- a. Does the company’s vendor management program address due diligence, contract provision, financial condition, risk assessment, ongoing monitoring requirements, and third-party relationships such as subcontractors and agents (Y/N)?
- b. Has the company identified and reported its service provider relationships (both domestic and foreign-based) to EISA (Y/N)?

If ‘NO’, identify the location (country) of the service providers.
- c. Are all of the company’s direct or indirect service providers located within Egypt (Y/N)?
- d. Has the company provided risk management policies; performance monitoring and oversight processes; legal and technical expertise; and access to critical, material, or sensitive customer information to address unique risks from these outsourcing relationships (Y/N)?
- e. Do licensing agreements for core processing or mission-critical applications require vendors to maintain application software so that the software operates in compliance with all applicable regulations (e.g. copy right laws) (Y/N)?
- e. Does the company review audits, summaries of test results, and other equivalent evaluations of the company’s service providers to confirm that they are fulfilling contractual obligations to implement appropriate measures designed to meet the objectives of information security standards (Y/N)?

If ‘YES’, get a copy of the last audit.

Clarifying or Additional Comments

Technical Assistance for Policy Reform II
BearingPoint, Inc,
8 EL Sad El Aali Street
18th Floor
Cairo, Egypt
Country Code:
Phone: +2 02 335 5507
Fax: +2 02 337 7684
www.usaideconomic.org.eg