**I**nformation **S**ecurity **M**anagement **S**ystem

# ISMS implementation project checklist

## Practical guidance on implementing an ISO/IEC 27001 ISMS

### Project definition, justification, scoping and planning

- ☐ Study the standards, in depth: complete lead implementer training if possible.
- ☐ Study the business, in depth, to understand its objectives, strategies, culture, governance arrangements, existing information risk and security management *etc*.
- ☐ If the organisation has a defined, structured approach for this phase, use it!
- ☐ Build a business case that identifies and promotes the business benefits of the ISMS.
- ☐ Look beyond 'security' and 'compliance' *e.g*. helping management to manage business risks, supporting/enabling other business initiatives and strategies.
- ☐ Identify, explore and elaborate on a broad set of business objectives relating to: information risk and security management; information, cyber, manual and automated security controls; compliance and assurance; resilience; good practice, maturity; efficiency, cost-effectiveness *etc*.
- ☐ Clarify relative priorities for the objectives *e.g*. by ranking them all or grouping them into categories such as 'essential', 'important', 'nice-to-have' and perhaps 'to be avoided'.
- ☐ Be honest about the organisational/governance changes ahead, including the potential disruption, costs and timescales.
- ☐ Be realistic about resourcing, priorities and capabilities.
- ☐ Build-in more than enough slack/contingency to allow for unforeseen difficulties.
- ☐ Offer a do-nothing straw man plus other options as appropriate *e.g*. distinguish essential from important from optional objectives, compare costs *and* benefits of differing ISMS scopes.

### Project approval

- ☐ Don't expect the business case to sell itself, no matter how exciting and positive it seems.
- ☐ Hawk it around management, informing them, gathering feedback and amending the proposal.
- ☐ Identify, explore and address genuine concerns, especially blockers.
- ☐ Look for opportunities to align with corporate strategies and other initiatives.
- ☐ Refine the objectives and project proposal, adding explicit details where clarity is needed or helps *e.g*. metrics.

- ☐ While awaiting approval, continue working on the planning and ideally progressing the essential aspects such as information risk assessment.
- ☐ Be crystal clear about those essentials and only compromise in other areas, even if that means the project is refused or deferred.

**Implementation activities**

- ☐ Aim low, strike high: focus intensely on those essentials, progressing other objectives at lower priority/urgency if resources allow.
- ☐ Where possible, re-use existing content, policies, procedures, controls *etc*., adapting as necessary.
- ☐ Collaborate closely with related teams/functions/organisations/individuals.
- ☐ Work to up-skill the core team through training, mentoring and experience on the job.
- ☐ Start operating elements of the ISMS as soon as practicable, practising and refining them *and* ideally accounting for the benefits gained (financial or otherwise).
- ☐ Look for early wins and promote them: positive feedback is invaluable for motivation and energy.

**Project management, oversight, progress reporting and project risk management**

- ☐ If the organisation has a project management method/approach, use it!
- ☐ Work with experienced programme and project managers.
- ☐ Establish suitable governance arrangements (*e.g*. structure, reporting, metrics, approvals) for the project as that will evolve into the ISMS governance in due course.
- ☐ Play snakes-and-ladders: identify and address risks/issues/setbacks, seizing and promoting opportunities to advance.
- ☐ Watch the critical path and anything that does or might consume your contingencies, like a hawk.
- ☐ Beware stress and burnout: don't exceed reasonable workloads for long periods, including yours.
- ☐ Work hard on clear communications and effective relationships: these will outlast the implementation phase.

**Certification and other assurance activities**

- ☐ Treat certification as an opportunity to improve, more than a hurdle to clear.
- ☐ Take time to clarify objectives, identify suppliers and contract with certification bodies.
- ☐ Specify experienced and competent certification auditors, anticipating less aggravation and more value-add.
- ☐ Line up certification prerequisites such as completed ISMS documentation, records of activities, ISMS internal audits *etc*.

- ☐ Line up management to see the purpose and value of assurance regarding the ISMS, information risk and security management, compliance *etc*.
- ☐ Line up marketing to promote the certification, enhancing corporate brands, opening new business opportunities *etc*.
- ☐ Liaise between the team, management and the certification body closely in the run-up to certification, maintaining alignment and expectations.
- ☐ Look beyond the award itself: there is always more to be done, more planning required *e.g*. integrating other management systems.

**Transition to business-as-usual**

- ☐ Plan for a gradual, sequential/piecemeal ISMS build-and-implementation, rather than a big bang.
- ☐ Start *using* those policies, procedures, metrics, reports *etc*. as soon as they are available: it inevitably takes time to discover and smooth-off the rough edges, and integrate them all into a coherent, self-sustaining management system, so they constitute 'improvement opportunities'.
- ☐ Keep up the communications within and without the team, squeezing more value from metrics through motivational feedback, direction and reprioritisation.
- ☐ Become ever more business- and externally-focused as the ISMS settles into a routine, without neglecting the team and individual needs.



## Disclaimer

This is a generic example checklist. It is not intended to suit all organisations and circumstances. It is merely guidance. Please visit www.SecAware.com for the full 37-page Pragmatic ISMS implementation guideline on implementing an ISMS, elaborating clause-by-clause on ISO/IEC 27001 - essentially, our version of ISO/IEC 27003.