Global-Mark P/L

Management Document G-80

Title: Information Security Management System Certification

Type: Program Information Brochure

This Document Is External

Document Information and Revision History

Document Number	G-80
Original Author(s)	Herve Michoux
Current Revision Author(s)	Herve Michoux

Revision History

Revision	Date	Author(s)	Notes
DRAFT	15/1/2006	Herve Michoux	Original Release ad Draft, 8/3/2006 Updated to reflect JASANZ review, 16/12/2006 Updated to reflect ISO27001
0	27/8/2011	Herve Michoux	Initial issue as Rev 0
1	10/9/2016	Herve Michoux	Updated in line with new JASANZ requirements
2	10/7/2017	Herve Michoux	Updated as a result of the JASANZ document review
3			
4			
5			
6			
7			
8			
9			
10			

Table of Contents

1 Why Do We Have This Document?

This document describes the Certification Program offered by Global-Mark Pty Ltd to Clients seeking Information Security Management Systems Certification (ISMS).
This document is subject to change without notice. The latest version is available on our web site: www.global-mark.com.au.

2 Overview

With the increasingly important reliance on IT systems, security should be considered as key aspect of the IT infrastructure.

IT security is not only about passwords and firewalls, but also requires a system approach to its management. ISO27001 provide a framework for developing and implementing Information Security Management Systems, and organisations like Global-Mark are able to certify compliance with these standards.

This provides your organisation, its Board, staff, and customers assurance that proper systems and accountabilities are in place and can be relied upon.

The standards are totally technology independent, and focus on the management of security using a systems approach.

The standards require organisations to have in place systems (policies, procedures and records) to control the following:

- Security policy
- Security organisation
- Security of third party access
- Outsourcing
- Asset classification and control
- Personnel security
- Physical and environmental security
- Communication and operations management
- Access control
- Systems development and maintenance
- Business continuity management
- Compliance (legal, review of policy and technical compliance, system audit)

Program Summary Card	
Issue	**Program Rules/Comments**
Standard	ISO27001
Any other relevant documentation	Nil
Target Audience	Any organisation, company, or business unit with a modern IT infrastructure.
Global-Mark output document	Certificate of Approval
Other Global-Mark output document	Certification Schedule (used if all information cannot be displayed on the Certificate of Approval)
Certificate Validity Period	3 years
Certification Mark that can be used by the Client	Trust-Mark® ISMS
Can this mark be used on product?	No
Periodicity of Post-certification Reviews?	12 monthly
Periodicity of Re-certification Review	3 years
Steps to and Post-certification	
Application	✓
Document Review	✓
Pre-certification Review	Optional
Certification Review	✓
Technical File Review	Nil
Follow-up Review	✓
Post-certification Review	✓
Re-certification Review	✓

3 In Simple Terms

If you care about your security, you are organised and you can prove it, Information Security Certification should be a simple, yet important step. Certification will assist you to prove and demonstrate that you have sound systems, and you are keeping them up-to-date, and in continued compliance.

4 Specific Program Conditions

Understanding the framework

It is for your organisation to define the criteria by which information security related threats to assets, vulnerabilities and impacts are identified as significant, and to develop procedure(s) and controls for doing this. In addition,, all information related threat to assets, vulnerability or impact on the organisation identified as being significant, should be managed and controlled by the ISMS. It is required that Client have and maintain a documented ISMS compliant with ISO27001.

Global-Mark will require the organisation to demonstrate that the analysis of security related threats is relevant and adequate for the operation of the organisation. Global-Mark will establish whether the procedures employed in analysis of significance are sound and properly implemented.

Any inconsistency between the organisation's policy, objectives and targets and its procedure(s) or the results of their application will be reported by Global-Mark.

The maintenance and evaluation of legal compliance is the responsibility of your organisation. Global-Mark will restrict itself to checks and samples in order to establish confidence that the ISMS functions in this regard.

An organisation with a Certified ISMS has a management system that should achieve continuing compliance with regulatory requirements applicable to the information security impacts of its activities, products and services. Our aim is to confirm that your ISMS has the ability to provide continued compliance.

Our reviews (Certification, Post-Certification and re-Certification) will include review of the following:

- The effectiveness of the System in light of changes, and;
- The commitment to maintain an effective System.
- The degree of reliance that can be placed on internal security reviews/audits.
- Whether the procedures employed in analysis of the significance information security related threats to assets, vulnerabilities and impacts on the organization are identified, effective, sound and properly implemented
- If an information related threat to assets, vulnerability or an impact on the organization is identified as being significant, it should be managed within the Client's ISMS

4.1 Access to information

Client are required to make all necessary arrangements for the access to internal audit reports and reports of independent reviews of information security.

At least the following information shall be provided by the client during stage 1 /pre-certification review:

- general information concerning the ISMS and the activities it covers;
- a copy of the required ISMS documentation specified in ISO/IEC 27001 and, where required, associated documentation.

4.2 Minimum system implementation before certification

The ISMS needs to be submitted for review to Global-Mark for a Document Review: this is typically completed off site and includes a review of the top level document (policy manual), and a sample of lower level documents (2 or 3 procedures).

After the Document Review, Global-Mark will also complete the Pre-certification Review to review and verify that the organisation must have completed as a minimum one full:

- Management review
- Internal management system audit
- Security review, and
- Must have evaluated legal and regulatory compliance and can show that action has been taken in cases of non-compliance with relevant regulations.

Ideally these activities should have been completed before the Global-Mark Certification Review and records should be available to demonstrate their effectiveness. These requirements are not specifically called for in the above mentioned standards, but should be based on the ISO9001 requirements.

The aim of the Pre-certification Review is also to review the Statement of Applicability, and confirm its relevance to the certification process.

4.3 Sensitive/Confidential information

Before the Business Review, the Client is allowed to advise Global-Mark of what records are to be considered as confidential or sensitive: after review of the records identified, Global-Mark will confirm which records will not be examined. Global-Mark will judge whether the records to be excluded will affect the validity of the business review. If not Global-Mark will confirm that the business review can take place only when appropriate access arrangements have been accepted by the organization.

We ask that you formally advise us (at least 6 weeks prior to any on site review) if any ISMS related information (such as ISMS records or information about design and effectiveness of controls) cannot be made available for review by the Global-Mark review team because it contains confidential or sensitive information. Global-Mark shall then determine whether the ISMS can be adequately audited in the absence of such information. If we conclude that it is not possible to adequately audit the ISMS without reviewing the identified confidential or sensitive information, we will advise you that the certification review cannot take place until appropriate access arrangements are granted.

4.4 Records of breaches, complaints, incidents, corrective and preventive action

The Client should have procedures in place to deal with these and the procedure should include measures for:

- notification to appropriate authorities if required by regulation
- restoring conformity as quickly as possible
- preventing recurrence
- evaluating and mitigating any adverse security incidents and their associated impacts
- ensuring satisfactory interaction with other components of the ISMS
- assessing the effectiveness of the remedial / corrective measures adopted

4.5 Statement of Applicability

The Client needs to prepare a Statement of Applicability describing which parts of the ISMS standard or normative document are relevant and applicable to its ISMS.

The Statement of Applicability should be forwarded to Global-Mark prior to the certification review and will be part of the working documents provided to the review team. The Statement of Applicability (and its version status) is also referenced on the Certificate of Approval.

4.6 Shared services or facilities

Interfaces with services or activities that are not completely within the scope of the ISMS should be addressed within the ISMS subject to certification and included in the organisation's information security risk assessment. An example of such a situation is the sharing of facilities (e.g. computers, telecommunication systems, etc.) with others, or hardware or software being maintained by others.

4.7 Multi-sited Clients

The sampling model and conditions will be as presented in Global-Mark's Guide Note for multi-sited Clients, G-02.

The important considerations include:

- all sites are operating under the same ISMS, which is centrally administered and audited and subject to central management review; and are included in the internal ISMS audit program
- all sites have been audited in accordance with the organization's internal security review procedure(s);
- a representative number of sites (within the scope of the ISMS) will be sampled by Global-Mark, taking into account the requirements below:
    - the results of internal audits of Head Office and sites
    - the results of management review
    - variations in the size of the sites
    - variations in the business purpose of the sites
    - complexity of the ISMS
    - complexity of the information systems at the different sites
    - variations in working practices
    - variations in activities undertaken
    - the determined information security controls into account.
    - variations of design and operation of controls;
    - geographical and cultural aspects
    - risk situation of the sites
    - information security incidents at the specific sites
    - potential interaction with critical information systems or information systems processing sensitive information
    - differing legal requirements
- the sample should be partly selective based on the above and partly non-selective and should result in a range of different sites being selected, without excluding the random element of site selection
- every site included in the ISMS which is subject to significant threats to assets, vulnerabilities or impacts should be audited by Global-Mark prior to certification
- the Post-certification Plan (3 year plan) should be designed in the light of the above requirements and should, within a reasonable time, cover all sites of the organisation or within the scope of the ISMS certification included in the Statement of Applicability
- in the case of a review finding classed as nonconformity by Global-Mark being observed either at the Head Office or at a single site, the corrective action procedure should apply to the head office and all sites covered by the certification.
- Reviews shall always include the Client's Head Office activities to ensure that a single ISMS applies to all sites, and delivers central management at the operational level.
-

4.8 Certification review

This will take place at your office(s), and aims to confirm compliance with the certification standard but will also include:

- An assessment of information security related risks and the resulting design of the ISMS
- the Statement of Applicability (which is referenced with the version on the Certificate of Approval).
- objectives and targets derived from this process
- performance monitoring, measuring, reporting and reviewing against the objectives and targets
- security audits, management system audits and management reviews
- management responsibility for the information security policy
- links between policy, the results of information security risk assessments, objectives and targets, responsibilities, programs, procedures, performance data, and security reviews

4.9 Scope of certification and audits

- The Global-Mark review team shall audit the ISMS of the client covered by the defined scope against all applicable certification requirements. The Global-Mark review team shall confirm, in the scope of the client ISMS, that clients address the requirements stated in ISO/IEC 27001, 4.3.
- The Global-Mark review team shall ensure that the client's information security risk assessment and risk treatment properly reflects its activities and extends to the boundaries of its activities as defined in the scope of certification. The Global-Mark review shall confirm that this is reflected in the client's scope of their ISMS and Statement of Applicability. The Global-Mark review shall verify that there is at least one Statement of Applicability per scope of certification.
- The Global-Mark review shall ensure that interfaces with services or activities that are not completely within the scope of the ISMS are addressed within the ISMS subject to certification and are included in the client's information security risk assessment. An example of such a situation is the sharing of facilities (e.g. IT systems, databases and telecommunication systems or the outsourcing of a business function) with other organizations.
- The criteria against which the ISMS of a client is audited shall be the ISMS standard ISO/IEC 27001. Other documents may be required for certification relevant to the function performed.

4.10 Multiple management systems:

We may accept documentation that is combined (e.g. for information security, quality, health and safety and environment) as long as the ISMS can be clearly identified together with the appropriate interfaces to the other systems.
The ISMS business review may be combined with audits of other management systems, provided that it can be demonstrated that the business review satisfies all requirements for certification of the ISMS. All the elements important to an ISMS shall appear clearly and be readily identifiable in the audit reports. The quality of the business review shall not be adversely affected by the combination of the standards/business reviews.

4.11 Specific Elements of the ISMS business review

It is required that the Client:

- Demonstrate that the assessment of information security related risks is relevant and adequate for the ISMS operation within the ISMS scope;
- Establish and demonstrate that it has in place procedures for the identification, examination and evaluation of information security related risks and the results of their implementation are consistent with the client's policy, objectives and targets.

We shall also establish whether the procedures employed in risk assessment are sound and properly implemented.

4.12 Special ISMS business review(s)

Global-Mark reserves the right to perform special audits shall be subject to special provision if a client with a certified ISMS makes major modifications to its system or if other changes take place which could affect the basis of its certification.

5 What Documents/Records Are Needed To Understand This Program

In order to understand our Program you should also access and be aware of the following documents:

- G-00: Welcome Pack
- MSP-00: Introduction to our Management Systems
- MSP-01: Nomenclature and Definitions
- MSP-24: Appeals

End of Document