

Information Security Manual

Reference: INFO SEC MAN

DocumentKits Issue No: 2.0

Organisation Issue No:

DocumentKits Issue Date: 01/06/2020

Organisation Issue Date:

ISO 27001 ISMS INFORMATION SECURITY MANUAL

Organisation Name

0. Introduction

1. Scope

2. Documentation

3. Information security management system

4. Context of organisation

5. Leadership

6. Planning

7. Support

8. Operation

9. Performance evaluation

10. Improvement

Annex A – Control objectives and controls

Control A.6 Organisation of Information Security

Control A.7 Human Resource Security

Control A.8 Asset Management

Control A.9 Access Control

Control A.10 Cryptography

Control A.11 Physical and Environmental Security

Control A.12 Operations Security

Control A.13 Communications Security

Control A.14 System Acquisition, Development and Maintenance

Control A.15 Supplier Relationships

Control A.16 Information Security Incident Management

Control A.17 Information Security Aspects of Business Continuity Management

Control A.18 Compliance

Document Owner & Approval

0. Introduction

0.1 This manual provides the framework for the policies and procedures that the Top Management of Organisation Name has adopted to implement an information security management system that complies with ISO/IEC 27001:2013 ("the ISMS").

"This manual was originally issued on [date] to comply with ISO/IEC 27001:2005, but has now been revised to comply with ISO/IEC 27001:2013 and this revised version was issued on [date]."

0.2 This manual explains Organisation Name's approach to information security and privacy and contains both the management policy statement on information security in Organisation Name and the controls identified in Annex A of ISO 27001:2013 that apply to Organisation Name.

ISO 27000:2018 provided definitions that are used in this ISMS.

ISO 27002:2013 provided guidance on the selection and implementation of controls.

"The ISMS is part of an integrated management system that also conforms to the requirements of ISO 9001/ISO 14001, etc. For this reason, the following clauses are dealt with like this:"

0.3 Organisation Name's document control procedures (reference 2.2 in this manual) apply to this manual and to all other documents within the ISMS.

0.4 Change history

Details of any changes to this manual are recorded in the Document owner and approval section at the end of this document.

Issue of this manual is authorised by:

"[]"

Signature of Chief Executive Officer (CEO)

On:
"[]"

1. Scope

1.1 Scope of the ISMS

"In this section, you need to set out the scope and boundaries of your ISMS, describing precisely the organisational entity that is covered by it and within which it will apply. Critically, this must include absolute precision about which information assets are included and where the boundaries are. As such, you should ensure that all relevant information assets are included within the scope, which may include personally identifiable information.

Cross-check your scoping work with the extended definition of information security that appears in the [Information Security Policy](#) in section 5. The final words that you agree with the certification body to go on your certificate should appear here. Also take guidance from [section 4.3](#) of this manual."

1.2 Definitions

Where terms that are used in ISO 27001:2013 or ISO 27002:2013 are used here, the definitions provided in ISO 27000:2018 are applied.

In particular, the information security management system ("ISMS") is defined as the part (which includes organisational structure, policies, planning activities, plans, responsibilities, working practices, procedures, processes and resources) of Organisation Name's overall management system that, based on a business risk approach, enables management to establish, implement, operate, monitor, review, maintain and improve information security within Organisation Name.

"For the purposes of Organisation Name, this extends to personally identifiable information held and processed, and protecting the rights of the PII principals concerned."

2. Documentation

2.1 Organisation Name's ISMS documentation consists of:

2.1.1 The [Scope Statement](#) (section 1 above), [Information Security Policy](#) (section 5 below) and the [Statement of Applicability](#). This manual is, together with any separately published policies, Organisation Name's primary ISMS documentation.

The control objectives described in this manual are achieved by controls that include policies (which provide Board of Directors approved guidelines on specific control areas)

and procedures. These policies are either included in, or referenced from, this manual (ISO 27001 7.5.1).

2.1.2 The separate, version-controlled risk assessment report and risk treatment plan, whose preparation follows the methodology described in section 6 of this manual (ISO 27001 6.1.2 and 6.1.3).

2.1.3 Records of how Organisation Name applied (and continues to apply) its continual improvement process, which is described in section 3 of this manual, in improving the suitability, adequacy and effectiveness of its ISMS (ISO 27001 4.4 and 10).

2.1.4 Those procedures, that describe how the policies are implemented, and which are identified in this manual but are separate from it, are second-level documents (ISO 27001 7.5.2 and 7.5.3).

2.1.5 Work instructions and operations work instructions, which set out specific requirements for the performance or execution of specific tasks, including for the measurement of the effectiveness of the controls, in Organisation Name generally and in the IT Department specifically, and which are identified in procedures, and similar documents, such as user agreements and job descriptions, are the third level of documentation.

2.1.6 Records of Organisation Name's control of its information security and privacy processes, including details of audits, information security and privacy incidents, and management reviews, are the fourth level of Organisation Name's ISMS documentation (ISO 27001 7.5.1b and 9.2g).

2.2 Authorisation levels

2.2.1 Organisation Name has clearly defined authorisation levels that cannot be delegated.

2.2.2 The Board of Directors has ultimate authority over the [Information Security Policy](#) and ISMS, and approves and authorises all changes to the [Information Security Policy](#), the [Statement of Applicability](#), the Information Security Manual and any separate policy statements (primary documents).

2.2.3 The Chief Information Security Officer (CISO) has lead executive authority for information security and works with the Information Security Committee to approve, authorise and issue all second-level documents.

2.2.4 The Information Security Manager and all

"Heads of Department / Divisional / Function"

approve and authorise third-level documents owned by individuals or entities in their areas of responsibility. Any information security documents personally owned by "Heads of Department/Divisional/Function"

have to be approved and authorised by the Chief Information Security Officer (CISO).

"2.2.5 Owners of information assets (see control A.8 below) are responsible for the security classification of their asset(s), the day-to-day protection of their asset(s) and for the day-to-day operation of related security processes. The responsibility for carrying out these processes or associated task(s) can be delegated to anyone within the owner's area of responsibility, provided that:

- a. The individual has the necessary skill, competence and resources to carry out the processes or task(s); and
- b. The owner retains accountability for ensuring that the process or task is carried out correctly."

2.2.6 Access rights are specified in control A.9 below. Access rights are personal, are set out in individual user agreements (see control A.9 below) and cannot be delegated.

2.3 Organisation Name's ISMS documentation is protected and controlled. There is a Document Control Procedure which takes 2.2 above into account and defines the management actions for document control (ISO 27001 7.5.3).

2.4 Organisation Name has a documented procedure (Control of Records) that defines the controls for identification, storage, protection, retrieval, retention time and disposal of records. (see control A.18.1.3 below) Documents are available to those who need and are authorised to access them in line with these requirements.

3. Information security management system

Organisation Name has established, implemented, maintained and continually improves the ISMS (ISO 27001 4.4 and 10).

3.1 Establish the ISMS

- a. Organisation Name defined the scope of the ISMS in section 1.
- b. Organisation Name has defined its Information Security Policy, which is set out in section 5, to apply throughout Organisation Name as defined in the scope (section 1

above). The policy includes:

b1. A framework for setting information security objectives for the ISMS

"In order to preserve its competitive edge, cash-flow, profitability, and commercial image"

("Which are established in the [Information Security Policy](#)" and "an enabling mechanism for information sharing, for electronic operations") and an overall sense of direction ("will continue to be aligned with organisational goals") and principles ("are committed to preserving the confidentiality, integrity and availability of all the physical and electronic information assets") for action with regard to information security (ISO 27001 5.1.a).

b2. The requirement for "legal, regulatory and contractual compliance" (ISO 27001 5.2.c).

b3. The strategic organisational and risk management context for the establishment and maintenance of the ISMS ("the organisation's current strategic business plan and risk management framework provide the context for identifying, assessing, evaluating and controlling information-related risks") (ISO 27001 5.2.b).

b4. Reference to a systematic approach to risk assessment, the risk management framework (4.2 below) in which the criteria for risk evaluation are described and the structure of the risk assessment is defined (4.4 below) (ISO 27001 6.1.2.a.2).

b5. The policy and this manual have been approved by Top Management (ISO 27001 5.2).

c. Organisation Name has identified a suitable, systematic approach to and framework for risk assessment that produces consistent, valid and comparable results and that is appropriate for its business, legal, regulatory and contractual requirements, and this is described in section 4 below (ISO 27001 6.1.2.b).

d. Identification of risks is carried out in line with the process set out in section 4 below (ISO 27001 6.1.2.c.1).

e. Assessment (the analysis and evaluation) of risks is carried out in line with the process set out in section 4 below (ISO 27001 6.1.2.d and 6.1.2.e).

f. Options for risk treatment are identified and evaluated in line with the process set out in section 4 below (ISO 27001 6.1.3.a).

g. Control objectives and controls are selected from
"any appropriate source"

to meet the criteria and requirements of the risk management framework, take into account the risk acceptance criteria (section 4 below) and legal and regulatory requirements and contractual obligations, have been compared with the controls listed in ISO 27001:2013 Annex A
"and others "

and are contained in the Statement of Applicability (ISO 27001 6.1.3.d).

h. The Statement of Applicability records whether the organisation is applying the controls of Annex A
"and other sources"

, along with the justification for or against this decision, as well as details of those controls selected that are not listed in Annex A (ISO 27001 6.1.3.d).

i. The Statement of Applicability is contained in the [Statement of Applicability Work Instruction](#). In approving this manual, the risk owners accept the residual risks (see section 6.6.3 below) (ISO 27001 6.1.3.f).

j. Top Management authorises implementation of the ISMS and any changes to this manual
"and approves the corporate-level residual risks"

(ISO 27001 5.1).

3.2 Implement the ISMS

a. Organisation Name's [Risk Treatment Plan](#) reflects the decisions made in 3.1 above, and identifies the management action, responsibilities and priorities for managing the identified information security and privacy risks (ISO 27001 6.1.3.e).

b. Appropriate funding and resources are, as described in the risk treatment plan, allocated to its implementation (ISO 27001 6.2.g).

c. The selected controls are implemented (and their implementation is co-ordinated

across Organisation Name) to meet the identified control objectives (ISO 27001 8.3).

d. Organisation Name has defined how it evaluates the performance of the ISMS and measures the effectiveness of its controls and has specified how to use these measurements to improve control effectiveness to produce comparable and reproducible results, and this is set out in the [Monitoring, Measurement, Analysis, Evaluation Procedure](#) (ISO 27001 9.1).

e. Awareness programmes, applicable to people doing work within the scope of the ISMS and under the control of Organisation Name, are implemented as required in the risk treatment plan, [Awareness Procedure](#) (ISO 27001 7.3).

f. Organisation Name has identified competence requirements in respect of the ISMS and has taken appropriate action to ensure that relevant roles have relevant competences, [Competence Procedure](#) (ISO 27001 7.2).

"Here you should reference the document that contains a competence needs analysis, required qualifications, actual staff qualifications, the gap to be closed and the plan for closing that gap."

g. Top Management uses its internal audit process to ensure that the operational management procedures and work instructions required in this manual are implemented (ISO 27001 8.1).

h. Organisation Name has committed specific resources to the effective management of the ISMS,

"including the appointment of a Chief Information Security Officer (CISO) and, an Information Security Manager, recruitment of additional training/technical staff, inclusion of information security in all job descriptions"

as well as investing in information security and privacy products and services as required by the [Risk Treatment Plan](#) (ISO 27001 7.1).

i. Organisation Name has implemented measurement and monitoring procedures and controls as described in controls 12.4 and 16.1 below (ISO 27001 8.1).

3.3 Maintain the ISMS

a. The controls implemented to meet control objectives 12.4 and 16 below are operated to

"promptly detect processing errors, and"

detect security and privacy events, to identify failed and successful security and privacy breaches and incidents, enable management to assess whether security and privacy activities are performed in line with the criteria set for them, and take action to resolve any breach of security or privacy in a way that reflects Organisation Name's priorities; also see section 3.4 below (ISO 27001 9.1).

b. Organisation Name and its management regularly review the effectiveness of the ISMS, in line with the policy and procedures identified in control 5.1.2 below, seek to continually improve the effectiveness of the ISMS through analysing audit results, and monitoring events and activity, all in the context of the business goals and risk treatment plan, and at least

"once a year"

(ISO 27001 9.2 and 9.3).

c. Organisation Name evaluates the performance of the ISMS, as set out in the [Monitoring, Measurement, Analysis, Evaluation Procedure](#), to verify that security and privacy requirements have been met (ISO 27001 9.1).

d. At planned intervals as well as whenever there are significant changes in Organisation Name, technology, business objectives and processes, identified threats or external (legal, regulatory, social) changes, Organisation Name reviews those aspects of its risk assessment and risk treatment plan, including levels of residual risk and acceptable risk (taking into account changes in the effectiveness of controls), that are affected by the changes, or carries out additional assessments of specific risks in relation to new technologies, and system or any other changes that affect organisational information or information assets (ISO 27001 8.2).

e. Management ensures that Organisation Name carries out regular internal ISMS audits in accordance with the [Internal Audit Procedure](#) and the [Internal Audit Schedule](#).

"If you already have a management system in place that includes internal audit you can reference the relevant documents here."

f. Other audits are conducted as required in controls 12.7.1 and 18.2 below, and the results of these audits inform the reviews identified in 3.3b) above (ISO 27001 5.1.e and 9.2.c).

g. Actions or events that could impact the effectiveness of the ISMS are recorded in line with sections 12.4 and 16 below (ISO 27001 6.2.e and 9.3) and are reviewed at management review.

h. The [Risk Treatment Plan](#) is updated to take into account the findings of monitoring and reviewing activities.

3.4 Continually improve the ISMS

a. Where improvement opportunities for the ISMS are identified during the maintenance phase (see 3.3 b) and d) above), they are implemented if they meet the criteria of the risk treatment plan (ISO 27001 10.2).

b. Organisation Name has a documented [Non-Conformity and Corrective Action Procedure](#) which is complemented by other procedures (including but not limited to those in controls 15.1, 16 and 18.2 below of this manual; control 6.1.4 enables it to learn from the experiences of other organisations, and control 16.1.6 ensures it learns from its own experiences) and these include evaluating the need for action in response to non-conformities (ISO 27001 10.1).

c. The results of reviews are communicated to everyone involved
"details"

and action delegated to the appropriate people, in line with the documented [Non-Conformity and Corrective Action Procedure](#) and controls 6.1.1 and 16.1 below (ISO 27001 7.4).

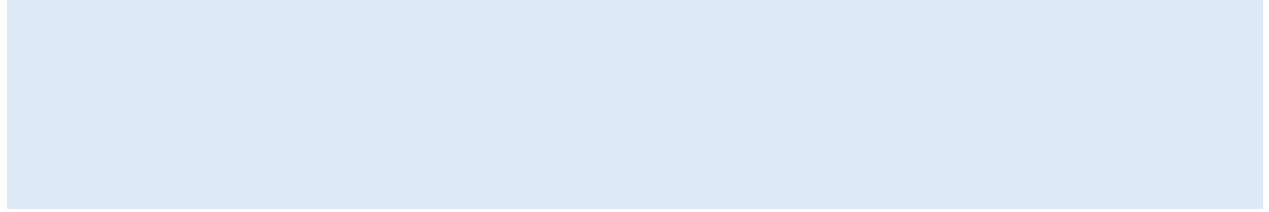
d. The implemented improvements are subject to monitoring and audit (see the [Internal Audit Procedure](#)) and control A.18 of this manual) to ensure that their intended objectives have been achieved (ISO 27001 10.1.d).

4. Context of organisation

"ISO 27001:2013 specifies in Clause 4.3 what must be considered in this regard - the external and internal issues relevant to the organisation's context, the needs and expectations of interested parties/stakeholders, (interested parties may include customers, suppliers, partners, employees, PII principals, etc.), the interfaces and dependencies between activities performed by the organisation and activities performed by other organisations/entities (such as PII controller/PII processor/joint controller considerations).

All these items – the requirements for which are set out in ISO 27001:2013 Clauses 4.1, 4.2 and 4.3 – should be separately documented (Within; [Context of the Organisation Procedure](#), [Identification of Interested Parties Procedure](#) and [Scope Statement](#)). This could be as part of the Board of Directors or management meeting that

determines the scope of the ISMS. This is also where you should identify and justify any exclusions from the scope."



<< Content removed for sample purposes >>

SAMPLE