

**Achievement of Market-Friendly Initiatives and Results Program
(AMIR 2.0 Program)**

Funded By U.S. Agency for International Development

Jordan e-Government Risk Assessment Methodology

Final Report

**Deliverable for ICTI Component, Task No. 431.4.4
Contract No. 278-C-00-02-00201-00**

May 2002

This report was prepared by Paul De Luca, in collaboration with Chemonics International Inc., prime contractor to the U.S. Agency for International Development for the AMIR Program in Jordan.

0 Document Control

Table of Contents

0	DOCUMENT CONTROL.....	3
0.1	Document History	5
0.2	Changes From Last Issue	5
0.3	Acknowledgements	5
0.4	Distribution List	5
0.5	Referenced Documents	5
0.6	Abbreviations	5
0.7	Glossary	5
1	INTRODUCTION.....	6
1.1	Purpose.....	6
1.2	Scope.....	6
1.3	Background.....	6
2	RISK ASSESSMENT METHODOLOGY	7
2.1	Overview	7
2.2	Preliminaries and Assumptions.....	8
2.3	Stage 1: Information Asset Valuation	8
2.4	Stage 2: Risk and Countermeasures	10
2.5	Stage 3: Business Security Requirements Specification	12
2.6	Finished?	13

Table of Figures

Figure 1: Stages in determining the BSRS 7

0.1 Document History

Version	Status	Approved by	Date
0.1	Draft	N/A	15 May 2002
0.2	Draft	N/A	28 May 2002

0.2 Changes From Last Issue

Ver	Date Updated	Revision Author	Summary of Major Changes Made	Reviewed By	Review Date
0.1	15 May 2002	Paul De Luca	Initial document created and internally reviewed.	Dave Arthur	22 May 2002
0.2	28 May 2002	Paul De Luca	Add project formatting standards Minor changes to readability of text	Dave Arthur	29 May 2002

0.3 Acknowledgements

N/A

0.4 Distribution List

Dave Arthur	EDS
Allan Gormley	EDS
Kendall Lott	EDS
Mahmoud Ali Khasawneh	MoICT

0.5 Referenced Documents

Number	Title	Reference	Note
1.	N/A		
2.			
3.			
4.			
5.			

0.6 Abbreviations

JOG	Jordan e-Government Programme

0.7 Glossary

BSRS	Business Security Requirements Specification
------	--

1 Introduction

1.1 Purpose

The purpose of this document is to define and walk through the high-level impact-based risk assessment methodology for defining an initial Business Security Requirements Specification (BSRS).

1.2 Scope

The risk assessment methodology defined here applies to all projects sponsored by Jordan e-Government Programme (JOG).

1.3 Background

To ensure that business processes are fulfilled by information processing facilities in a secure manner, it is necessary to conduct a comprehensive risk assessment of the detailed end-to-end solution. However, by the time sufficient architectural, implementation, and operational details exist, it is possible that the project sponsor may not be in a position to implement the findings of the risk assessment. (This may be due to constraints on finance, time, technical solution, personnel, etc.) In some cases, this may not be a significant issue as the risk profile, i.e. the shape and scale of the risk, is sufficiently self contained to allow the project sponsor to decide whether the risk can be managed and take the project into production. However, where the risk profile potentially affects those beyond the project scope, e.g. where other departments or Ministries also use the same information assets, the project sponsor may be forced to halt their project (and write off significant funds). Performing a high level impact based risk assessment at the time of project inception significantly mitigate against this exposure, and provides a timely indication of the fundamental security requirements, i.e. before significant funds have been consumed by the project.

2 Risk Assessment Methodology

2.1 Overview

The process of arriving at a BSRS is somewhat involved and requires informed discussion between the key stakeholders, e.g. project sponsor, project manager, business lead, technical lead, security lead, etc., with the aim to ultimately arrive at a consensus view. The stages of the process are illustrated in Figure 1 below and briefly outlined here.

- Preliminary Stage: During the preliminary stage, information asset groups and their components are defined, key stakeholders are confirmed, and a high level context diagram is produced which clearly identifies those information processing facilities, physical and logical domains, and supporting infrastructure which interfaces to the various information asset groups.
- Stage 1: For each information asset group, this and subsequent stages must be completed. During stage 1, considering potential business impact arising from a breach of confidentiality, integrity, or availability derives the value of an information asset group.
- Stage 2: The impact profile for the information asset group under consideration is used to derive a relatively coarse measure of risk. (For a high level generic assessment where fine-grained implementation details are not known, the risk profile is purely based on impact levels.) The risk profile is then managed down by selecting appropriate countermeasure controls.
- Stage 3: Finally, for the information asset group under consideration, the countermeasure controls identified in stage 2 are translated into security recommendations that ultimately form the BSRS.

It is possible to become too focused on a particular part of the process and consequently lose track of where you are in the context of the whole process, naturally this can lead to some confusion. In order to minimise the chance of this, please ensure you have really do understand Figure 1.

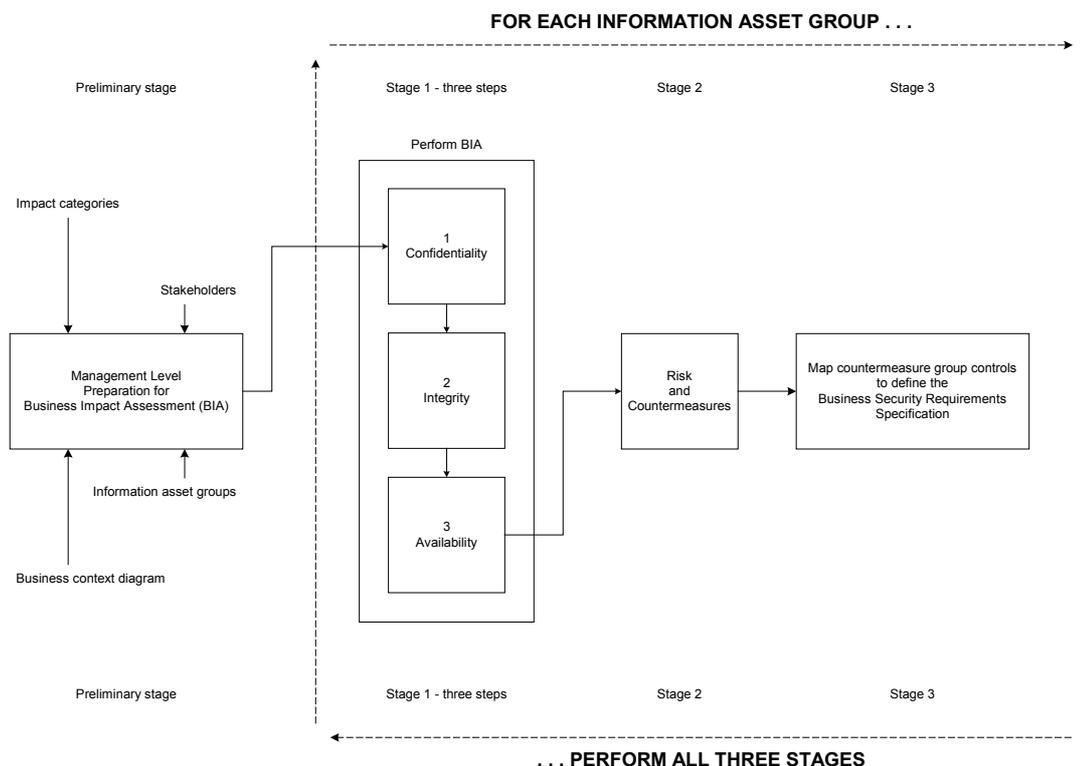


Figure 1: Stages in determining the BSRS

Each of the stages is addressed in separate section below.

2.2 Preliminaries and Assumptions

The first key output of this preliminary stage is the definition of the information asset groups. Together these groups contain all the information assets that are required to fulfil the desired suite of business processes. Clients' personal details would be an example of an information asset group and may comprise Name, Date of Birth (DOB), Tax Reference Number (TRN), Address, etc., similarly clients' financial details may comprise Name, Bank Accounts, Salary, Tax Code, Mortgage, Loans, etc. Clearly, some information will be of a particularly sensitive nature, examples of which may include medical histories, criminal records, etc. The second key output of the preliminary stage is to produce a high level context diagram depicting those information processing facilities, physical and logical domains, and supporting infrastructure which interfaces to the various information asset groups. Finally, agreement must be reached on the contextual definition of the impact level used in stage 1, i.e. minor, significant, substantial, and exceptional.

2.3 Stage 1: Information Asset Valuation

For each information asset group, determine its value to the organisation by considering the business impact profile that could result from a breach of:

- Confidentiality, i.e. unauthorised disclosure;
- Integrity, i.e. unauthorised modification (including unauthorised commitment to a transaction);
- Availability, i.e. unauthorised denial of service.

It is important that you consider each information asset group as a whole, e.g. Clients' personal details, rather than separately considering their individual components, e.g. Name, DOB, TRN, Address, etc. However, it is also important not to lose sight of particularly sensitive components as they may prove pivotal in determining primary impact categories and corresponding impact levels.

Table 1 below should be used three times for each information asset group to identify the consequential impacts arising from a breach of confidentiality, integrity, and availability. The results arising from each application of table 1 should be recorded in Table 2 below to document the information asset group's fine-grained impact profile.

Impact category	Impact level			
	1	2	3	4
Personal safety	MINOR injury to a few people.	SIGNIFICANT injury to several individuals.	SUBSTANTIAL injury to a many individuals.	EXCEPTIONAL long-term injury to several individuals or even loss of life.
Personal distress	MINOR distress to a few people.	SIGNIFICANT distress to several individuals.	SUBSTANTIAL distress to many individuals.	EXCEPTIONAL long term distress to several individuals.
Legal, regulatory, and contractual obligations	Civil suit or criminal offence resulting in MINOR damages/penalty.	Civil suit or criminal offence resulting in SIGNIFICANT damages/penalty.	Civil suit or criminal offence resulting in SUBSTANTIAL damages/penalty.	Civil suit or criminal offence resulting in EXCEPTIONAL damages/penalty.
Law enforcement	Facilitate the commission or prejudice the investigation of a crime.	Cause the investigation or trial of a crime to be abandoned.	Facilitate the commission or prejudice the investigation of a SERIOUS crime.	Cause the investigation or trial of serious a crime to be abandoned.
Financial loss and disruption to activities	Result directly or indirectly in MINOR financial loss.	Result directly or indirectly in SIGNIFICANT financial loss.	Result directly or indirectly in SUBSTANTIAL financial loss.	Result directly or indirectly in EXCEPTIONAL financial loss.
Management and business operations	Introduce MINOR localised inefficiencies.	SIGNIFICANTLY undermine wider operations and management.	SUBSTANTIALLY disrupt key operations and management functions.	EXCEPTIONAL long term disruption to key operations and management function.

Impact category	Impact level			
	1	2	3	4
Reputational damage	MINOR internal but transitory relational damage.	SIGNIFICANTLY affect external relations but confined to the immediate geographic vicinity and with no lasting effects.	SUBSTANTIALLY affect external relations resulting in widespread adverse publicity.	EXCEPTIONALLY affect external relations resulting in long term widespread adverse publicity.

Table 1: Information Asset Valuation – impact categories and levels

As stated above, the impact profile for each information asset group is defined by following three application of Table 1 above. An example of the fine-grained impact profile for an example information asset group is summarised in Table 2 below.

Impact category	Impact level corresponding to a breach of		
	Confidentiality	Integrity	Availability
Personal safety	2	1	N/A
Personal distress	3	2	1
Legal, regulatory, and contractual obligations	2	1	2
Law enforcement	0	0	0
Financial loss and disruption to activities	2	1	1
Management and business operations	1	1	1
Reputational damage	1	2	1

Table 2: Information Asset Valuation – fine-grained impact profile

(Note, for the example impact, Table 2 indicates that security breaches do not result in law enforcement related business impacts.)

For a high level assessment, the primary BSRS is simply defined by the greatest impacts arising from a security breach. Table 3 below summarises this for the information presented in Table 2.

Breach category	Category of greatest impact	Impact level
Confidentiality	Personal distress	3
Integrity	Personal distress Reputational damage	2 2
Availability	Legal, regulatory, and contractual obligations	2

Table 3: Information Asset Valuation – coarse-grained impact profile

2.4 Stage 2: Risk and Countermeasures

Given the impact profile for each information asset group, identify the corresponding countermeasure groups and associated controls. These countermeasure groups address specific aspects of the risk profile in a consistent manner.

Analysis of each component depicted in the context diagram will indicate whether the risk profile is low, medium, high, or possibly extreme. However, for this relatively high level generic assessment, where implementation, and vulnerability details are not yet known, the risk profile is based on impact levels. Therefore, the confidentiality, integrity, and availability components of the impact profile, summarised in Table 3 above, should be used as inputs to Table 4 below in order to determine the corresponding baseline countermeasure controls.

The relationship between impact arising from a breach of confidentiality, integrity, and availability and controls from the corresponding confidentiality, integrity, and availability countermeasure group should be clear. However, the relationships to the remaining countermeasure groups are less obvious (as they follow from fundamental information security first principles which is beyond the scope of this document). To ease this situation, each countermeasure group is associated with the type of breach that it primarily mitigates. For example, as the logical access control countermeasure group primarily mitigates the risk arising from a confidentiality breach, the control hierarchy, or rating, for the logical access control countermeasure group should, therefore, be the same as that for the confidentiality countermeasure group, i.e. 3 as per Table 3 above. The countermeasure control hierarchy for each countermeasure group are **highlighted (in yellow)** in Table 4 below and effectively forms the basis of the Business Security Requirements Specification (BSRS).

Countermeasure groups	Countermeasure control hierarchy			
	1	2	3	4
Confidentiality	Password protected files.	Baseline standards based commercial encryption (56-bit key)	Strong standards based commercial encryption (112-bit key).	Very strong standards based commercial encryption (168-bit key) or privately commissioned encryption.
Integrity	Checksum and trusted sources.	Baseline standards based commercial hash.	Commercial standards based keyed-hash (Message Authentication Code).	Commercial standards based keyed-hash (Message Authentication Code) with token-based key.
Availability	Full and incremental back-up of software, information assets, and transactions.	Real-time information asset mirroring.	Resilient load balanced architecture (with recovery options).	High availability architecture (with hot standby).
Identification and authentication (closely related to confidentiality)	Baseline password (at least 6 characters).	Long strong password (at least 10 characters).	Unpredictable user identifier and authentication via a Token.	Unpredictable user identifier and authentication via a Biometric.
Non-repudiation (closely related to integrity impact)	Strong, auditable, operating procedures must be implemented to ensure accountability for (in)actions.			Strong, auditable, operating procedures and security mechanisms to prevent non-repudiation of events.

Countermeasure groups	Countermeasure control hierarchy			
	1	2	3	4
Business continuity (closely related to availability impact)	Plans should be developed to maintain or restore business operations in the required time scales.			Comprehensive provisions must be made to cater for full disaster recovery.
Logical access control (closely related to confidentiality impact)	The owner of each information asset, including security management information, must specify the mode of access, e.g. read, write, execute, delete, append-only, etc., available to each user, process, and group.		Information stored, or in transit, should be encrypted to ensure that it is only of use to the authorised.	Physical segregation of information processing system, n-man control.
Accounting (closely related to integrity impact)	Details of each event, including user identity, time, event type, location, etc., must be logged.		Accounting logging processes must be self policing, i.e. support proactive alerting, e.g. capacity, access via non-standard applications, etc.	Unauthorised attempts to modify accounting logs must be proactively detected.
Audit (closely related to integrity impact)	The audit requirement for each accounting log must be defined.	Trends in accounting logs must be identified and appropriately investigated to a satisfactory conclusion.	Access to audit trails and tools must be controlled.	
User controls (universal)	Effective end user best practice operating procedures must be implemented to ensure correct user actions.			
Operations controls (universal)	Effective targeted best practice operating procedures must be implemented to ensure correct actions by those providing/managing information processing facilities and underlying architectures.			
Data Protection Act (universal)	Data must be: <ul style="list-style-type: none"> • fairly and lawfully processed; • processed for limited purposes; • adequate, relevant and not excessive; • accurate; • not kept longer than necessary; • processed in accordance with the data subject's rights; • secure • not transferred abroad without protection. 			
Compliance checks (universal)	All relevant statutory, regulatory, and contractual requirements should be explicitly defined, and supported by appropriate operating procedures and security measures to ensure fulfilment of these requirements.			

Table 4: Countermeasure Groups and Control Hierarchy

Addressing the confidentiality, integrity, and availability countermeasure groups only serves to identify a baseline of controls; the remaining countermeasure groups identify additional controls necessary to proactively manage down risk.

2.5 Stage 3: Business Security Requirements Specification

The controls identified in the second stage, for each information asset group, should be collated into the formal BSRS document. To this end, the appropriate components of the countermeasure control hierarchy selected from Table 4 are transferred to column 2 of Table 5 below. Table 5 illustrates the possible contents of the BSRS corresponding, in this case, to the example impact profile for the information asset group summarised in Table 2 above. The Advice column is merely a pointer to recommended means of implementing security requirements well in advance of conducting a comprehensive risk assessment, which would be expected to generate supplementary and complementary implementation advice. It must be noted that the fundamental aim of the BSRS is to produce security requirements, not granular implementation advice.

Information asset group	Clients' personal details
-------------------------	---------------------------

Control id	Countermeasure group	Security requirement	Advice
1	Confidentiality	Strong standards based commercial encryption (112-bit key) should be applied to information while stored and in transit.	Two-key (112-bit) Triple-DES, and 128-bit RC4 are recommended options. (The Data Encryption Standard and Ron's Code are commonly known as DES and RC respectively.)
2	Integrity	Baseline standards based commercial hash should be applied.	The Secure Hash Algorithm (SHA-1) is recommended.
3	Availability	Real-time mirroring must be implemented on each information processing facility that interfaces to the information asset group.	Redundant Array of Independent Disks (RAID) should be deployed.
4	Identification and authentication	User identifiers must not be predictable while authentication must be via a Token.	To produce user identities a one-way function should be applied to user details (first name, initial, last name, employee number, etc.) to produce an alphanumeric string of at least 6 characters in length, e.g. cd2r8k. Recommended Token options include magnetic stripe cards, memory devices, and smartcards.
5	Non-repudiation	Strong, auditable, operating procedures must be implemented to ensure accountability for (in)actions.	Each and every action must be tied back to its unique initiator.
6	Business continuity	Plans should be developed to maintain or restore business operations in the required time scales.	Each information processing facility that interfaces to the information asset group must be supported by a documented business contingency and recovery plan which identifies and prioritises dependencies.
7	Logical access control	Information stored, or in transit, should be encrypted to ensure that it is only of use to the authorised.	Two-key (112-bit) Triple-DES, and 128-bit RC4 are recommended options.
8	Accounting	Details of each event, including user identity, time, event type, location, etc., must be logged.	Rather than simply providing write access to the log file, which implies full editing rights, the event log should only ever be appended to.
9	Audit	Trends in accounting logs must be identified and appropriately investigated to a satisfactory conclusion.	No further advice.

Control id	Countermeasure group	Security requirement	Advice
10	User control	Effective end user best practice operating procedures must be implemented to ensure correct user actions.	Access to each information processing facility with interfaces to the information asset group is conditional on satisfactory completion of on-line awareness training.
11	Operations controls	Effective targeted best practice operating procedures must be implemented to ensure correct actions by those providing/managing information processing facilities and underlying architectures.	Access to the management and support functions of each information processing facility with interfaces to the information asset group is conditional on satisfactory completion of awareness training. Comprehensive key management procedures must be documented and implemented.
12	Data Protection Act	Data must be: fairly and lawfully processed; processed for limited purposes; adequate, relevant and not excessive; accurate; not kept longer than necessary; processed in accordance with the data subject's rights; secure; not transferred abroad without protection.	The project manager, technical and business leads, together with the information processing facility owner and custodian must have satisfactorily completed awareness training on the Data Protection Act.
13	Compliance checks	All relevant statutory, regulatory, and contractual requirements should be explicitly defined, and supported by appropriate operating procedures and security measures to ensure fulfilment of these requirements.	Formal documented legal advice must be sought identifying the scope to which statutory, regulatory, and contractual requirements apply.

Table 5: Business Security Requirements Specification for clients' personal details

2.6 Finished?

Thus far, the BSRS has been determined, in this example, for the clients' personal details information asset group. As depicted in Figure 1 above, the process needs to repeat, from stage 1, for the next information asset group identified during the preliminary stage. Ultimately, a BSRS will be produced for each information asset group detailing the means by which the risk profile is proactively managed down to an acceptable level. These individual BSRS can be used to form the basis of compliance checks to provide information asset owners assurance that their assets are appropriately secured.