ISO 27001 Certification Support Service

ISO 27001 is the de facto security framework for the majority of the organisations on the planet. While frameworks like NIST Cybersecurity Framework v1.1[1] and COBIT v5.0 absolutely have their place (particularly in the US), it's the ISO 27001 standard that finds its way into most due diligence questionnaires and contractual obligations. Not to mention validation against EU regulation and legislation.

However, few organisations need to go all the way to full ISO 27001 certification. Somewhat counterintuitively, the benefits to the *business* rarely justify the level of effort and expense to get there.

Do you know exactly what you need? And why?

The CCS ISO 27001 Certification Support service has been developed by experienced practitioners in order to provide the necessary guidance to align yourself to the ISO 27001 standard. Most importantly, the service ensures that your alignment is:

1. demonstratable and defensible (to both clients and regulators);
2. sustainable;
3. a comprehensive stepping-stone to full certification[2] if desired; and above all
4. appropriate to *your* business

In the end, all regulatory compliance and industry certifications spit out the back-end of a security program done well, the SSC ISO 27001 Certification Support service will lay the groundwork for whatever your end goals are.

Methodology

True alignment with ISO 27001 requires a significant investment in time and resource. And to be performed properly, inclusion of all of the guidance in ISO 27002 must be part of the process.

For example, ISO 27001 ('Requirements') has this for Control Objective A.5.1.1:

A.5.1.1	*Policies for information security*	*Control* *A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.*

Which leaves the definition of 'alignment' very subjective and difficult to demonstrate.

However, ISO 27002 ('Code of Practice') includes not only implementation guidance, like:

[1] In fact, the deliverables provided by CCS include a mapping to this framework.
[2] Full certification can be achieved through the use of CCS Partners.

Implementation guidance

At the highest level, organizations should define an "information security policy" which is approved by management and which sets out the organization's approach to managing its information security objectives.

Information security policies should address requirements created by:

a) business strategy;

b) regulations, legislation and contracts; - [remainder redacted]

...etc...

Then it also includes examples of the topics you include:

Examples of such policy topics include:

a) access control (see Clause 9);

b) information classification (and handling) (see 8.2);

c) physical and environmental security (see Clause 11);

d) end user oriented topics such as:

1) acceptable use of assets (see 8.1.3);

2) clear desk and clear screen (see 11.2.9); - [remainder redacted]

All told there are over 60 pages of guidance for the 15 Control Objectives, all of which must be included in the alignment process.

Like all security, this is simple, just difficult, and a qualified determination must be made regarding control scope and applicability.

Alignment with ISO 27001 involves examination of all Control Objectives:

Control Objectives
A.5 Information security policies
A.6 Organization of information security
A.7 Human resource security
A.8 Asset management
A.9 Access Control
A.10 Cryptography
A.11 Physical and environmental security
A.12 Operations security
A.13 Communications security
A.14 System acquisition, development and maintenance
A.15 Supplier relationships
A.16 Information security incident management
A.17 Information security aspects of business continuity management
A.18 Compliance

Assessment Plan

A more detailed Project Definition Plan (PDP) will be made available well in advance of project kick-off, but in essence:

Phase 1: Kick-Off / Program Goal Confirmation (performed on-site)

- Meet with senior leadership to reinforce commitment and agree the overarching *business* goals for the ISO 27001 alignment program;
- Meet with key stakeholders to agree project activities;
- Meet individually with key stakeholders to discuss department / LoB specifics with regard priorities and resource availability;
- Agree all next steps, timelines, and functional responsibilities;

Phase 2: Project Plan Definition (performed off-site) - *Optional*

- Work with client project manager to produce comprehensive project plan.[3]

Phase 3: Program Execution (performed on and off-site)

- Details vary significantly per unique business, but this Phase encompasses the execution of work across all departments / LoB.

Phase 4: Project Close (performed on-site)

- The CCS ISO Certification Support service can be seen as a stand-alone service, or as a stepping-stone towards full certification. Whatever the goals of the organisation, the project close is designed to hand-over all remaining action items to designated owners.

Timeframe

The process for executing an ISO 27001 alignment program can only ever be unique to each organisation. Depending on available resources/skill-sets/budget, the consulting time required will vary enormously.

In the end the timeframe will depend entirely on the organisation in question, CCS is there to support the work performed, not [in most cases] to do it.

Deliverables

- Detailed report against all ISO 27001 Control Objectives that includes the:
  - 'compliance' status of each control;
  - outstanding actions to be performed;
  - gap between alignment and full certification (if applicable); and
  - names of any 'records' received during the project
- Mapping of ISO Controls to NIST Control Framework v1.1;
- Recommended next steps

[3] CCS does not provide a project management function but will work with whomever client assigns (if applicable).