CERTIFICATION OF INFORMATION SECURITY MANAGEMENT SYSTEMS TO MS ISO/IEC 27001

By:

SIRIM QAS International

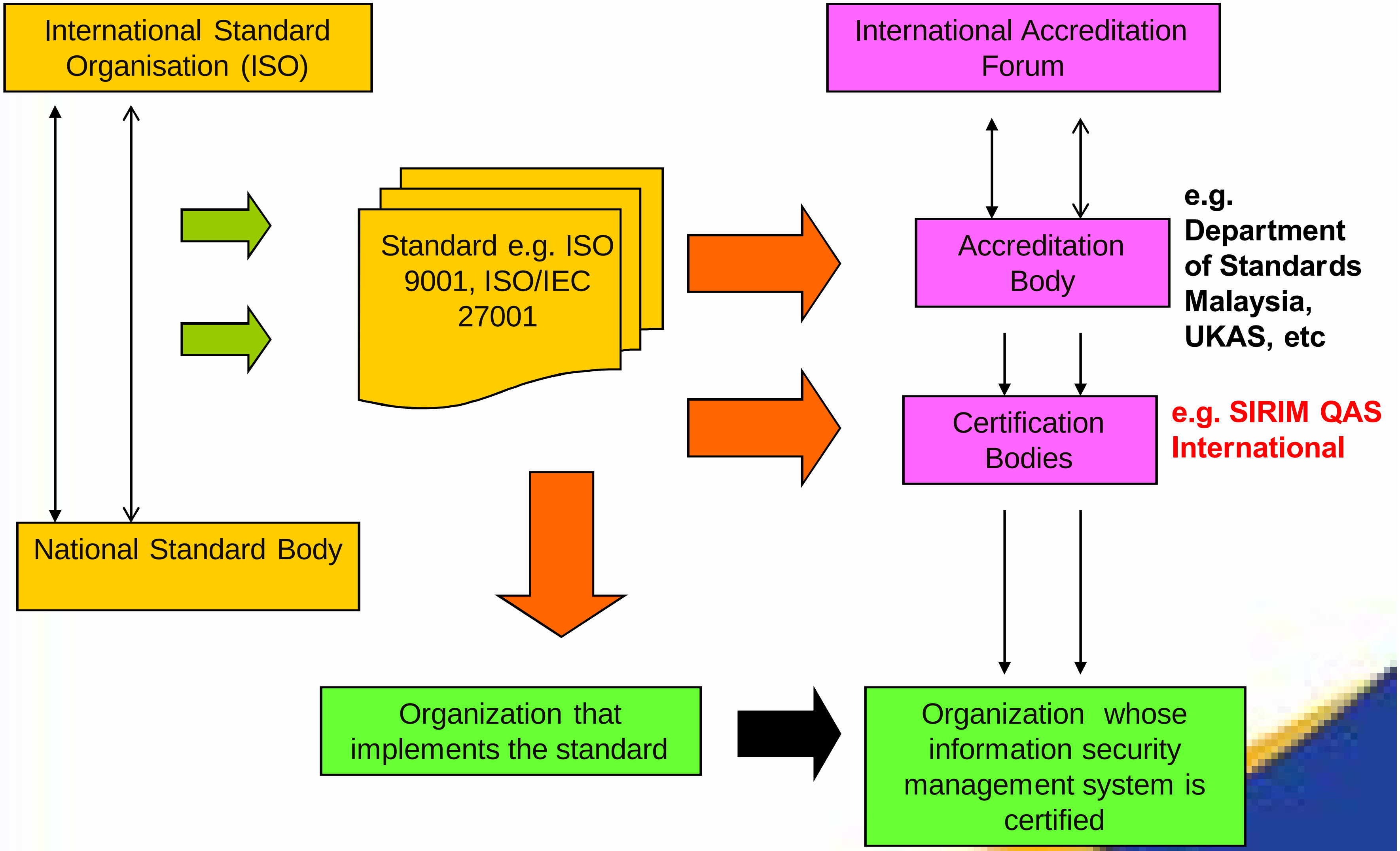
CONTENT

1. BRIEF OVERVIEW

2. ISO/IEC 27001:2005
   INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

3. CERTIFICATION TO ISO/IEC 27001

SSMENT FRAMEWORK


International Standard Organisation (ISO)

International Accreditation Forum

Standard e.g. ISO 9001, ISO/IEC 27001

Accreditation Body

e.g. Department of Standards Malaysia, UKAS, etc

Certification Bodies

e.g. SIRIM QAS International

National Standard Body

Organization that implements the standard

Organization whose information security management system is certified

ement systems?

An organizationôs structure for the identification, establishment, control, monitoring and improvement of processes and their interfaces within the organization, aimed at fulfilling specific policies and achieving related objectives of the organization

These policies and objectives could relate to quality, environmental performance, occupational health and safety, social accountability, information security etc.

IT SYSTEMS

Å **Quality Management System Certification**

ï	ISO 9001	Generic QMS
ï	ISO/TS 16949	QMS for automotive sector
ï	ISO 13485	QMS for medical device

Å **Environmental Mgt. System Certification**

ï ISO 14001

Å **Occ. Health & Safety Mgt. System Certification**

ï OHSAS 18001

ï MS 1722 Part 1

Å **Info. Security Mgmt. System Certification**

ï ISO/IEC 27001

T SYSTEMS *…continued*

Å **Food Safety Management System Certification**

ï ISO 22000

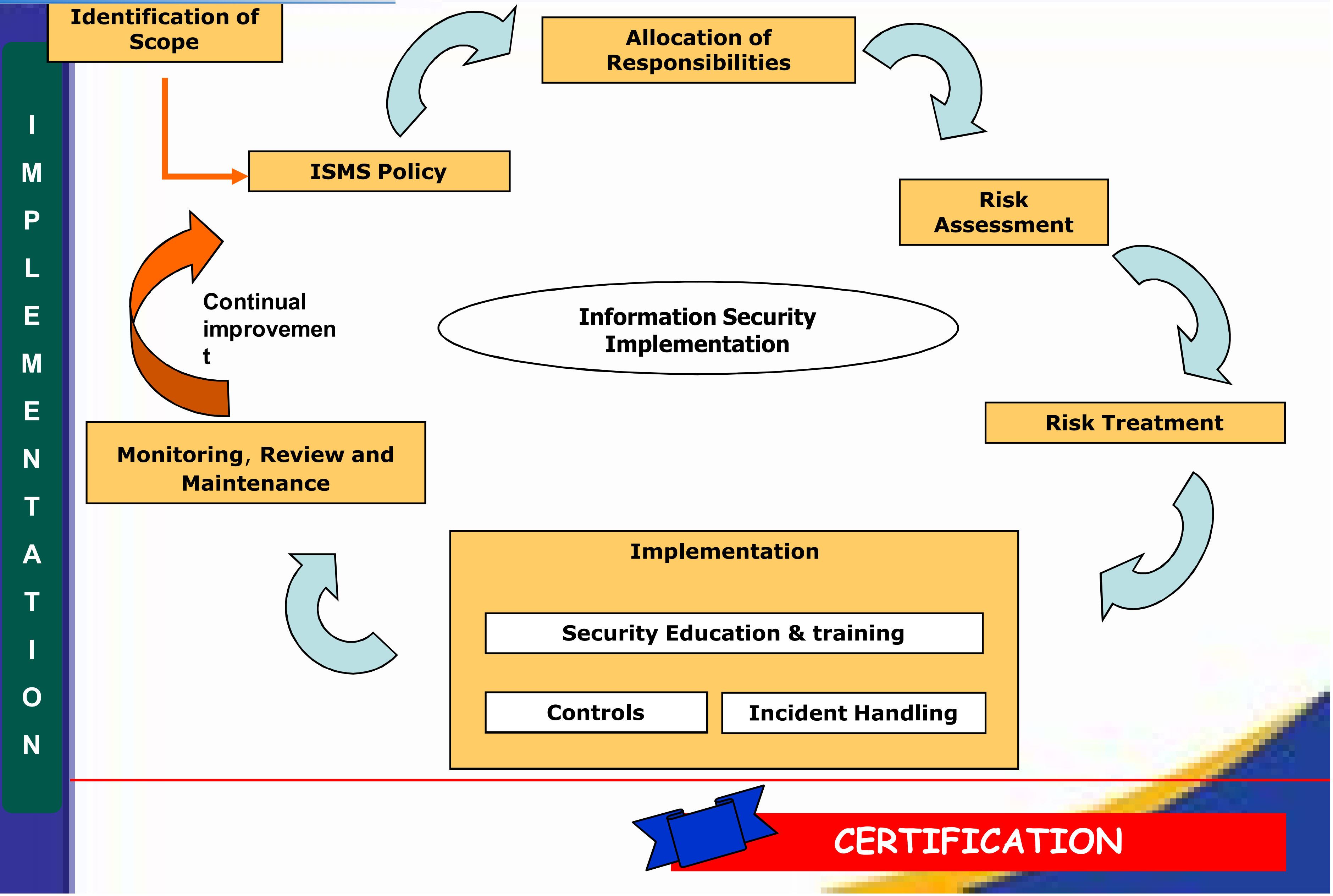
Å **Quality Management System based on Islamic Principles**

ï MS 1900

Å **IT Service Management System Certification**

ï ISO/IEC 2000 Part 1

ISMS Implementation Roadmap



IMPLEMENTATION

Identification of Scope

ISMS Policy

Allocation of Responsibilities

Risk Assessment

Risk Treatment

Information Security Implementation

Implementation

Security Education & training

Controls

Incident Handling

Monitoring, Review and Maintenance

Continual improvement

CERTIFICATION

rty certification ?

Third-party certification → carried out by an independent body

Auditing and certification carried by a body that is independent of the both the organization being audited /certified and its customer organizations

Third-party certification may be required in certain business sectors by government regulations or, may be specified by a customer or, chosen by organization as a way of differentiating its product or service

RNATIONAL’s ISMS Certification Scheme

Å ISMS certification offered since 2003

Å Certification was initially to BS 7799 Part 2

Å ISO/IEC 27001 published in 2005

Å Accredited by UKAS in March 2006

Å 1st CB in this region to be accredited

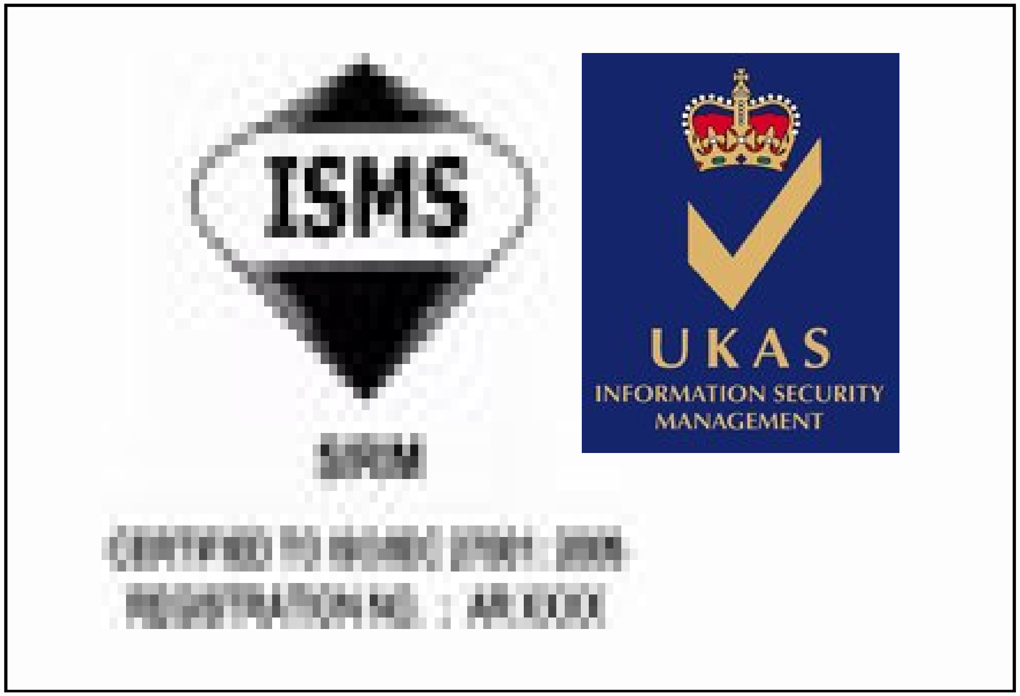
Å In the process of accreditation from STANDARDS MALAYSIA

Å Accreditation provides assurance on competence, consistency and impartiality of our auditing and certification services

ertified to ISO/IEC 27001 (ISMS) in Malaysia

- ✓ Malaysian Centre For Remote Sensing (MACRES) - Ministry of Science, Technology and the Environment
- ✓ Heitech Padu Berhad
- ✓ ISM Insurance Services Malaysia Berhad
- ✓ Malaysia Airports Technologies Sdn Bhd
- ✓ Technip Geoproduction (M) Sdn Bhd
- ✓ TM Net Sdn Bhd
- ✓ Malaysian Electronic Payment System (1997) Sdn Bhd (MEPS)
- ✓ Securities Commission
- ✓ Extol MSC Berhad (Extol Corporation (M) Sdn Bhd)
- ✓ CyberSecurity Malaysia
- ✓ EPF
- ✓ GITN
- ✓ YGL Multimedia
- ✓ Panasonic HA

ark


ISMS
SIRIM
CERTIFIED TO ISO/IEC 27001 : 2005
REGISTRATION NO. : AR XXXX
UKAS
INFORMATION SECURITY
MANAGEMENT

se of ISMS around the world

o27001certificates.com

Å ISMS certifications in **80+** countries all over the world

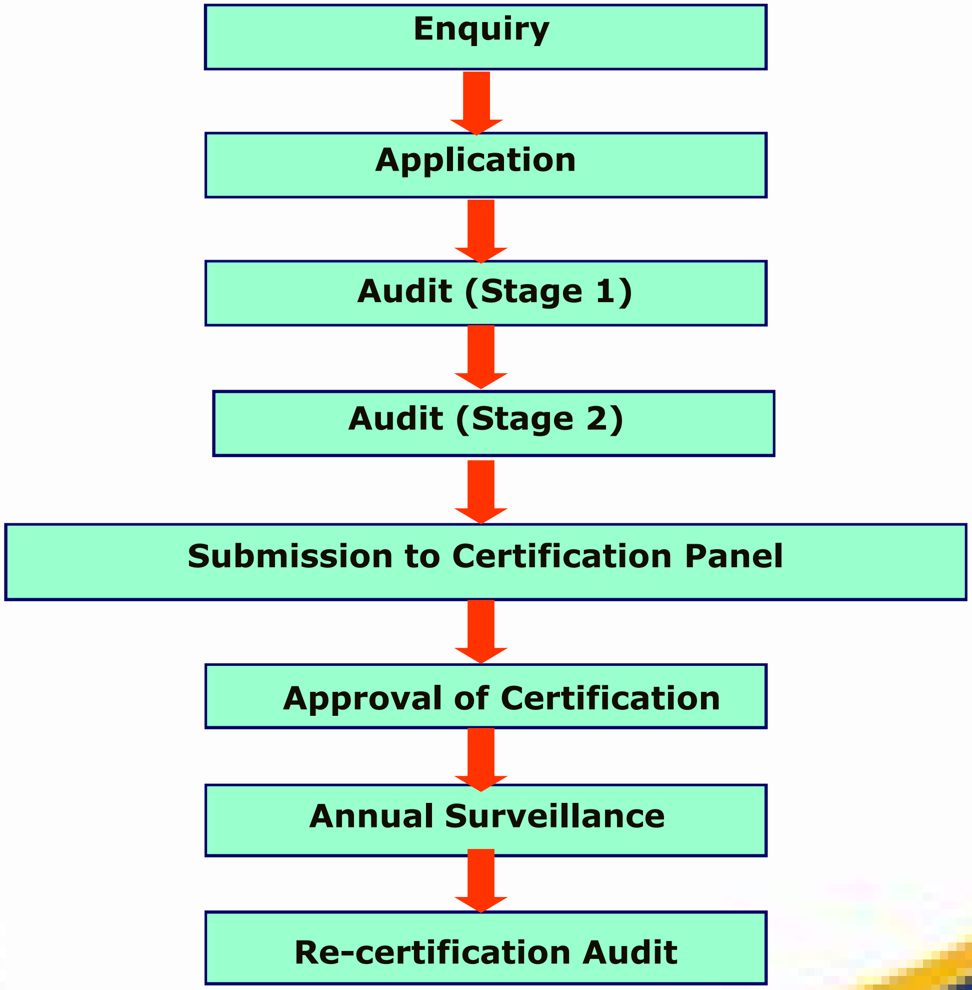
Å **6573** certificates have been issued worldwide:

Ranking by no. of certifications	Country	2009	To-date 2010
1	Japan	3480	3572
2	India	495	490
3	UK	444	448
4	Taiwan	385	373
5	China	347	373
6	Germany	136	138
7	Korea	95	106
14	Malaysia	27	39
17	Thailand	34	34
34	Singapore	12	13

cess

UKAS
INFORMATION SECURITY MANAGEMENT

ISMS
SIRIM
CERTIFIED TO ISO/IEC 27001 : 2005
REGISTRATION NO. : AR XXXX



Enquiry

Application

Audit (Stage 1)

Audit (Stage 2)

Submission to Certification Panel

Approval of Certification

Annual Surveillance

Re-certification Audit

ÅApplication package, including questionnaire sent to client

ÅClient returns filled questionnaire, providing details of organization’s scope of certification and other information needed for determining audit team composition and audit duration

ÅQuotation issued to client based on information in filled questionnaire

ÅAudit duration (Stage 1 and Stage 2) w ill vary from client to client, and is guided by accreditation requirements

ning Audit Duration

ÅStarting point for calculation is number of employees

ÅOther factors

Åsize of ISMS scope e.g. number of information systems used, volume of information processed, number of users, number of privileged users, number of IT platforms, number of networks

Åcomplexity of ISMS e.g. criticality of information systems, risk situation of the ISMS, volumes and types of sensitive and critical information handled, number and types of electronic transactions, extent of remote working taking place

Ånumber of sites within the scope, how similar or different these sites are and whether all will be audited

Åextent of outsourcing

scope

Å Management to determine key business area for an ISMS pilot project in the organization

Å Could consider the most critical information to be protected such as new product design, market research, customer’s information

Å Identify how the information flows:

- ï where it originates from;
- ï where it is transferred to;
- ï where it is stored

Å Document the scope defining:

- ï boundaries of the ISMS
- ï characteristics of the business
- ï location
- ï assets & technology
- ï justification for any exclusion from the scope

cope - Examples

Jabatan Pendaftaran Negara

Å ISMS for data centre operations covering SIREN, AFIS, IJPN/ GSCB Systems, Enterprise System Monitoring and related maintenance and support activities.

Panasonic HA Air-Con Sdn. Bhd. (including R&D Centre)

Å Information security management system for room air-conditioner manufacturing plant and R&D centre.

MACRES

Å Information Security Management System For MACRES's satellite data services.

Kem. Pertahanan M’sia, Jab Arah dan Rekod

Å Information security management system for management of service records and retirement benefits for members of the Malaysian Armed Forces

Technip Geoproduction (M) Sdn.Bhd.

Å Information Security Management System relating to engineering database for supporting project management, engineering design, procurement and construction management activities

Documentation & Readiness Review

Å To gain understanding of the organization's ISMS and assess state of readiness

Å Provide focus for planning of the Stage 2 audit

Å Review documentation as required under clause 4.3.1 of ISO/IEC 27001: 2005

Å Audit findings reported at the end of the audit, highlighting deficiencies

Å Deficiencies to be resolved before proceeding to Stage 2 audit

Å Internal ISMS Audit & Management Review to be conducted prior to the Stage 2 audit

Å Client to indicate ISMS records whose accessibility may be limited due to confidentiality or sensitivity; CB to decide on feasibility of proceeding with Stage 2 without access to these records

Implementation Audit

Å To confirm that the organization adheres to its own policies, objectives & procedures

Å To confirm that the ISMS conforms to all the requirements of the standard and is achieving the organization’s policy objectives

Å Detailed audit plan sent to client prior to audit – what activities will be audited, when and by whom

Å Auditors review records, interview personnel and generally observe operations & implementation of controls

Å Certification recommended if no major non-conformance raised

Å Report presented to client at the end of audit

Å All non-conformances have to be responded to and closed out before recommendation is progressed further

tification

Å Audit team follows up on non-conformities and puts up recommendation after satisfactory resolution of all non-conformities

Å Report and recommendation by audit team is reviewed by independent reviewer

Å Supported recommendation presented to the weekly Certification Panel (internal committee) meeting for approval

Å Applicant notified of approval after meeting

Å Certificate is valid for three years from certification decision date

Å Certificate sent to client upon payment of relevant fees

nce

Å Minimum one surveillance audit per year required – has to be carried out within 12months of Stage 2 audit

Å Duration based on guidelines - annual surveillance audit duration ~ ⅓ the initial audit duration

Å Carried out to verify that system is maintained satisfactorily

Å Coverage includes:

ï Re-assessment of risk, updated security plans
ï Statement of Applicability
ï Sampling of controls and sites
ï Corrective Action
ï Preventive Action
ï Internal ISMS Audit
ï Management Responsibility (management review results & action)
ï Progress towards continuous improvement

Å Carried out every third year for renewal of certificates

Å Recertification audit and decision shall be before the expiry of the certificate

Å Audit duration is ~ ⅔ the initial audit duration

Å Complete system covered to ensure that the system as a whole is implemented satisfactorily

Å New certificate issued only after all non-conformances are closed out

ication Cost

Application fee	RM 500

Initial Certification Audits:

Å Stage 1 audit	@RM1200 X Auditor Day
Å Stage 2audit	@RM1200 X Auditor Day
Å 1st Year Certification Fee	RM 1000.00

Yearly Audits (Year 1 & Year 2) :

Å Surveillance Audits	~1/3 of Initial Certification audit costs
Å Yearly Certification Fee	RM1000.00

Renewal (Prior to expiry of certificate in Year 3)

Å Re-Certification Audit	~2/3 of Initial Certification audits costs
Å Yearly Certification Fee	RM 1000.00

Note: The above audit related charges do not include incidental costs which cover travel, accommodation and daily subsistence

Å You cannot be certified to ISO/IEC 27002 (previously known as ISO/IEC 17799); it is a Code of Practice

Å Do not fit yourself into the Standard – the Standard fits you, whatever size your organization is

Å You do not have to implement all the controls specified in ISO/IEC 27002 to get certified. Controls should be selected based on the result of a risk analysis

Å You do not have to certify the whole organization all at once; you can scope part of the organization to be certified

in implementation

Å Lack of senior management commitment

Å Lack of employee awareness on the developed policies or procedures

Å Lack of clear understanding on asset classification

Å Implementation flaws ï failure to integrate ISMS into the existing operations

Å Lack of resources

Å Focus only on controls implementation

s

Å Provides a structured and sustainable approach for protecting one of the organizationâs most important assets ï INFORMATION

Å Improved management to address the ever increasing security threats from a wide-range of sources: computer assisted-fraud, espionage, sabotage, vandalism and natural disasters

ification

Å Implementing and obtaining certification of an organizationôs Information Security Management System provides assurance to customers and stakeholders that their information is protected and secured from damage, loss and misuse.

Å Certification to ISO/IEC 27001 is a recognition that an organization has implemented an Information Security Management System based on an internationally accepted standard.

THANK YOU

SIRIM QAS International Sdn. Bhd.
Building 8, No. 1, Persiaran DatoôMenteri
Section 2, P.O. Box 7035
40911 Shah Alam
Selangor Darul Ehsan