PROJECT MANAGEMENT TOOLS

These two tools follow the same principles, but contain different content and have different objectives and uses within an ISMS project.

ISO 27001 Gap Analysis and Audit Tool

This tool has a very specific, high-level purpose in any ISMS project, which is to quickly and clearly identify the controls and control areas in which an organization does not conform to the requirements of the standard. It is designed to help prioritize work areas in initial project planning and for final, pre-certification audit review of the ISMS. It is not designed to carry out a detailed gap analysis, as this requires a far more granular approach to assessing an organization’s current information security control structure.

The tool is a self-assessment questionnaire. It lists all 134 controls that are in ISO27001/17799:2005, not all of which are necessarily included in your Statement of Applicability. The default setting for the tool is that all the controls are required (which is why they all show as green) and that none of the controls have been implemented (which is why they’re all in red).

ISO 27001 Entity Security Assessment Tool

This tool has a very specific, high-level purpose in any ISMS project, which is to quickly and clearly identify the areas of potential security weakness (vulnerabilities) in the organization’s ISMS and to identify, for each of those areas, the probability of a threat exploiting the vulnerability and the potential impact on the organization if this occurred. The tool is ideal for demonstrating to people within the organization (e.g. management or project staff) where the key vulnerabilities are.

This assessment tool is cross-referenced to ISO/IEC 17799:2005 and deals with the 134 controls of the standard in 33 questions. It is not a risk assessment tool and is not designed to carry out the detailed asset level risk assessment required by the standard, as that requires a far more detailed and granular approach than is provided for in this tool.

The tool is a self-assessment questionnaire. It cross references to the 134 controls that are in ISO17799:2005. The default setting for the tool is that there is inadequate security in all areas, that all vulnerabilities are highly likely to be exploited and that the impact in each case will be high. That’s why they’re all in red.

Implementation Manager

Here is an abridged version of the user instructions for this tool:

1. One of the more complex parts of your task is keeping track of all the work required to document your ISMS. You need to be sure, before you can proceed to certification, that all the controls you have selected in your Statement of Applicability have been fully documented.

2. It is not easy for one person to carry out all the project management tasks so you should consider who can take some of them on. The obvious person would be the Information Security Manager – there is a lot of sense in having one person managing the project and a different person taking on the role of Information Security Manager.
3. At the beginning of the project, you should plan the dates by when you intend to have each section completed and then track actual completion dates. Remember to allow for staff shortages, holidays and illnesses and remember that, where you have a critical dependency on one or another person or event, you will need to take early action to ensure that you are not caught out by it.

4. Your asset inventory (DOC 5.1) will identify an Owner for every information asset, in line with the requirements of the ISMS Manual. The owner of each asset is responsible for drafting (using the models and the templates in this toolkit) the documentation that reflects the necessary controls in relation to his or her asset. DOC 8.1 is the relevant document here, as it sets out the documentation requirements.
   a. Where one asset (eg the SAP system), or asset type (eg the DNS Servers), has a single owner, your task is simple: that person gets to draft the documents.
   b. Where an asset type (eg mobile phones, desktop workstations) has multiple owners, only one person can actually draft the appropriate procedures. This person needs to be selected (however you go about doing it, the person selected needs to be willing, otherwise nothing will happen) and needs to be capable of reflecting user requirements (within your organizational context) so that the procedures which are produced ENABLE the business rather than disable it. You may need, in some circumstances, to ensure that a representative person gathers input from all the parties affected (after all, you will be standardizing what they do) and ensures that practical documentation decisions are taken that the majority of users will support/accept. All of the templates in this toolkit have nominated Owners; and you will need to amend the templates to ensure that they reflect your own organizational structure. On balance, though, you will need someone in each of the positions identified in the templates.
   c. Each Owner is then responsible for drafting the procedure(s) and working instructions that will give life to the control decisions that are contained in your SoA. Remember that a number of procedures address more than one control area, which is why we suggested that you get familiar with the ISMS manual in advance. The implementation task management sheets should be used to identify who is responsible for producing each set of documentation (and how the set will be made up, in terms of procedure and number of Work Instructions) and by when.

PRESENTATIONS

There are two presentations, both using PowerPoint. Some of the slides from these presentations are used within the publicly available presentation (on our toolkit trial web page) “The Complete ISMS Toolkit”.

PDCA Cycle and documentation pyramid

The first describes the PDCA cycle at both the project and the individual control level. It also links the key steps of the ISO 27001 project to each of the four stages of the PDCA cycle and identifies which of the ITG tools are useful for dealing with each area. It is useful for providing corporate management with an overview of the project lifecycle and key steps within the required quality management framework. This
presentation also shows the documentation pyramid, identifying how corporate authority levels are linked to appropriate document origination, ownership and authorization requirements.

The ISMS Overview

This presentation is designed to introduce the ISO 27001 project to the project team. It describes the standards, why they are important, what the key stages and timelines in the project will be and what the next stages are. It is designed to be customised for each organization and guidance is provided as to the purpose of individual slides and what customisation (eg with examples of corporate security issues, etc) might be appropriate. This presentation is an essential part of ensuring that the project team – which usually includes many people who own processes or systems that fall within the scope of the ISMS but who have no previous exposure to a formal information security management system – get a good understanding of what is expected of them and why.