Overview of Implementation of Information Security Management System (ISMS) to ISO/IEC 27001

1 Get the Standards

(1) Download **ISO/IEC 27000** free from the following link (or buy it from ISO as PDF and EPUB).

http://standards.iso.org/ittf/PubliclyAvailableStandards/c073906_ISO_IEC_27000_2018_E.zip

(2) Buy **ISO/IEC 27001** and **ISO/IEC 27002**.

NOTE *ISO/IEC 27002 provides guidance on how to implement the controls of ISO/IEC 27001, Annex A.*

2 Assign Key Roles

Assign responsibilities for some or all of the following, as appropriate.

(A) Person responsible for secure operation of ICT facilities, e.g. Network Manager

(B) Person(s) responsible for operation of the ISMS.

(C) ISMS Auditor(s)

NOTE *If your organisation operates a computer network and/or any other Information and Communications Technology (ICT) facilities, one auditor must possess ICT competence, to audit the operation of the ICT facilities.*

(D) Person responsible for oversight of the ISMS.

NOTE *One person, an ISMS Manager, may perform both functions (B) and (D). If so, an auditor must audit ISMS work that the ISMS Manager does.*

2 Train People

Procure some or all of the following training, as required.

(1) Technical ICT Security – For Role (A).

(2) ISO/IEC 27001 Introduction – For all Roles (A), (B), (C) and (D).

(3) ISO/IEC 27001 (Lead) Implementer – For Roles (B) and (D).

(4) ISO/IEC 27001 Internal Auditor – For Roles (B) and (C).

(5) General Data Protection Regulation (GDPR):

- (a) Introduction;
- (b) Data Protection Officer (DPO);
- (c) Data Protection Impact Assessment (DPIA);
- (d) Subject Access Request.

4 Establish the ISMS

(1) Compile the Information Asset Register.
(2) Compile the Context and Interested Parties.
(3) Compile the Opportunities and Risks Register.
(4) Compile the Information (Security) Risk Register.

(5) Compile the Statement of Applicability (SoA).
This document details the following for each ISO/IEC 27001, Annex A control.
  (a) Whether you ***Include*** or ***Exclude*** the control.
  (b) The ***Reason*** that you include or exclude the control.
  (c) If you include it, whether it is ***Implemented*** (yet) or ***Not***.
  (d) If implemented; ***How*** you implement it. – THIS IS NOT REQUIRED.

(6) Compare the Information Risk Register and SoA against Annex A to ensure completeness.
(7) Write the Policies, Objectives and Procedures.
(8) Determine how to Measure and/or Monitor the Objectives.
(9) Complete all Required (and Additional) Documentation.

5 Operate the ISMS (initially for at least 6 months)

(1) Operate the ISMS.

  (a) Train all workers.
  (b) Implement Policies and Procedures.
  (c) Measure and/or Monitor Objectives.
  (d) Manage Incidents and Non-Conformities

(2) Perform Internal Audits (except for Internal Audit of Management Review).

(3) Review the Context and Interested Parties.
Review the Opportunities and Risks Register.
Review the Information (Security) Risk Register.
Review the Statement of Applicability.

(4) Perform Management Review (and then perform Internal Audit of Management Review).
(5) Improve the ISMS.

6 Certify the ISMS to ISO/IEC 27001

(1) Certification Audit – Stage 1 – Review of Documentation of ISMS.
(2) Certification Audit – Stage 2 – Review of Operation of ISMS.
(3) Achieve certification and receive the certificate and certification logo.

7 Publicise Your Certification

(1) Put the certification logo and certificate on your website.
(2) Put the certification logo on your marketing materials and documentation.

8 Continually Operate, Improve and Recertify the ISMS

(1) Continually operate the ISMS.
(2) Continually improve the ISMS.
(3) Recertify the ISMS every three years.