



ABC PTY LTD
RISKVIEW® IT REPORT
(SAMPLE)

Moore International Marketing Pty Ltd ATF
The Moore Investment Trust ABN 77 529 452 966 trading as Risk Point

38 Oxford Close
Leederville WA 6007
Ph. 9422 5580
review@riskpoint.com.au
www.riskpoint.com.au

9 September 2004

TABLE OF CONTENTS	PAGE
1. Executive Summary	2
2. RISKVIEW® Methodology	3
3. RISKVIEW® IT Profile.....	4
4. Data Analysis and Interpretation	5
5. Findings.....	5
6. Review Scope and Definitions	6
7. Appendix 1 – Output from Questionnaire.....	7

Disclaimer

The information in this report has been prepared from the responses and input from ABC Pty Ltd. RISK POINT does not assume responsibility for the outcome or accuracy of neither the data, nor the actions that ABC Pty Ltd takes following the production of this review. The information contained herein is based on the application of Australian and world standards for the execution of Information Security Management Systems risk management and RISK POINT takes no responsibility for the accuracy or validity of this report or the actions taken by ABC Ltd to its contents and findings.

1. Executive Summary

This document is a report on the output from the RISKVIEW® IT questionnaire completed by ABC Pty Ltd. The information is designed to provide a high level overview of the vulnerabilities and exposures in the Information Security Management System (ISMS) and to provide an assessment of operational activities against best practice for managing information security. It also provides a decision-making framework for risk management.

The questionnaire was completed by ABC and contains the findings from ABC's own evaluation of current business and operational activities. The information contained in this report is designed to provide an introductory investigation into ABC's business processes, policies and procedures. It is intended to provide a measurement against best practice for conducting and maintaining information security management. RISKVIEW® IT is a review and not a detailed risk assessment.

ABC has four (4) areas of the ISMS framework that do not achieve best practice for information security management. These are Asset Classification and Control, Personnel Security, Systems Development and Maintenance, and Business Continuity Planning. The last area has a score less than 20 that indicates that immediate management action is required (see section 4). It is recommended that ABC conduct an information security risk assessment to fully identify areas of exposure and to develop management action plans (risk treatment plans) to minimise risk. A risk assessment will also provide the foundation for the achievement of information security management best practice.

2. RISKVIEW® Methodology

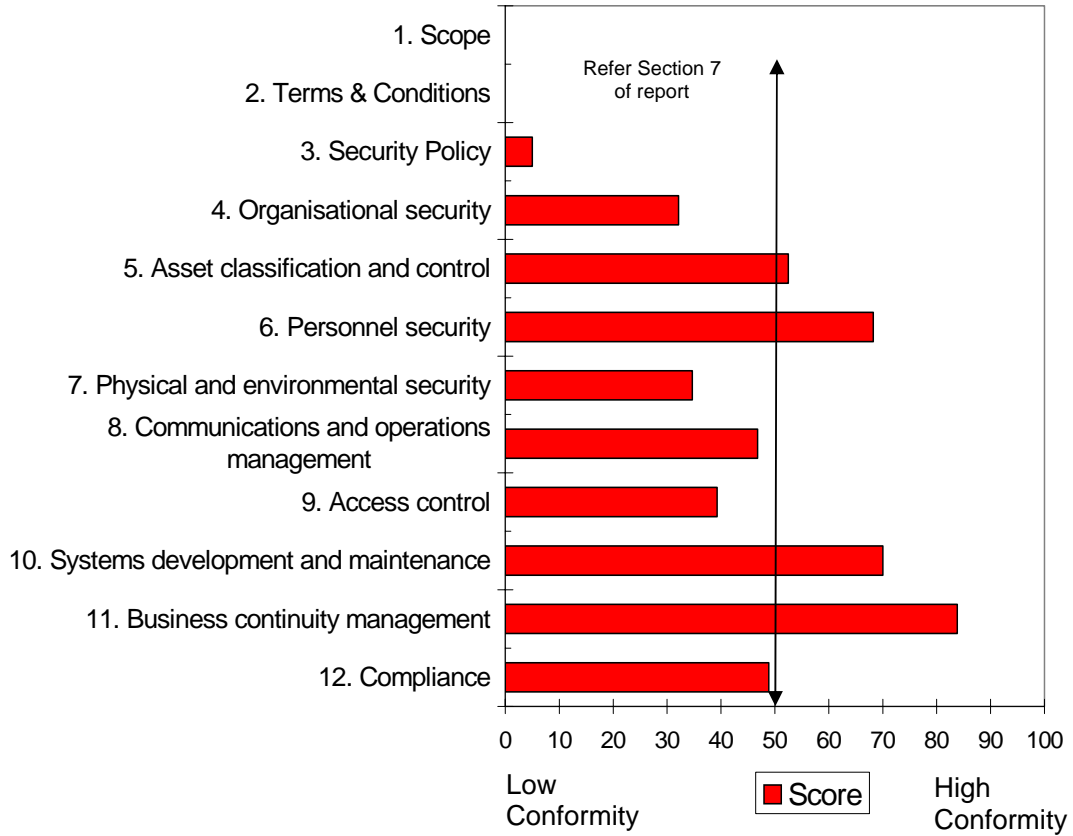
RISKVIEW® IT is based on the Australian and New Zealand Standard 7799.2:2003 (Information Security Management) and addresses the ten operational areas of the information security management process. **RISKVIEW® IT** is a questionnaire containing 135 questions which are weighted such that no one area of the framework carries greater or lesser importance than another. The maximum score in any one area is 100, being the highest level of conformity with respect to information security management best practice. The minimum score possible in any one area is zero, indicating non conformity to information security management best practice.

A score of 75 or higher in any one area indicates that ABC is conducting its information security management activities in accordance with the Standard, with a higher score indicating an even closer compliance to best practice standards. A score of between 50 and 75 indicates that the information security management system may be adequate, but management effort is required to improve operational performance.

A score of less than 50 indicates there are deficiencies in the information security management system and management action is required to improve the system. A score of less than 25 indicates significant non-conformity to information security management best practice and immediate management action is required to develop the system, practices, policies and procedures.

3. RISKVIEW® IT Profile

The following diagram is ABC's ISMS profile.



4. Data Analysis and Interpretation

A low score represents high exposure or vulnerability as a result of a great disparity between ABC'S operational activities and best practice for information security management. A high score represents closer conformity to best practice.

Table 1 provides a matrix for evaluating ABC'S performance against best practice.

Table 1: Information Security Management Performance Evaluation

Score in Framework	<25	25-50	50-75	>75
Interpretation	Systems, procedures and policies do not meet best practice standards and <i>immediate</i> management action is required	Systems, procedures and policies generally do not meet best practice standards and require management review	Systems, procedures and policies may be adequate but require review	Systems, procedures and policies most closely meet best practice standards

5. Findings

The aggregate score of just under 50 in area 5 of the framework (Asset Classification and Control) is due to the lack of a data or information asset register and that there is no policy for the destruction of data and information. The score of 70 in area 6 (Personnel Security) occurred due to good controls in the area of security of job definition and resourcing, and inadequate user training.

The score of 70 in area 10 (Systems Development and Maintenance) is due to good security in application systems. The score of 85 in area 11 (Business Continuity Management) is due to the business continuity plan and that a business impact analysis is in place.

6. Review Scope and Definitions

6.1 Scope

A. This assessment is designed to provide a high level review of the risks and vulnerabilities of the information systems organisation. It contains 135 questions with the option for "Yes"/"No" answers. The default configuration is flagged "Not Yet Answered". It is important that all questions be answered either yes or no, as leaving a default setting will alter the risk profile.

B. The questionnaire has two sections which are informative and provide the scope and definitions of the review, and ten sections addressing the IS framework. Sections 1 and 2 provide the scope and definitions and sections 3 to 12 contain the questions in the review. In some cases, additional questions are asked (e.g. "If a policy is in place when was it reviewed"). These are optional and assist in the profiling process. It is not a requirement that these questions be completed.

C. Each question on the form has a space to allow any additional information to be added should you wish to provide it. This can be done in the box immediately below the question by entering information into the editable field. This is optional and may assist in the response process.

D. Depending upon the level of complexity of the organisation, the questionnaire should take between 45 and 60 minutes to complete. In some instances, some internal investigations may be required in order to obtain all the information necessary before a question may be answered.

6.2 Terms & Definitions

Information Security: The preservation of confidentiality, integrity and availability of information to ensure minimal risk to the organisation.

Risk: The chance of an event occurring that will have an impact on the achievement of objectives, measured by likelihood of occurrence and consequence or impact upon occurrence.

Risk Assessment: The process of assessing threats to, impacts on and vulnerabilities of information and information processing facilities, and determining the likelihood of their occurrence and impact on the organisation.

Risk Management: The process of identifying, controlling and minimising or eliminating security risks that may affect information systems and establishment of organisational culture to support the risk management system.

7. Appendix 1 – Output from Questionnaire

3. Security Policy

C.1 3.1 Information security policy

Does the organisation have a security policy document?

Response: Yes

Was the policy reviewed and evaluated within the past twelve months?

Response: Yes

4. Organisational security

D.1 4.1 Information security infrastructure

Has a management forum been established to address IS risk issues?

Response: Yes

Is there information security co-ordination across the organisation?

Response: Yes

Is there allocation of information security responsibilities within the organisation?

Response: Yes

Is there a management authorisation process in place for the establishment of new information processing facilities?

Response: Yes

Has specialist security advice been sought in establishing the information processing systems?

Response: Yes

Is there a process of co-operation between relevant authorities in the event of a security breach?

Response: Yes

Has an independent review of information systems security been carried out?

Response: No

D.2 4.2 Security of third party access

Do third parties have physical access to the information systems?

Response: No

Do third parties have logical access to the information systems?

Response: No

Do support persons have access to hardware/software systems and/or low level application functionality?

Response: No

Do support persons have access to hardware/software systems and/or low level application functionality?

Response: Yes

Do trading partners have access to information and databases?

Response: Yes

Do third party contractors have access to information systems and databases?

Response: Yes

Are there procedures are in place to manage risks associated with third parties having access to the information systems?

Response: No

D.3 4.3 Outsourcing

Does the organisation's outsourcing contracts contain the information systems security policy?

Response: Yes

5. Asset classification and control

E.1 5.1 Accountability for assets

Does your organisation have a data or information asset register?

Response: No

Does your organisation have a software asset register?

Response: Yes

Does your organisation have physical asset register (processors, monitors, routers etc)?

Response: Yes

E.2 5.2 Information classification

Does the organisation have an information classification system to prioritise assets?

Response: No

Is there a defined set of procedures for copying, storing and transmitting data and information?

Response: Yes

Dependant on the project and client involved. the procedures are contained in the Project/Quality Plan

Is there a defined set of procedures for destruction of data and information?

Response: No

6. Personnel security

F.1 6.1 Security in job definition and resourcing

Are security roles and responsibilities included in the security policy?

Response: No

Are verification checks carried out on employees at time of employment?

Response: No

Are checks carried out on their qualifications?

Response: No

Are identity checks carried out (ie passport)?

Response: No

Do employees sign a confidentiality or non-disclosure agreement?

Response: Yes

Is there a review process for casual and third parties?

Response: Yes

Do the terms and conditions of employment state employees' information security responsibility?

Response: Yes

Are employees required to sign an IS acceptable use agreement?

Response: No

F.2 6.2 User training

Are all employees and relevant third parties trained on the policies and procedures relating the use of information systems?

Response: No

Is the training reviewed on a regular basis?

Response: No