ISO27001 CERTIFICATION PROCESS

The following outlines the typical stage in an ISO27001 certification process:

Gap Analysis

The importance of a Gap Analysis is to gain a full understanding of exactly where you currently are in relation to compliance with Mandatory Clauses and appropriate ISO27001 controls. The Gap Analysis examines the level of compliance to the 18 control areas and ISMS requirements of the standard and highlights any areas that need to be implemented or improved.

The Gap Analysis consists of 3 phases:

• Phase 1 – Interviews with key functions of your organisation in order to answer questions in relation to all 114 controls of the standard and the ISMS requirements;
• Phase 2 – High level review of your existing information security policies, standards and guidelines within your organisation;
• Phase 3 – Produce a report outlining your compliance status against the Mandatory Clauses and appropriate ISO27001 controls, highlighting your key areas of Compliance, Non-Compliance or Partial Compliance.
• Following the Gap Analysis, you should not attempt to simply address gaps identified. The findings should be used in conjunction with a Risk Assessment to determine those controls appropriate to address business specific risks. Not all controls may be appropriate or have a high priority risk profile.

Business Context & Scope

Organisations are required to provide documented evidence of how the Information Security Management System (ISMS) is aligned to organisational objectives and requirements. Our Consultants will work with you during this phase to ensure the relevant information is captured and that the ISMS is fully aligned to your business as well as fully supporting and enabling your personnel to achieve your operational outputs and objectives.

Risk Management

Following the Gap Analysis, our Consultant will mentor you through the Mandatory requirements for addressing Risk Management in the context of the standard. This mentoring phase will be conducted through workshops and one to one meetings with asset owners and managers and cover:

• Developing and documenting an appropriate risk assessment methodology; • Identifying risk at the asset level; • Identifying and documenting risk owners and risk acceptance criteria; and • Conducting the Information Security Risk Assessment.

ISO27001 CERTIFICATION PROCESS

ISMS Implementation, Review & Auditing

Following the competition of the Gap Analysis and Risk Management stages, the Consultant will mentor you through the implementation of the Mandatory Clauses for the ISMS. If you have existing management processes and structures present it may be possible to use these.

These include:

- ISMS Scope;
- Documented Information Requirements;
- Management Responsibility and Governance;
- Roles, Responsibilities and Resourcing;
- Information Security Objectives and Metrics;
- Internal ISMS audits;
- Management Review of the ISMS;
- ISMS improvement:
- Continuous improvement;
- Corrective Actions; and
- Monitoring effectiveness.

Controls Implementation

Once the ISMS requirements have been established, our Consultant will then mentor you on how to implement the applicable ISO27001 Annex SL controls as identified through the Gap Analysis and Risk Management stages. This may include any or all elements of the following:

- Information security policies;
- Organisation of information security;
- Human resource security;
- Asset management;
- Access control;
- Cryptography;
- Physical and environmental security;
- Operations security;
- Communications security;
- System acquisition, development and maintenance;
- Supplier relationships;
- Information security incident management;
- Information security aspects of business continuity management; and
- Compliance (legal, policy, standards and technical).

ADVENT IM

ISO27001 CERTIFICATION PROCESS

Statement of Applicability

At the end of the project and prior to any Certification Audit, the Consultant will mentor you through the completion of the Mandatory Statement of Applicability (SoA) Document. This document is produced from the outputs of the Gap Analysis and Risk Assessment work packages and essentially lays out:

- Those ISO27001 controls that have been determined as necessary to the security of your information assets;
- How compliance to those controls has been achieved;
- Where evidence of that compliance can be found; and
- Justification for those cases where an ISO27001 control has been determined to not be necessary.

This statement can also be useful if you do not require formal certification but need to demonstrate compliance to a third party.

Certification Audit

Although we do not conduct the Certification Audit, we can facilitate selection of an appropriate certification body and attend with you during the audit itself. Pricing for this has not been included in this proposal.

The Certification Audit takes place on your premises over a number of days, usually in two separate stages. Approaches to certification audits may vary depending upon the Certification Body chosen, but generally during the audit, the Accredited Certification Body will:

- Conduct a desk top review reviewing formal documentation to understand your scope, the risk methodology and assessments, the security policy and other key policies and procedures.
- Follow audit trails, paying particular attention to the risks identified, control objectives and establishing that there is evidence to demonstrate that the ISMS is working in practice.
- Look at responsibilities at all levels within your organisation, communications and controls inside and outside of the organisation, the monitoring of incidents and actions for continuous improvement.
- Identify opportunities for improvement. Where necessary, they will raise non-conformance reports and, if issues are identified, agree corrective actions and timescales with the customer.

At the close of the audit, the Lead Auditor leaves recommendations. Following the audit, the auditor's report goes before the Accreditation Board for review. They also review the corrective actions implemented to resolve any nonconformances raised. On satisfactory completion of these two activities a certificate will be issued.