United Nations Development Programme - Iraq

Providing Technical Assistance to Offices of the Inspectors General (OIGs) in Iraq

IT Forensic Audit Capacity Needs Assessment Report

March, 2013

This project has been supported by the US Department of State

Table of Contents

1. Project Introduction and Background 3
2. Executive Brief 5
3. Project Work Constraints 8
4. Project Work Plan 10
5. The Team Involved in the Project 12
6. Methodology and Implementation Mechanism of the Team Implementing the Project 15
7. Outputs and Findings 20
   - 7.1. General Environment and Infrastructure of Information Technology 20
     - 7.1.1. General Assessment for the situation of "General Environment and Infrastructure of Information Technology" in the OIGs 20
     - 7.1.2. Consultants Team Notes on the General Environment and Infrastructure of Information Technology 21
   - 7.2. IT and Computer Forensic Audit 27
     - 7.2.1. General Assessment for the capacities of "IT and Computer Forensic Audit" in the OIGs: 27
     - 7.2.2. Advisory Team notes on the capacities of "IT Audit and Computer Forensic Audit" 28
8. Recommendations and Suggestions 30
   - 8.1. Internal Environment and Infrastructure of IT 30
     - 8.1.1. Main Recommendations: 30
     - 8.1.2. Sub Recommendations 35
   - 8.2. IT & Computer Forensic Audit 41
     - 8.2.1. Main Recommendations 41
     - 8.2.2. Sub Recommendations 45
9. Challenges and Obstacles during Assessment Implementation 53
10. Comments of the Participating Offices 55
11. Lessons Learned 56

1. Project Introduction and Background

Due to the technological development and qualitative leap in modern software and hardware used in the government sector in Iraq after 2003, which were not systematic or controlled in governmental, formal or planned manner. Due to the direct general government to establish, implement and enforce the "Iraqi e-Governance initiative" according to a national strategic action plan, which leads the ministries in their work to use information technology in providing services to citizens in addition to the implementation of their internal tasks and procedures using software applications. For that, it was necessary to anticipate the planned progress in the ministries and to prepare the offices of inspectors general (OIGs) for the implementation of audit and inspection programs specialized in the topics related to Forensics and IT Audit, which made UNDP presents the idea of Assessing the Forensics & IT Audit Capacity Needs, in terms of infrastructure, technological and capacity for the OIGs staff to perform and implement of information technology for such a specialized audit activity in their ministries, organizations and institutions, besides assessing the OIGs staff's training needs in order to improve the concerned specialized audit and inspection team to advanced stages of work, use and employment of information technology in the implementation of qualitative and advanced audit and inspection plans to fight corruption that can occur due to the misuse of information technology (software\ hardware\ networks) in the Iraqi governmental institutions. This can be achieved in a proactively planned manner that ensures the OIGs readiness to face any malfunction or misuse of information technology.

The TOR of the project was set to fit with the overall objective as referred to above, which ordered the conducting consulting firm to implement a field study through which specifies the requirements of developing the OIGs in the field of Forensics and IT Audit, in terms of inputs material resources, scientific and technology inputs and information technology inputs (hardware, software, applications and networks), in addition to propose a curriculum for the training program required to elevate the available human resources in the OIGs and the necessary skills for future phase in the OIGs for the implementation of the IT & Computer Forensic Audit via conducting a general review of the internal environment situation and infrastructure for information technology in the OIGs and the assessment of training needs required by human resources:

(Conducting a Forensics & IT Audit Capacity Needs Assessment)

Particular, this study aims to the following:

1. Study and assess the current situation, including the internal and external environments.
2. Study the internal systematization.
3. Determine the current performance problems.
4. Determine future needs.
5. Gap analysis.
6. Suggest recommendations.
7. Conceptualize infrastructure needed in terms of people, organizational structure, required capacity and how to build, budgets that go with it -as necessary- and the plan of implementation, devices, applications and licenses.

8. Provide these results by organizing a one-day dedicated workshop for 45 OIGs employees in Baghdad (the Iraqi capital).

BDO Jordan Consultants (Moore Stephens – Jordan), within the plan of the project "Provision of Technical Assistance to Iraq Offices of the Inspectors General (OIGs)", it organized –as a part of its activity- field visits to group of OIGs in Baghdad (14 offices) during (8) work days period, in addition to distributing (2) questionnaires via email –in coordination with the 'Office of the Coordinator of Iraqi Prime Minister for Regulatory Affairs'- to the rest of the (33) offices listed in the study sample. That aimed to collect information and assess the OIGs' current situation and to expose the real position of these offices on the ground concerning the conducting of Forensics and IT Audit Needs' Assessment, in terms of infrastructure, technological and capacity for the OIGs staff to perform and implement of information technology for such a specialized audit activity, besides assessing the OIGs staff's training needs in order to improve the concerned specialized audit and inspection team to advanced stages in that domain. On that basis, this report has been prepared to document the study mechanism, methodology, outputs, findings, recommendations and proposals related to developing the scope of information technology in general and Computer Forensic Audit in particular in the Offices of Inspectors General.

2. Executive Brief

Based on the study conducted by the team of IT & Computer Forensic Audit specialized consultants in the OIGs, the team concluded the following:

1. Severe lack of internal infrastructure in most of the OIGs in terms of Organization and Governance and not in terms of hardware and tools used, which directly and apparently affects the mechanism of reports submission and management.
2. Severe lack of the knowledge and technological culture and ways of use and manage it to serve the key tasks of the office. This can be noted in most of the OIGs at the level of operational and planning higher administrations.
3. Actually, there isn't a dedicated audit for "IT and Computer Forensic Audit" in the OIGs. What some teams in some offices do can be called "Technical Audit of IT Procurement", and in some cases it is part of the technical audit of each Ministry according to its function. Some cases that was referred to as IT and Computer Forensic Audit, they was just routine visits to the IT facilities and departments in the Ministries and Entities.
4. The is no coordination between the OIG and IT Department in the Ministry/Entity to acquire periodically updated lists that the ministry can use to record the logs of (Operating Systems, Networks, Applications, Databases, Internet, Programs, Technology used…), which makes the process of auditing the Ministries such a difficult task.
5. Most OIGs hadn't developed any official and standard policies or procedures to include:
    a. IT Audit
    b. Computer Forensic Audit
    c. Incidents and Problems Management
6. Not all OIGs follow the basic steps of IT audit process, which include:
    a. Setting the scope of IT Audit
    b. Inclusion of laws and regulations
    c. Forming of Audit Objectives
    d. Defining the methodology/strategy of Audit
7. Most of the offices do prepare official reports about findings, despite of that we noted the following points concerning the stage of reports preparing:
    a. Most offices do not discuss the findings with the auditee.
    b. Most offices do not have any pre-specified standards to determine the material of findings.
    c. Most offices do not provide the risks related to each of the findings.
    d. Most offices do not suggest recommendations related to each of the findings.
8. Most of the offices do document the achieved work in addition to maintaining the documents. Despite of that, most of the offices do not document the meetings' minutes.
9. Most offices do not follow-up after some time to ensure the treatment of findings.
10. Most offices do not use any tools/applications to assist in accomplish the following:
    a. IT Audit process
    b. Computer Forensic Audit process

11. Some offices do not find dedicated Information Systems auditors to work with them. Furthermore, we noticed the following with respect to some offices that have dedicated Information Systems Auditors:
    a. Not all IT auditors carry scientific certificates relevant to Information Systems.
    b. None of the information systems auditors carry any certificates in the field of information systems audit or information systems security.
    c. Most of the offices didn't developed any training plan for information systems auditors.
    d. Most of the offices do to take evidences on the tasks carried out.
12. Most offices examine the sample rather than the entire audited population.
13. Most offices do not audit the changes in information systems.
14. Most offices do not audit passwords settings.
15. Most offices do not audit logical and physical access operations.
16. Most offices do not audit taking backups of information systems.
17. Most offices do not audit application controls.
18. Most offices do not audit the process of incidents and problems management and have no special team to respond to incidents.
19. Most offices do not urge ministries to capture system logs.
20. Most offices didn't setup procedures that the various parties in the ministry should follow when an accident or malfunction occur.
21. Most offices do not follow stages in the process of Computer Forensic Audit, and these activities include:
    a. Identify information that may constitute evidence of an accident.
    b. Maintaining of information.
    c. Processing and interpretation of evidences.
    d. Showing evidences in a convincing manner.
22. There is no coordination between the Office of the Inspector General and the Department of Information Technology at the Ministry to acquire the periodically updated lists that the ministry rely on to record systems logs (operating systems, networks, applications, databases, Internet, software, technology used ...) and used in the Ministry, which makes the process of auditing the ministries difficult.
23. The need to build a specialized program to generally raise the capabilities and competencies of employees in the IT department and specialists of IT Audit and Computer Forensic Audit process.
24. The staff of OIGs do not focus on collecting internationally accredited certificates, that are specialized in the IT & Computer Forensic Audit field.
25. The need to hold awareness workshops at the leadership and planning level in the OIGs to increase awareness in modern scientific fields of IT Audit and Computer Forensic Audit, which serves the nature of the work and functions of the OIGs.

The detailed report below shows the study carried out by the Advisory Team, and its methodology, outputs, results and recommendations in addition to proposals for developing the scope of IT in general and Computer Forensic Audit in particular for the OIGs.

3. Project Work Constraints

The constraints of the study functions that can affect the path of the Advisory Team can be summarized in the following table:

Constrain	Details
Time Constrains	▪ Project work plan (please refer to the "Project Work Plan" section of this report. ▪ The official work hours of OIGs and availability of concerned employees at that period. ▪ Official holidays at Iraq and Jordan and their effect on the project.
Location/Physical Constrains	▪ Implementing field visits in Baghdad through visiting 14 offices. ▪ Locations of OIGs and taking that in consideration when the team relocates (from and to offices during rush hours). ▪ Implementing analytic study at Amman/Jordan. ▪ Implementing a workshop at Baghdad/Iraq.
Knowledge Constrains	▪ Knowledge level of the Iraqi OIG team of the topics for discussion. ▪ Acceptance level of the Iraqi OIG team of the topics for discussion. ▪ Readiness level of the Iraqi OIG team to adopt the topics for discussion.
Communication Constrains	▪ Level of coordination between UNDP team (Baghdad) and the Office of the Coordinator of Iraqi Prime Minister for Regulatory Affairs. ▪ Level of coordination between UNDP team (Baghdad) and the OIGs. ▪ Level of coordination and consultation between UNDP team (Baghdad) and the team of the Advisory Company. ▪ Level of coordination and consultation between the team of the Advisory Company and the UNDP team in Baghdad and Amman. ▪ Level of OIGs compliance to reply on the Advisory Team questionnaires within the specified time period.
Security Constrains	▪ Security checkpoints to reach for the OIGs. ▪ Difficulties and security precautions that must be considered to reach the OIGs.

Time Constrains

- Project work plan (please refer to the "Project Work Plan" section of this report.
- The official work hours of OIGs and availability of concerned employees at that period.
- Official holidays at Iraq and Jordan and their effect on the project.

Location/Physical Constrains

- Implementing field visits in Baghdad through visiting 14 offices.
- Locations of OIGs and taking that in consideration when the team relocates (from and to offices during rush hours).
- Implementing analytic study at Amman/Jordan.
- Implementing a workshop at Baghdad/Iraq.

Knowledge Constrains

- Knowledge level of the Iraqi OIG team of the topics for discussion.
- Acceptance level of the Iraqi OIG team of the topics for discussion.
- Readiness level of the Iraqi OIG team to adopt the topics for discussion.

Communication Constrains

- Level of coordination between UNDP team (Baghdad) and the Office of the Coordinator of Iraqi Prime Minister for Regulatory Affairs.
- Level of coordination between UNDP team (Baghdad) and the OIGs.
- Level of coordination and consultation between UNDP team (Baghdad) and the team of the Advisory Company.
- Level of coordination and consultation between the team of the Advisory Company and the UNDP team in Baghdad and Amman.
- Level of OIGs compliance to reply on the Advisory Team questionnaires within the specified time period.

Security Constrains

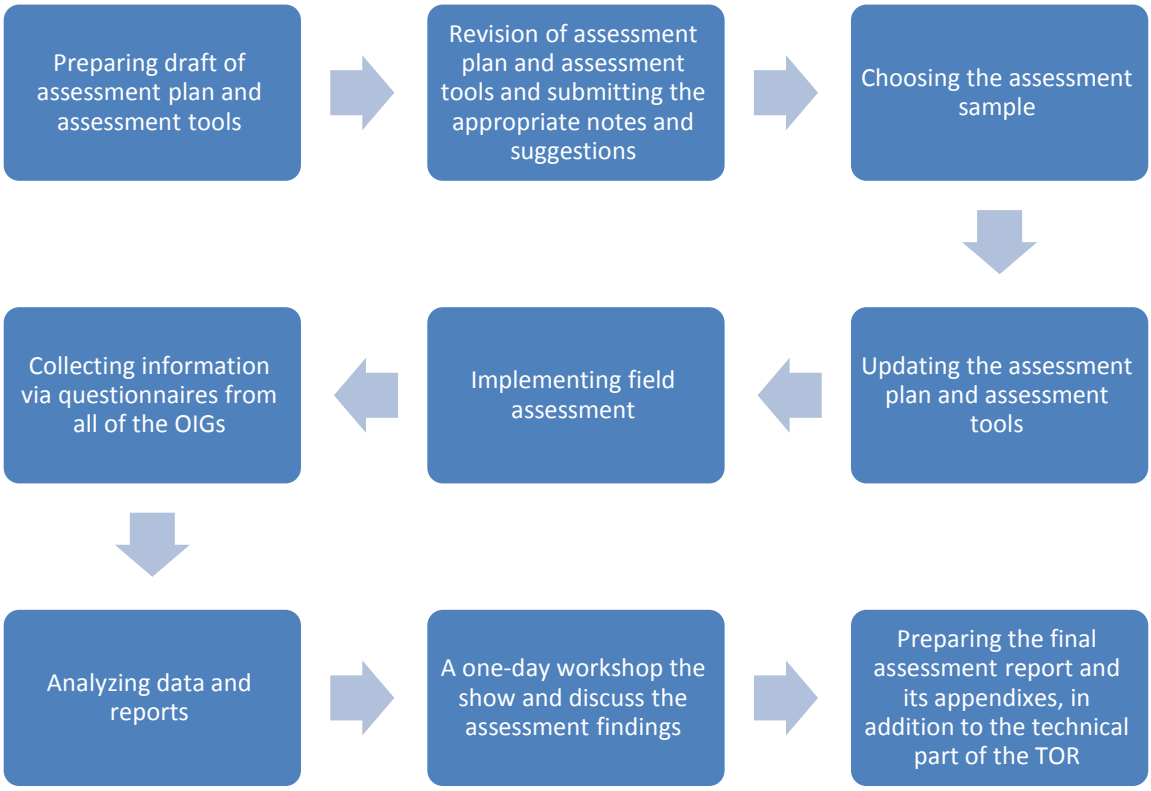
- Security checkpoints to reach for the OIGs.
- Difficulties and security precautions that must be considered to reach the OIGs.

4. Project Work Plan

We have committed to the detailed plan based on the inception report prepared by the Advisory Team and delivered to the UNDP Team, which provided a timetable explaining the team's work plan as detailed in the following table:

Key activities	Outputs	Implementation Responsibility	Timeframe
1. Preparing draft of assessment plan and assessment tools. Assessment tools include: (1) a questionnaire to collect data on the ground from (10) OIGs, (2) a questionnaire sent to the rest of the OIGs and filled by the employee himself/herself.	▪ Assessment plan (Arabic and English). ▪ Tools of collecting data.	BDO Jordan	9/9/2012
2. Revision of assessment plan and assessment tools and submitting the appropriate notes and suggestions.	▪ Notes to develop the assessment plan.	UNDP	15/9/2012
3. Choosing the assessment sample.	▪ List of OIGs titles that will be included by the assessment.	UNDP & BDO Jordan	16/9/2012
4. Updating the assessment plan and assessment tools. Assessment tools include: (1) a questionnaire to collect data on the ground from (15) OIGs, (2) a questionnaire sent to the rest of the OIGs and filled by the employee himself/herself.	▪ Final assessment plan. ▪ Assessment tools.	BDO Jordan	20/9/2012
5. Implementing field assessment.	▪ Field assessment report.	BDO Jordan	1/10/2012 Till 30/10/2012
6. Collecting information via questionnaires from all of the OIGs.	▪ Findings of information collection.		30/10/2012
7. Analyzing data and reports.	▪ Draft of assessment report.	BDO Jordan	10/11/2012
8. A one-day workshop the show and discuss the assessment findings.	▪ Notes of the committee supervising	BDO Jordan	1/12/2012

	the assessment findings.		
9. Preparing the final assessment report and its appendixes, in addition to the technical part of the TOR.	▪ Final assessment report. ▪ Technical part of TOR.	BDO Jordan	15/12/2012



5. The Team Involved in the Project

Name	Specialization	Function
1. Dr. Qasem Ne'washi	Management and Planning	- Project Manager
2. Mr. Rami Samman	Financial Audit	- General Assessment for the capacities of "IT and Computer Forensic Audit" from the Financial perspective. - Design of the training curriculum of the training needs related to the capacities of OIGs concerning "IT and Computer Forensic Audit" from the Financial perspective.
3. Mr. Mazen Shaker	Financial Audit	- General Assessment for the capacities of "IT and Computer Forensic Audit" from the Financial perspective. - Design of the training curriculum of the training needs related to the capacities of OIGs concerning "IT and Computer Forensic Audit" from the Financial perspective.
4. Eng. Mohammad Al-Taji	IT Audit	- General Assessment for the capacities of "IT and Computer Forensic Audit" from the IT Audit perspective. - Design of the training curriculum of the training needs related to the capacities of OIGs concerning

Name	Specialization	Function
		"IT and Computer Forensic Audit" from the IT Audit perspective.
5. Eng. Mohammad Asha	IT Audit	- General Assessment for the capacities of "IT and Computer Forensic Audit" from the IT Audit perspective. - Design of the training curriculum of the training needs related to the capacities of OIGs concerning "IT and Computer Forensic Audit" from the IT Audit perspective.
6. Mr. Reyad Horani	IT Governance Planning	- General Assessment for the situation of "General Environment and IT Infrastructure" in the OIGs. - Suggested design of the typical environment and IT infrastructure in the OIGs.
7. Mr. Ahmad Ibrawish	IT Governance Planning	- General Assessment for the situation of "General Environment and IT Infrastructure" in the OIGs. - Suggested design of the typical environment and IT infrastructure in the OIGs.
8. Mr. Mohammad Nabelsi	Business Analysis & Research	- Statistically analysis of questionnaires.
9. Mr. Ahmad Kablawi	Business Analysis & Research	- Statistically analysis of questionnaires.

Name	Specialization	Function
10. Ms. Nada Nofal	Business Analysis & Research	- Statistically analysis of questionnaires.

6. Methodology and Implementation Mechanism of the Team Implementing the Project

The Consultants Team followed the following axis as a methodology for implementing the project:

Stage	Stage Description	Stage Mechanism
1st	Planning and Coordination	During this phase, action plans and coordination has been developed with the concerned parties related to the project (UNDP team In Baghdad and Amman, the Office of the Coordinator of Iraqi Prime Minister for Regulatory Affairs, offices of inspectors general... etc.), determine the work schedule of the Consultants Team, identify the concerned team and the distribution of roles assigned to each consultant. During this stage, a visit to the Office of Inspector General of the Ministry of Industry and the Ministry of Health was conducted (through August 2012), where -during this visit- general diagnosis was conducted for the situation of information technology in offices and got an overview on the status of IT and Computer Forensic Audit in the both offices. That illustrated the idea of the whole project and the delivery of the project objectives.
2nd	Research and Information Collection	During this stage, we returned to the OIGs and Iraqi Integrity Committee's publications and specifically carried out on the related annual reports, laws, regulations and procedures in-order-to build an overall image of the problems that are addressed in the OIGs, which are close linked to electronic activities and IT information in the ministries. Also, during this stage, we returned to some of the Iraqi, Arab and international printed and published media, whether electronic or paper, to carry on cases and issues related to IT and Computer Forensic Audit that occurred in Iraq, which the OIG played a role in them. During this stage, we conducted a study, assessment and follow-up for the general governmental orientation in Iraq to establish, implement and enforce the "Iraqi e-Governance initiative" through visiting the websites of the initiative and visit the locations of the Iraqi ministries and assessing the electronic services provided to citizens and examine some electronic forms that are available on the Web to learn about the technology used in the ministries and the level of confidentiality and security of information.
3rd	Preparation and Processing	At this stage, assessment tools was built, which include: (1) A form to collect data in the field from (15) OIGs,

Stage	Stage Description	Stage Mechanism
		which is structured as follows: ▪ A special form to assess the risk of internal information systems environment for the OIG ▪ A special form to assess the Computer Forensic Audit of the OIG Where these forms were used during field visits and send it to the rest of the offices via e-mail to be filled by the same office . During this stage, the framework and content list of the first draft of the final report of this study was built.
4th	Field Visits	During this phase, we scheduled visit to 10 offices, but it was agreed with the project management team in the UNDP to increase it to 15 offices, that is to increase the actual field discharge and diagnostic in-order-to be visited during the period between September 17th to September 27th 2012. Actually, 14 office visit were conducted due of an office apology. The visited offices were: 1 - OIG in the Ministry of Commerce 2 - OIG in the Ministry of Human Rights 3 - OIG in the Ministry of Agriculture 4 - OIG in the Ministry of Environment 5 - OIG in the Ministry of Municipalities and Public Works 6 - OIG in the Iraqi Public Authority for transmission and broadcasting services 7 - OIG in the Ministry of Electricity 8 - OIG at the Ministry of Construction and Housing 9 - OIG in the Ministry of Education 10 - OIG in the Ministry of Youth and Sports 11 - OIG in the Ministry of Water Resources 12 - OIG in the Ministry of Planning 13 - OIG in the Ministry of Displacement and Migration 14 - OIG in the Ministry of Oil During these visits, a meeting with the concerned IT team and the forms of the study were filled after giving a detailed

Stage	Stage Description	Stage Mechanism
		explanation of its goals.
5th	Electronic Questionnaires	The above mentioned questionnaires were sent to the rest of the 33 office included in the study via e-mail through coordination with the Office of the Coordinator of Iraqi Prime Minister for Regulatory Affairs. The offices were equipped with guidance for completing the forms, where they received 13 additional forms only until January 1st 2013, which are: 1 - OIG and the Ministry of Industry and Minerals 2 - OIG of the Secretariat of Baghdad 3 - OIG of the Sunni Endowment 4 - OIG and the Ministry of Communications 5 - OIG and the Ministry of Finance 6 - OIG and the Ministry of Transport 7 - OIG Foundation of Political Prisoners 8 - OIG and the Ministry of Communications 9 - OIG Secretariat of Baghdad 10 - OIG of the Hajj and Umrah 11 - OIG and the Department of Justice 12 - OIG and the Ministry of Labor 13 - OIG and the Ministry of Culture The 27 offices out of 33 were approved as final sample to complete the study .
6th	Information Analysis	During this stage, the questionnaires' answers were analyzed by a specialized team as a whole for presentation during the meetings of the results assessment team.
7th	Information Assessment	During this stage to evaluate the results of the questionnaires as a whole from a specialized team out with a list of "outputs and outcomes" for the study. Assessment was based on two perspectives: 1 - Assess the internal situation of the environment infrastructure for information technology in general, and focus on the circle / IT department in the offices of inspectors general in particular, so as to build a general perception of the needs of offices so that it is linked with the assessment of audit services information technology and audit criminal computerized.

Stage	Stage Description	Stage Mechanism
		2 - Assessment audit of It and Computer Forensics provided by the offices of inspectors general.
8th	Building Recommendations	During this stage, the construction and development of recommendations and proposals from a specialized team out with a list of "recommendations and proposals" for the study.
9th	Reporting	During this stage, building for the study (drafts and final copies modified by revisions and amendments).
10th	The Workshop	The submission and review of the study and its results through the organization of a special workshop for one day's 45 employees of OIGs in the Iraqi capital --Baghdad.

Planning and Coordination
Research and Information Collection
Preparation and Processing
Field Visits
Electronic Questionnaires
Information Analysis
Information Assessment
Building Recommendations
Reporting
The Workshop

7. Outputs and Findings

7.1. General Environment and Infrastructure of Information Technology

7.1.1. General Assessment for the situation of "General Environment and Infrastructure of Information Technology" in the OIGs

This part of the study discussed (22) standards from the Assessment Standards of General Environment and Infrastructure of Information Technology. The specialists in the OIGs were requested to answer the questions objectively and transparently. The standards used for this study are the following:

الرقم	المعيار
Standards #1	Supreme Administrative Follow-up of Information Systems
Standards #2	Electronic storage
Standards #3	External supply of IT services
Standards #4	Security of Information Technology
Standards #5	Flow Maps
Standards #6	System capabilities
Standards #7	Separation of information technology functions
Standards #8	The duties and responsibilities of information technology
Standards #9	Protection of confidential passwords
Standards #10	Software packages support
Standards #11	Rapid change in creating information systems and its software
Standards #12	Physical access to information systems and its software
Standards #13	Physical access to the information systems servers and its software
Standards #14	Monitoring of information systems and its software
Standards #15	Backups
Standards #16	Alternative Energy
Standards # 17	Information systems and internal-development software

الرقم	المعيار
Standards # 18	Operating systems
Standards # 19	Protection of information systems and software from virus attacks
Standards # 20	Protection of information systems and software security attacks
Standards #21	Internet use
Standards #22	Internal organization

The results of these standards analysis are detailed in Annex (2).

7.1.2. Consultants Team Notes on the General Environment and Infrastructure of Information Technology

What follows are the most important observations gathered by the Consultants Team of the analyzed data and relying –primarily- on interviews and field visits in the 14 OIGs. These observations are collectively **the most current performance issues** concerning the general environment and internal infrastructure for information technology:

Standard #	Standard	Notes, General Performance Issues and Gaps
Standards #1	Supreme Administrative Follow-up of Information Systems	- The lack of a strategic plan for most offices to employ and develop the information technology in the office within a specified time frame that ensures the performance progress of the office.
Standards #2	Electronic storage	- Official policy of electronic data retention duration is linked to the often paper-based data retention policies followed in the government institutions, although these periods can be increased by virtue of the flexibility and ease of electronic data storage.
Standards #3	External supply of IT services	- Often, there is a dependence on external supply in what is related to Hardware & Software , which may threaten the confidentiality and security of information.
Standards #4	Security of Information	- Severe weakness in the development of a clear strategy for risk and information

Standard #	Standard	Notes, General Performance Issues and Gaps
	Technology	technology incidents management. Since most offices do not have such a plan and existing team is not qualified to develop such plans. (Disaster Recovery Planning)
Standards #5	Flow Maps	- The lack of flow maps in most offices to clarify the mechanism of the information reports flow and its archiving locations.
Standards #6	System capabilities	- The possibility of harnessing the capabilities of current information technology in most of the OIGs in a better and effective way to provide higher quality services and add additional services.
Standards #7	Separation of information technology functions	- The lack of fit between the size of the IT team, the size of the OIG and the nature of the risks of information technology in the office, which negatively reflected on the security and confidentiality and protection of information.
Standards #8	The duties and responsibilities of information technology	- Failure to effectively separate the IT department staff from the staff of the OIG, where it was observed that they perform other functions in most cases. - It was observed that the privileges of IT staff includes entering the transactions to information systems movements or approving it, and sometimes they enter data for other departments, which threatens the integrity of the information entered. - Severe lack of understanding the importance of the Audit Login verifying the security of the system and unauthorized intrusion into the system applications. It was noted that the design of internal programs, are not lending any attention to setting conditions of system security.
Standards #9	Protection of confidential passwords	- Not to change passwords secret) Passwords (Periodically in most offices, which threatens the security of systems in general and the possibility of penetration. - -Lack of policy governing force passwords

Standard #	Standard	Notes, General Performance Issues and Gaps
		secret) Passwords (In most offices, which leads to the existence of porous passwords, which in turn threatens the security systems in general and the possibility of penetration.
Standards #10	Software packages support	- Observed lack of uniformity Types of copies of the software in the office one) Software Version ,(Which makes the support process) Support (And updates) Upgrades (Tough on a team of information technology. - No rights to use the software used within the World Activity Office" Licensing " - Microsoft Office, Adobe, etc. Which is a violation of international laws and regulations, and that this also makes devices porous and unsafe and affect the process of software updates.
Standards #11	Rapid change in creating information systems and its software	- Observed generally very weak in documenting the formal procedures governing the status of the rapid changes and modification in the terms of the consent order specialists and managers to document changes and test the changes, and a commitment to building cycle and the design of information systems (SDLC) Software Development Life Cycle
Standards #12	Physical access to information systems and its software	- The absence of a healthy environment physical access control mechanism to the information systems and software, as observed in most cases it is possible for any person to use devices that contain information systems office.
Standards #13	Physical access to the information systems servers and its software	- The lack of a sound control environment mechanism physical access to the Information systems and software servers, as observed in most cases that the servers found in the office anyone can access them, and not in a private room a special security system for entry. - -In cases where servers found exist in a private room, it was observed not to create room / hall fits well with devices and nature in terms of the lack of air

Standard #	Standard	Notes, General Performance Issues and Gaps
		conditioning to control the high temperatures or special extinguishing systems or servers cabinets… etc.
Standards #14	Monitoring of information systems and its software	- Monitoring of information systems and software is systematic, organized and programmed within approved a formal plan for information technology team. (Business Continuity and Disaster Recovery Plan)
Standards #15	Backups	- Noted that all backups are kept in one place (within the Office of the Inspector General) and not directed by any backups outside the Office of the Inspector, which poses a significant risk of loss of information and the inability team Office of the Inspector to return to this information in cases of fires, explosions, earthquakes, floods and disasters destructive other public. - Policy taking backups in most cases is systematic, organized and programmed within approved a formal plan for information technology team, and it was noted and there is a large variation in the time period to repeat to keep backups between the offices of the inspectors.
Standards #16	Alternative Energy	- Alternative energy system is independent of the alternative energy system in the ministry, which threatens the independence of the work of the Office of the Inspector.
Standards # 17	Information systems and internal-development software	- Observed generally very weak in documenting the formal procedures governing the status of information systems and internal software development in terms of adoption and testing, archiving and documenting the software within a sound methodology for the development of information systems.As noted non-compliance with building cycle and the design of information systems (Software Development Life Cycle) - Severe weakness in **the presence** of **a complementary policy between systems**

Standard #	Standard	Notes, General Performance Issues and Gaps
		<u>and software developed in-house</u> ,where it was noted that no coordination and linkage between the software in general, and are sometimes repeated efforts lead to a repeat of the software.
Standards # 18	Operating systems	- No rights to use operating systems "Licensing , "It is against the international laws and regulations, and that this also makes devices porous and unsafe and affect the process of updates for operating systems.
Standards # 19	Protection of information systems and software from virus attacks	- Protection of information systems and software from virus attacks is a systematic, organized and programmed within approved a formal plan for information technology team. (Business Continuity and Disaster Recovery Plan) - It was noted the absence of prior tests that must be performed by a team of information technology to identify these risks, such as : ▪ Business Impact Analysis (BIA) ▪ Threat and Risk Analysis (TRA)
Standards # 20	Protection of information systems and software security attacks	- Protection of information systems and software from security attacks is systematic, organized and programmed within approved a formal plan for information technology team. (Business Continuity and Disaster Recovery Plan) - It was noted the absence of prior tests that must be performed by a team of information technology to identify these risks, such as : ▪ Business Impact Analysis (BIA) ▪ Threat and Risk Analysis (TRA)
Standards #21	Internet use	- Observed the presence of staff use of the Internet to face in most offices of inspectors general although not a full block in most of the offices unsafe sites on the Internet in the office network, which affects the performance of the network and the possibility of breakthroughs over the Internet.

Standard #	Standard	Notes, General Performance Issues and Gaps
Standards #22	Internal organization	- Significant differences were observed between offices regarding the **level of administrative organization for the IT team in the Office of the Inspector General**) **Unit/ Division/ Department, (and subordination to a team of information technology in EDM … etc.** (Which affects the growth of information technology plans and marginalize its role in strengthening the performance of the office. - Significant differences were observed between offices regarding the **level of administrative organization for the IT team in the Office of the Inspector General**) **Unit / Division/ Department** (**compared to the number of employees who work in the Office of the Inspector General and the number of devices and systems and software supported**. Which affects the level of internal services. - Significant differences were observed between offices regarding the number of IT staff compared to the number of employees who work in the Office of the Inspector General and the number of devices and systems and software supported.Which affects the level of internal services. - Observed great weakness regarding the e-mail system for the Office of the Inspector General, the ministry system is used most often or free email system.Which makes the probability of penetrating the office e-mail and incoming. - Weakness in building an internal network serve and connect all sections of the Office of the Inspector observed the lack of independence of the system in most cases and the use of the ministry system.Which makes the probability of penetrating devices incoming office. - With respect to the Internet system Office of the Inspector General, noted the lack of independence of the system where the system is used ministry in most

Standard #	Standard	Notes, General Performance Issues and Gaps
		cases.Which threatens electronic protection system in the office. - Regarding the internal communication network system Office of the Inspector General, noted the lack of independence of the system where the system is used ministry in most cases.Which makes the probability of penetrating incoming communications office.

7.2. IT and Computer Forensic Audit

7.2.1. General Assessment for the capacities of "IT and Computer Forensic Audit" in the OIGs:

This part of the study addressed 7 assessment areas related to IT and Computer Forensic Audit, where the specialists in the OIGs were asked to answer the questions objectively and full transparently. The assessed areas of this study are the following:

Area #	Area
Area #1	**Overview of Information Systems Audit in the OIGs**
Area #2	**Information Systems Audit - changes management**
Area #3	**Information Systems Audit - logical access**
Area #4	**Information Systems Audit - backup**
Area #5	**Information Systems Audit - controls applied software**
Area #6	**Information Systems Audit - managing emergency incidents and problems**
Area #7	**Information Systems Audit - computer forensics**

The results of these standards analysis are detailed in Annex (2).

7.2.2. Advisory Team notes on the capacities of "IT Audit and Computer Forensic Audit"

The notes below, are the key notes that the Advisory Team collected from the analyzed data based on the interviews, field visits and questionnaires in the OIGs. These notes -as a whole- shape the current main issues of performance concerning the capacities of "IT Audit and Computer Forensic Audit" in the OIGs:

1. Actually, there isn't a dedicated audit for "IT and Computer Forensic Audit" in the OIGs. What some teams in some offices do can be called "Technical Audit of IT Procurement", and in some cases it is part of the technical audit of each Ministry according to its function. Some cases that was referred to as IT and Computer Forensic Audit, they was just routine visits to the IT facilities and departments in the Ministries and Entities.
2. The is no coordination between the OIG and IT Department in the Ministry/Entity to acquire periodically updated lists that the ministry can use to record the logs of (Operating Systems, Networks, Applications, Databases, Internet, Programs, Technology used…), which makes the process of auditing the Ministries such a difficult task.
3. Most of the offices have not developed formal consolidated policies and procedures covering:
   a. IT Audit.
   b. Computer Forensic.
   c. Incident and Problem Management.
4. Not all the offices follow major phases within IT Audit process, such activities are:
   a. Defining IT Audit scope.
   b. Involving laws and regulation.
   c. Formulating audit objectives.
   d. Identifying audit approach/strategy.
5. Most of the offices report the findings in a formal report. However, we noted the following regarding reporting phase:
   a. Most of the offices do not discuss the findings with the auditee.
   b. Most of the offices do not have predefined criteria to specify the materiality of the findings.
   c. Most of the offices do not present risks related to each finding.
   d. Some of the offices do not suggest recommendations related with each finding.
6. Most of the offices document the work performed and maintain the documentation. However, meeting minutes are not being documented by all the offices.
7. Some of the offices do not follow-up after a reasonable time to ensure that the findings have been resolved.
8. Most of the offices do not use tools/software to help accomplish:

a. IT Audit process.

b. Computer Forensic process.

9. Some of the offices do not have dedicated IT Auditors working with them. Moreover, we noted the following regarding some of the offices that have dedicated IT Auditors:

   a. Not all of the IT Auditors hold IT-related certificate.

   b. None of the IT Auditors hold IT Audit / IT Security certificate.

   c. Training plan for the IT Auditors has not been developed for most of the offices.

10. Not all the offices take evidences for their work performed.

11. Not all the offices test sample instead of testing whole population.

12. Most of the offices do not audit IT changes.

13. Most of the offices do not audit the password settings.

14. Most of the offices do not audit the logical and physical access.

15. Most of the offices do not audit the IT backup process.

16. Most of the offices do not audit the application controls.

17. Most of the offices do not audit the Incident and Problem Management process and do not have incident response team.

18. Most of the offices do not force the ministries to capture systems logs.

19. Most of the offices do not have set procedures that different parties should follow once an incident or event occurs.

20. Most of the offices do not follow major phases within Computer Forensic process, such activities are:

   a. Identifying the information that might form the evidence of an incident.

   b. Preserving the information.

   c. Processing and interpret the evidences.

   d. Presenting the evidences in a convincing manner.

8. Recommendations and Suggestions

8.1. Internal Environment and Infrastructure of IT

8.1.1. Main Recommendations:

What follows are the most important observations gathered by the Consultants Team of the analyzed data and relying –primarily- on interviews and field visits in the 14 OIGs. These observations are collectively **the most current performance issues** concerning the general environment and internal infrastructure for information technology:

Standard #	Standard	Recommendations
Standards #1	Supreme Administrative Follow-up of Information Systems	- Holding awareness workshops in the office in the presence of senior management (Inspector, Associate... Etc.) to clarify the importance of information technology and services team can provide office ,and the requirements of the development plans for the team. - Action plan should be developed formal strategy ,supported and documented and clearly defined and enforceable and measurement specific office to employ information technology and development in the office within a specified time frame ensures progress performance of the work of the OIG.And senior management to pursue this plan directly. - Current capacity utilization and development within a comprehensive training plan serves the office internally and computerized audit serves in particular.
Standards #2	Electronic storage	- Develop a formal policy and supported and documented and clearly defined and viable private audit and the duration of storage and retention of electronic data storage periods included high time to exploit the flexibility and ease of electronic data storage and provide the size of the storage and exchange data retention and hardcopy.
Standards #3	External supply of IT services	- Reduce reliance on external supply including about Hardware Maintenance & Software Development As much as possible, and by doing all maintenance work Pal Hardware And build all software Pal Software Internally.
Standards #4	Security of Information	- Develop a formal strategic plan and supported

Standard #	Standard	Recommendations
	Technology	and documented and clearly defined and viable private and measurement of risk management and information technology incidents. (Disaster Recovery Planning)
Standards #5	Flow Maps	- Mapping the flow of specific office to clarify the mechanism of the flow of information reports and places archived.
Standards #6	System capabilities	- Re-inventory software in each of the offices of inspectors general by doing (b Software Inventory (With the aim of re-evaluated in terms of global program standards and a holistic vision of the possibility of harnessing the capabilities of current information technology in every office better and effective way to provide higher quality services and add additional services.
Standards #7	Separation of information technology functions	- Develop a policy fit between the size of the IT team and the size of the OIG and the nature of the risks of information technology in the office, taking into account the security and confidentiality of information and protection.
Standards #8	The duties and responsibilities of information technology	- Separate IT department staff effectively for Career in the OIG, so do not do any other functions not related to information technology. - IT staff are not data-entry and no movements of their powers introduction to information systems or vacationed, and must be dismissed in a clear and official from carrying out such tasks to ensure the integrity of the information you have entered) Integrity of Information(- Training IT staff on the use and recruitment) Audit Log (More effectively to verify the security of the system and unauthorized intrusion into the system applications. - Training IT staff to design programs concerned with the conditions of internal security system) Security.(
Standards #9	Protection of confidential passwords	- Develop a formal, supported, documented, clearly defined and viable for audit especially in changing secret passwords regularly and systematically, which generally increase the systems security and reduces the probability of penetration.

Standard #	Standard	Recommendations
Standards #10	Software packages support	- Develop a formal, supported, documented, clearly defined and viable for audit to unify types of software versions in the one office, Which will contribute to facilitating the process of support and upgrades for the IT team. - Purchase rights to use the international software used within the office activity.
Standards #11	Rapid change in creating information systems and its software	- Develop a formal, supported, documented, clearly defined and viable for audit especially for official procedures that govern the placement of changes and amendments on the system in terms of the consent order specialists and managers to document changes and test the changes, and commitment to building cycle and the design of information systems (SDLC) and approved as a methodology in the process of internal development of information systems and software. (Software Development Life Cycle)
Standards #12	Physical access to information systems and its software	- Building a healthy environment to control physical access to the mechanism of information systems and software, in terms of making software work on the internal network security style allows only authorized users to enter the program and using private Usernames and Passwords.
Standards #13	Physical access to the information systems servers and its software	- Building a healthy environment control mechanism physical access to the Information systems servers and software, and through the allocation of room / lounge private security system especially for entry, and create room / hall well commensurate with existing hardware and nature in terms of the availability of air conditioning to control the high temperatures and systems amortization and private servers cabinets… etc.
Standards #14	Monitoring of information systems and its software	- Develop a mechanism to monitor information systems and software systematic, organized and programmed within approved a formal plan for information technology team. (Business Continuity and Disaster Recovery Plan)
Standards #15	Backups	- Develop a formal policy and supported and

Standard #	Standard	Recommendations
		documented and clearly defined and enforceable and audit control mechanism save backups) Backups (So that it is keeping copies in more than one place and different geographical areas, so that the output of any backups outside the Office of the Inspector, and archiving of secret places safe which significantly reduces the risk of information loss and the inability team Office of the Inspector to return to this information in cases of fires, explosions , earthquakes, floods and other destructive disasters. - Develop a formal policy and supported and documented and clearly defined and enforceable and audit control mechanism taking backups) Backups (So that they are systematic, organized and programmed within approved a formal plan for information technology team and a time frame repeatedly commensurate with the size and seriousness of the information and its importance.
Standards #16	Alternative Energy	- Work as much as possible to build and develop alternative energy system in the offices of inspectors general independently of the alternative energy system in the ministry.
Standards # 17	Information systems and internal-development software	- Develop a formal policy and supported and documented and clearly defined and enforceable and audit documenting official procedures governing the status of information systems and software internal development on the one hand the adoption and testing, archiving and documenting the software within a sound methodology for the development of information systems, and commitment to turn the construction and design of information systems (SDLC) (Software Development Life Cycle) - **Building a complementary policy between systems and software developed in-house** and through coordination and linkage between software in general. - Information systems and internal software development must be within centralized management, so that it is not building the program more than once.

Standard #	Standard	Recommendations
		- Duplication of Systems
Standards # 18	Operating systems	- Purchase rights to use operating systems "Licensing "And within international laws and regulations.
Standards # 19	Protection of information systems and software from virus attacks	- Develop a formal policy and supported and documented and clearly defined and enforceable and checking the protection of information systems and software from virus attacks, so that the policy of systematic, organized and programmed within approved a formal plan for information technology team. (Business Continuity and Disaster Recovery Plan) - Work on the implementation of prior tests that must be performed by a team of information technology office to determine the risk of IT-related information such as: ▪ Business Impact Analysis (BIA) ▪ Threat and Risk Analysis (TRA)
Standards # 20	Protection of information systems and software security attacks	- Develop a formal policy and supported and documented and clearly defined and enforceable and checking the protection of information systems and software from virus attacks, so that the policy of systematic, organized and programmed within approved a formal plan for information technology team. (Business Continuity and Disaster Recovery Plan) - Work on the implementation of prior tests that must be performed by a team of information technology office to determine the risk of IT-related information such as: ▪ Business Impact Analysis (BIA) ▪ Threat and Risk Analysis (TRA)
Standards #21	Internet use	- Blocking full implementation of the unsafe sites on the Internet in the office network. - Prevent personal use of the Internet in the OIG.
Standards #22	Internal organization	- Work to strengthen information technology by strengthening **the organizational level administrative team of information technology in the OIG and the subordination of a team of information technology in the administrative organization**. - Develop a recruitment policy for information technology team to ensure proportionality

Standard #	Standard	Recommendations
		between the number of IT staff team compared to the number of employees who work in the OIG and the number of devices and systems and software supported. - E-mail system for the OIG must be independent and that the system is not used ministry or free email system. - Build an internal network serve and connect all sections of the OIG so as to ensure the independence of the inspector. - Work as much as possible to build and develop the private office system independent of the ministry regarding system online system OIG, and work to find an alternative backup Internet service to ensure technical support in the event of a malfunction in the system of the main Internet. - -Work as much as possible to build and develop the private office system independent of the ministry regarding system communications network system Interior OIG.

8.1.2. Sub Recommendations

8.1.2.1. Administrative Structure

Based on a study conducted by the consultants team and the field visits carried out to 14 OIGs in Baghdad, the consultants team reached a **proposed** management structure for the team of information technology in the offices of inspectors general and shown by the following chart:

Administrative level proposed model for the IT team in the OIG is :**Department of balancing private financial independent of the other sections**

The following table shows explaining and a brief description of the functions and responsibilities of the people proposed in the organizational structure :

Division	Description general administrative proposal
Internet Services Division	- Construction and maintenance of Internet networks, operation and maintenance of the systems for the Internet service in the office (main and backup) and ensure the stability of their work and their efficiency and issue follow-up reports and monitoring their own. - Securing the stability of the Internet service, protection

	and control of any viral attacks or security of all computers connected to the service and address the problems and bottlenecks that reduce efficiency and hinder the stability of the service. - Service Management Office's e-mail " E-mail." - Establish training courses for employees of the office and whenever the need to train and develop their performance at work on Internet browsers, such as programs -)Google Chrome, Internet Explorer (And the use of e-mail "E-mail." - Provide counseling and advice to all employees on the Internet by addressing the problems they face at work immediately. - Participate in the audit and technical committees on the subject of the Internet and its networks and information technology and e-government. - - Design the website of the OIG and continuously updated as needed.
Intranet Services Division	- Establishment, installation and delivery of internal networks of various technologies in the OIG) ,LAN, WAN, ... etc (In addition to video chat systems and computer servers that are running operating systems) Servers (And is supervised, and for the purpose of implementation of data systems and software that operate in a network environment and providing linkages between departments. - Providing design, installation and management and maintenance of the network and activate internal Intranet service by connecting the main office branches nationwide. - Manage users on the internal network and ensure that the powers given to each user and the access to information process on the network. - Provide security and maintain the computer network by using appropriate protective equipment such as firewalls) Firewalls (To ensure the security and protection of information Office, including the network protection from all programs that affect the performance of the network, and work quickly and efficiently, follow the daily work of the network and protection from viruses, and denial of

	service for hackers and Almtzbben Balochteraqat unauthorized network, and follow-up security clearances about working on the network. - Taking backups) Backups (Within the policies pursued in the office. - Follow the technological development in the field of internal networks and keep up with what's new. - Building an integrated wireless network in the OIG as needed and necessary to reach an integrated electronic environment. - - Building networks of telecommunications services internal video and audio in the OIG and connects branches located in the provinces.
Computerized business systems Services Division	Responsible for building, implementing and write software for new systems, as well as the modernization and development programs for existing systems to be developed.
Information Analysis Division	Responsible for systems analysis and give guidance to programmers to directly typing programs after the analysis and design of systems in consultation with the beneficiaries of the programs in the OIG, as well as supervising the progress of implementation (project management and testing.(
Computer Maintenance Services Division	This Division maintenance Servers And personal computers and mobile phones and accessories of all kinds (such as printers, scanner ,power protection devices... Etc (.and maintaining and installing operating systems and software assistance.

8.1.2.2. Human Resources

First :Train current staffs on systematic and targeted programs to serve the strategic plan for the development of Information technology in the OIG in particular, and the Supreme strategic plan for the OIG In general .

Generally, the consultants Team believes that information technology teams should be trained in the OIG on the following topics as part of a special capacity building program, while preserving the privacy sometimes of technology used in the OIGs :

Domain	Domain name	General Description for the	Domain name	General

#	in English	Domain in English	in Arabic	Description for the Domain in Arabic
No. 1	Concepts of Information Systems Analysis & Design	The use, analysis, and design of information systems and technologies to organize, coordinate, and build information systems, including software engineering and business requirements engineering	تحليل وتصميم نظم المعلومات	استخدام وتحليل وتصميم أنظمة المعلومات والتقنيات لتنظيم وتنسيق وبناء أنظمة المعلومات بما في ذلك هندسة البرمجيات وهندسة متطلبات العمل.
No. 2	Concepts of Database Analysis & Design	Introduction to the concept of databases, including the storage, manipulation, evaluation, and display of data, and related issues	تحليل وتصميم قواعد البيانات	مقدمة إلى مفهوم قواعد البيانات، بما في ذلك التخزين والتعديل والتقييم وعرض البيانات وما يتعلق بها من قضايا.
No. 3	Database Administration	(1) Oracle, (2) MySQL and (3) Microsoft SQL Databases Administration skills	إدارة قواعد البيانات	مهارات إدارة قواعد بيانات كل من: Oracle MySQL Microsoft SQL
No. 4	Computer Networking Administration	Introduction to computer network topologies & administration: transmission media, signal modulation, digital packet switching and routing, systems integration, communications management, and security	إدارة الشبكات الحاسوبية	مقدمة إلى هندسة وإدارة شبكات الحاسوب: نقل الوسائط، تحوير الإشارات، تحويل وتوجيه الحزم الرقمية، تكامل الأنظمة، إدارة عمليات الاتصال، والحماية.
No. 5	Computer Network Security	Introduction to computer network security including Communication media, Communications protocols and network programming	أمن وحماية الشبكات الحاسوبية	مقدمة إلى حماية شبكات الحاسوب بما في ذلك وسائط الاتصال، وبروتوكولات الاتصالات، وبرمجة

				الشبكات.
No. 6	IT Project Management	The PMP Certification Course	شهادات عالمية في مجال تكنولوجيا المعلومات موصى بها	دورة شهادة إدارة المشاريع المهنية PMP و إدارة مشاريع تكنولوجيا المعلومات
	Computer Hardware, Maintenance & Repair Training Courses	The A + Certification Course		دورة شهادة التدريب القياسية لفنيي تكنولوجيا المعلومات A+ و صيانة الحاسبات
	Computer Networking	Cisco Certified Network Associate Routing & Switching (CCNA)		دورة سيسكو المرخصة للمبتدئ في الشبكات في مجال التوجيه والتحويل CCNA Routing & Switching الشبكات الحاسوبية
No. 7	Business Continuity and Disaster Recovery Planning	Business Continuity and Disaster Recovery Planning	استمرارية العمل والتخطيط لمواجهة الطوارئ	استمرارية العمل والتخطيط للتعافي من آثار الكوارث

Second : Recruiting the competencies who are holding specialized international certificates in the field of information technology that commensurate with the needs of the OIG.

8.1.2.1. Equipment

- **Prepare a full and comprehensive inventory of all equipment (computers, servers , Routers... etc.)** in each office and the names of users and update this list periodically and continuously as part of the management of computerized equipment in the office Computer Hardware Inventory Management.
- To unify devices and computerized equipment in the OIG, which will help support teams in repairs and provide the appropriate pieces.
- Operation of all equipment without exception by buying rights" Licensing "For the use of operating systems (Operating Systems) And within international laws and regulations.

8.1.2.2. Software

- **Prepare a full and comprehensive inventory of all software used and purchased / obtained from external bodies**

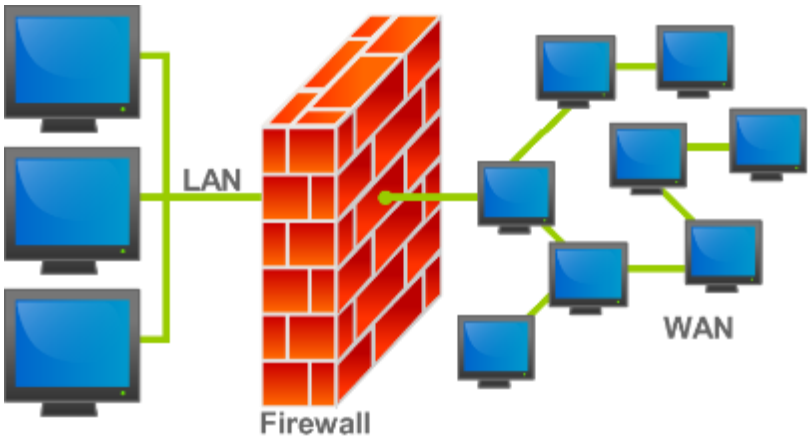
  (Microsoft Office, Adobe... Etc.) in each office and the names of users and update this list periodically and continuously as part of the management software in the office Software Inventory Management.

- **Prepare a full and comprehensive inventory of all software developed in-house and build private files on each program History Since the beginning of its use** in every office and the names of users and update this list periodically and continuously as part of the management software in the office Software Inventory Management.
- Run all software without exception by buying rights" Licensing "And within international laws and regulations

  .

8.1.2.3. Intranets

- Building and the establishment, installation and delivery of internal networks of various technologies in the OIG) ,LAN, WAN, ... etc. (In addition to video chat systems and computer servers that are running operating systems) Servers (And is supervised, and for the purpose of implementation of data systems and software that operate in a network environment and providing linkages between departments.
- Seconded the notion of Computer Security Greater interest by providing computer network security and maintain them using appropriate protective equipment such as firewalls) Firewalls (To ensure the security and protection of information Office, including the network protection from all programs that affect the performance of the network, and work quickly and efficiently, and continue to work daily for the network and protection from viruses, and denial of service for hackers and unauthorized hacking cases of network, and follow-up security clearances about working on the network.



8.2. IT & Computer Forensic Audit

8.2.1. Main Recommendations

After comprehensive analysis and deep study to the status of the IT and Computer Forensic Audit in the OIGs, we list the following as the most important recommendations and major future needs, which the OIG requires to establish the core of a strong technical team to carry out the tasks of IT and Computer Forensic Audit in the Ministries and Iraqi Entities:

1. Developing comprehensive policies and procedures covering:
   a. IT Audit.
   b. Computer Forensic.
   c. Incident and Problem Management.

   Moreover, management should ensure distributing policies and procedures through formal awareness programs to all employees within the OIGs.

   In addition, policies and procedures should be approved by Management and reviewed in a periodic basis.

   Furthermore, an independent assessment is necessary to ensure that policies and procedures have been properly understood and executed.
2. Enforcing OIGs to follow a complete and holistic IT Audit process. IT Audit process consists of the following phases:
   a. Formulate audit charter.
   b. Identify audit subject.
   c. Define audit objectives.
   d. Identify audit scope.
   e. Perform pre-audit planning.
   f. Identify audit approach.
   g. Perform audit procedures.
   h. Reporting.
   i. Follow-up.
3. IT Auditors report the findings after each IT Audit assignment. Moreover, the IT Auditor should consider the following in the Reporting phase:
   a. Once the first draft of the report is finalized, the findings and recommendations should be discussed and agreed with the auditee's management.
   b. The report should minimum include the following parts:

i. Introduction, which includes the scope, limitations, objectives, period of coverage, and extent of the audit work performed.

ii. Findings.

iii. Risks related with each finding.

iv. Recommendations for each finding in order to eliminate or diminish the risks.

v. Auditee's comments and action plans.

4. IT Auditor document all the work performed. Documentation should be complete, clear, structured, indexed, and easy to use and understandable by the reviewer. Furthermore, it is advisable to have dated, initialized, numbered, and properly labeled documentation.

5. OIGs gather and verify relevant information to conclude if appropriate action has been taken by auditee's management in a timely manner that addresses the findings.

6. It is advisable to use tools/software to accomplish IT Audit and Forensic assignments rapidly, since such tools:

   a. Independent.

   b. Safe: data will not be corrupted.

   c. Using audit-specific routines; such as sampling.

   d. Document tests performed.

7. Having IT Auditors with varied experiences in every office. IT Auditors should hold IT-related certificate as well as IT Audit / IT Security certificates. Moreover, IT Audit training plan should be developed and every IT Auditor should attend it. IT Audit training plan should consist of technical skills as well as soft skills.

8. Enforcing IT Auditors to gather evidences while performing IT Audit assignments. Audit evidence may include the following:

   a. IT Auditor's observations.

   b. Interview notes.

   c. Documentations, records, and contracts.

   d. Results of audit test procedures.

   e. Data extracted from applications and systems.

   f. Email communications.

   Moreover, the evidence should be reliable, sufficient, relevant and competent.

9. OIGs consider testing sample instead of testing whole population. Sampling used when limited time and cost prevent a full testing of all transactions or events in a predefined production.

10. Changes to IT environment are authorized, tested, approved and monitored by IT Auditors. Moreover, offices should ensure that duties within manage change environment are segregated.
11. OIGs audit password settings for all technical components available in the auditee environment. Recommended password settings are shown below:
    a. Minimum password length (8 characters).
    b. Initial log-on uses a onetime password.
    c. Password composition (alpha, numeric and special characters).
    d. Frequency of forced password changes (minimum 60 days).
    e. The number of unsuccessful log on attempts allowed before lockout (3-20 attempts).
    f. Ability of users to assign their own passwords.
    g. Number of passwords that must be used prior to using a password again (3-10 password history).
    h. Idle session time out (10-20 minutes).
    i. Logging of unsuccessful login attempts.
12. OIGs test the authorization of user access, the appropriateness of establishing user accounts, and monitoring of user access process. Moreover, offices should test that physical access is limited to appropriate individuals. Furthermore, offices should ensure that duties within logical access environment are segregated.
13. OIGs test that the data has been backed-up properly and data is recoverable.
14. OIGs test the completeness and accuracy of the records and the validity of the entries made, resulting from both manual and programmed processing.
15. OIGs test that the IT operations incidents and problems are identified, resolved, reviewed, and analyzed in a timely manner. Moreover, incident response team should be established and trained to solve incidents and problems in a timely manner, and capable of escalating problems.
16. Ministries capture systems logs in order to prepare for investigating a case once happened.
17. Enforcing the Ministries and the Audited Entities to provide the OIGs with a full and comprehensive restriction of logs for the operating systems in the Ministry (Operating Systems, networks, applications, databases, internet, programs, technology used…), and granting the OIGs the right to access any of these systems when required.
18. OIGs have a predefined plan and procedures to be followed by affected parties.
19. Enforcing OIGs to follow a complete and holistic Computer Forensic process. Computer Forensic process consists of the following phases:

a. Preparation.

b. Data protection.

c. Data acquisition.

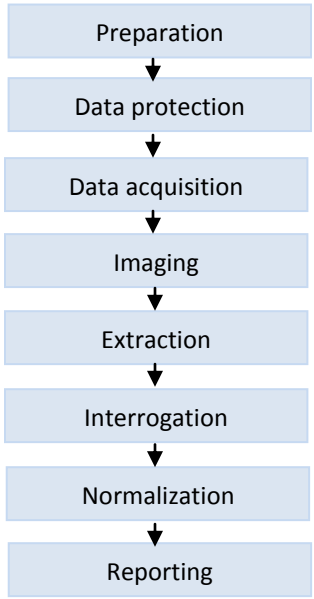
d. Imaging.

e. Extraction

f. Interrogation

g. Normalization.

h. Reporting.



8.2.2. Sub Recommendations

8.2.2.1. Administrative Structure

Due to the current status of OIGs and –generally- the limited number of staff in the office, especially in IT departments, we recommend instructing the IT Department in the OIG to take control over supervising the IT Audit and Computer Forensic Audit in the Ministries and Iraqi Entities. In the future, a special division should be built within the IT department that is specialized in the IT Audit and Computer Forensic Audit.

8.2.2.2. Training Needs Concerning "IT & Computer Forensic Audit"

The training needs concerning building the capacity of the IT team in the domain of IT and Computer Forensic Audit can be summarized as follows:

Domain #	Domain title in Arabic	Domain title in English
Technical Domains		
Domain #1	تدقيق نظم المعلومات	Information Systems Auditing
Domain #2	تدقيق الشبكات	Computer Networks Auditing
Domain #3	تدقيق أنظمة التشغيل	Operating Systems Auditing
Domain #4	تدقيق قواعد البيانات	Database Auditing
Domain #5	تدقيق تطبيقات الـ WEB	Web Applications Auditing
Domain #6	تدقيق قواعد البيانات جنائياً	Database Forensics
Domain #7	تدقيق الشبكات جنائياً	Network Forensics
Domain #8	تدقيق أجهزة الحاسب الآلي جنائياً	Computer Forensics
Domain #9	تدقيق المعلومات الأمني	Information Security Auditing
Domain #10	تدقيق الشبكات الأمني	Network Security Auditing
Administrative Domains		
Domain #11	مبادئ التدقيق، تقييم المخاطر، والإبلاغ	Audit Principles, Risk Assessment, and

	الفعال	Effective Reporting
Domain #12	حوكمة وإدارة تكنولوجيا المعلومات	Governance and Management of IT
Domain #13	تقييم مخاطر تكنولوجيا المعلومات	IT Risk Assessment
Domain #14	البنية التحتية لتكنولوجيا المعلومات	The Information Technology Infrastructure
Domain #15	تدقيق الإمتثال لإجراءات العمل	Business Process Compliance Auditing
Total Domains: 15 Domains		

We also recommend training the specialized Audit Team on the CISA international certificate: Certified Information Systems Auditor (CISA)

What follow, are the main topics that should be discussed during the training of the –above-recommended topics:

Area #	Training Area	Training Area Description
1	Information Systems Auditing	Definition of Internal Control Internal Controls Key Controls Operational Controls General Controls Application Controls IT Governance Objectivity IS Auditing Ethics IS Auditing Planning Examining and Evaluating of Information IS Auditing Survey Design: Criteria for defining Procedures INFORMATION SECURITY RISK MANAGEMENT - What is a process? - Objectives - Controls - Policies - Identifying and classifying risk - Implementing a risk mitigation strategy - Plan do check act - Risk management, security compliance & audit controls

		RISK ANALYSIS: TECHNIQUES AND METHODS - Overview of Risk Methods - General risk analysis - Risk analysis models CREATING AN INFORMATION SYSTEMS RISK TESTING PROGRAMME - Stages to Learning and Developing Risk Assessment Skills - Data Classifications - Data Collection Process - Actual Data Collection - Analysis of the Collected Data
2	Computer Networks Auditing	• Risk Analysis and the place of the Network in IS Governance o Identifying the expectations and needs of the business o Relating business needs tnetwork issues • Business and IS Strategies and Policies relating tNetworks o Starting out with a solid foundation o Addressing the common, global problems through Policies o Setting appropriate standards • Security Infrastructure & Management: an introduction tISO27001:2005. o Using available “tools” thelp with the Audit o A brief look at CobiT & ITIL for the Auditor • Network Topography & communications media o Different ways of moving data o The importance of network design • Issues associated with different media o Specific risks associated with communications & how taddress them o Choosing & using the most appropriate communications media • Using an Intranet for network management o Benefits and some not-so-obvious problems o An invitation tinternal hackers? • Single Sign-on concepts o Positives & negatives o The auditor’s approach • Securing Data in Transmission o Types of Data Encryption o PKI & Digital Signatures • External connections o The Internet & E-mail o Firewalls, Proxy Servers & the DMZ o Virtual Private Networks (VPN’s) • Wireless Networks & Bluetooth o A non-technical overview of “developing” network technologies • Getting intthe Network o Auditing logical security management o Looking for the loopholes • Reaching the Business Applications

		○ Using hierarchic access control ○ Auditing compliance with Business policies • Attacks and how tdetect and react tthem ○ Intrusion Detection Systems & Honeypots ○ Denial of Service, Viruses, Worms etc • Network Performance ○ Evaluating line capacity & usage ○ Identifying& addressing the problems • Network availability ○ Building in automated recovery ○ Back-up & redundancy ○ Business Continuity • Common Network weaknesses tlook for ○ Some real-life examples of Network failures ○ A discussion on how taddress them • Concepts of Materiality ○ Identifying what goes in the Report ○ Reaching the target of a "clean" network • Audit Recommendations ○ "Selling" the audit findings ○ Getting things fixed quickly & effectively • "People" issues ○ Social Engineering & Identity Theft ○ Running an awareness campaign
3	Operating Systems Auditing	- Auditing Unix and Linux Operating Systems - Auditing Microsoft Windows Operating System
4	Database Auditing	Types - Authorization Auditing - Access & Authentication Auditing - User & Administrator Auditing - Security Activity Monitoring - Vulnerability & Threat Auditing - Change Auditing - Replication Auditing Methods - Audit within the DBMS (traces) - Audit from the database transaction log files - Audit over the network - Audit directly against the DBMS server
5	Web Applications Auditing	- Application Security - Applications Interfaces - Data Validation - Data Protection - Error Handling - Communication Security - Authentication

		- Authorization - Session Management
6	Database Forensics	- Analyzing the physical file structures - Analyzing concurrency mechanisms - Analyzing security mechanisms - Query optimization and data warehouse techniques

7	Network Forensics	Basics Of Protocols
		- IP Protocols
		- Breakdown of an IP Packet
		- Demonstration : An IP Header
		- ICMP
		- ARP
		Packet Analysis
		- Wire shark
		- Tcpdump
		- ColaSoft Packet Builder
		- Tcpextract
		- Tshark
		- hPing
		Introduction to Legal and Jurisdictional Issues
		Importance Of Server Logs
		In Depth Data Tunneling
		- DNS Tunneling
		- ICMP Tunneling
		Network Forensics Methodology
		- Analyzing TCP/IP Traffic
		  o Establishing Patter and Timeline
		  o Getting the Entire Session
		  o Setting our Target
		  o Simple traffic Capture
		- Analyzing Common protocols
		  o FTP
		  o Telnet
		  o HTTP
		  o HTTPS
		  o DNS
		- Looking for Malicious Traffic
		  o How Malicious traffic Looks like.
		  o Excessive/Oversized/Fragmented packets
		  o TCP Flags
		  o ICMP Attacks
		  o Spoofing
		Attack Prediction
		- Examine IDS Alerts and Understand the Attack
		- Carve Files out of IDS Traffic Captures

		- Gather Evidence from Network Devices Web Forensics - Web Proxies, Encryption, SSL Interception - Analyzing Web Access Histories (using Squid) - Web Cache Page Reconstruction (using Squid) - Reconstruct Web Histories and Cached Web Content Network Log Analysis - Firewall Logs - Central OS Logs - IDS Logs - WAP Log Analysis Analyze DHCP Logs - Centralized Logging with syslog and syslog-ng - OS and Authentication Logs Network Based Evidence Gathering - Active Evidence Acquisition - Interactive Evidence Acquisition - Prioritizing Evidences - Gathering Evidences from Networking Practical Applications - Network Troubleshooting - Intrusion Detection - Defeating Traffic Analysis
8	Computer Forensics	- Computer Forensics for the First Responder - Computer Forensics: Evidence Collection and Preservation - Cybercrime and Digital Forensic Tools - Criminal Law - E-Discovery & Data Analytics
9	Information Security Auditing	- Strategic Security Plans - Code of Ethics - Risk Analysis - Business Impact Analysis & Business Continuity - Legal Compliance - Tactical Security Planning - Information Security - Network Security Plan - Physical Security Plan - Incident Response - Personnel Security Plan - Operational Security Plans - Information Security - Computer & Server Security - Network Security - Physical Security - Business Continuity - Personnel Security

		- Audit Standards - Audit Planning - Audit Plan Standard - Audit Report Standard - Equipment Baseline Audit
10	Network Security Auditing	- The five pillars of network security auditing: assessment, prevention, detection, reaction, and recovery. - The foundational roles of security policies, procedures, and standards. - Current laws related to hacking, cracking, fraud, intellectual property, spam, and reporting. - Security governance - People, processes, and technical security controls through a system-based approach. - Security policy and compliance requirements for networks. - Assessment of infrastructure security and intrusion prevention systems. - Auditing network access control and secure remote access systems. - Auditing security in clients, hosts, and IP communications. - Evaluating the performance of security monitoring and management systems
11	Audit Principles, Risk Assessment, and Effective Reporting	- Filling in any foundational gaps in auditing principles - Useful risk assessment methods that are effective in measuring the security of a system and the level of compliance and identifying weak or non-existent controls. - Effective risk-based method for the specification or selection of controls. - Analysis methods of an existing set of controls, a business process, an audit exception, or a security incident, identifying any missing or ineffective controls. - Identify corrective actions, eliminating future problems. - Method for conducting audits and presenting findings that actually help to move the organization toward rapid compliance.
12	Governance and Management of IT	- Corporate Governance - IT Governance (ITG) - Information Technology Monitoring and Assurance Practices for Board and Senior Management - Information Systems Strategy - Maturity and Process Improvement Models - IT Investment and Allocation Practices - Policies and Procedures - Risk Management - IS Management Practices - IS Organizational Structure and Responsibilities - Auditing IT Governance Structure and Implementation - Business Continuity Planning - Auditing Business Continuity

13	IT Risk Assessment	- Identifying common IT project risks - Recognizing the threats and opportunities on IT projects - Understanding what qualifies as risk with IT projects - Learning the difference between negative and positive IT risks - Developing an IT risk management plan - Planning risk response methods for IT risks - Understanding the most common IT risk sources - Qualifying and quantifying IT risks - Creating risk mitigation and contingency plans - Monitoring and controlling project risks - Overcoming resistance from stakeholders and team members
14	The Information Technology Infrastructure	- Service strategy - Service design - Service transition - Service operation - Continual service improvement (CSI)
15	Business Process Compliance Auditing	Economy Efficiency Effectiveness

9. Challenges and Obstacles during Assessment Implementation

The challenges that faced the Advisory Team during their work on this study which, directly or indirectly, affected the their work path, can be summarized in the following table:

Constrain	Details
Time Constrains	▪ The official work hours of OIGs and availability of concerned employees at that period. Sometimes the Team reached to the OIG before the concerned officials and employees, either because of traffic jams or far distances or even for security reasons, which affected the daily work schedule and the programmed visits during afternoon hours to other offices. ▪ Official holidays at Iraq and Jordan and their effect on the project. Where the time of Hajj and 'Eid Al-Adha Al-Mubarak came in the same period that the OIGs has been requested to fill the electronic forms.
Location/Physical Constrains	▪ Difficulty in the team movement from and to the OIGs during field visits to 14 offices in multiple locations and different districts in Baghdad during peak hours. Where the team faced great difficulty in gaining access to the agreed upon field visits during afternoon hours.
Knowledge Constrains	▪ The great disparity between of scientific and practical levels for IT staff in the OIGs, where the knowledge of the Iraqi team in the OIGs of the topics under discussion varies from one office to another, which affects the optimization of time per visit to fill the forms, where it was necessary to deliver the idea of team and the objectives of the study to the OIGs.
Communication Constrains	▪ Constraints of communication and coordination between the UNDP team (Baghdad) and the Office of the Coordinator of Iraqi Prime Minister for Regulatory Affairs, which caused the delay in communication with the OIGs. ▪ Constraints of communication and coordination between the UNDP team (Baghdad) and the OIGs, which affected getting the replies on the questionnaires. ▪ Constraints of communication and coordination between the Office of the Coordinator of Iraqi Prime Minister for Regulatory Affairs and the OIGs, which affected getting the replies on the questionnaires. ▪ Not all the OIGs replied on the questionnaires on the time specified in the UNDP letter, which affected the sample size of the study, where we satisfied with %64 of the original sample size.

Constrain	Details
Security Constrains	▪ Security barriers in front of the Ministries' OIGs had significant impact on the delay and disrupt the Advisory Team from entering the OIG, either for security reasons or for a specific defect in the coordination between the OIG and the Security Bureau in the Ministry

10. Comments of the Participating Offices

As a part of the Advisory Team work, it was necessary to seek the opinion of OIGs for the content of study and its objectives, and the extent of the OIGs need for such assessment study, besides the extent of the need for these offices to implement and apply IT & Computer Forensic Audit in Ministries. Reactions were largely positive, especially that it will add additional responsibilities of great importance and a close relationship with the OIG functions to the role of IT, which elevates to a leading level of knowledge role in Iraq as a whole and the government institution in particular.

Ministries in general and media offices in particular concerned with the field visits and what it carries of connotations and continuous efforts being made by the United Nations Development Programme (UNDP) to support and develop OIGs.

The link below is a published articles about this study:

http://mmpw.gov.iq/ArticleShow.aspx?ID=351

11. Lessons Learned

- To totally depend on field visits and interviews of office, instead of sending forms to the OIGs.
- Depend more and intensively on the field and interactive visits of such studies, which provides an open communication with concerned team in the OIG, in addition to what it offers of carry out the reality of the current situation closely.
- One of the main obstacles in doing this study was conducting two field visits per day, where we see that it is advisable to increase the number of days of field and interactive visits for such studies, which can allow one field visit a day at the most.
- Focus on developing the effectiveness of the communication method between the team and project management in the Office of United Nations Development Programme (UNDP) in Baghdad on the one hand, and between the Office of the Coordinator of Iraqi Prime Minister for Regulatory Affairs and OIGs on the other hand, regarding the work schedule of the project and timings required to complete the study more effectively.
- Focus on developing the effectiveness of the communication method between the team and project management in the Office of United Nations Development Programme (UNDP) in Baghdad on the one hand, and between the Office of the Coordinator of Iraqi Prime Minister for Regulatory Affairs and OIGs on the other hand, regarding the security arrangements for the entry of Advisory Team to the offices of inspectors general.