



# MSC Malaysia Information Security Management System (CDP ISMS) Programme

## Application Guidebook



# TABLE OF CONTENTS

Preface.....	3
Programme Overview.....	4
Programme Objective .....	4
International Organisation for Standardization ( ISO ).....	5
Programme Approach.....	6
Eligibility Criteria.....	6
Application Process.....	7
Overall Approval Process.....	10
Contractual Requirements.....	11
Funding Arrangements.....	11
Incentive Reimbursement Guidelines.....	11
Administrative Highlights.....	12
Participation Guidelines.....	12
Mandatory Requirement.....	12
Implementation Agent.....	12
Change of Company Status and Project Details.....	12
Programme Information and Contact.....	13
Appendixes.....	14
Appendix I.....	14
Appendix II.....	15
Glossary and Terms.....	17

# PREFACE

## MSC Malaysia

MSC Malaysia is a national initiative spearheaded by the Malaysian Government to promote both the national ICT industry and provide a test-bed for the global ICT industry. MSC Malaysia provides a conducive enabling environment designed to facilitate companies to harness the full potential of ICT and multimedia technologies. With its ideal business environment coupled with availability of talent resources, the MSC Malaysia has attracted participation from major global ICT companies to develop and host their leading edge technologies in the designated MSC Malaysia Cybercities. MSC Malaysia also provides the ideal growth environment for Malaysian ICT SMEs to transform themselves into world-class companies.

## MSC Malaysia Capability Development Programme

### *Maximising Your Potential*

MSC Malaysia Capability Development Programme (CDP) is an MDeC initiative designed to help ICT organisations and individuals to maximise their potentials by adopting global good practices, process improvements and professional certifications. It aims at enabling them to focus on their core competency and hone their competitive edge. CDP provides monthly dialogues, seminars, workshops, clinics and financial incentives developed to gear the MSC Malaysia status companies to achieve certifications that would ensure business continuity.

# PROGRAMME OVERVIEW

## MSC Malaysia Information Security Management System (CDP ISMS)

Page | 4

An Information Security Management System (ISMS) is an organisational approach to information security. It is a management system based on a systematic business risk approach, to establish, implement, operate, monitor, review, maintain, and improve information security. As the market gets more competitive and customers become more demanding and sophisticated, it is important for the local ICT organisations to implement an organisation-wide information security management framework (beyond the technical and physical aspects) to give their customers and users greater confidence and assurance.

Upon implementing an ISMS, organisations should consider going through the process to be certified against the ISO 27001:2005 standard. This requires an organisation to undergo auditing processes by a respected, independent and competent third party known as Certification Body. Ultimately, it provides an assurance that the certified organisation has implemented a system for the management of information security in line with an international standard. The organisation is seen to be more credible and serious about information security management, although may not be perfect but demonstrates continuous and managed improvement.

Multimedia Development Corporation (MDeC) concurs that local ICT organisations should be encouraged to obtain recognition in the form of attainment of an internationally recognised certification/assessment. ISO 27001:2005 certification will help the MSC Malaysia status organisations improve their information security management capabilities and to be more competitive in the global market. This is also in line with the MSC Malaysia vision to realise Malaysia as a global hub and preferred location for ICT and multimedia innovations, services and operations.

The CDP ISMS programme aims to furnish assistance & initiatives to local MSC Malaysia status organisations in implementing information security management system best practices and attain ISO 27001:2005 certification.

### Programme Objectives

- Provide support to MSC Malaysia status organisations to attain ISO 27001:2005 certification.
- Raise the information security management system capabilities of participating organisations to compete successfully in the global market and to be a global player.

## International Organisation for Standardization (ISO) and ISO Standards

International Organisation for Standardization (ISO) is the world's leading developer of International Standards. ISO is a non-governmental organisation; a federation of the national standards bodies of 157 countries. It is the global network that identifies what International Standards are required by business, government and society, develops them in partnership, adopts them in transparent procedure based on national input and delivers them to be implemented worldwide. Page | 5

ISO standards specify the requirements for the state of the art products, services, processes, materials and system, and good for conformity assessment, managerial and organisational practice. It is based on international consensus by industry expert makes it widely respected and accepted by public and private sectors internationally. The standards ensure vital features of quality, ecology, safety, economy, reliability, compatibility, efficiency and effectiveness. Once ISO International Standards are published, it may be adopted and translated as a national standard by ISO members. The transparency of requirements in ISO standards makes it organisations to be able to compete in an equal basis in any market in the world.

### ISO/IEC 27001:2005

ISO/IEC 27001:2005 covers all types of organisations (e.g. commercial enterprises, government agencies, not-for profit organisations). ISO/IEC 27001:2005 specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System within the context of the organisation's overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual organisations or parts thereof.

ISO/IEC 27001:2005 is designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties.

ISO/IEC 27001:2005 is intended to be suitable for several different types of use, including the following:

- use within organisations to formulate security requirements and objectives;
- use within organisations as a way to ensure that security risks are cost effectively managed;
- use within organisations to ensure compliance with laws and regulations;
- use within an organisation as a process framework for the implementation and management of controls to ensure that the specific security objectives of an organisation are met;
- definition of new information security management processes;
- identification and clarification of existing information security management processes;
- use by the management of organisations to determine the status of information security management activities;

- use by the internal and external auditors of organisations to determine the degree of compliance with the policies, directives and standards adopted by an organisation;
- use by organisations to provide relevant information about information security policies, directives, standards and procedures to trading partners and other organisations with whom they interact for operational or commercial reasons;
- implementation of business-enabling information security;
- use by organisations to provide relevant information about information security to customers.

(Source: <http://www.iso.org>).

## Programme Approach

To encourage the adoption of global best practices, Multimedia Development Corporation (MDeC) has come up with another specially designed programme model to introduce and encourage MSC Malaysia Status Organisations to embark on the journey for quality excellence. The programme is developed to assist organisations in terms of lessening their financial burden by providing incentives to those who successfully obtained the ISO/IEC 27001:2005 certification.

Participating organisation is given the flexibility to choose any registered consulting organisations that specialises in ISMS, hereafter termed as “service provider”, to guide them in attaining ISO/IEC 27001:2005 certification. Key guidelines for selecting consulting organisations are attached in Appendix I.

Incentive to participating organisation will be provided based on reimbursement model; which is claimable upon attainment of the certification. For more details on funding, please see under funding arrangement below.

## ELIGIBILITY CRITERIA

Interested Organisation must satisfy the following set of criteria in order to qualify for the Programme.

The eligibility criteria are as follows:

- Must be a MSC Malaysia Status Organisation.
- At least 51% Malaysian owned.
- Staff strength of equivalent or more than 20.
- Revenue of equivalent or more than RM 500,000
- Must be willing to commit resources (Financial and Human Capital resources) to complete the whole programme.
- Must be willing to participate in activities organized by MDeC, such as dialogues and workshops.
- QMS (ISO 9000) and ITSM (ISO 20000) certifications are an added advantage for consideration.

- Successful Organisation must be willing to participate in activities undertaken by MDeC in relation to capability development including surveys, benchmarking and community projects.

## APPLICATION PROCESS

### Application Process and Deadlines

*Before applying for the programme, those interested are strongly encouraged to contact the [ISMS Programme Secretariat](#) first for discussion.*

The application form can be downloaded from the CDP website <http://cdp.mscomalaysia.my/>. All sections of the application form have to be completed with supporting documents wherever required.

Before filling in an application form, please read this Guide carefully. Each applicant organisation should submit only one application form for the Programme. No application fee will be charged.

The application form with all supporting documents should be sent to the Secretariat.

MDeC reserves the right to amend or delete any section of this Application for Incentive at any time without prior notice in order to give effect to any change in policy or to correct any error, omission, ambiguity or inconsistency that may arise. In the event of any amendments to the application document, all applicants will be notified accordingly.

All applications shall be in English; or if not in English, shall include an English translation as an attachment. The appendices can be submitted in Bahasa Malaysia or English.

MDeC shall not be liable to any payment or costs incurred in the preparation and submission of the Application Form. All expenses incurred by the applicants in providing the application shall be borne by the applicants themselves.

No advertisement or press release regarding the application shall be published in any newspaper, magazine or any other form of media, electronic or otherwise.

After the issuance of the Application Form, information relating to the contents, examination, evaluation and recommendations concerning will not be disclosed to persons not officially concerned with the process. MDeC is not obliged to inform or provide the details of the incentive evaluation process either the successful or unsuccessful applicants in Application of Incentive.

The application will be screened for completeness. If an application cannot be accessed due to insufficient information, the secretariat will send a Request for Information letter to the applicants.

The successful application (if any) shall be notified in writing through Letter of Eligibility.

## Vendor Selection and contractual requirement

Page | 8

Upon receiving of Letter of Eligibility, successful applicants should start to select a vendor to provide consultancy for its ISMS project through competitive bidding. The applicant should ensure that the selection must be carried out in an unbiased and fair manner with **minimum three vendors'** quotations to be obtained.

As each applicant may have its own considerations on cost, practice and quality requirement, the applicant is free to choose any vendor for its ISMS assessment. However, if the lowest bid is not selected, a justification must be given. In case that less than three vendors' quotations are obtained, explanation must also be given.

Once the vendor is selected, the applicant should submit to the Secretariat the received quotations, the quotation selection justification and a schedule of project for reference. The Secretariat will check the reasonableness of the price and the schedule in the quotations. If the Secretariat is not satisfied, the applicant will be required to discuss with the vendors and resubmit the related documents. If the submission is still found to be unsatisfactory or exceeds the deadline of re-submission as specified by the Secretariat, the Secretariat reserves the right to cancel the approved application and give the chance to other applicants in the waiting list.

Completed submission will be reviewed by the Committee. Following that the recommendations will be made to MDeC Management. Upon approval, a notification email will be sent out to the applicant on the decision.

The successful applicant will be required to sign a formal agreement with the MDeC and comply with all the terms and conditions laid down in the agreement, this Guide and all instructions and correspondences issued by the Secretariat from time to time in respect of the Programme and the approved application.

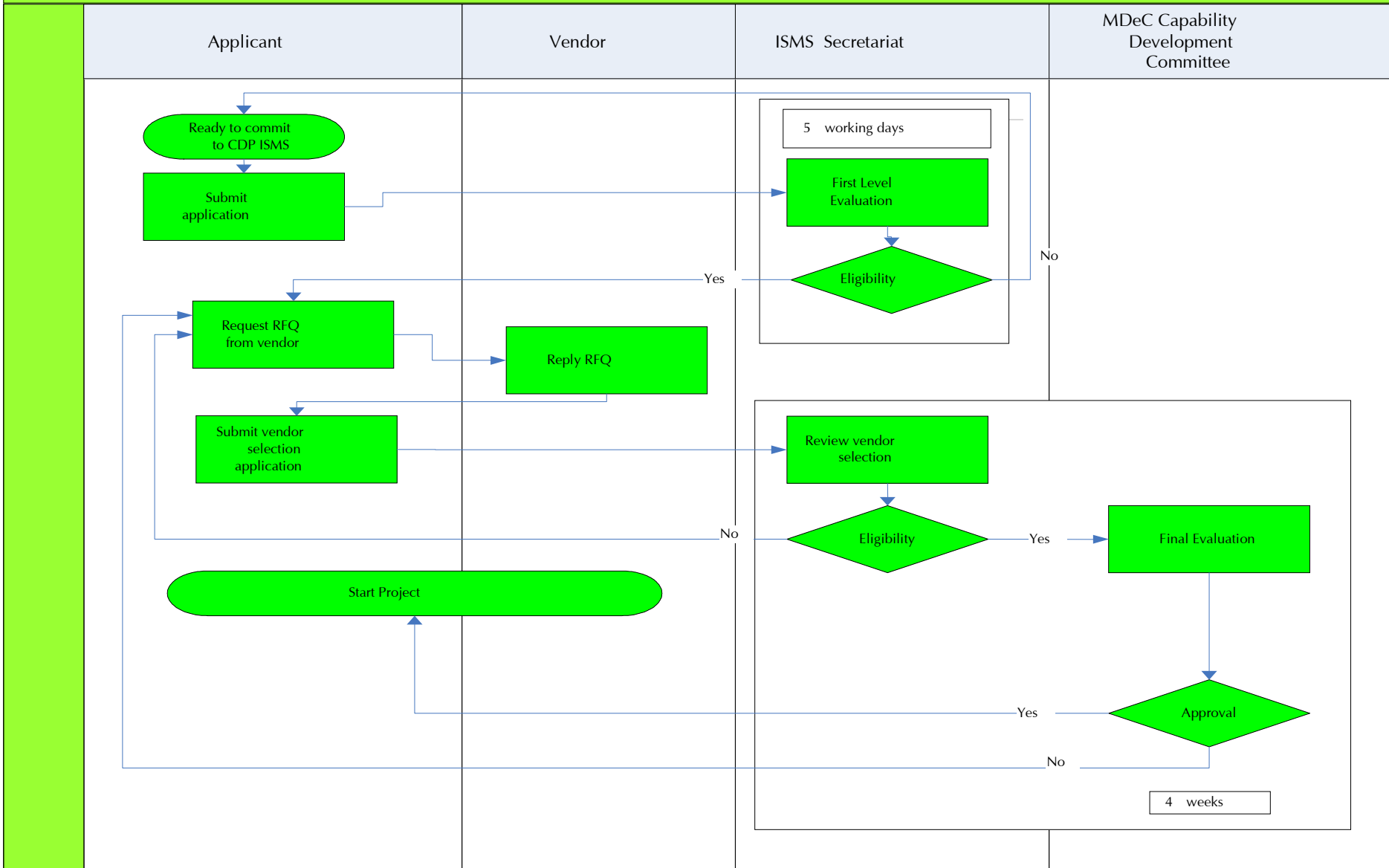
The applicant can only award the ISMS project to the vendor once the agreement has been signed.

The vendor selection process can be summarised as below:

- Applicant is required to select a vendor based on a competitive bidding exercise.
- A minimum of **3 quotations must be obtained**.
- Applicant is then required to present the selection result to the ISMS Programme Secretariat.
- The findings will be presented to the Capability Development Committee.
- The Committee will review and approve or reject the vendor selection.

- The applicant signs a formal agreement with MDeC.
- The ISMS project can only be initiated upon signing of the formal agreement.
- The award to the vendor also can only be done upon signing of the formal agreement.

# Overall Approval Process



## CONTRACTUAL REQUIREMENTS

The successful applicant (Participating Organisation) will be required to sign a formal agreement with MDeC and comply with all the terms and conditions laid down in the agreement, this Guidebook and all instructions and correspondences issued by the Secretariat from time to time in respect of the Programme and the approved application. Applicants will have 14 days from the date of the letter of approval in which to sign the agreement and return it to the Programme Secretariat. Should the applicant is unable to finalise the agreement within this period the offer of funding incentive may lapse.

Offer of funding incentive is conditional upon MDeC and the applicant signing the agreement. Programme funding is subject to appropriation period of the Ninth Malaysian Plan Funding (RMK9).

## FUNDING ARRANGEMENTS

Incentive to participating organisations will be provided based on a reimbursement model; which is claimable upon achievement of the ISO 27001:2005 certification. A maximum incentive of RM 50,000 or 50% of total project cost (subject to terms and references), whichever is lower is offered to the participating organisations.

### Incentive Reimbursement Guidelines

- Participating organisations shall bear the total cost of the project.
- The approved incentive will be in accordance with the selected quotation and the condition of a maximum predetermine cap amount.
- Once the agreement is signed, unless approved by the Capability Development Committee, no amendment can be made to the approved funding, even if additional services are added to the selected quotation.
- Upon completing the project, all original payment documentations on investments costs on consultancy and certification must be submitted to MDeC for reimbursement.
- A copy of the ISO certificate received shall be furnished to MDeC before the incentive is disbursed.
- Reimbursement must be sought within 12 months upon signing agreement with MDeC.
- Reimbursement covers:
  - Consultancy costs
  - Training costs
  - Accredited Certification Body's application fee
  - Accredited Certification Body's audit and certification fee (first year only)
- Reimbursement shall not cover:

- Any out of pocket expenses.
- Technical aspects of project implementation such as tools, penetration testing, vulnerability assessments and etc.
- Incidental expenses for Auditors ( travel, accommodation and etc)
- MDeC has the right to amend the reimbursement payment amounts or maximum value, if deemed necessary.
- Without limiting MDeC's rights, MDeC may withhold or suspend any payment in whole or in part until the participating organisation have performed its obligations in accordance with agreed terms.

## ADMINISTRATIVE HIGHLIGHTS

### Participation Guidelines

1. Participating Organisations are entitled for **ONE time** reimbursement only and reimbursement for recertification will not be covered. However, applications from organisations to undergo recertification are acceptable for those eligible organisations that have attained ISO/IEC 27001 certification prior to the establishment of the CDP ISMS Programme.
2. Agreements are to be signed between the Participating Organisations and MDeC.

### Mandatory Requirement

Applicants are required to comply with the CDP ISMS Application Form instructions, procedures, eligibility criteria described in this document. Failure to do so may cause the application to be disqualified and rejected.

### Implementation Agent

MDeC is the implementation agent of the Programme; and the Programme Secretariat under MDeC is responsible for the overall administration of the Programme. In detail, the Secretariat will process all applications submitted by applicants, monitor the progress of each approved application and arrange for funding disbursement based on the disbursement guidelines upon the satisfactory achievement of the ISO 27001:2005 certification and the documentary proof submitted. Therefore participating organisations are required to invite secretariat into project review meetings with their service providers.

### Change of company status and project details

An approved application is required to be carried out strictly in accordance with its application form appended to the agreement. The applicant organisation must inform the Secretariat in writing for any modification, amendment or addition to the application form or the agreement, including change of company status, project in-charge, management structure, project commencement or completion dates, assessment scope, methodology, fee schedule and etc. The Secretariat reserves the right to react to these changes.

## **Programme Information and Contact**

Enquiries can be submitted in writing by mail, fax or e-mail to:

### **MSC Malaysia Information Security Management (CDP ISMS) Programme Secretariat**

---

Page | 13

Capability Development Department  
Multimedia Development Corporation  
MSC Headquarters  
Persiaran APEC  
63000 Cyberjaya  
Selangor Darul Ehsan

Phone : + (603) 8312 3012  
Fax : + (603) 8318 8511  
E-mail : kmuhu@mdec.com.my

**Attention: Mr. Muhundhan Kamarapullai, CPM (Asia Pacific)**

# APPENDIXES

## APPENDIX I : Key Guidelines in Selecting Qualified Service Provider

Page | 14

1. Must be able to prove past experience in ISO 27001/ BS 7799 with references sites (local and / or regional)
2. Must have at least 1 local / foreign references Certified to ISO 27001/ BS 7799.
3. Must have at least 1 Lead Assessor as the senior consultant.
4. Must have all other consultants certified to ISO 27001/ BS 7799.
5. Possess partnerships on Technical Side (e.g. CISSP, Certified Ethical Hackers).
6. Minimum industry experience of 2yrs.
7. Duration of project proposed should not be more than 10 months.
8. The final objective / output proposed must be an ISO 27001 certificate for the applicant.
9. Must have significant training track records.
10. Proposed project cost is fixed. Service Provider must see the project through at no additional costs in case if the project is delayed or the participating organisation is not certified to ISO 27001 in the timeframe stipulated.
11. Scope of the project should not include Technical Aspects such as Tools or Penetration testing, Vulnerability assessment and etc.

## APPENDIX II : Selecting An Accredited Certification Body

(Adapted from: [www.iso.org](http://www.iso.org))

When choosing a certification body to carry out ISO certification, these are **the aspects the organisation needs to take into account.**

Page | 15

1. The first point is that **an organisation can implement ISO 27001 without seeking certification.** The best reason for wanting to implement the standards is to improve the efficiency and effectiveness of company operations. Certification of your management system is not an ISO 27001 requirement.
2. Deciding to have an independent audit of your system to confirm that it conforms to ISO 27001 is **a decision to be taken on business grounds:** for example:
  - if it is a contractual or regulatory requirement
  - if it is a market requirement or to meet customer preferences
  - if it falls within the context of a risk management programme
  - or if you think it will motivate your staff by setting a clear goal for the development of your management system.
3. **Criteria to consider** include:
  - evaluate several certification bodies.
  - bear in mind that the cheapest might prove to be the most costly if its auditing is below standard, or if its certificate is not recognized by your customers.
  - establish whether the certification body has auditors with experience in your business sector.
  - following the publication of the ISO 9000:2000 series, establish whether the certification body has integrated the evolution in the focus of the standards from conformity to performance.
4. **Another point to clarify is whether or not the certification body has been accredited and, if so, by whom.** Accreditation, in simple terms, means that a certification body has been officially approved as competent to carry out certification in specified business sectors by a national accreditation body. **In most countries, accreditation is a choice, not an obligation** and the fact that a certification body is not accredited does not,

by itself, mean that it is not a reputable organisation. For example, a certification body operating nationally in a highly specific sector might enjoy such a good reputation that it does not feel there is any advantage for it to go to the expense of being accredited. That said, **many certification bodies choose to seek accreditation**, even when it is not compulsory, in order to be able to demonstrate **an independent confirmation of their competence**.

For more information, kindly log on to [www.iso.org](http://www.iso.org)

## Glossary and Terms

ICT	Information and Communication Technologies
MSC Malaysia	Multimedia Super Corridor Malaysia
MDeC	Multimedia Development Corporation Sdn. Bhd.
ISMS	Information Security Management System
CDP ISMS	MSC Malaysia Information Security Management System Programme
Applicant Organisation	MSC Malaysia status companies that have submitted applications to MDeC to enrol in the SPI Programme
Participating Organisations	MSC Malaysia status companies that have been accepted by MDeC into the CDP ISMS programme
ISO	International Organisation for Standardisation
Accredited Certification Body	A certification body that has been officially approved as competent to carry out certification in specified business sectors by a national accreditation body
QMS	Quality Management System
ITSM	Information Technology Service Management