
IT Audit

Information System & Business Applications Controls

Client	Jordan Insurance Federation (JOIF)
Project	JOIF/Amon Technologies/2009-03
Document	Findings & Recommendations Report
Prepared By	Vatche G. Dakessian
Version	Final For Delivery
Circulation	Private & Confidential
Date	April 2009

Table of Contents

- Executive Summary 5**
 - Background 5
 - Introduction 5
 - Document Structure 6
- 1 Business Applications 8**
 - 1.1 Current Status 8
 - 1.2 Controls Compliance Matrix 9
 - 1.3 Recommendations 10
 - R1.a Automatic Mapping of Vehicle Class and Use Codes 10
 - R1.b Change default settings on Vehicle Class to blank 10
 - R1.c Placing of JOIF Staff at Border Exit Points 10
 - R1.d Activate Vehicle Exit Function Logging on NEMIS 11
 - R1.e Disable Anonymous Access on NEMIS Applications 11
 - R1.f Restrict Accessibility to NEMIS Application Code Files 11
 - R1.g Activate NEMIS Application Code Backup 11
- 2 Servers 12**
 - 2.1 Current Status 12
 - 2.2 Controls Compliance Matrix 13
 - 2.3 Recommendations 14
 - R2.a Resolution of Server Issues in Table 14
- 3 Communications & Networking 15**
 - 3.1 Current Status 15
 - 3.2 Controls Compliance Matrix 15
 - 3.3 Recommendations 16
 - R3.a Resolution of Networking Issues - (x) 16
 - R3.b Resolution of Networking Issues - (w) 16
- 4 Operating Systems 17**
 - 4.1 Current Status 17
 - 4.2 Controls Compliance Matrix 17
 - 4.3 Recommendations 19
 - R4.a Resolution of Operating System Issues - (x) 19
 - R4.b Resolution of Operating System Issues - (w) 19
- 5 IT Security Systems 20**
 - 5.1 Current Status 20
 - 5.2 Controls Compliance Matrix 23
 - 5.2.1 General Features 23
 - 5.2.2 Physical Data Security 23
 - 5.2.3 Password Security 24
 - 5.2.4 Hardware Security 24
 - 5.2.5 Workstation Security 24
 - 5.2.6 LAN/Domain Server Security 25
 - 5.2.7 Network Equipment Security 27
 - 5.2.8 Router/Firewall Security 27
 - 5.2.9 Web Server Security 28
 - 5.3 Recommendations 29
 - R5.a Resolution of IT Security Issues - (x) 29
 - R5.b Resolution of IT Security Issues - (w) 30
- 6 Technical Documentation 31**
 - 6.1 Current Status 31
 - 6.2 Controls Compliance Matrix 31
 - 6.3 Recommendations 32
 - R6.a Technical Documentation - RSS 32
- 7 User Documentation 33**

7.1	Current Status	33
7.2	Controls Compliance Matrix	33
7.3	Recommendations	34
R7.a	User Documentation - RSS	34
8	IT & IS Policies	35
8.1	Current Status	35
8.2	Controls Compliance Matrix	36
8.3	Recommendations	37
R8.a	Information Technology Policies & Procedures	37
R8.b	Information Security Policies & Procedures	37
R8.c	Unified structure for IT & IS Policies & Procedures	38
9	Physical Security Systems	39
9.1	Current Status	39
9.2	Controls Compliance Matrix	39
9.3	Recommendations	40
R9.a	IT Department / Office Space Reallocation	40
R9.b	IT Department / Secure Access Door	40
R9.c	IT Department / Test Server	40
R9.d	IT Department / Disaster Recovery & Business Continuity	41
R9.e	IT Department / CCTV Monitoring & Intrusion Detection	41
R9.f	Border Offices / CCTV Surveillance & Monitoring System	41
10	IT Department Organization	42
10.1	Current Status	42
10.2	Controls Compliance Matrix	42
10.3	Recommendations	43
R10.a	Relocate Production Control Section	43
R10.b	IT Department / New SW Quality Assurance Section	44
R10.c	IT Department / Office Space Reallocation	44
R10.d	IT Department / Secure Access Door	44
R10.e	IT Positions / Job Functions and Job Descriptions	45
R10.f	IT Staff / Qualifications and Requirements	45
R10.g	Promote Current Staff / DB & Applications Section	45
R10.h	New Staff / DB & Applications Section	45
R10.i	Information Security Officer	46
Appendix I – List of Reviewed Documents		47
D.06	Technical Documentation	47
MenaHR Manual	47	
MenaME Manual	47	
MenaPAY Manual	47	
OFFTIME Manual	47	
FingerTEC Manual	47	
D.07	User Documentation	47
MenaHR Manual	47	
MenaME Manual	47	
MenaPAY Manual	47	
OFFTIME Manual	47	
FingerTEC Manual	47	
NEMIS User Manual – RSS / Undated	47	
Production & Auditing User Manual 2009	47	
NEMIS Networking User Manual – March 2009	47	
NEMIS DB & Applications User Manual – March 2009	47	
D.08	IT & IS Policies	48
JOIF Information Technology Policies & Procedures, May 2008	48	
D.09	Physical Security	48
JOIF IT Department Site Plan	48	
JOIF IT Department Electrical Equipment Description	48	
D.10	IT Department	48
IT Department Organization Chart	48	

CV / Fadi Dababneh	48
CV / Faris Al Salman	48
CV / Abdul Majeed Al Sharadikah.....	48
CV / Malek Tarawneh	48
CV / Jafar Daoud	48
CV / Ayed Fakhouri.....	48
Job Description / Assistant IT Manager	48
Job Description / Production Control Section	48
Job Description / Networking Section	48
Appendix II – List of Recommendations	49
R.01 Business Applications.....	49
R1.a Automatic Mapping of Vehicle Class and Use Codes	49
R1.b Change default settings on Vehicle Class to blank.....	49
R1.c Placing of JOIF Staff at Border Exit Points.....	49
R1.d Activate Vehicle Exit Function Logging on NEMIS	49
R1.e Disable Anonymous Access on NEMIS Applications.....	49
R1.f Restrict Accessibility to NEMIS Application Code Files	49
R1.g Activate NEMIS Application Code Backup.....	49
R.02 Servers.....	49
R2.a Actions Required For Resolution of Issues in Table.....	49
R.03 Communications & Networking	49
R3.a Resolution of Networking Issues - (x)	49
R3.b Resolution of Networking Issues - (w)	49
R.04 Operating Systems	49
R4.a Resolution of Operating System Issues - (x)	49
R4.b Resolution of Operating System Issues - (w).....	49
R.05 IT Security Systems	50
R5.a Resolution of IT Security Issues - (x)	50
R5.b Resolution of IT Security Issues - (w)	50
R.06 Technical Documentation	50
R6.a Technical Documentation - RSS.....	50
R.07 User Documentation	50
R7.a User Documentation - RSS	50
R.08 IT & IS Policies	50
R8.a Information Technology Policies & Procedures.....	50
R8.b Information Security Policies & Procedures	50
R8.c Unified structure for IT & IS Policies & Procedures	50
R.09 Physical Security	50
R9.a IT Department / Office Space Reallocation.....	50
R9.b IT Department / Office Space Reallocation.....	50
R9.c IT Department / Test Server	50
R9.d IT Department / Disaster Recover & Business Continuity	50
R9.e IT Department / CCTV Monitoring & Intrusion Detection	50
R.10 IT Department	51
R10.a Relocate Production Control Section.....	51
R10.b IT Department / New SW Quality Assurance Section	51
R10.c IT Department / Office Space Reallocation.....	51
R10.d IT Department / Secure Access Door	51
R10.e IT Positions / Job Functions and Job Descriptions.....	51
R10.f IT Staff / Qualifications and Requirements.....	51
R10.g Promote Current Staff / DB & Applications Section.....	51
R10.h New Staff / DB & Applications Section	51
R10.i Information Security Officer	51

Executive Summary

Background

Many clients, including government departments, semi-governmental agencies and large corporations make extensive use of Information Technology (IT) to automate and to assist their operations. The use of IT can bring enormous business benefits. However, IT also introduces new risks to control and accountability and this adds a new twist to the traditional audit concerns. A comprehensive IT Audit must be able to recognize, identify and recommend solutions to respond to such risks. A typical IT Systems & Services Audit examines the following:

- Document and review the strategic framework within which IT systems are developed and managed by the client - in order to scope the use of IT and identify systems of audit interest.
- Document and review computer controls within key computer applications - in order to ensure availability and integrity and accuracy of data.

Introduction

This IT Systems & Services Audit Report was compiled for Jordan Insurance Federation - **JOIF** in order to gauge and evaluate the status of IT systems and services, evaluate the performance of IT staff and implement recommendations for their enhancement and improvement. The IT Systems & Services Audit covers the major sites and locations operated by **JOIF** where IT systems exist. The sites form part of the Nationwide Electronic Motor Insurance System (NEMIS) implemented by JOIF starting in 2005.

JOIF operates from a Head Office building located in western Amman and provides Third Party Liability mandatory insurance services through its (20) offices located in the various Driver & Vehicle Licensing Sections of the Directorate of Public Security distributed in the various governorates and (10) land border entry points into Jordan. The Head Office currently houses the server and encrypted WAN communications hub of NEMIS with managed Frame Relay links to all the relevant sites. The IT Audit consists of two major components:

Information System Controls: This covers the areas of Security Management, Access Controls, Configuration Management, Segregation of Duties and Contingency Planning.

Business Applications Controls: This covers the areas of Completeness, Accuracy, Validity, Confidentiality and Availability.

Document Structure

This document contains the functional and technical specifications, terms and conditions as well as instructions to prospective bidders. The document consists of six sections and one Appendix as follows:

1. Business Applications: This section reviews the various business applications in terms of completeness, confidentiality, accuracy and validity.
2. Hardware: This section reviews the various hardware configurations deployed.
3. Communications & Networking: This section reviews the various communications and networking systems in place.
4. Operating Systems: This section reviews the various operating system software deployed in terms configurations, updates and access privileges.
5. IT Security Systems: This section reviews the existing IT Security Systems in place in terms of configuration, updates and access policies.
6. Technical Documentation: This section reviews the current version of technical documentation in terms of structure, standards, accuracy and suitability.
7. User Documentation: This section reviews the current version of user documentation in terms of structure, standards, accuracy and suitability.
8. IT & IS Policies: This section reviews the existing IT and IS Policies in terms of scope, structure and content in accordance with international best practices.
9. Physical Security Systems: This section reviews the existing physical security systems and services.
10. IT Department Organization: This section reviews the existing organization structure and staffing requirements of the IT Department.
11. Appendix I: This section provides a list the various documents that were reviewed during the preparation of this IT Audit.
12. Appendix II: This section provides a quick reference list of the recommendations tabled in this IT Audit Report

A number of different recommendations are tabled in this report. They are divided as follows:

Business Applications	(7)	Separate Recommendations
Servers	(1)	Compound Recommendation
Communications	(2)	Compound Recommendations
Operating Systems	(2)	Compound Recommendations
IT Security Systems	(2)	Compound Recommendations
Technical Documentation	(1)	Recommendation
User Documentation	(1)	Recommendation
Policies & Procedures	(3)	Separate Recommendations
Physical Security	(5)	Separate Recommendations
IT Department	(9)	Separate Recommendations