



LAND BANK OF THE PHILIPPINES

ISO 14001 CERTIFIED

Official Depository of the Republic of the Philippines

**BID BULLETIN NO. 1
For ITB No. 2014-4-005**

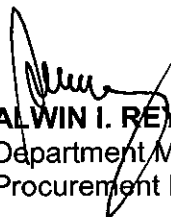
PROJECT : **Enterprise IT Security Risk Assessment and Review of the Bank's Information Security Program**

IMPLEMENTOR : **Procurement Department**

DATE : **October 23, 2014**

This Bid Bulletin is hereby issued for the information and clarification of the participating bidders that the Terms of Reference (TOR) has been revised, particularly on Item 3.5 (Scope of Services), 6.2 (Proposal Submission) and Section 10.A.1 & 10.A.2 (Firm Credentials).

Please see attached revised TOR – Pages 1 to 16.


ALWIN I. REYES
Department Manager
Procurement Department



Land Bank of the Philippines

**Enterprise IT Security Risk Assessment and
Review of the Bank's Information Security Program**

TERMS OF REFERENCE

Version Number : 1.0
Final as of : 04 August 2014
Printed on : 04 August 2014
Author : Head Office and System Technology
Review Department (HOSTAD)
Contact Number : 405-7698
E-mail Address : RVillanueva@mail.landbank.com



1.0 Name and Description of the Project

Enterprise IT Security Risk Assessment and Review of the Bank's Information Security Program

Land Bank of the Philippines, "LANDBANK" or "LBP" is a government financial institution whose banking activities are heavily driven by information technology (IT). The emerging IT security threats and vulnerabilities challenge LANDBANK's system of governance, risk management and controls. Likewise, new regulations from BSP generate the need to assess the current state of the Bank's Information Security Program.

In response to business and regulatory requirements and to provide the Board of Directors and Senior Management of LBP a reasonable assurance that the Bank's IT components are operating in a secured environment and its Information Security Program is adequate and working effectively, an independent assessment with handholding of technology of the Project identified shall be procured from a competent third party service provider.

2.0 Objectives of the Project

The proposed project requires the assistance of a third party to do an independent assessment of the Bank's IT security by undertaking a technical review such as Penetration Testing and Vulnerability Assessment and review of the adequacy and effectiveness of the Bank's Information Security Program. Its primary objectives are the following:

- To identify all existing inherent and potential risks and vulnerabilities related to the Bank's systems, media, devices and facilities (as detailed in Section 3 –Scope of Services);
- To validate the effectiveness and efficiency of the Bank's existing defenses;
- To review the configuration and security of the Bank's Operating System Platforms, Database Storage and Virtualized environment
- To recommend action plans on how to mitigate the identified risks and secure LANDBANK from internal and external intrusions;
- To provide an assessment of the adequacy and effectiveness of the Bank's Information Security Program.
- To handhold/transfer to LANDBANK internal audit personnel the methodology on the review of LANDBANK's Information Security Program to enable them to subsequently perform similar tasks; and
- To conduct presentation to stakeholders of LANDBANK regarding the existing risks facing the bank after the completion of the project.

Internal Audit Group	Version No.: 1.0
Head Office and System Technology Audit Department	Last Revision Date: 15 August 2014



3.0 Scope of Services

1. Penetration testing of the bank's network environment from various access points to be performed by the Penetration Testing (PT) Team independently from the Vulnerability Assessment (VA) Team:
 - Internet
 - Intranet
 - Dial-up (RAS)

2. Vulnerability assessment and review of network, host and database (covering above-noted applications/servers) including at least the following activities:
 - Host Identification – to identify various devices comprising the network and server infrastructure.
 - Server Scan – scanning the type of services and which port they are enabled on the identified "live" devices comprising the network.
 - Information Retrieval – extraction of specific information of the device and service configuration and user information to determine the types of vulnerability pertaining to specific device, service and application as well as identifying the appropriate scanning tools to be used.
 - Vulnerability Scan – using appropriate scanning tools to identify the specific vulnerabilities for each device and systems.
 - Vulnerability Analysis and Validation – careful evaluation of the scanned vulnerabilities and identification of possible vulnerability linkages through a detailed analysis of the results.
 - Assessment of the security configuration - identify specific vulnerabilities in the configuration set up of the Bank's Operating Systems(OS), Database Storage(DB) and Virtualized Environment
 - Risk Analysis – risk analysis on identified vulnerability including its impact, likelihood and the corresponding recommendations to mitigate risk.
 - Manual Review of infrastructure not running on Transmission Control Protocol (TCP) – identify specific vulnerabilities in the Bank's OS, DB not running on TCP. Handholding of technology with IT Auditors of the Bank.

3. Enterprise IT Security Risk Assessment will cover a detailed review of the security risks and control on the following areas:
 - Network Security (data communication, network equipment, architecture design and firewall rules)
 - Platform Security (e.g. Mainframe (IBM Z Series), Linux, AIX, and Windows Systems, Unix)
 - Database Security (Virtual Storage Access Method (VSAM), Oracle and MS SQL)
 - Virtualized Environment Security
 - Internet Security (web server)

Internal Audit Group	Version No.: 1.0
Head Office and System Technology Audit Department	Last Revision Date: 15 August 2014



4. The review will specifically focus on the bank's technology infrastructure that supports the following applications:

- Microsoft Domain Infrastructure and services
- Application Systems Servers
- Web Servers
- Email Server
- External Routers
- Firewalls
- Proxy Servers
- Remote Access Service
- Anti-virus Server
- Domain Name Service
- Database Servers
- Internet Banking Application Servers

5. Review with Handholding of Technology of the Bank's Information Security Program (ISP), the consultants are expected to: (To be done separately after the VA/PT)

1st Week	2nd Week	3rd Week	4th Week	5th Week	6th Week	7th Week	8th Week	9th Week	10th Week	11th Week	12th Week
				VA/PT							
ISP											

- Provide technical training to selected LANDBANK personnel on the audit area prior to commencement of the planning phase of the review/validation. The training shall provide the technical foundation on the fundamentals of the project components to prepare IAG's counterpart teams and the process owners concerned in the project.
- Assess the LANDBANK's ISP on the following areas:
 - The suitability of the Information Security (IS) Management System to the nature and complexity of the Bank's operations
 - IS Governance structure/oversight and support of the Board of Directors and Senior Management
 - IS Risk Management (IS Risk Identification, Assessment, and mitigation/treatment)
 - The adequacy and completeness of the Information Security Program
 - IS Controls Implementation
 - Asset Classification and Control
 - Physical & environmental Protection
 - Security Administration and Monitoring
 - Authentication and Access Controls
 - System Security

Internal Audit Group	Version No.: 1.0
Head Office and System Technology Audit Department	Last Revision Date: 15 August 2014



- Network Security
 - Remote Access
 - Encryption
 - Malicious Code Protection
 - Personnel Security
 - Information System Acquisition, Development and Maintenance
 - Insurance
 - IS Process Monitoring and Updating
 - Activity Monitoring
 - IS Incident Management
 - Ongoing Risk Assessment
 - Communications and Operations Management
 - Business Continuity Management (related to Information Security Program)
 - Regulatory Compliance
- Conduct coaching sessions with the IAG counterpart teams and ensure that there is effective knowledge transfer.

4.0 Deliverables

The winning Bidder shall deliver the following:

1. At the end of the engagement, the winning bidder shall deliver the following:
 - **For Penetration Testing**
 - Executive Summary
 - Details of all attacks undertaken
 - Result of each attack
 - Recommendations on how to mitigate those attacks

 - **For Vulnerability Assessment**
 - Vulnerability Assessment Report (Executive Summary, Conclusion for Management Area, Information Security Roadmap and Specific Action Plan)
 - Security Profiling Results (including reports from automated scanning tools)
 - Handholding of technology with the Bank's IT Auditors of the assessment of configuration and security of the Bank's Operating System (e.g., Mainframe (IBM Z Series), Linux, AIX, and Windows Systems, Unix), Database Storage (VSAM, Oracle, MS SQL) and Virtualized Environment
 - Handholding of technology with the Bank's IT Auditors of the manual review of infrastructure not running on Transmission Control Protocol (TCP) – identify specific vulnerabilities in the Bank's OS, DB not running in TCP.
 - Detailed Observations and Recommendations

<i>Internal Audit Group</i>	<i>Version No.: 1.0</i>
<i>Head Office and System Technology Audit Department</i>	<i>Last Revision Date: 15 August 2014</i>



- For review with handholding of technology of the Bank's Information Security Program

Project Phase	Deliverables for each Component
Training	<ul style="list-style-type: none"> • At least 1-day training sessions • Training Materials • Literatures relevant to the project component • Certificate of Training for all participants
Review/Validation	
<ul style="list-style-type: none"> • Planning 	<ul style="list-style-type: none"> • Risk Assessment and Work Program
<ul style="list-style-type: none"> • Execution 	<ul style="list-style-type: none"> • Audit Procedures/ Review Checklists
<ul style="list-style-type: none"> • Reporting 	<ul style="list-style-type: none"> • Initial Report • Pre-exit conference with Process Owners • Final exit conference with Process Owners • Final Report • Executive Summary for Audit Committee, Risk Management Committee and Senior Management • Presentation to Audit Committee, Risk Management Committee and Senior Management
Handholding /Knowledge Transfer	<ul style="list-style-type: none"> • Handholding/Coaching Sessions • Assessment Report on the effectiveness of the knowledge transfer

2. Winning bidder shall conduct:

- Technical presentation to LANDBANK Project Team regarding the results of the penetration test and vulnerability assessment,
- Presentation of the results of Review of the Bank's Information Security Program,
- High profile presentation of the results of the engagement and orientation of key stakeholders of LANDBANK regarding the existing risks facing the Bank after the completion of the project.

5.0 Documentary Requirements

In addition to those required under Republic Act No. 9184, the technical proposals/bids must include the following required information/documents:

- Detailed Point-by-Point response to Project scope of work, objectives and deliverables
- Draft Contract
- Organizational Chart of the Project
- Project schedule

Internal Audit Group.	Version No.: 1.0
Head Office and System Technology Audit Department	Last Revision Date: 15 August 2014



- Detailed description of all major tasks/milestones
- Deliverable items or resource requirements, if any for each of the major tasks
- Delivery Schedule
- Project Schedule (Major Tasks, duration, start and end dates, Gantt Chart) and project status tracking
- List of Projects and Project Team Information using the Project Team Information Form (Annex A)
- Assumptions (Constraints and Dependencies)
- LBP Responsibilities (Specific responsibilities relating to resources, skills, infrastructure, documentations, processes, etc., that LBP must satisfy)
- Penetration test and vulnerability assessment approach/methodology,
- Information Security Program Review approach/methodology,
- Tools to be used for the engagement
- Exchange of confidential information and other agreements
- Company Profile

6.0 Other Terms and Conditions

1. Proposal Preparation

To be eligible for consideration, the Management Advisory Services Firm must meet all the intent of the scope of work and deliverables. Compliance with the intent of the requirements shall be determined by the LBP HOBAC in accordance with Sections 3.0 and 4.0 of this TOR and on the following:

Point-by-point Response

- The Consulting Firm must submit a point-by-point response to all numbered sections, subsections, appendices, annexes and attachments of the TOR. If no exception, explanation, or clarification is required from its response to a specific item, Consulting Firm shall indicate so in the point-by-point response with the following:

“(Name of Consulting Firm) understands and will comply.”

- It must organize its proposal into sections following the format of this TOR, with tabs separating each section;
- In case its proposal does not comply with the specified proposal format, or is difficult to understand, reads or lacks any of the requested information, the proposal will be returned for immediate revision; and
- Responses similar to “Refer to our literature...” or “Please see www... com” are not acceptable. All materials related to a response must be submitted together with the proposal and not just referenced. Any references in an answer to another location in the TOR materials must indicate the specific

<i>Internal Audit Group</i>	<i>Version No.: 1.0</i>
<i>Head Office and System Technology Audit Department</i>	<i>Last Revision Date: 15 August 2014</i>



page numbers and sections stated in the reference.

2. Proposal Submission

- Consulting Firm must submit three (3) sets (one original and two photocopies) of their technical and financial proposals. The authorized representative(s) of a particular bidder is/are required to sign/initial all the documents for authentication.
- Facsimile or electronic submissions are not acceptable
- Compliance with Laws, Policies, Processes, Regulations and Standards

It must, in performance of work under this contract, fully comply with all applicable national or local laws and executive orders

3. Contract Contents

This TOR and any addenda, Consulting Firm's responses including any amendments, any best and final offers, and any negotiations shall be included in any resulting contract. Section 4.0 enumerates all the required information and documents that it must submit as part of its proposal to qualify for further consideration, and will serve as basis for any contract between LBP and Consulting Firm.

7.0 Project Timeline

The project must be completed within a twelve-week period from the acceptance of Notice to Proceed by the winning bidder. The service provider must therefore provide a project schedule which should show the project milestones and deliverables at each milestone.

All deliverables shall become LANDBANK's property.

8.0 Project Engagement Team (PET)

1. **Number and Structure** – shall be composed of at least seven (7) members, with one Project Manager, one leader and one member for each project component.

Project Manager	
<i>Penetration Testing</i>	<i>Vulnerability Assessment</i>
Leader (1)	Leader (1)
Member/s (at least 1)	Member/s (at least 1)
Handholding Review of the Bank's Information Security Program	
Leader (1)	
Member/s (at least 1)	

Internal Audit Group	Version No.: 1.0
Head Office and System Technology Audit Department	Last Revision Date: 15 August 2014



2. **Minimum Competencies of the members of the Project Engagement Team (PET)-**
The Consultant shall send full-time employees who shall possess the qualifications/core competencies indicated in the Short listing Criteria.
3. The Team Leader to be assigned in the conduct of Review with handholding of the Bank's Information Security Program shall direct/supervise the team to be provided by the Bank to conduct the engagement.
4. The overall Head of the Project Engagement Team must be a Partner of the consultancy firm/Service Provider.
5. The Project Engagement Team shall complete the engagement within the prescribed period. In extreme case where replacement of any of the member is inevitable, the new member must possess the required minimum qualifications/competencies and such replacement shall be subject to the approval of the Head, IAG.

9.0 Approved Budget for the Contract (ABC)

The Approved Budget for the Contract (ABC) is **PHP2,500,000.00** inclusive of value added tax, all applicable taxes and out-of-pocket expenses. It is understood that all charges to remittance of payment shall be for the account of the Vendor.

10.0 Short Listing

1. Hurdle Rate to be met – 70%
2. Short-listing Criteria

ITEMS	WEIGHT	SCORE	MINIMUM REQUIREMENT	DOCUMENT TO BE SUBMITTED
A. FIRM CREDENTIALS	40%			
1. Has been in the business of information security management advisory services for at least 10 years and has completed and/or handled consulting services of size, complexity and technical specialty comparable to proposed project engagement of a Philippine universal/ commercial bank/ATM Consortium. Vulnerability Assessment/ Penetration Testing >5 projects 20% 2-5 projects 15% 1 project 5% 0 project 0%	30%			Certificate of Satisfactory Performance for all completed projects stated in the list to be submitted to LANDBANK (if with previous engagement with LANDBANK, a Certificate



Land Bank of the Philippines
Enterprise IT Security Risk Assessment and
Review of the Bank's Information Security Program
TERMS OF REFERENCE

<p>Information Security Program Review</p> <table style="margin-left: 20px;"> <tr><td>>3 projects</td><td>10%</td></tr> <tr><td>2-3 projects</td><td>5%</td></tr> <tr><td>1 project</td><td>2%</td></tr> <tr><td>0 project</td><td>0%</td></tr> </table>	>3 projects	10%	2-3 projects	5%	1 project	2%	0 project	0%				of Satisfactory Performance signed by the Unit Head shall be submitted)
>3 projects	10%											
2-3 projects	5%											
1 project	2%											
0 project	0%											
<p>2. Has completed and/or currently handling consulting services of size, complexity and technical specialty comparable to proposed project engagement of an international bank or firm. (combination of the 2 types of engagement)</p> <table style="margin-left: 20px;"> <tr><td>>3projects (equal number of engagement, e.g. 2 VAPT/ 2 ISP)</td><td>10%</td></tr> <tr><td>2-3 projects (combination of engagement e.g. 2 VAPT/ 1 ISP)</td><td>5%</td></tr> <tr><td>1 project(any of the engagement)</td><td>2%</td></tr> </table>	>3projects (equal number of engagement, e.g. 2 VAPT/ 2 ISP)	10%	2-3 projects (combination of engagement e.g. 2 VAPT/ 1 ISP)	5%	1 project(any of the engagement)	2%	10%			Certificate of Satisfactory Performance for all completed projects stated in the list to be submitted to LANDBANK		
>3projects (equal number of engagement, e.g. 2 VAPT/ 2 ISP)	10%											
2-3 projects (combination of engagement e.g. 2 VAPT/ 1 ISP)	5%											
1 project(any of the engagement)	2%											
B. PERSONNEL QUALIFICATION AND NUMBER OF PROJECT ENGAGEMENT TEAM	60%											
<p>1. Project Manager (PM) to be assigned to the project is highly qualified to manage the engagement.</p> <table style="margin-left: 20px;"> <tr><td>Exceeds minimum competencies</td><td>15%</td></tr> <tr><td>Meets minimum competencies</td><td>10%</td></tr> <tr><td>Less than the minimum</td><td>0%</td></tr> </table>	Exceeds minimum competencies	15%	Meets minimum competencies	10%	Less than the minimum	0%	15%		<p>PM has performed and managed at least 5 engagements comparable to the proposed engagement and has at least 2 of the following professional certification Certified Information System Security Professional (CISSP),</p>	Certification (i.e. CISA, CISM, CISSP, CEH)		
Exceeds minimum competencies	15%											
Meets minimum competencies	10%											
Less than the minimum	0%											
			<p>Certified Information Systems Auditor (CISA), Certified</p>									



Land Bank of the Philippines
Enterprise IT Security Risk Assessment and
Review of the Bank's Information Security Program
TERMS OF REFERENCE

ITEMS	WEIGHT	SCORE	NOTES	DOCUMENT TO BE SUBMITTED
<p>2. Team Leader (TL) to be assigned to the project is highly qualified to perform the engagement.</p> <p>Exceeds minimum competencies 15% Meet minimum competencies 10% Less than the minimum 0%</p>	15%		<p>Ethical Hacker (CEH), Certified Information Security Manager (CISM)</p> <p>TL has functioned as lead in the performance of at least 4 engagements comparable to the proposed engagement and has at least 2 of the following professional certification CISSP, CISA, CEH, CISM,</p>	Certification (i.e. CISA, CISM, CISSP, CEH)
<p>3. Team Member (TM) to be assigned to the project is highly qualified to perform the engagement.</p> <p>Exceeds minimum competencies 20% Meets minimum competencies 15% Less than the minimum 0%</p>	20%		<p>Each TM has performed at least 3 engagements comparable to the proposed engagement and has at least 1 of the following professional certification CISSP, CISA, CEH, CISM</p>	Certification (i.e. CISA, CISM, CISSP, CEH)
<p>4. Sufficient number of PET to perform the engagement</p> <p>With more than 7 personnel 10% With 7 personnel 5% Less than 7 personnel 0%</p>	10%			



<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td colspan="2" style="text-align: center;">Project Manager</td> </tr> <tr> <td style="width: 50%; text-align: center;">Penetration Testing</td> <td style="width: 50%; text-align: center;">Vulnerability Assessment</td> </tr> <tr> <td style="text-align: center;">Leader (1)</td> <td style="text-align: center;">Leader (1)</td> </tr> <tr> <td style="text-align: center;">Member/s (at least 1)</td> <td style="text-align: center;">Member/s (at least 1)</td> </tr> <tr> <td colspan="2" style="text-align: center;">Handholding Review of the Bank's Information Security Program</td> </tr> <tr> <td colspan="2" style="text-align: center;">Leader (1)</td> </tr> <tr> <td colspan="2" style="text-align: center;">Member/s (at least 1)</td> </tr> </table>	Project Manager		Penetration Testing	Vulnerability Assessment	Leader (1)	Leader (1)	Member/s (at least 1)	Member/s (at least 1)	Handholding Review of the Bank's Information Security Program		Leader (1)		Member/s (at least 1)		
Project Manager															
Penetration Testing	Vulnerability Assessment														
Leader (1)	Leader (1)														
Member/s (at least 1)	Member/s (at least 1)														
Handholding Review of the Bank's Information Security Program															
Leader (1)															
Member/s (at least 1)															
TOTAL	100%														

11.0 Bid Evaluation

1. Bid Evaluation Procedure – Quality-Cost Based Evaluation/Selection
2. Criteria and Rating System

CRITERIA	WEIGHT	RAW SCORE	SCORE	NOTES		
	a	b	ab			
1. TECHNICAL CRITERIA <i>(Firm Credentials, Personnel Competence and Number, and Methodology)</i>	85%					
a. Shortlist Criteria <i>(Firm Credentials, Personnel Competence and Number)</i>	68%			Raw Score based from short listing criteria result.		
b. Methodology Plan of approach and methodology is comprehensive (clear, feasible, timely) <table border="1" style="width: 100%; margin-top: 10px;"> <tr> <td style="width: 70%;"> Criteria: <ul style="list-style-type: none"> Methodology and tools to be used are clearly stated Procedures to be performed are viable, appropriate to the size of the organization </td> <td style="width: 30%; text-align: center; vertical-align: top;">100%</td> </tr> </table>	Criteria: <ul style="list-style-type: none"> Methodology and tools to be used are clearly stated Procedures to be performed are viable, appropriate to the size of the organization 	100%	17%			Methodology will be rated in a collegial manner by the TWG.
Criteria: <ul style="list-style-type: none"> Methodology and tools to be used are clearly stated Procedures to be performed are viable, appropriate to the size of the organization 	100%					



<ul style="list-style-type: none"> Activities are well defined and timelines are explicitly stated and within the timeline of the TOR 											
Not Comprehensive	0%										
2. FINANCIAL CRITERIA (PROJECT COST) The proposed bid price of the participating bidder :			15%								
<table border="1" style="width: 100%;"> <thead> <tr> <th>Condition</th> <th>Raw Score</th> </tr> </thead> <tbody> <tr> <td>Lowest Bid</td> <td>100%</td> </tr> <tr> <td>Other Bids</td> <td>SF</td> </tr> </tbody> </table>		Condition	Raw Score	Lowest Bid	100%	Other Bids	SF				
Condition	Raw Score										
Lowest Bid	100%										
Other Bids	SF										
<p>SF = 100 * FI / F Where: SF – score of bid under consideration FI – price of lowest bid F - price of bid under consideration</p>											
GRAND TOTAL			100%								



TECHNICAL WORKING GROUP

NAME	SIGNATURE
1. REGINA C. VILLANUEVA, HOSTAD	
2. CATHERINE C. CRUZ, HOSTAD	
3. CICERO P. CRUZ, HOSTAD	
4. ARCHIEVAL TOLENTINO, NOD	
5. CARY BRIAN M. SANTOS, DCMD	
6. LOLITA L. SUMAYLO, TMG-ITSO	
7. Atty. JOHN DARWIN C. CUNANAN, LSG	
8. REMEDIOS S. LACADEN, PROCD	
9. MARIA ROSA LORELIE H. CONCEPCION, BRMD	



ANNEX A

**Audit Engagement
 TERMS OF REFERENCE**

**Project Team Information
 (PROJECT ROLE)**

(Surname, First Name, Middle Name)

I. Responsibilities: (Enumerate the details)

II. Educational Attainment:

NAME OF INSTITUTION /SCHOOL	PERIOD OF ATTENDANCE	DIPLOMA/DEGREE/ EQUIVALENT	AWARDS/ DISTINCTIONS RECEIVED

III. Work/Project Experience

JOB TITLE	WORK DESCRIPTION	COMPANY	PERIOD COVERED

IV. Certifications

Certification Title	Year Acquired



V. Proficiency (*Provide certificate and other documents to support your answers*)

1. Number of years of being a constituent partner/employee of the third party service provider.	
2. Number of years of actual experience in providing the proposed project engagement for any institution.	
3. Number of years of actual experience in providing the proposed project engagement for the banking institution.	
4. Number of years of direct involvement or participation in the proposed project engagement in a local universal bank and/or any reputable international bank.	
5. Number of projects with direct involvement or participation in the proposed project engagement for a local universal bank and/or any reputable international bank. (<i>please specify type of participation, e.g. member, TL, PM</i>)	



Response to Request for Information (RFI)

CONSULTING FIRM	COMPANY'S BRIEF DESCRIPTION	ESTIMATED DURATIONS (MONTHS)	CONSULTING FEE
A	Leading Management Advisory Services Company in the field of financial/IT Security audit related services		4.5 - 5.2M
B	One of the major players in the management advisory services and financial/IT Security auditing field.	7 weeks	1.88M
C	One of the major players in the management advisory services and financial/IT Security auditing field.		4.0 - 5.0M