ISO27001 Goals

Annex A controls are Annex A of ISO/IEC 27001 contains a set of controls that organizations can implement to address various information security risks. These controls are designed to help organizations establish, implement, maintain, and continually improve an information security management system (ISMS) tailored to their specific needs.

Annex A controls

Define scope & context

- A) Scope and the context of business activities
- B) Define Interested parties and their needs
- C) Define Internal and External issues

Leadership

- Define Leadership commitment by having an IS Policy Stataement
- Define the Roles & Responsibilities of all key staff who have a direct input to the management systems activities

Risk Assessment

As this can be a time consuming activity it is wise to start work on this early on or in parallel with early policy development

This is a "Key aspect" of ISO27001 and the main goals are to identify the major risks to the IS assets of the business

- Risk assessment document
  - Output - a fully documented Risk Assessment that needs to be maintained periodically
  - Output - Risk Treatment plans for the critical risks

Statement of Applicability

The SoA defines which controls are "relevant" to address the risks identified and in addition and controls the business determines that it needs to apply based on its risk appetite and the nature of the work that it performs

A review exercise is to be done to annotate the Annex A controls to each risk then after that review what controls the organisation wants to apply

Support processes

Human Resources

HR touches upon a number of key areas of ISO27001 in particular, onboarding and off boarding of staff, handling PI data, establishing with line managers the competency requirements for each role in the business, security or general vetting of staff before employment, central points for managing performance reviews of staff and retaining training information.

- Onboarding
  - Having a defined recruitment process that shows where the staff vetting process is carried out and in addition the interface with other groups like IT for equipment allocation, access controls by communicating start dates of the employee
  - HR Induction process
    - General induction of staff NDA
  - IS Induction
    - Establishing a process that ensures new starters receive orientation in the management system and its core policies
    - Establishing an ongoing strategy (inc tools if required) for providing ongoing awareness to new and existing staff on a periodic basis
- Offboarding
  - Reminding staff of their obligations of nondisclosure when leaving the company's employment
    - NDA's?
    - Sign asset return
  - Receiving back company assets that have been assigned to the individual
  - Liaison with IT on leaving dates and assets. IT to ensure accounts are disabled I.a.w policy and aligned to leaving dates
- Roles & Job Descriptions
  - JD's not only to define the role but key competencies that the role is set against
  - Define the competency requirements for all key ISMS roles such as IS Manager, Legal, IT Management, HR, Physical Security etc.
    - Establish any skills gaps and provide training or development for any gaps
- Training records
  - Ensure that there is a centralised or location centric collation of formal training, mentoring or development for employees.

Document controls

Established mechanisms for: Classifications of documents and data Control of ISMS documents Control of project or companywide documents Methods defined on authoring, reviewing and approvals

- Master list of ISMS documents and versions
- List of records and classifications

Operational

Critical processes A defined set of processes that the business has determined critical to its operations. These can be variable depending on the business itself so it is important to take a view on what processes make a big impact organisationally and the impacts of Information Security. Such processes can be: Access control, Management of PI data, Vulnerability management etc..

IT Operational - Clause 8.1 can be the pigeon hole for many of the IT operational procedures that are required for example: Backup & Restore procedures, Vulnerability scanning procedures, Network configuration procedures

8.2 Ongoing Risk assessment It is important to ensure that risks are periodically reviewed and updated as new risks become evident or if existing risks are no longer a risk so can be removed. Ongoing risk assessment should be performed by a risk committee or similar (i.e Steering Groups for example).

8.3 Ongoing Risk Treatment - the status and progress of risk treatments should be proactive to ensure that they are implemented. Risk treatments that remain stagnant pose an issue because the risk is not addressed until the risk treatment is fully in place.

Improvement

Clause 10 Improvement is about establishing mechanisms for recording employee suggestions for improvement of the management system. When received improvement suggestions should be evaluated for cost-benefit and management agree what improvements should be given time and resources to be implemented. After the improvements are done then it is useful to establish what benefit the improvements have made and the success of these, this can be by measures (quantitative) or bt quantitative analysis.

Performance Management

- 9.1 Measurement
  - This clause is about determining what measures will give you and indication of whether your management system is performing or not across the requirements. It is important to establish "what is important to measure" and "is it feasible to collect the measures"? In ISO27001, there will be sources of data that will give you an indication of process conformity such as "audit findings", results of PEN testing vulnerabilities, IS Incidents etc.
- 9.2 Internal audits
  - Internal audits should be defined to establish compliance with internal policies and procedures as well as evaluating those against The ISO requirements. In addition it is recommended to audit and test the controls as well to ensure that they are effective in managing the risks
    - Testing the controls in ISO 27001 refers to the process of evaluating and verifying the effectiveness of the security controls implemented within an organization's Information Security Management System (ISMS). These controls are designed to mitigate risks and protect the confidentiality, integrity, and availability of the organization's information assets.

      Testing the controls typically involves:

      Validation: Ensuring that the controls are implemented correctly according to the defined policies and procedures outlined in the ISMS.

      Verification: Confirming that the controls are operating as intended and are effective in addressing the identified risks to the organization's information assets.

      Evaluation: Assessing the adequacy and strength of the controls in mitigating risks and achieving the desired level of security for the organization.
- 9.3 Management Review
  - 9.3 Management Review The Management Review is the key review at discussing how the management system is performing so the inputs to this rely on measurements (9.1) and trends and findings from Internal Audits (9.2) as well as other sources of information in order to make decisions about policies, procedures and risk management. The output of the MR should be formally documented against the input agenda requirements and key management decisions made.