CERTIKIT
Compliance made easy

ISO/IEC 27001 Implementation Guide

ISO/IEC 27001 Toolkit: Version 12

Contents

Tables

Figures

1 Toolkit support and services

The CertiKit ISO/IEC 27001 toolkit includes 160+ templates and guides to allow your organization to align to the requirements of the standard and comes with the following support.

1.1 Email support

We understand you may need some extra support and advice, so this is why we offer unlimited email support for as long as you need after buying this toolkit.

1.2 Toolkit updates

This toolkit includes lifetime updates, which means whenever there is a revised toolkit (usually when a new version of the standard is released, or there is a significant amendment), you will receive an email notification and the new toolkit will be available to download.

1.3 Review of completed documents

If you need that extra piece of mind once you have completed your documentation, our experts will review up to three of your documents to check everything is in order and complies to the ISO27001 standard.

1.4 Exclusive access to customer discussion group

Complying to the ISO27001 standard can be a daunting journey, which is why we offer a range of support channels to suit you. This includes our social media discussion group.

1.5 Video library

Your toolkit purchase comes with access to the ISO27001 video library, which gives guidance on everything from getting started to the certification audit – and all steps in between. This can be accessed via your online CertiKit account, which will be automatically created when you buy the toolkit.

1.6 ISO27001 Services

Whilst our ISO27001 toolkit has all the documentation and guidance you'll need to implement an ISMS and achieve certification to the standard, we do offer both consultancy and internal auditing services to speed up the process and offer expertise in key areas.

1.6.1 Implementation Consultancy

Our ISO consultants have successfully helped many organizations prepare for their certification audits. Our flexible consultancy options are available to assist your project however you need.

Our clients use our consultancy in the following ways:

- Ad-hoc hours or days to cover a few specific areas
- Weekly or monthly meetings to keep the project moving forward
- Documentation writing to speed up the process
- A fully managed project to get you to certification fast

We're often asked to assist with the key stages such as Scope, Gap Analysis, Risk Assessment and even integrating multiple management systems. We can create a phased proposal for you to choose what meets your timescale and budget constraints. Find out more about our consultancy services here.

1.6.2 Internal audits

In order to meet the requirements of clause 9.2 of the ISO27001 standard certification audit you need to have evidence of a completed internal audit of your management system by a qualified auditor. If you haven't got an internal auditor within your organization or resource to train one, then outsourcing your internal audit is the best option.

From full pre-certification audits to ongoing survielance audits, our qualified auditors can help you achieve the requirements of the standard. Find out more about our internal auditing services here.

Please Note: CertiKit are not a Registered Certification Body and cannot provide you a formal management system certification. All services are conducted remotely via MS Teams by our consultants in the UK time zone, and are only available to organizations +/- two hours of the UK time zone.

2 Introduction

This concise guide takes you through the process of implementing the ISO/IEC 27001 international standard for information security using the CertiKit ISO/IEC 27001 Toolkit. It provides a recommended route to certification against the standard starting from a position where very little is in place. Of course, every organization is different and there are many valid ways to embed the disciplines of information security. The best way for you may well depend upon factors including:

- The size of your organization
- The country or countries in which you operate
- The culture your organization has adopted
- The industry you operate within
- The resources you have at your disposal
- Your legal, regulatory and contractual environment

View this guide simply as a pointer to where you could start and a broad indication of the order you could do things in. There is no single "right way" to implement information security; the important thing is that you end up with an Information Security Management System (ISMS) that is relevant and appropriate for your specific organization's needs.

2.1 The ISO/IEC 27001 Standard

The ISO/IEC 27001 international standard for "Information technology — Security techniques — Information security management systems — Requirements" was originally published by the ISO and IEC in 2005 and is based upon the earlier British standard BS7799. Revised in 2013 and again in 2022, ISO/IEC 27001 specifies the requirements that your ISMS will need to meet in order for your organization to become certified to the standard. The requirements in ISO/IEC 27001 are supplemented by guidance contained in ISO/IEC 27002 and this is where the controls in Annex A of ISO27001 come from. ISO/IEC 27002 is well worth reading as it fills in some of the gaps in understanding how the requirements in ISO/IEC 27001 should be met and gives more clues about what the auditor may be looking for.

2.1.1 What's new in the 2022 standard

It's fair to say that this update has been driven almost exclusively by two forces; a desire to make the management system requirements match up with the latest Annex SL structure and wording, and the need to align Annex A of the standard with the 2022 version of the ISO27002 guidance.

Let's take these two factors in turn and explore what's changed.

ISO27001 was one of the first standards to adopt the Annex SL high level structure back in 2013 and since then the structure has been tweaked a little by ISO with the release of updates to ISO9001 and others from 2015 onwards. But the changes are small and are unlikely to give most certified organizations any sleepless nights.

Firstly, there are some wording changes in the following clauses:

- *4.2 Understanding the needs and expectations of interested parties*
    - A third bullet is added to specify "which of these requirements will be addressed through the information security management system".
- *4.4 Information security management system*
    - The phrase "including the processes needed and their interactions" is added, requiring more definition of the processes of the ISMS.
- *5.3 Organizational roles, responsibilities and authorities*
    - The phrase "within the organization" is added at the end of the first sentence.
- *6.1.3 Information security risk treatment*
    - The notes are replaced.
- *6.2 Information security objectives and planning to achieve them*
    - The need to monitor objectives is added to the list.
- *7.4 Communication*
    - The current wording about communication processes has been replaced with a simple "how to communicate".
- *8.1 Operational planning and control*
    - The need to establish criteria for the processes of the ISMS has been added.

There's a new sub-clause *6.3 Planning of changes* which deals with changes to the management system and requires any changes to be considered from the point of view of their purpose and consequences, the integrity of the ISMS, the resources available, and whether any changes to responsibilities and authorities are involved. This will require a simple planning process to be in place, with evidence that these areas have been considered.

Within Clause 9 (*Performance evaluation*) sub-clauses 9.2 (*Internal audit*) and 9.3 (*Management review*) have been further subdivided into *9.2.1 General*, *9.2.2 Internal audit program*, *9.3.1 General*, *9.3.2 Management review inputs* and *9.3.3 Management review results* respectively. The two sub-headings in Clause 10 have been swapped around. This is mainly to aid readability and to match the latest definition of Annex SL (also known as the "Harmonized Structure").

But the main change in the 2022 version of ISO/IEC 27001 is the adoption of a new control set from the ISO/IEC 27002 guidance standard. This is included as Annex A of ISO/IEC 27001. Annex A in its new form consists of a total of ninety-three controls (there were previously 114), of which eleven are stated to be additions to the previous control set. Many controls

from the previous version have been merged together, hence why there are now fewer controls than before, and yet also some new ones.

The number of control categories has been reduced from fourteen down to just four, which are:

- A.5. Organizational controls (37 controls)
- A.6. People controls (8 controls)
- A.7. Physical controls (14 controls)
- A.8. Technological controls (34 controls)

The new controls are as follows:

- A.5.7 Threat intelligence
- A.5.23 Information security for use of cloud services
- A.5.30 ICT readiness for business continuity
- A.7.4 Physical security monitoring
- A.8.9 Configuration management
- A.8.10 Information deletion
- A.8.11 Data masking
- A.8.12 Data leakage prevention
- A.8.16 Monitoring activities
- A.8.23 Web filtering
- A.8.28 Secure coding

If you need to understand how the old and new sets of controls relate to each other, this information is included at the back of the ISO/IEC 27002 guidance standard. But if you're starting afresh with the 2022 version of ISO/IEC 27001, you probably won't need to know this.

2.1.2 The ISO/IEC 27000 family

There are quite a few documents published within the ISO/IEC 27000 series and many of them provide useful supporting information for organizations going for ISO/IEC 27001 certification (or simply using it for guidance). Some of the common ones are:

- ISO/IEC 27000 — Information security management systems — Overview and vocabulary
- ISO/IEC 27002 - Information security, cybersecurity and privacy protection — Information security controls (as mentioned previously)
- ISO/IEC 27003 — Information security management system implementation guidance
- ISO/IEC 27004 — Information security management — Monitoring, measurement, analysis and evaluation
- ISO/IEC 27005 — Information security risk management

- ISO/IEC 27017 – Information security for cloud services
- ISO/IEC 27018 – Protecting Personally Identifiable Information in the cloud
- ISO/IEC 27032 — Guidelines for cybersecurity
- ISO/IEC 27033 — Network security (multiple parts)
- ISO/IEC 27034 — Application security (multiple parts)
- ISO/IEC 27035 — Information security incident management (multiple parts)
- ISO/IEC 27036 — Information security for supplier relationships (multiple parts)
- ISO/IEC 27037 – Identification, collection, acquisition and preservation of digital evidence
- ISO/IEC 27039 – Intrusion prevention
- ISO/IEC 27042 - Analysing digital evidence
- ISO/IEC 27043 — Incident investigation
- ISO/IEC 27701 – Privacy information management

It's worth pointing out that, although useful, none of these are required reading for certification to the ISO/IEC 27001 standard so if you are limited in time and budget, just a copy of ISO/IEC 27001 itself will suffice (although if you haven't purchased the standard yet, we would recommend you look at our Enhanced Gap Assessment Tool as an alternative as it includes all of the requirements in the standard but in a more useful format).

There's no obligation to go for certification to ISO/IEC 27001 and many organizations choose to simply use the standard as a set of good practice principles to guide them along the way to managing their information security risks.

2.1.3 The Annex SL structure

One subject worth mentioning in more detail is that of something the ISO calls "Annex SL" (also called the "High Level Structure", "Harmonized Structure" and more recently "Annex L"). This is a very obscure name for a concept that represents a big change in ISO management system standards and ISO/IEC 27001 was an early adopter of this concept. There are some ISO standards that involve operating a "management system" to address the specific subject of the standard. Some of the main examples are:

- ISO 9001: Quality management
- ISO 14001: Environmental management
- ISO 45001: Occupational health and safety
- ISO 50001: Energy management
- ISO 22301: Business continuity management
- ISO/IEC 20000: IT service management

Traditionally, all these standards have had a slightly different way of implementing and running a management system and the wording of the standards has varied sometimes quite significantly. This is ok until an organization decides to try to run a single management system across multiple standards, for example ISO9001 and ISO/IEC 27001. Then it becomes

difficult for the organization to marry up differing ways of doing the same thing and it makes the auditors' job harder (and longer and more expensive) too.

So, to get around this problem of "multiple management systems" the ISO decided to standardise the wording of the management system parts of the standards. They produced a long document with numerous appendices, one of which was "Annex SL" containing a first draft of the standard wording. Over time the ISO is now phasing in this common "Annex SL" wording and all new standards or new versions of existing standards will have it. ISO/IEC 27001 was one of the first to adopt this new layout and so may be called one of the first "Annex SL" standards. ISO has made good progress in phasing Annex SL in and all of the relevant standards, including ISO 22301 (business continuity) ISO 9001 (quality management systems) and ISO 14001 (environmental management systems) now have it.

The good news for an organization implementing an ISMS based on ISO/IEC 27001 is that they will by default be putting in place an "Annex SL" management system. This will make it much easier for them to implement other standards such as ISO 9001 later, if they wish to (see the section on integrating management systems within this document for more information). The ISO/IEC 27001 standard consists of major headings which will be common across other standards (because they are the "Annex SL" headings) which are:

0. Introduction
1. Scope
2. Normative references
3. Terms and definitions
4. Context of the organization
5. Leadership
6. Planning
7. Support
8. Operation
9. Performance evaluation
10. Improvement

2.1.4 Meeting the requirements of the standard

Clauses 0 to 3 don't contain any requirements and so an organization wouldn't be audited against those. They are worth a read however as they provide some useful background to what the standard is about and how it should be interpreted.

Clauses 4 to 10 set out the requirements of the standard. Requirements are often referred to as the "shalls" of the standard because that is the word usually used by ISO to show that what is being stated is compulsory if an organization is to be compliant. The (internal and external) auditing process is basically an exercise to check whether all the requirements are being met by the organization. Requirements are not optional and, if they are not being met, then a "nonconformity" will be raised by the auditor and the organization will need to

address it to gain or keep their certification to the standard (see the section on auditing later in this guide).

In order to show that the requirements are being met the auditor will need to see some evidence. This can take many forms and until recently was defined as a combination of "documents" (evidence of intention such as policies, processes and procedures) and "records" (evidence that something has been done). In the new version of the standard the term "documented information" is generally used instead to cover anything that is recorded (the official ISO definition is "information required to be controlled and maintained by an organization and the medium on which it is contained"). But the point is you need to have something to show the auditor.

This is often a major culture change in many organizations. Just doing something is no longer enough; you must be able to prove that you did something. This means keeping records in areas you maybe don't keep records now; a good example often being meeting minutes. Meetings happen, things are discussed and decisions are made, but the auditor won't just accept your word for it. The auditor will want to see the minutes. Other examples could be training records – who was trained to do what and when? Information security vulnerability tests – what was tested, by whom, when and what was the outcome?

If all of this sounds rather onerous, then it's true, it can mean more work at least in the short term. But doing information security according to the ISO/IEC 27001 standard is about doing it right. You will be taking advantage of the knowledge of a wide variety of experienced people who have come together to define the best way to create an ISMS that works; people from all over the world in a wide variety of industries and organizations large and small.

From our experience what often happens during the process of implementing an international standard such as ISO/IEC 27001 is that initially you will put things in place because the standard says you should. Some of the requirements may seem unnecessary or over the top. But gradually you will start to see why they are included and the difference it makes to your organization. After a period, you will begin to implement procedures and methods that go further than the requirements of the standard because you can see that they would be useful and will provide better protection for your organization. You'll start to see that it's about becoming more proactive in everything you do and in the long term this reduces the amount of reactive activities necessary. In simple terms, you'll start to "get it" (but be patient, it can take a while!).

But in the meantime, you'll need to create some of that "documented information". And that's where the CertiKit ISO/IEC 27001 Toolkit comes in….

2.2 The CertiKit ISO/IEC 27001 toolkit

When looking at information security the emphasis is usually on risk assessment and the maintenance of controls to protect against risk. And it's right that this should be the focus; it is, after all, the main deliverable of the whole information security idea.

In a perfect world we would just assess our risks, based on our intimate knowledge of the business and the threats to it and nothing would ever change. The controls would always be appropriate and effective, never need improving and everyone would know how to use them.

But we live in a far from perfect world where things can and do change on a regular basis, we don't know everything about the business, risks and threats change, people come and go from the organization and our definition of what's important moves all the time.

The ISO/IEC 27001 standard proposes that we don't just need a plan; we need an Information Security Management System or ISMS. The function of the ISMS is to wrap itself around the risk assessment and controls and ensure (among other things) that:

1. Everyone understands what we're trying to achieve (Objectives)
2. The risk assessment is based on the right information about the business (Business context)
3. We have a good idea of what the current main threats are (Risk management)
4. Everybody knows about the controls (including policies and procedures) and how to use them (Awareness and training)
5. We update the risk assessment when things change around it (Management review)
6. The level of protection in place gets better over time (Continual improvement)

The CertiKit ISO/IEC 27001 Toolkit (referred to within this document simply as the "Toolkit") provides not only the plan, but also a large part of the ISMS that supports it. Within your Toolkit you will have an array of useful documents which provide a starting point for all the different areas of the standard. The documents are in Microsoft Office 2010® (or above) format and consist of Word documents, Excel workbooks, PowerPoint presentations, Visio diagrams and Project plans.

Each document is located within a folder structure that maps onto the various sections of the standard and is placed under the section that is most relevant to its content. Some documents are relevant to multiple sections of the standard and are placed in the one of greatest relevance. We include an index of the documents and the sections of the standard that they address.

A document reference naming convention is used throughout the Toolkit which is described in an *Information Security Management System Documentation Log*. This includes a reference to the section number of the ISO/IEC 27001 standard to which the document refers. The standard doesn't require that you use this specific naming convention so feel free to change it if you need to.

The documents themselves have a common layout and look and feel and adopt the same conventions for attributes such as page widths, fonts, headings, version information, headers and footers. Custom fields are used for the common items of information that need to be tailored such as [Organization Name] and these are easily changed in each document.

Every document starts with an “Implementation Guidance” section which describes its purpose, the specific areas of the ISO/IEC 27001 standard it is relevant to, general guidance about completing and reviewing it and some legal wording about licensing etc. Once read, this section, together with the CertiKit cover page, may be removed from the final version of the document.

The layout and headings of each document have been designed to guide you carefully towards meeting the requirements of the standard and example content has been provided to illustrate the type of information that should be given in the relevant place. This content is based upon an understanding of what a “typical” organization might want to say but it is very likely that your organization will vary from this profile in many ways, so you will need to think carefully about what content to keep and what to change. The key to using the Toolkit successfully is to review and update each document in the context of your specific organization. Don’t accept the contents without reading them and thinking about whether they meet your needs – does the document say what you want it to say, or do you need to change various aspects to make it match the way you do things? This is particularly relevant for policies and procedures where there is no “right” answer. The function of the document content is help you to assess what’s right for you so use due care when considering it. Where the content is very likely to need to be amended, we have highlighted these sections but please be aware that other non-highlighted sections may also make sense for you to update for your organization.

2.3 Transitioning from ISO/IEC 27001:2013 to 2022

If your organization is currently certified to the 2013 version of the ISO/IEC 27001 standard or you’re working toward that using a previous version of the CertiKit Toolkit, you have a number of options.

For the first 18 months of the three year transition period for ISO/IEC 27001:2022 you could still become certified to the 2013 version of the standard, especially if you’ve already put a lot of work in towards that. You would then need to move over to the 2022 version before the end of the transition period.

If you’d rather go straight for certification to ISO/IEC 27001:2022 then (as well as ensuring you address the relatively minor changes to the management system requirements) you’ll need to map your documentation across to the new Annex A controls. All of the previous controls are included in the new set, and there are eleven new ones. Helpfully, there is a mapping both ways included in the Annexes of the ISO/IEC 27002:2022 guidance standard and that is what we have used in migrating our toolkit across from the 2013 to the 2022 set of controls. This is really another reason to invest in a copy of ISO/IEC 27002:2022 for your organization.

Additionally, within the Toolkit *Release Notes* for Version 12 we have listed the previous reference for each document so you can see which control area it previously related to, and which control it now relates to, as well as listing the documents associated with the new

controls. The *CERTIKIT ISO27001 Toolkit Index* and *ISO27001 Assessment Evidence* will also help in this.

Another main area that will need some attention is *Clause 6. Planning* which covers risk assessment and the statement of applicability. You may need to update your risk assessment if it makes reference to specific Annex A controls, and your statement of applicability will need to list the new 2022 control set rather than the one from the 2013 version of the standard. These are both included in the Toolkit.

If your document referencing scheme includes the Annex A control areas in its structure you may need to consider amending that so that it remains consistent.

Lastly, the list of policies referenced by your *Information Security Policy* may need updating with the additional policies required for the new controls in Annex A of ISO/IEC 27001:2022.

This transition is a good opportunity to check through all of your ISMS documentation to find any other references you may have made to specific Annex A controls, and which will need to be amended.

Once you can satisfy your auditor that your ISMS has moved across to the 2022 set of controls, your certification is ready to be updated to ISO/IEC 27001:2022.

2.4 If yours is a small organization

The CertiKit ISO27001 Toolkit has been deliberately designed to be flexible and easy to adapt to your needs. The standard itself doesn't dictate any specific structure of documentation so you're free to do whatever makes sense for you if the requirements are met. Some smaller organizations decide to merge some of the supplied documents together so that the total number of documents in the ISMS is reduced. This makes sense if the number of people involved is small and approval cycles are short. To help with this process, you make like to consider the following suggestions for documents that could be merged:

The *Information Security Management System Manual* could also incorporate:

- *Information Security Context, Requirements and Scope*
- *Information Security Roles Responsibilities and Authorities*
- *Procedure for the Control of Documented Information*
- *Procedure for Internal Audits*
- *Procedure for Management Reviews*
- *Procedure for the Management of Nonconformity*

The *Information Security Policy* could be expanded to directly address the detail of all areas rather than referring to topic-specific policies. In this case, the following (or a subset) could be incorporated:

- *Internet Acceptable Use Policy*

- *Cloud Services Policy*
- *Mobile Device Policy*
- *BYOD Policy*
- *Remote Working Policy*
- *Access Control Policy*
- *Dynamic Access Control Policy*
- *Cryptographic Policy*
- *Physical Security Policy*
- *Anti-Malware Policy*
- *Backup Policy*
- *Logging and Monitoring Policy*
- *Software Policy*
- *Technical Vulnerability Management Policy*
- *Network Security Policy*
- *Electronic Messaging Policy*
- *Secure Development Policy*
- *Information Security Policy for Supplier Relationships*
- *Availability Management Policy*
- *IP and Copyright Compliance Policy*
- *Records Retention and Protection Policy*
- *Privacy and Personal Data Protection Policy*
- *Clear Desk and Clear Screen Policy*
- *Social Media Policy*
- *HR Security Policy*
- *Threat Intelligence Policy*
- *Asset Management Policy*
- *Acceptable Use Policy*
- *CCTV Policy*
- *Configuration Management Policy*
- *Information Deletion Policy*
- *Data Masking Policy*
- *Data Leakage Prevention Policy*
- *Monitoring Policy*
- *Web Filtering Policy*
- *Secure Coding Policy*

It's up to each small organization to decide if this approach would be right for them; inevitably there are pros and cons of having more or fewer documents and some form of compromise solution based on our suggestions might also be appropriate.

2.5 Integrating management systems

If your organization has already achieved certification to an ISO standard, such as ISO9001, then you will probably want to incorporate your ISO27001 ISMS into an integrated

management system, rather than run your management systems in isolation. This should speed things up, save administration time and hopefully reduce the ongoing costs of certification too. So, for example, your existing QMS becomes an integrated management system that meets the requirements of both ISO9001 and ISO27001 at the same time. Because of the ISO Annex SL structure, we talked about earlier, this integration process should be reasonably straightforward to achieve.

In toolkit terms, each CertiKit product includes all of the documents you need to address the requirements of the specific standard it is aimed at. But if you have already put a management system in place using one of our toolkits, how do you go about merging a second toolkit into a streamlined, integrated management system? There are a number of key documents that have the same (or very similar) titles in each toolkit, and it is mainly these that will need to be merged. We suggest you start with the existing version of your document and add in the new content relevant to the additional standard that you are implementing. For example, if you already have ISO9001 certification you will be adding in content relevant to ISO27001.

The main Toolkit documents (ISO27001 or other standard) that will be involved in this merging process are shown in Table 1.

EXISTING DOCUMENT	RECOMMENDED ACTION TO INTEGRATE ISMS
Context, Requirements and Scope	Add additional relevant context, internal and external issues, interested parties and their requirements and state the scope of the ISMS in addition to the existing management system scope(s)
(Management System) Policy	Add references to information security responsibilities.
Roles Responsibilities and Authorities	Include information security-specific roles where they are separate from existing roles. Update existing roles to include information security-specific responsibilities and authorities.
Top Management Communication Programme	State information security topics that will be communicated on, and how.
Risk Assessment and Treatment Process (and opportunity assessment process)	Add criteria for when information security risk assessments will be carried out. Adjust impact assessment criteria to cater for information security issues if required.
Procedure for the Control of Documented Information	Adjust naming convention of documents if required (depends on the convention you decide to adopt).
Documentation Log	Add the new documents that are part of your integrated management system.
Competence Development Procedure	Cover the additional information security roles.
Process for Monitoring Measurement Analysis and Evaluation	Include information security-related metrics.
Procedure for Internal Audits	Add ISO27001 to the standards to be audited.
Procedure for Management Reviews (if included)	Adjust attendees and areas to be reviewed.

EXISTING DOCUMENT	RECOMMENDED ACTION TO INTEGRATE ISMS
Internal Audit Schedule	Cover the specifics of ISO27001 that need to be audited, for example controls from Annex A.
Management Review Meeting Agenda	Include additional agenda items in existing agenda, for example information security policy.

Table 1 - Main toolkit documents to be merged in an integrated management system

The remaining documents will be ISO27001-specific and so should generally be used as they are. An exercise to ensure that all documents in your integrated management system cover both (or all) of the standards involved should also be carried out.

Remember that just because you operate an integrated management system this does not mean you must be audited for all standards at the same time. You can still choose to split your audits and even use different certification bodies if that suits your needs better.

2.6 Where to start

Relevant Toolkit documents

- *ISO27001 Gap Assessment Tool*
- *ISO27001 Assessment Evidence*
- *CERTIKIT ISO27001 Toolkit Index*
- *ISO27001 Benefits Presentation*

Optional Add-Ons (available at additional cost via our website)

- *ISO27001 Enhanced Gap Assessment Tool*

Note: the Enhanced Gap Assessment Tool also comes with a full ISO-text ISO27001 Statement of Applicability as a separate document.

Before embarking on a project to achieve conformity (and possibly certification) to the ISO/IEC 27001 standard it is very important to secure the commitment of top management to the idea. This is probably the single most significant factor in whether such a project (and the ongoing operation of the ISMS afterwards) will be successful. Indeed, “Leadership” has its own section within the standard and without it there is a danger that the ISMS will not be taken seriously by the rest of the organization and the resources necessary to make it work may not be available. In order to help your management decipher the meaning of the standard we have provided a Simple English translation of the requirements which aims to explain clearly each point without using “ISO-speak”.

The first questions top management are likely to ask about a proposal to become certified to the ISO/IEC 27001 standard are probably:

- What are the benefits – why should we do it?
- How much will it cost?
- How long will it take?

In order to help answer these questions the CertiKit ISO/IEC 27001 Toolkit provides certain resources.

The *ISO27001 Gap Assessment Tool* is an Excel workbook that breaks down the sections of the ISO/IEC 27001 standard and provides a way of quantifying to what extent your organization currently meets the requirements contained within them. By performing this gap assessment, you will gain a better appreciation of how much work may be involved in getting to a point where a certification audit is possible.

The gap assessment tool breaks the standard down by section and sub-section and a series of key questions are asked in order to assess how close to meeting the standard your organization is. The questions are designed to address the main requirements of the standard and a positive answer means that you are likely to be conformant.

The gap assessment includes a dashboard showing an analysis of where your organization meets the standard – and where work must still be carried out.

However, if you would prefer to have all of the exact requirements of the standard laid out for you without needing to refer to a copy of the standard document then we provide a further tool which is a chargeable extra to the Toolkit and available via the CertiKit website. We can provide this because we have a licensing agreement with the ISO, via BSI, to include the full contents of the requirements of the standard (for which CertiKit pays a license fee).

The *ISO27001 Enhanced Gap Assessment Tool* goes several steps further than the default gap assessment by breaking down the text of the ISO/IEC 27001 standard itself into individual requirements (with the full text of each requirement) and providing a more detailed analysis of your conformance. It can also be used to allocate actions against individual requirements.

The key to making the gap assessment as accurate as possible is to get the right people involved so that you have a full understanding of what is already in place. The gap assessment will provide hard figures on how compliant you currently are by area of the standard and will even show you the position on radar and bar charts to share with top management.

It's a good idea to repeat the exercise on a regular basis during your implementation project in order to assess your level of progress from the original starting point.

The accompanying workbook *Assessment Evidence* allows you to start to build a picture of what evidence (including toolkit documents, your own existing documents and your records) may be appropriate to show conformity. This may help when deciding whether a requirement is met or not. This can be used in conjunction with the *CERTIKIT ISO27001 Toolkit Index* which gives a detailed breakdown of how the documents in the toolkit map onto the requirements sections of the standard.

Having gained an accurate view of where you are against the standard now, you are then armed with the relevant information to assess how much effort and time will be required to achieve certification. This may be used as part of a presentation to top management about the proposal and a template *ISO/IEC 27001 Benefits Presentation* is provided in the Toolkit for this purpose. Note that budgetary proposals should include the costs of running the ISMS on an ongoing basis as well as the costs of putting it in place.

As part of your business case you may also need to obtain costs from one or more external auditing bodies for a Stage One and Stage Two review and ongoing surveillance audits (see later section about external auditing).

2.7 A suggested project plan

Relevant Toolkit documents

- *ISO27001 Project Plan*
- *Information Security Management System Project Initiation Document (PID)*
- *ISO27001 Progress Report*
- *Certification Readiness Checklist*

Having secured top management commitment, you will now need to plan the implementation of your ISMS. Even if you're not using a formal project management method such as PRINCE2® we would still recommend that you do the essentials of defining, planning and tracking the implementation effort as a specific project.

We have provided a template *Project Initiation Document* (or PID) which prompts you to define what you're trying to achieve, who is involved, timescales, budget, progress reporting etc. so that everyone is clear from the outset about the scope and management of the project. This is also useful towards the end of the project when you come to review whether the project was a success.

Having written the PID, try to ensure it is formally signed off by top management and that copies of it are made available to everyone involved in the project so that a common understanding exists in all areas.

The CertiKit ISO/IEC 27001 Toolkit provides a Excel-based plan as a starting point for your project. This is fairly high level as the detail will be specific to your organization, but it gives a good indication as to the rough order that the project should be approached in.

It's fair to say that in general if you implement your ISMS in the order of the ISO/IEC 27001 standard from section 4 to section 10 you won't go far wrong. This isn't necessarily true of some of the other management system standards we have mentioned such as ISO/IEC 20000 but for ISO/IEC 27001, because it includes much of the information security content within a separate Annex A, it flows quite well.

The main steps along the way to certification are described in more detail later in this guide and there are some parts that need to be done in a certain order otherwise the right information won't be available in later steps. An example is that you need to complete your risk assessment before completing your *Statement of Applicability* because otherwise you won't have enough information to assess whether each control applies to your organization.

A simple twelve-step sequence for the route to certification is shown in figure 1 below. As suggested, this effectively steps through the standard in order although it starts with the foundation for the project (and for the ongoing ISMS) which is obtaining management commitment.

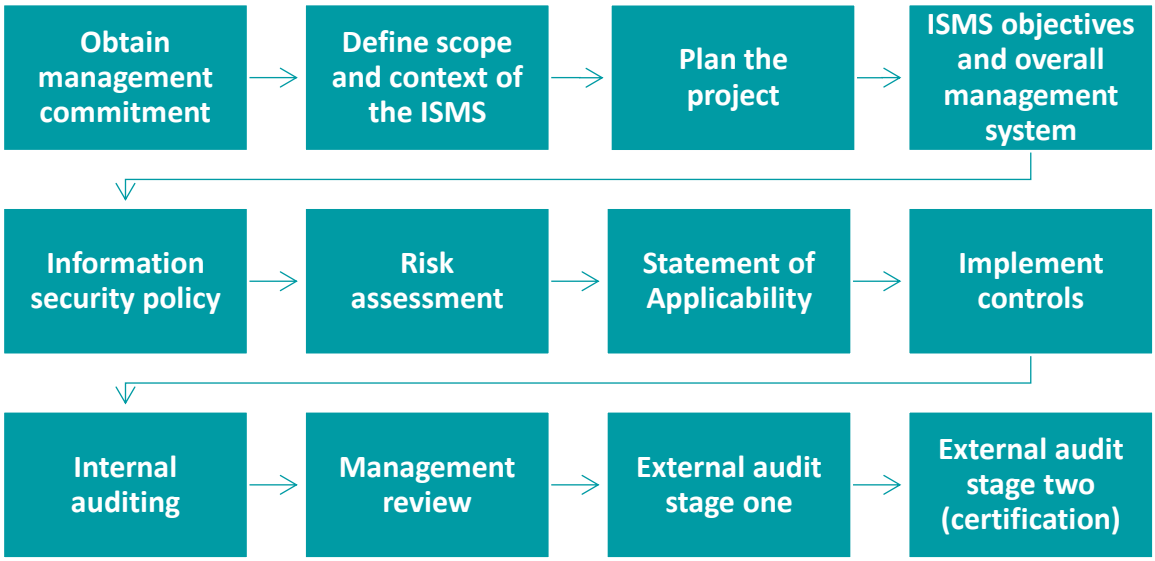

Figure 1: Overall ISMS implementation order

Once a project manager has been appointed and the project planned and started, it's a good idea to keep an eye on the gap assessment you carried out earlier and update it as you continue your journey towards certification. This updated measurement of your closeness to complete conformity with the standard can be included as part of your regular progress reports and the CertiKit ISO/IEC 27001 Toolkit includes a template for these.

The timing of when to go for certification really depends upon your degree of urgency (for example you may need evidence of certification for a commercial bid or tender) and how ready you believe the organization to be. Certainly, you will need to be able to show that all areas of the ISMS have been subject to internal audit before asking your external auditing body to carry out the stage two (certification) assessment. But you don't need to wait until you're "perfect", particularly as the certification audit will almost certainly throw up things you hadn't thought of or hadn't previously regarded as important. The *Certification Readiness Checklist* provides a simple way to check whether the main components are in place when considering certification.

2.8 How this guide is structured

The remainder of this guide will take you through the sections of the ISO/IEC 27001 standard one by one, explaining what you may need to do in each area and showing how the various items in the CertiKit ISO/IEC 27001 Toolkit will help you to meet the requirements quickly and effectively.

As we've said earlier, regard this guide as helpful advice rather than as a detailed set of instructions to be followed without thought; every organization is different, and the idea of an ISMS is that it moulds itself over time to fit your specific needs and priorities.

We also appreciate that you may be limited for time and so we have kept the guidance short and to the point, covering only what you need to know to achieve conformity and hopefully certification. There are many great books available about information security and we recommend that, if you have time, you invest in a few and supplement your knowledge as much as possible.

3 Implementing the ISO/IEC 27001 Standard

3.1 Clause 0 Introduction

The introduction to the standard is worth reading, if only once. It gives a good summary of what the ISO sees as the key components of an ISMS; this is relevant and important when understanding where the auditor is coming from in discussing what might be called the "spirit" of the ISMS. The detail in other sections of the standard should be seen in the context of these overall principles and it's important not to lose sight of that when all attention is focussed on the exact wording of a requirement.

There are no requirements to be met in this section.

3.2 Clause 1 Scope

This clause refers to the scope of the standard rather than the scope of your ISMS. It explains the fact that the standard is a "one size fits all" document which is intended to apply across business sectors, countries and organization sizes and can be used for a variety of purposes.

There are no requirements to be met in this section.

3.3 Clause 2 Normative references

Some standards are supported by other documents which provide further information and are very useful if not essential in using the standard itself. For ISO/IEC 27001 the one quoted here is ISO/IEC 27000 which sets out the overview and vocabulary for an ISMS.

There are no requirements to be met in this section.

3.4 Clause 3 Terms and definitions

Unlike many other standards, ISO/IEC 27001 doesn't list any definitions at all, simply referring the reader to ISO/IEC 27000. If you feel you need to know the exact definitions of some of the terms used in ISO/IEC 27001 then this is the place to look, although in many cases you may not feel much more enlightened after reading the definition.

There are no requirements to be met in this section.

3.5 Clause 4 Context of the organization

Relevant Toolkit documents

- *Information security Context, Requirements and Scope*

This clause is about understanding as much as possible about the organization itself and the environment in which it operates. The key point about the ISMS is that it should be appropriate and relevant to the specifics of the business it is protecting. To ensure this, the people implementing and running the ISMS must be able to answer questions about what the organization does, where, how and who for (plus many others).

The ISMS will also be affected by the situation within the organization (internal issues) and outside the organization (external issues). Internal issues are factors such as the culture, management structure, locations, management style, financial performance, employee relations, level of training etc. that define the organization. External issues are those less under the organization's control such as the economic, social, political and legal environment that it must operate within. All these issues (internal and external) will have bearing on the priorities, objectives, operation and maintenance of the ISMS. This is particularly relevant when we discuss the areas of risk assessment and control selection where a comprehensive knowledge of how the organization operates and what could affect it are essential.

The standard also requires that the way in which the ISMS fits in with the controls already in place within the organization such as corporate risk management, business strategies and policies is defined and that all interested parties are identified, together with their relevant requirements, such as legal, regulatory or contractual obligations.

One of the items that should be defined and documented is the organization's risk appetite. This refers to the overall attitude to risk; is the organization risk-averse and therefore wants to minimize risk at every level? Or is the attitude that of high risk/high reward where not everything will work out well but enough will deliver results to keep the company going? Or is it somewhere in between?

This needs careful consideration and discussion with top management; unless the organization is obviously very conservative or obviously very "high stakes" the answer is probably somewhere around the middle. This factor is used later when deciding what to do about risks identified during a risk assessment – to treat them or to accept them. Risk appetite can be defined at many levels within the organization and so may vary according to what is being risk assessed and at what point in time, so a clear understanding is very helpful.

The context section is also the one where the scope of the ISMS is defined. Again, this needs careful consideration. If your organization is small, it usually makes sense to place everything it does within the scope because often it can be more difficult to manage a limitation to the scope than to simply cover everything. As the organization grows so do the issues with scope. There are three main areas in which the scope might be limited; organization structure (e.g. one division or group company but not others), location (e.g. the

Rome office but not the San Diego one) and product/service (e.g. the outsourcing/hosting service but not the software development service). It is perfectly acceptable to start with a smaller scope for certification and then widen it out year by year as the ISMS matures and everyone becomes more familiar with what's involved. In fact, if you need to achieve certification within a short timescale this may well be the best route. You must ensure however that your exclusions make sense and can be justified to the auditor.

One point to note is the difference between the scope of the ISMS and the scope of certification to the ISO/IEC 27001 standard; they don't have to be the same. You can (if it's useful to do so) have a wide ISMS scope but only ask for certification to a part of it initially. If the part in question meets all the requirements of the standard, then it should be acceptable.

The Toolkit provides a template document that prompts for most of the information described above and groups the documented information required for context, requirements and scope into one place. It is perfectly acceptable to split this content into more than one document if that works better for you.

3.6 Clause 5 Leadership

Relevant Toolkit documents

- *Information Security Management System Manual*
- *Information Security Roles, Responsibilities and Authorities*
- *Information Security Policy*
- *Executive Support Letter*
- *Meeting Minutes*

3.6.1 Clause 5.1 Leadership and commitment

The leadership section of the standard is about showing that top management are serious about the ISMS and are right behind it. They may do this in various ways. The first is by demonstrating management commitment; partly this is by simply saying that they support the ISMS in meetings, in articles in internal and external magazines, in presentations to employees and interested parties etc. and partly by making sure the right resources and processes are in place to support the ISMS, for example people, budget, management reviews, plans etc. Sometimes these kinds of activities can be difficult to evidence to an auditor so within the Toolkit we have provided certain documents that may help in this, including an executive support letter and a template for relevant meetings to be minuted.

3.6.2 Clause 5.2 Policy

The second way for top management to show they are serious about the ISMS is to ensure that there are appropriate information security policies in place. These need to be signed off by top management and distributed to everyone that they might be relevant to. A template information security policy is provided in the Toolkit that addresses the areas of commitment required by the standard and further topic-specific policy documents are provided under the relevant sections within Annex A.

Generally, most organizations take one of two approaches to policy creation; they either go for a single, all-encompassing information security policy or they go for a more modular approach with individual policies used to address specific issues. Both approaches have pros and cons, often depending on the size of your organization and how much work in involved in getting policy changes approved. If your organization is relatively small then we would recommend having a single policy document which covers all areas; however, you will still need to consider the audience for the policy – there is no point in having technical detail about server security in a document that is intended to be understood by users, so you may still end up with a user-focussed policy and a more technical corporate policy anyway. If your organization is larger you may be best with a hierarchical structure of policies with the main points being approved at board level and the details defined at a lower management level. This means that if the detail changes you don't need to wait for a slot on the board agenda to get them approved each time. There isn't a single right answer for information security policies in the context of the ISO/IEC 27001 standard; the main point is that whatever you do choose to state in your policies, you can show that it is being communicated, understood and followed within the organization.

3.6.3 Clause 5.3 Organizational roles, responsibilities and authorities

Lastly, top management need to make sure that everyone involved in the ISMS knows what their role(s) and associated responsibilities and authorities are. Again, a document is provided in the Toolkit as a starting point for this. Remember to ensure that information security is included in the day-to-day responsibilities of existing roles rather than trying to create a parallel organization structure just for information security; it needs to be business as usual not an add-on.

Remember also that demonstrating leadership is an ongoing process, not a one-off activity solely during implementation.

3.7 Clause 6 Planning

Relevant Toolkit documents

- *Information Security Objectives and Plan*
- *Risk Assessment and Treatment Process*

- *Risk Assessment Report*
- *Risk Treatment Plan*
- *ISMS Change Process*
- *ISMS Change Log*
- *Asset-Based Risk Assessment and Treatment Tool*
- *Statement of Applicability*
- *Scenario-Based Risk Assessment and Treatment Tool*
- *Opportunity Assessment Tool*

Optional Add-On (available at additional cost via our website)

- *ISO27001 Statement of Applicability (Full ISO-text version)*

Note: The above option is part of the *ISO27001 Enhanced Gap Assessment Tool*.

3.7.1 Clause 6.1 Actions to address risks and opportunities

The general ethos of the ISO/IEC 27001 standard is to be proactive in managing information security and a central concept to this is risk assessment. This involves considering what could go wrong and then taking steps to do something about it in advance rather than waiting for it to happen. The standard points out that not everything that happens is necessarily negative and that there may be positive "opportunities" along the way too.

The whole idea of a risk-based approach is that the amount you spend on controls is appropriate to your level of risk and takes account of how much risk you are prepared to live with. Risk is very much a spectrum as the wider debate on "privacy versus security" shows and your organization will need to take a considered approach to the level of controls it chooses to introduce and maintain to provide the "right" level of security. A risk assessment needs to be conducted to analyse and evaluate the impact and likelihood of various events occurring. This will give you the opportunity to do something about those risks that are both likely and have a significant impact i.e. to treat the risks.

There are many ways of analysing risk and the ISO/IEC 27001 standard mentions that another standard, ISO31000, should be used as a framework for this. ISO31000 is worth a read and sets out how to establish an organization-wide framework for risk assessment, not just for information security purposes but for all potential risks to the business. But ISO31000 itself doesn't go into detail about how risks should be identified; there are yet two more standards that fill this gap - ISO31010 and ISO/IEC 27005. You may realise from this that risk assessment is a very big subject in itself and there are very many techniques available to use if you choose to; ISO/IEC 27001 doesn't dictate which one to use and our recommendation is that you keep it as simple as possible, depending on the size of your organization and how much time you have.

One point to note is the need to consider the external and internal issues you described from Clause 4 and the requirements of your interested parties when identifying risks (and

opportunities). This should help to ensure that your ISMS delivers what it should for your interested parties.

The previous version of the ISO/IEC 27001 standard (published in 2005) required that an organization take an "asset-based" approach to risk assessment. This involved focussing on the organization's information assets and then considering the threats to them and their vulnerabilities to those threats. The 2013 version of the standard removed the requirement to take this approach, although it remains a perfectly valid way to assess risk. In the Toolkit we have provided a choice of an asset-based approach and a simplified scenario-based approach; either is compatible with the standard and it is up to you to decide which one works best within your organization.

Both risk assessment processes are compatible with the ISO31000 standard. Effective risk identification can often be done by simply getting the right people with the relevant knowledge into a room and asking them about what they worry about most about their area of responsibility. This should give you a good starting point to assess the risks that they identify. Consult other parties such as external consultants and authorities where appropriate to get as good a picture as possible.

The identified risks may be entered the appropriate *Risk Assessment and Treatment Tool* which helps you to assess the likelihood and impact of each risk, giving a risk score. The workbook uses a defined classification scheme to label each risk as high, medium, or low risk, depending on its score. A template *Risk Assessment Report* is provided in the Toolkit to communicate the findings of the risk assessment to top management and so that they can sign it off.

Whether or not each risk needs to be treated depends upon the risk appetite you defined in section 4.1 of the ISO/IEC 27001 standard (Understanding of the organization and its context). For those risks that do need treatment there are three main options:

1. **Modify**: Take some action to reduce the likelihood or impact of the risk
2. **Avoid**: Stop performing the activity that gives rise to the risk
3. **Share**: Get another party to assume all or part of the risk (for example insurance)

Each of these options will have some effect on either the likelihood or impact of the risk, or both. The *Risk Assessment and Treatment Tool* allows you to define what effect you believe the treatment will have in order to decide whether it is enough.

Once the risks have been identified, assessed and evaluated, the risk treatment plan is created. Again, the Toolkit has a template plan which may be used to obtain top management approval of the recommended risk treatments, some of which may involve spending money. Top management also need to agree to the levels of residual risk after the treatments have been implemented (i.e. the risks we're left with once we've done everything proposed).

At this point the standard requires that a specific document called the "Statement of Applicability" be prepared which shows which of the reference controls in Annex A have been adopted and which haven't. Each decision to adopt or not must be justified, ideally

(but not necessarily) by reference to a specific risk you have found that needs to be treated. Some of the reference controls will only apply in certain circumstances so if these don't apply to your organization (or your ISMS scope) then it is acceptable to state that you are not implementing them. Examples might be that *Control A.6.7 Remote working* may not apply if you have no remote workers or *Control A.8.28 Secure coding* may not be relevant if no software development takes place.

The key point to remember in treating risk is that it is a trade-off. Few organizations have limitless funds and so the money spent in treating risk needs to result in a larger benefit than the cost. There are many ways of performing this kind of "quantitative" analysis so that the potential loss from a risk can be expressed in financial terms. The methods used in the Toolkit are "qualitative" in that they simply categorize the risks; if your organization wishes to use more detailed quantitative methods to assess risk loss against cost of treatment then that is perfectly acceptable within the ISO/IEC 27001 standard.

Don't forget to consider the positive aspects of risk i.e. opportunities. The standard requires that these are considered, so that you're as ready as possible if some good news comes your way. The *Opportunity Assessment Tool* provides a way to document and assess these, with resulting preparation actions.

3.7.2 Clause 6.2 Information security objectives and planning to achieve them

Within the planning section of the standard we need to set out what the ISMS is intended to achieve and how it will be done. In terms of the ISMS there are two main levels of objectives. The first is the high-level objectives set out when defining the context of the ISMS. These tend to be quite broad and non-specific in order to describe why the ISMS is necessary in the first place and these objectives probably won't change much.

The second level of objectives is more action-oriented and will refer to a fixed timeframe. In the Toolkit we have provided an information security management plan for a financial year on the assumption that a one-year planning horizon will be used, but this could be a two or three-year plan if that makes sense in your organization. The plan sets out specific objectives, including how success will be measured, the timeframe and who is responsible for getting it done. You may choose to create a Gantt chart in MS Project to support this.

3.7.3 Clause 6.3 Planning of changes

It's important to keep the ISMS up to date, so changes to it need to be thought about and implemented carefully. Changes could be as a result of unexpected events such as a pandemic, or based on reasonable notice, for example with amended legislation or regulation. In both cases, the types of activities required will be similar to those in the previous section – the what, who, when, how etc. and it may be appropriate to add an agenda item to the regular meetings you hold so that changes are managed effectively.

3.8 Clause 7 Support

Relevant Toolkit documents

- *Information Security Competence Development Procedure*
- *Information Security Communication Programme*
- *Procedure for the Control of Documented Information*
- *ISMS Documentation Log*
- *Information Security Competence Development Report*
- *Awareness Training Presentation*
- *Competence Development Questionnaire*

Covering resources, competence, awareness, communication and documented information, this section describes some of the background areas that need to be in place for the ISMS to function properly.

3.8.1 Clause 7.1 Resources

The standard simply requires that adequate resources are provided for the ISMS to function effectively. This is really a test of the level of management commitment as described earlier.

3.8.2 Clause 7.2 Competence

The Toolkit provides a method of defining the competences needed, conducting a survey of the people involved in the implementation and running of the ISMS, collating the results and then reporting on those areas in which further training or knowledge needs to be gained. You will need to ensure that appropriate records of training are kept and are available to view by the auditor.

3.8.3 Clause 7.3 Awareness

A template information security awareness presentation is also provided. This may be delivered in various ways, including at specially arranged events or at regular team meetings, depending on the timescale required and the opportunities available. Note that the focus of this is awareness rather than detailed training and that anyone with a more involved role to play in the ISMS may need more in-depth training.

3.8.4 Clause 7.4 Communication

Specific procedures may be required relating to business-as-usual communication with internal and external parties about information security; these may be relevant to this section of the standard and a template document *Information Security Communication Programme* is provided in the Toolkit.

3.8.5 Clause 7.5 Documented information

Documented information required by the standard must be controlled which basically means keeping it secure, managing changes to it and ensuring that those that need it have access to it. A procedure that covers the requirements for document control is provided and you will need to decide where such documentation is to be held. In modern times this is usually electronically and could be on a shared network drive, an intranet, a full-blown document management system or any other arrangement that is appropriate to your organization.

3.9 Clause 8 Operation

Relevant Toolkit documents

- *ISMS Process Interaction Overview*

Interestingly, this section of the ISO/IEC 27001 standard is very short and basically repeats what has been stated in other sections. This contrasts with other standards, such as ISO22301 (business continuity) and ISO 9001 (quality management), where most of the requirements are within the *Operation* clause.

However, there is a need to set out the processes of the ISMS and how they interact, and an overview of this is provided in the Toolkit.

3.10 Clause 9 Performance evaluation

Relevant Toolkit documents

- *Process for Monitoring, Measurement, Analysis and Evaluation*
- *Procedure for Internal Audits*
- *Internal Audit Plan*
- *Internal Audit Programme*
- *Internal Audit Checklist*
- *Internal Audit Report*
- *Internal Audit Action Plan*

- *Procedure for Management Reviews*
- *Management Review Meeting Agenda*

The performance evaluation section of the standard is about how you determine whether the ISMS is doing what it is supposed to do.

3.10.1 Clause 9.1 Monitoring, measurement, analysis and evaluation

The ISO/IEC 27001 standard does not tell you what you should measure. It simply requires that you be precise about what it is you have decided to measure and that you do something about it if your measurements show problems. The auditor will expect you to have put some thought into the appropriate measurements to take, how they can be taken and how the results can be reasonably interpreted. The Toolkit provides a document entitled *Process for Monitoring, Measurement, Analysis and Evaluation* which includes suggestions for the types of measurements that might be suitable for a typical organization, but you will need to look at these carefully before using them. It's a good idea to create a documented procedure for the collection and reporting of each measurement because if it is done differently each time then the results will not be helpful.

This is an area that can start relatively small and expand over time; our recommendation is that you select some basic measurements that are easy to collect and interpret and use those for a while. After some time has passed it will probably become obvious that other specific measurements are needed to be able to assess whether things are going well so these can be added gradually. Be careful not to start with a wide range of possibly meaningless, hard to collect measurements that will simply slow everything down and give the ISMS a bad reputation before it has got going.

Having chosen your measurements you need to decide what does "good" look like; what numerical values would mean that performance is in line with expectations? Again, the definition of your objectives may need tweaking over time as you gain experience with taking the measurements and your ISMS moves from implementation mode into ongoing operation mode.

If you find that your objectives are not being met, then an improvement may be required to bring the situation back into line; such improvements should be added to the *Nonconformity and Corrective Action Log* provided within the Toolkit and tracked through to completion.

3.10.2 Clause 9.2 Internal Audit

The standard requires that there is an internal auditing programme in place which audits all aspects of the ISMS within a reasonable period. If you embrace the idea of internal auditing as a useful early warning of any issues at external audit, then you won't go far wrong. Internal audits should ensure that there are no surprises during the annual

certification/surveillance audit which should allow everyone a higher degree of confidence in the ISMS.

In terms of where to start auditing, the standard suggests that you consider the importance of the processes concerned, problem areas identified in previous audits and those parts of the ISMS where significant risks have been identified. Beyond that, there is no order in which internal audits need to happen. Auditors need to be suitably qualified either through experience or training (or both) and must be impartial i.e. they are not involved in the setting up or running of the ISMS.

The Toolkit has documents to help with the internal auditing process, including a schedule, plan, procedure, checklist of questions, report and post-audit action plan. In general, all aspects of internal auditing need to be documented and an external auditor will almost always want to see the most recent internal audit report and track through any actions arising from it.

3.10.3 Clause 9.3 Management review

Management review is another key part of the ISMS which, if you get it right, will hold together everything else and make audits (internal and external) a relatively straightforward experience. The ISO/IEC 27001 standard is specific about what these reviews should cover but it is less forthcoming about how often they should take place. This is one of those areas where you will need to try it and see what works for your organization; too often and it becomes an unacceptable administrative overhead; too infrequent and you risk losing control of your ISMS. The generally accepted minimum frequency is probably once a year. In this case, it would need to be a full review covering everything required by the standard. A more common approach is to split the management review into two parts; perhaps a quarterly review of the main areas with a more complete review on an annual basis. You may even decide that in the early days of the ISMS a monthly review is appropriate. There is no wrong answer, there's just a decision about how much control you feel you need to exercise at management level.

In all cases, every management review must be minuted and the resulting actions tracked through to completion.

3.11 Clause 10 Improvement

Relevant Toolkit documents

- *Procedure for the Management of Nonconformity*
- *Nonconformity and Corrective Action Log*
- *ISMS Regular Activity Schedule*

3.11.1 Clause 10.1 Continual improvement

Continual improvement used to get a lot more attention in previous version of this and similar standards, but the requirements have now become considerably watered down, with only a general commitment needed to show conformity. The best place to evidence improvement is probably as part of management reviews where this is one of the standard agenda items – make sure your improvement actions are minuted.

We have also included a template schedule of regular activities which may be used to guide the maintenance and improvement of your ISMS on an ongoing basis. After the flush of success associated with certification has faded, it can be all too easy to neglect ongoing tasks, and your first surveillance visit will come around all too soon.

3.11.2 Clause 10.2 Nonconformity and corrective action

Despite the section heading of “Improvement”, this section of the standard talks mostly about nonconformities and corrective actions. The ISO definition of a nonconformity is the rather general “non-fulfilment of a requirement” and since a requirement can be pretty much anything, it is best to bring any actions, requests, ideas etc. together in a single place and manage them from there. The Toolkit provides the *Nonconformity and Corrective Action Log* for this purpose. A procedure is also provided which explains how items are added to the list, evaluated and then tracked through to completion.

4 The Annex A Controls

The reference controls within Annex A of the ISO/IEC 27001 standard form a significant part of the overall document and of the implementation effort involved. But it's easy to make the mistake of assuming that, because these controls are listed in the standard, they must be implemented to become certified. This is not necessarily the case.

The 93 controls within Annex A are effectively a menu to be chosen from when creating your risk treatment plan. Some of them may not be required because they address a risk you don't have. Similarly, you may decide to address a risk using a different control than the suggested one from Annex A; this is acceptable. However, it may also be the case that you need to introduce more controls than those in Annex A if your level of risk in a certain area is high.

The key is to adopt a considered, sensible approach based on what your risk assessment is telling you. If you feel you can justify your actions to an auditor, then varying the controls from those in Annex A is not a barrier to certification.

Having said this, the controls within Annex A are very sensible measures which, taken together, allow many different areas of risk to be addressed in a comprehensive way so think hard before you decide to do anything different; your default position should be that you will implement the Annex A control.

Remember that ISO/IEC 27002 provides more detail about each of the controls; the advice given below is a summary of the main points about each control area and how the documents within the Toolkit will help you to implement the set of controls.

Note also that Annex A of the ISO/IEC 27001 standard simply states the main description of the control, taken word for word from ISO/IEC 27002. If you have a copy of the ISO/IEC 27002 guidance document, it's easy to make the mistake of considering its entire contents to be requirements, which it isn't; it is *guidance* and an auditor isn't able to raise a nonconformity at audit time if you haven't implemented the advice from ISO/IEC 27002. Many people don't purchase a copy of ISO/IEC 27002 and work solely from the control description in Annex A of ISO/IEC 27001. That's a reasonable thing to do (although we believe the extra guidance is useful) and it then becomes a case of interpreting what's required for the control purely from Annex A. This can have the effect of leaving a little "wiggle room" in how you approach a control's implementation.

As previously stated, the controls are grouped into four fairly uneven categories:

- A.5. Organizational controls (37 controls)
- A.6. People controls (8 controls)
- A.7. Physical controls (14 controls)
- A.8. Technological controls (34 controls)

Let's take each of these in turn.

4.1 A.5 Organizational controls

This group is the largest of the four, and the controls in here have a largely policy and procedure-driven focus, although it must be said that it's a bit of a mixed bag, ranging from threat intelligence to classification of information to access control and much more. You'll need significant business engagement in putting these controls in place as they also cover topics such as project management, supplier relationships, cloud services and intellectual property rights.

4.1.1 A.5.1 Policies for information security

Relevant Toolkit documents

- *Social Media Policy*
- *HR Security Policy*
- *All other policies*

Policies are an important part of the ISMS and are either required or recommended in many places within the standard. The approach taken in the Toolkit is to have an overarching *Information Security Policy* which then references the list of topic-specific policies to form a comprehensive set. Such policies set out the general approach that the organization is taking to a subject and usually include the "dos and don'ts" for that area. They don't have to be lengthy; in fact, many would recommend that they be as short as possible because, unless they are read by people they are aimed at, they will have little effect.

In most cases, the ISO/IEC 27001 standard doesn't dictate what should be said in a policy (the main exception being the overarching *Information Security Policy*). However, it does emphasise that a policy should be approved by top management and communicated to those it is intended to apply to, so it may be useful to either get employees to sign a copy to say they have read it or keep records of attendees at briefing sessions (or both). It is also important that the contents of the policy are taken seriously, and an auditor will often raise a nonconformity if a policy states that something should be done but isn't. Measures to implement all the contents of your policies should either already be in place or on your improvement plan to do soon. Lastly, make sure you review your policies at least annually and record the fact that a review was carried out.

4.1.2 A.5.2 Information security roles and responsibilities

Relevant Toolkit documents

- *This control is addressed by documents in other folders - See Toolkit Index*

To some extent, this control mirrors the requirements of *Clause 5.3 Organizational roles, responsibilities and authorities* from the management system part of the ISO/IEC 27001

standard. This means you will need to have defined your roles and allocated them to meet the main requirements of the standard anyway, so this control shouldn't be difficult to achieve. A common approach is to appoint an Information Security Manager (or, more commonly, a CISO – Chief Information Security Officer) to hold overall responsibility for information security within the organization. Don't forget these are roles and not necessarily full-time jobs and could be allocated to existing people as additional responsibilities.

4.1.3 A.5.3 Segregation of duties

Relevant Toolkit documents

- *Segregation of Duties Guidelines*
- *Segregation of Duties Worksheet*

This is about reducing the risk of insider fraud or attacks by ensuring that more than one person would need to be in on the action to make it possible. In some traditional areas such as finance, segregation of duties may already be in place (such as one person must create a supplier and a different one must pay them) but give this some thought where new processes are implemented. In small organizations this control may be less applicable but should still be considered in areas such as change control, software development and system administration.

4.1.4 A.5.4 Management responsibilities

Relevant Toolkit documents

- *Information Security Whistleblowing Policy*

Related to control A.5.2 (and Clauses 5.1 and 5.3 of the management system requirements), this control is about ensuring that managers have good information security awareness and apply this to their management of employees so that the awareness gets passed down the chain. This could involve specific training for managers and support for them to identify training requirements and spot noncompliance amongst their teams.

There is also scope for allowing instances of bad practice to be reported by whistleblowers and a policy is provided for this within the Toolkit.

4.1.5 A.5.5 Contact with authorities

Relevant Toolkit documents

- *Authorities Contacts*

If your organization operates in a regulated industry such as Finance or Gambling, then this control may be fairly straightforward to understand, and will already be in place. However, even if this is the case, there may be other authorities that would be useful to establish contact with as a precaution. These could include supervisory authorities (from a data protection viewpoint) and emergency services (in connection with business continuity). Contact could consist simply of receiving their newsletter or defining procedures for how to contact them in specific circumstances, such as during a data breach that affects PII (personally identifiable information).

4.1.6 A.5.6 Contact with special interest groups

Relevant Toolkit documents

- *Special Interest Group Contacts*

Contact with authorities and special interest groups is generally easy nowadays with the growth of online facilities such as discussion forums but it may be better to focus on a few important and relevant groups rather than spreading your time too thinly. This control is often related to the maintenance of professional qualifications which require membership and CPE (continuing professional education) points to be logged. Contact may be achieved via various methods such as social media, attendance at webinars and conferences, subscription to newsletters and participation in local regional groups.

4.1.7 A.5.7 Threat intelligence

Relevant Toolkit documents

- *Threat Intelligence Policy*
- *Threat Intelligence Process*
- *Threat Intelligence Report*

There is a wealth of information available, often free, about the types of threats your organization may face, and this control is concerned with bringing this together into a form that can be actioned by your employees to reduce risk. Generally approached at the strategic, tactical and operational levels, a regular effort is required to obtain relevant information and process it so that its implications for your defences can be defined and action taken, such as patching and device reconfiguration.

A number of companies and authorities publish annual reviews of threats at the strategic and tactical levels and there are several common information sharing forums available to join to find out what is happening almost in real time.

4.1.8 A.5.8 Information security in project management

Relevant Toolkit documents

- *Information Security Guidelines for Project Management*

If your organization doesn't have a formal project management approach then this may be a good time to start to define one, even if it simply includes the basics. It would help to get your information classification scheme in place first (see control *A.5.12 Classification of information*) as this will provide a framework to use within your projects.

A good first step is to introduce risk assessment into your project method so that the threats and required controls for any specific project can be identified.

4.1.9 A.5.9 Inventory of information and other associated assets

Relevant Toolkit documents

- *Asset Management Policy*
- *Information Asset Inventory*

A good asset list is fundamental to the operation of the ISMS so this is another area where your time will be well spent. It's important to understand exactly what it is you are trying to protect and what value these assets have to your organization, so make sure you involve the right people in assessing them. Note that the emphasis here is on information assets, such as customer databases and product designs, rather than physical ones such as computers and software. Physical assets are relevant, and you should certainly keep track of them, but they have a supporting role in information security (referred to in the standard as "other associated assets"), rather than being the focus of attention.

This is about knowing where to find the required information, rather than necessarily having a single, separate list of assets (although you can do this if you prefer) so asset information could be held in a number of data sources such as spreadsheets or databases. Knowing how to access them, the information they hold and how they are updated are all key issues.

A specific requirement of this control is that assets must have owners, so you will need to have a way to define which role in your organization owns which assets.

4.1.10 A.5.10 Acceptable use of information and other associated assets

Relevant Toolkit documents

- *Acceptable Use Policy*
- *Internet Acceptable Use Policy*
- *Electronic Messaging Policy*

- *Asset Handling Procedure*
- *Procedure for Managing Lost or Stolen Devices*

This control is often addressed by the definition of an *Acceptable Use Policy* which sets out the rules for how information and other associated assets must be used, for example what can and can't be done with them. This may be supported by procedures which go into more detail regarding how each type of asset should be handled, for example how it should be stored and disposed of.

4.1.11 A.5.11 Return of assets

Relevant Toolkit documents

- *New Starter Checklist*

In those cases where assets have been issued to individuals, it is important that they are returned when no longer required, for example upon leaving the organization. The key aspect of this is to ensure that accurate records are kept of which assets have been issued in the first place, so that checks can be made when the time comes. The kinds of assets typically involved are endpoint devices such as laptops or phones, MFA (multifactor authentication) tokens and peripheral devices that may have been used for remote working.

4.1.12 A.5.12 Classification of information

Relevant Toolkit documents

- *Information Classification Procedure*

Information classification is central to the success of many other areas so put some thought into this; aim for a scheme that is practical, understandable and usable by everyone rather than trying to overcomplicate the situation. The ISO/IEC 27001 standard doesn't state many specifics about information classification (although the ISO/IEC 27002 guidance publication has some useful tips) so the details of how you implement the control are pretty much left up to you. The first decision to make is how many levels of classification to have. It's tempting to over-complicate this in order to reflect the various nuances of your information, but our advice would be to resist this temptation and stick to the lowest number you can reasonably get away with. The trend amongst governments is in this direction, with the UK having reduced its classification levels from five to three (Official, Secret and Top Secret), so you'll be in good company. This doesn't include information that isn't classified at all, often referred to as "Public" and which doesn't need to be protected or labelled.

Choice of names for your classification levels are also up to you. Some of the most common choices are (listed from highest to lowest):

1. Top secret
2. Secret
3. Confidential
4. Restricted
5. Protected
6. Internal Use Only

Names chosen should be appropriate to your organization and a clear definition given of what they mean in practical terms.

4.1.13 A.5.13 Labelling of information

Relevant Toolkit documents

- *Information Labelling Procedure*

Having decided what you're going to call your classification levels, how do you make it clear to everyone involved which information carries which level? Often organizations feel slightly overwhelmed with the thought that they must suddenly label every single electronic and paper document they have, whilst working out what to do with data held in computer systems too.

The key here is to define an approach that addresses the important stuff first and puts a stake in the ground so that labelling starts from a specified point. Look to label the confidential, high-value information first as this is likely to be a much smaller volume than the day-to-day less sensitive information. This requires you to have an accurate asset inventory (*Control A.5.9 Inventory of information and other associated assets*) so that you know what you're dealing with. An approach that begins to label all new assets from a certain date will make you feel you are starting to get some control over the issue, whilst considering how to address the historical items. Information assets should have owners and they are the ones who should be looking at labelling so it's not all down to a single person or department to achieve it; spread the load as much as possible.

Grouping items with the same classification level will also help to make things clear without a huge administrative overhead. Maybe everything held in a room is confidential and locking the door and labelling it as such will be enough to meet the need. You may need to invest in a stamp for existing paper copies that need to be individually labelled, but obviously items that are printed in the future should be electronically labelled using headers, footers, watermarks etc.

There are software tools available to help you with this task. These can use metadata to reflect classification level and then prevent certain types of documents being used in particular ways according to a defined policy, for example confidential documents should not be emailed outside the organization. In some cases, a home-grown solution using existing facilities within office software etc. may work just as well.

4.1.14 A.5.14 Information transfer

Relevant Toolkit documents

- *Information Transfer Procedure*
- *Information Transfer Agreement*

Having classified and labelled our assets, we also need to make sure that they remain appropriately protected throughout their lives, particularly if they go beyond the organization's boundaries, for example to another location via courier or to a third party via electronic transfer. This is about understanding the ways in which your information assets are used and ensuring that procedures are in place to keep them secure. Again, starting with the highest-level assets is usually a good idea. This is an area in which there have been many notorious public breaches to do with government departments with sensitive information such as names, addresses and tax information going missing, sometimes in unencrypted form.

Think about whether your information is saved onto other media, printed, transmitted, emailed, or otherwise processed in a way that makes a procedure necessary.

Removable media is a common subject of attention from the auditor so try to ensure that everyone is aware of the policy and that items are not left lying around the office.

4.1.15 A.5.15 Access control

Relevant Toolkit documents

- *Access Control Policy*

Most organizations will have access control in place so addressing these control requirements is mainly a case of tightening things up rather than starting from scratch. An access management audit is often a good starting point to identify users who have access they shouldn't and to highlight areas where existing procedures aren't working. A clear policy and revised procedures that are strictly followed will address most requirements, supplemented by a regular repeat of the access management audit/review.

Don't forget to address the access control issues associated with the use of cloud services, including the implementation of multi-factor authentication where appropriate and available.

4.1.16 A.5.16 Identity management

Relevant Toolkit documents

- *This control is addressed by documents in other folders - See Toolkit Index*

This control is about being able to uniquely identify users, including proving who they are when a user account is created, avoiding the sharing of user accounts and handling situations where a computer process (or “non-human entity”) needs an account of its own. This is separate to the assignment of access rights to a user, which is covered in a later control.

4.1.17 A.5.17 Authentication information

Relevant Toolkit documents

- *Passwords Awareness Poster*

Although there are several widespread used methods of authenticating a user (that is, proving who they are) the most common one for now remains the password. This control addresses the way in which passwords (and other forms such as PINs) are created, stored, used, changed and disposed of, including the use of SSO (single sign on). You will need to establish rules for the creation of passwords (for example length and complexity) and look at the systems used to check that your rules are supported. The correct way to communicate initial passwords to new users will also need to be addressed procedurally.

The use of a password management system may also be worth considering, along with user education about what a strong password looks like.

4.1.18 A.5.18 Access rights

Relevant Toolkit documents

- *User Access Management Process*

Once a user has been created, the process of assigning access rights needs to be addressed according to documented procedures which ensure that the user gets the correct level of access and no more. Common ways of achieving this are by using roles and by cloning an existing user who does the same job. Your procedures should incorporate appropriate authorisation for the assignment of access rights and address the full lifecycle of granting, changing and removal of these rights, particularly where an employee’s departure is not cordial.

4.1.19 A.5.19 Information security in supplier relationships

Relevant Toolkit documents

- *Information Security Policy for Supplier Relationships*

Suppliers can be a key route in for attackers, so it's important to pay attention to how your organization interacts with them and to ensure they have a decent set of controls in place too. This involves identifying those existing suppliers who have the potential to affect your security and to carry out due diligence on those you have yet to contract with. This control covers cloud suppliers and supplements the specific control on that topic – *A.5.23 Information security for use of cloud services*.

You will need a policy to define your approach to supplier security, together with a risk assessment process which helps to focus on those that justify more time being spent on them. Further actions could include second-party audits, examination of supplier certifications (such as ISO/IEC 27001) and review of supplier access to your organization's assets, including your network.

A chain is only as strong as its weakest link and if you share sensitive information with your suppliers then the standard requires you to take adequate measures to ensure that they protect it as well as you do. This may be achieved via a combination of second party audits (see *Supplier Information Security Evaluation Process*), contractual agreements and strong access control over remote links to and from suppliers.

Much of this will depend on how important a customer you are to your suppliers; small organizations who are customers of large suppliers may have less influence over contractual terms and the security controls in place. This should be considered when deciding which supplier to choose in any situation.

Supply chain security is increasing in importance, as many high-profile attacks have succeeded via this route, so due diligence is required to try to reduce the risk.

4.1.20 A.5.20 Addressing information security within supplier agreements

Relevant Toolkit documents

- *Supplier Information Security Agreement*

It's vital that written agreements with suppliers contain clauses and schedules that address information security specifically. These should include the controls mandated, use of sub-suppliers and interactions in the event of a breach, particularly for PII where legal obligations may apply. You'll need to review existing contracts to assess whether they offer sufficient protection and potentially renegotiate or vary contracts that don't. You may also need to design a new standard contract with your legal department that includes the required areas.

4.1.21 A.5.21 Managing information security in the ICT supply chain

Relevant Toolkit documents

- *Supplier Due Diligence Assessment Procedure*
- *Supplier Due Diligence Assessment*

This control focuses on the supply chain for ICT products and services specifically, including hardware, software and cloud services. This will become increasingly relevant as the use of Internet of things (IoT) devices increases, especially before good security standards in this area have been internationally recognised or mandated by governments.

To implement this control you will need to focus on the suppliers of ICT infrastructure and ask relevant questions about the security attributes of their products and services, including security within sub-contractors, testing carried out, traceability, certifications held and recommended configurations.

As an example, investigations into the supply chain for a cloud service provider could involve looking at the physical hardware providers used, the data centre environment, virtual software providers and telecommunication links employed.

4.1.22 A.5.22 Monitoring, review and change management of supplier services

Relevant Toolkit documents

- *Supplier Information Security Evaluation Process*
- *Supplier Evaluation Covering Letter*
- *Supplier Evaluation Questionnaire*

Once in place, supplier relationships and the services they provide need to be monitored and managed carefully to ensure that the contracted services are delivered effectively. This may involve the production of service reports against a service level agreement, together with service reviews at which issues and changes are discussed. Each supplier should have a named relationship manager within your organization who keeps in regular contact with the supplier and manages performance and change.

4.1.23 A.5.23 Information security for use of cloud services

Relevant Toolkit documents

- *Cloud Services Policy*
- *Cloud Services Process*
- *Cloud Service Specifications*
- *Cloud Services Questionnaire*

New in the 2022 version, this is the first time a control has specifically addressed the use of cloud services within the ISO/IEC 27001 standard. This control takes a lifecycle approach to cloud services, requiring that all stages are managed, including acquisition, use, management and exit from them. Key to achieving this is a clear understanding of the respective roles and responsibilities undertaken by the CSP (cloud service provider) and the cloud customer in areas such as access control, anti-malware, backups and incident management.

4.1.24 A.5.24 Information security incident management planning and preparation

Relevant Toolkit documents

- *Incident Response Plan Ransomware*
- *Incident Response Plan Denial of Service*
- *Incident Response Plan Data Breach*

Information security incident management is becoming increasingly important as organizations realize that preventing all breaches is virtually impossible. If you already have an ICT incident management process (usually provided via an ICT service or help desk) it may make sense to enhance this to cover information security incidents rather than have a separate process running side by side.

For major breaches with potentially significant consequences for the reputation of the organization the best approach is to be prepared and well drilled in your response. This situation has a lot in common with a business continuity event and should be managed in much the same way, with senior management involvement from the outset. Template response plans for three of the more common scenarios – ransomware, denial of service and data breach – are included in the Toolkit, together with a procedure covering the specifics of notification under the GDPR.

4.1.25 A.5.25 Assessment and decision on information security events

Relevant Toolkit documents

- *Information Security Event Assessment Procedure*

It's easy to ignore the event management requirements of the standard and focus on incidents, but to do so risks falling foul of the auditor. In your information security environment, you will most likely be bombarded with things that happen daily that may or may not be incidents and being able to work out the difference quickly will be key. Ensure you have a clear approach to assessing events to decide whether you've been breached as crying wolf too often will get you a bad reputation. Use of a software tool (such as Microsoft

Sentinel in an Office365/Azure environment) will help to automate the process and reduce the load.

4.1.26 A.5.26 Response to information security incidents

Relevant Toolkit documents

- *Information Security Incident Response Procedure*

Having planned for them, you will need to make sure that your organization's response to information security incidents follows the defined plans and procedures. The auditor will want to see clear evidence of this in the form of incident logs, evidence collected, communications made and liaison with third parties, such as authorities and specialist groups.

4.1.27 A.5.27 Learning from information security incidents

Relevant Toolkit documents

- *Incident Lessons Learned Report*

We would recommend that some analysis is done after a significant incident has been experienced (such as a breach of personal data) to identify the lessons learned from the way it was discovered and managed, and a template report is provided in the Toolkit for this purpose, together with an example of a completed report.

4.1.28 A.5.28 Collection of evidence

Relevant Toolkit documents

- *This control is addressed by documents in other folders - See Toolkit Index*

One of the main differences for information security incidents (compared to normal technical incidents) may be the need to preserve evidence for later investigation and possibly legal action or prosecution, particularly where there may have been fraud carried out by an insider. The basic rules for this may be defined for your internal staff to follow, but it is likely you will need the help of a specialist provider to achieve this effectively. Part of your planning should be to select such a provider in advance, check them out, and have their contact details to hand.

4.1.29 A.5.29 Information security during disruption

Relevant Toolkit documents

- *This control is addressed by documents in other folders - See Toolkit Index*

The key point to make with regard to business continuity in the context of the ISO/IEC 27001 standard is that the requirements in this control refer to the information security aspects of your BC plan, if you have one; there is no explicit requirement to have a BC plan as such (this is covered by a separate international standard, ISO 22301). The requirements are to ensure that, if a disruptive event occurs, your information remains protected as far as possible and that any actions you take as part of recovery do not circumvent the controls you have in place (or other compensating controls should be used).

Having said this, an auditor might reasonably expect you to have at least a basic business continuity plan so it's definitely a good idea to put some thought into this, if you haven't already.

4.1.30 A.5.30 ICT readiness for business continuity

Relevant Toolkit documents

- *Business Impact Analysis Process*
- *Business Impact Analysis Report*
- *ICT Continuity Incident Response Procedure*
- *ICT Continuity Plan*
- *ICT Continuity Exercising and Testing Schedule*
- *ICT Continuity Test Plan*
- *ICT Continuity Test Report*
- *Business Impact Analysis Tool*

New with the 2022 version of ISO/IEC 27001, this control introduces the requirement to have a plan to recover your ICT systems in the event of a disruption. Still commonly known in ICT circles as "disaster recovery", this will involve conducting a business impact assessment (BIA) to establish recovery priorities and timescales as input to your planning. Although this control focusses on ICT recovery, you may decide to take the opportunity to widen this exercise into a more general business continuity one, covering non-ICT disruptions such as a pandemic or supply shortage too.

4.1.31 A.5.31 Legal, statutory, regulatory and contractual requirements

Relevant Toolkit documents

- *Legal and Regulatory Requirements Procedure*

- *Legal, Regulatory and Contractual Requirements*

It is important that your organization has a full understanding of its information security responsibilities from a legal and statutory viewpoint, such as employment law (for example monitoring employee usage of system), and contractually, such as its commitments to customers or suppliers. Depending on your industry there may also be other requirements specified by a regulator, for example in the finance, gambling or health industries.

Legislation and contract law vary significantly by country so you will need to either take appropriate legal advice or conduct adequate research to establish which requirements apply, and your responsibilities under them. You will also need to keep this understanding up to date as things change.

4.1.32 A.5.32 Intellectual property rights

Relevant Toolkit documents

- *IP and Copyright Compliance Policy*

This control is not only about protecting your organization's IP (intellectual property) but also about ensuring that your employees don't infringe other parties' rights in their use of external assets such as documents, software and images. You will need to identify your IP and then consider how best to protect it. Correct use of external IP is usually covered by the provision of adequate awareness training, together with appropriate procedures.

4.1.33 A.5.33 Protection of records

Relevant Toolkit documents

- *Records Retention and Protection Policy*

The protection of records, in whichever format they exist, is important to ensure that legal obligations are met, and the business continues to function as needed. This control requires that records are stored appropriately and that access to them is controlled so that they are not destroyed, altered or seen by unauthorised people. A clear definition of the retention rules for different types of records is also essential, supported by technical or procedural methods to delete or destroy them when their time is up.

4.1.34 A.5.34 Privacy and protection of PII

Relevant Toolkit documents

- *Personal Data Breach Notification Procedure*

- *Privacy and Personal Data Protection Policy*
- *Personal Data Breach Notification Form*
- *Breach Notification Letter to Data Subjects*

With the increasing number of countries which have enacted privacy legislation, legal obligations in this area have potentially widened in recent years. You will need to have a clear picture of the legislation that applies (for example depending on the markets you serve and where you are based) and the requirements of that legislation, such as privacy notices, record keeping and the rights of the PII (personally identifiable information) principal.

4.1.35 A.5.35 Independent review of information security

Relevant Toolkit documents

- *Information Systems Audit Plan*

This control is about looking at the organization's approach to information security overall (for example the use of ISO/IEC 27001 as a framework) is appropriate and is delivering results and meeting objectives. This is an opportunity to identify improvements and get the benefit of an independent viewpoint, which may see items that managers are too close to spot. The requirements of this control may be substantially met by the internal and external (certification) audit cycle, but additional reviews may also be considered.

4.1.36 A.5.36 Compliance with policies, rules and standards for information security

Relevant Toolkit documents

- *Information Security Summary Card*

Information security reviews should be undertaken on a regular basis; some of these can be done as part of the internal audit and management review processes but technical compliance reviews of key systems may need to be performed as separate, discrete exercises which must be documented. These could be carried out by a central resource, an external third party, or responsibility for them could be delegated to managers (in which case training may be required). The point is to check that the policies, procedures and controls that are in place are working and are being followed.

4.1.37 A.5.37 Documented operating procedures

Relevant Toolkit documents

- *Operating Procedure*

Operating procedures are vital to ensure that activities are carried out in the same way each time and that they can be performed by more than one person. Often ICT teams lack documented procedures which means they rely upon the local knowledge and memory of support staff, placing the services at risk. Documentation is also an opportunity to define the correct way to perform a task, so that risks are minimised. This involves creating a list of procedures (documented and undocumented) and working through them methodically, ensuring that good version control is used. Once created, they also need to be made available to the people who will use them, and their correct use recorded and reviewed.

4.2 A.6 People controls

You will need to work with your Human Resources department to implement most of the controls in this section. In most cases this will involve reviewing the existing procedures and documents to see if they cover information security sufficiently. Be careful that you will need to check that any changes you make comply with the laws of the country in which they will be implemented as employment law can be a bit of a minefield.

The human factor is often cited as being the single most important issue in promoting effective information security; this section is intended to ensure that you recruit the right people, they know their responsibilities and action can be taken if they don't fulfil them adequately.

4.2.1 A.6.1 Screening

Relevant Toolkit documents

- *Employee Screening Procedure*
- *Employee Screening Checklist*

This control requires that background verification checks are carried out on candidates for employment with your organization, and for temporary and supplier staff with access to your systems. The emphasis is on the checks being proportionate to the risk, which is largely determined by the classification of the information they will have access to. Basic level checks will typically include verification that a CV or resume is accurate, references, qualifications and nationality or right to work. For more sensitive posts, additional checks could include criminal record searches, financial reviews and possibly medical tests. Make sure that all legal obligations are complied with in the country involved, as these can vary significantly.

4.2.2 A.6.2 Terms and conditions of employment

Relevant Toolkit documents

- *Guidelines for inclusion in Employment Contracts*

Information security needs to be considered when employment contracts are prepared, covering the employee's responsibilities for areas such as confidentiality, ownership of IP, and compliance with the organization's policies, including acceptable use. Again, if particularly sensitive information is involved in the role, additional contractual restrictions may be warranted. It should also be emphasised that the employee's information security responsibilities in areas such as confidentiality continue after their employment ends.

4.2.3 A.6.3 Information security awareness, education and training

Relevant Toolkit documents

- *Email Awareness Poster*

The management system part of ISO/IEC 27001 contains brief requirements for awareness in clause 7.3 and training is also part of clause *7.2 Competence*. So to some extent this control simply reaffirms that commitment rather then introducing anything new. The expectation is that there will be an information security awareness programme in place, covering new starters and regular updates for existing employees. These could be delivered in various ways including face to face briefings, virtual meetings and online course programmes or a combination of these.

More detailed training on information security matters could be led by the various qualification schemes available at different levels (such as CISSP or CISM), together with the need to maintain knowledge with continual professional education (CPE).

4.2.4 A.6.4 Disciplinary process

Relevant Toolkit documents

- *Employee Disciplinary Process*

There's little point in requiring employees to follow the organization's information security policies if there are no consequences of not doing so. This control requires there to be a disciplinary process in place; although this is described with an information security focus, it is likely that existing disciplinary processes may be applicable, just as they would be for other forms of misconduct within the organization, such as bullying, negligence or dishonesty.

4.2.5 A.6.5 Responsibilities after termination or change of employment

Relevant Toolkit documents

- *Employee Termination and Change of Employment Checklist*
- *Leavers Letter*

Related to control *A.6.2 Terms and conditions of employment*, there is a need to ensure that the continuing information security obligations defined in the contract of employment are emphasised to leavers and are enforced if they are found to have been breached. This also applies in cases where the employee has changed roles within the same organization.

4.2.6 A.6.6 Confidentiality or non-disclosure agreements

Relevant Toolkit documents

- *Schedule of Confidentiality Agreements*
- *Non-Disclosure Agreement*

Non-disclosure agreements (NDAs) are commonly used between organizations when discussions are being held involving most forms of information; although they can be one-way, they are often mutual and commit both parties to protect the information that is shared. The expectation is that they will be used, and their existence recorded and tracked.

Confidentiality agreements are similar documents which are often used to commit employees to an undertaking to protect the information they have access to. For example these may be used within a cloud service provider (CSP) to meet legal obligations and reassure cloud customers that their data is protected.

4.2.7 A.6.7 Remote working

Relevant Toolkit documents

- *Remote Working Policy*

Formerly referred to within the ISO/IEC 27001 standard as “teleworking”, remote working has become much more widespread as a result of the COVID-19 Pandemic, during which it was mandated in many countries. The control requires that the security implications of having employees based at home are assessed for individual cases, and appropriate mitigations put in place, such as lockable furniture, equipment siting and the use of VPNs (virtual private networks).

4.2.8 A.6.8 Information security event reporting

Relevant Toolkit documents

- *ISMS-DOC-A08-6-1 Information Security Event Reporting Procedure*

Part of the required awareness training is to encourage employees and other interested parties to tell someone if they become aware of security risks or breaches. This control requires there to be an easy way to do this, whether this is to their line manager, help desk or other defined point of contact. Whichever mechanism is used, it must be ensured that the information is passed to someone who has the authority and responsibility to follow it up.

4.3 A.7 Physical controls

This set of controls will involve more work the larger and more numerous the offices and other facilities you have. You may need to spend some money to upgrade the security precautions in place and ensure that the different types of area (for example delivery and loading areas) are well-defined. However, a key part of this will be to ensure that all employees have an awareness of their responsibilities for physical security, for example challenging unescorted strangers, closing windows.

4.3.1 A.7.1 Physical security perimeters

Relevant Toolkit documents

- *Physical Security Policy*

You will need to ensure that the outside of your premises or facilities is appropriately protected, probably using the standard mix of locks to doors and windows, fences and other forms of external barriers. The appropriate degree of protection will depend on various risk factors, including the location of the site (for example, in a high-crime area), the value of the contents to others (for example a jewellery workshop) and the nature of the business (such as in a politically sensitive industry).

4.3.2 A.7.2 Physical entry

Relevant Toolkit documents

- *Physical Security Design Standards*

The points of entry of your location must also be appropriately protected using a suitable method such as swipe-card access, turnstiles or old-fashioned keys. A process for visitors

should include their registration, escort and the wearing of visible identification. Attention needs to be paid to how deliveries are received and shipments loaded, if that applies to your location.

4.3.3 A.7.3 Securing offices, rooms and facilities

Relevant Toolkit documents

- *Data Centre Access Procedure*

Once inside the building, there may be a need to secure specific rooms separately, again via access controls, and to ensure that what goes on there is no visible or obvious to unauthorised people.

4.3.4 A.7.4 Physical security monitoring

Relevant Toolkit documents

- *CCTV Policy*

This control covers the use of monitoring systems such as security guards, CCTV (closed circuit television) and intruder alarms to detect when an unauthorised person has entered a building. For CCTV, the requirements of privacy legislation must be considered, along with the correct siting of cameras so that security objectives are achieved without capturing public activities unnecessarily.

4.3.5 A.7.5 Protecting against physical and environmental threats

Relevant Toolkit documents

- *This control is addressed by documents in other folders - See Toolkit Index*

Where justified by a risk assessment, it may be necessary to implement protection against events such as fire, flood and earthquakes. Again, the emphasis is on implementing controls that are justified by the threat and this is likely to be highly location-specific, from the country or area involved (for example forest fires in California) to the local geographical features such as nearness to rivers.

4.3.6 A.7.6 Working in secure areas

Relevant Toolkit documents

- *Procedure for Working in Secure Areas*

For those parts of a building or facility that are justified to be designated secure areas, rules must be established, communicated and enforced to address the specific levels of risk associated with them. This could involve not being able to take mobile phones inside, being escorted at all times or banning food and drink within them. This is common in locations such as datacentres and laboratories.

4.3.7 A.7.7 Clear desk and clear screen

Relevant Toolkit documents

- *Clear Desk and Clear Screen Policy*

This control requires that screens are locked when not in use (that is they display a screen saver) and desks are kept tidy with sensitive information locked away.

In many organizations the adoption of a clear-desk policy can be challenging, and the cost of additional secure storage can add up. Remember however that the policy is likely to only apply to items of a certain security classification so publicly available information may still be sited on desks.

4.3.8 A.7.8 Equipment siting and protection

Relevant Toolkit documents

- *This control is addressed by documents in other folders - See Toolkit Index*

If you have equipment that is outside of a typical office environment (perhaps a public kiosk or ICT equipment in remote locations) it may be that you will need to consider how best to protect the kit and the information it processes from a number of threats. These threats could include environmental damage perhaps due to excessive heat, light or water and unauthorised access or viewing by other people.

4.3.9 A.7.9 Security of assets off-premises

Relevant Toolkit documents

- *Procedure for Taking Assets Offsite*

When assets are taken away from the protection of office buildings they may become more vulnerable to attack. This is particularly true of assets that are permanently located off-site such as automated teller machines (ATMs). Closely related to control *A.8.1 User endpoint devices*, this control considers the additional precautions that may need to be taken such as tamper-proofing and physical monitoring with cameras or alarms.

4.3.10 A.7.10 Storage media

Relevant Toolkit documents

- *Procedure for the Management of Removable Media*
- *Physical Media Transfer Procedure*

To comply with this control you will need to firstly identify the removable storage media that are in use within your organization. These could be devices such as computer hard disks, USB memory devices, digital storage cards and perhaps even backup tapes or cartridges. For each use of such devices it is necessary to define the lifecycle of the device, from how it is initialised and used through to storage and final destruction. The controls required will depend strongly on the classification of the information stored on the device, and encryption is a very useful tool in many of these cases.

4.3.11 A.7.11 Supporting utilities

Relevant Toolkit documents

- *This control is addressed by documents in other folders - See Toolkit Index*

Particularly if you have a datacentre or server room with physical computers in it (rather than your processing being exclusively cloud-based), you will need to review how utilities such as electricity, water, gas, air conditioning are provided and the effect on your operations if these fail. Where appropriate, backup facilities may be prepared such as a UPS (uninterruptible power supply) and generator to cover power loss.

4.3.12 A.7.12 Cabling security

Relevant Toolkit documents

- *This control is addressed by documents in other folders - See Toolkit Index*

Cables that are easily accessible by unauthorised people are a potential route into your organization's systems and so must be protected. This may involve them being underground or, when above ground, being protected by conduit casings to prevent access.

4.3.13 A.7.13 Equipment maintenance

Relevant Toolkit documents

- *Equipment Maintenance Schedule*

Unmaintained equipment is subject to failure so those items that require scheduled attention must be identified and a process put in place to ensure they receive it. Typically, such items may include fire and intruder alarms, UPS equipment, air conditioning and smoke detectors. An auditor would expect to be able to view an up-to-date maintenance history for all those items of equipment that are relevant.

4.3.14 A.7.14 Secure disposal or re-use of equipment

Relevant Toolkit documents

- *Procedure for the Disposal of Media*

When storage media reaches the end of its useful life it must be disposed of in a way that protects any information that could still be on it. This may involve the use of a third party service to shred hard drives in a secure way with the provision of a certificate afterwards. Care must be taken if a device with storage media is to be reused, to ensure that any sensitive data has been securely overwritten and is unrecoverable.

4.4 A.8 Technological controls

If your organization develops its own software, it is likely that all these controls will apply. If it doesn't then the number of applicable controls will depend upon whether software development is outsourced or purely commercial off the shelf (COTS) software is used. Remember that even COTS software still needs to be tested in a secure way so test-related controls will still be needed.

4.4.1 A.8.1 User endpoint devices

Relevant Toolkit documents

- *Mobile Device Policy*
- *BYOD Policy*

Previously referred to within the standard as mobile devices, user endpoint devices such as laptops, tablets and smartphones are obviously an area of increasing importance as they

become more powerful and widespread so it's worth spending some time to ensure your policy on this subject is as appropriate as possible. Much of the management of such devices will be achieved by the use of configuration tools and this control is closely related to control *A.8.9 Configuration management*.

If you allow users to use personal devices to access corporate data, then you will need to put some thought into how this will work securely. We provide a *BYOD Policy* (bring your own device) which is intended as a starting point for this thought process.

4.4.2 A.8.2 Privileged access rights

Relevant Toolkit documents

- *This control is addressed by documents in other folders - See Toolkit Index*

You will need to keep privileged access rights (such as account administration) and the user accounts that hold them under close control as they are a clear target for hackers. This will involve a process of understanding who holds them, validated such access and reviewing it on a regular basis. The use of MFA (multifactor authentication) for these accounts is a must and will be expected by the auditor.

4.4.3 A.8.3 Information access restriction

Relevant Toolkit documents

- *Dynamic Access Control Policy*

Although it is closely related to control *A.5.15 Access control*, this control specifically refers to the use of dynamic access management techniques which are associated with information even when it leaves the confines of the organization. This allows the organization to control what is done with the information (such as printing or copying) and to change levels of access even after the information has been distributed.

4.4.4 A.8.4 Access to source code

Relevant Toolkit documents

- *This control is addressed by documents in other folders - See Toolkit Index*

If your organization undertakes bespoke software development, you will need to be able to show that your source code is well protected and that access to it is managed carefully. This is likely to be achieved via the use of a source code repository which is either on premise or in the cloud (or in some cases both). Make sure you consider other items associated with

the code, such as functional and technical specifications, development tools and test platforms.

4.4.5 A.8.5 Secure authentication

Relevant Toolkit documents

- *This control is addressed by documents in other folders - See Toolkit Index*

Related to control *A.5.17 Authentication information*, this control is about the technology and process used for someone (or an entity such as a process) to prove who they are via the provision of authentication information such as a password. For COTS (commercial off the shelf) and SaaS (software as a service) applications, you will need to look carefully at the facilities provided by the software vendor in this area, to ensure they meet your policy. If you're in the business of providing such a system, this control provides a basic specification of what you need to provide to customer users to be secure.

4.4.6 A.8.6 Capacity management

Relevant Toolkit documents

- *Capacity Plan*

The main aspect to note with regard to this control is that it adopts a wider perspective than purely ICT capacity, encompassing people, offices and other facilities too. The principles are the same as for traditional ICT capacity planning, namely understanding the resources available and their current use, then getting the most out them (for example by tuning them) and planning adjustments for future estimated usage.

A documented capacity plan would be required for high priority systems.

4.4.7 A.8.7 Protection against malware

Relevant Toolkit documents

- *Anti-Malware Policy*

It is likely that malware controls are already in place as they are standard ICT procedures, and these may simply need revisiting to ensure they are comprehensive and accurate (although beware of increasingly sophisticated ransomware attacks which may also encrypt your backups). The control places emphasis on user awareness (which is also addressed both within the management system and in control *A.6.3 Information security awareness, education and training*) as a supplement to anti-malware software and links with other controls, such as those for web filtering and vulnerability management.

4.4.8 A.8.8 Management of technical vulnerabilities

Relevant Toolkit documents

- *Technical Vulnerability Management Policy*
- *Technical Vulnerability Assessment Procedure*

Technical vulnerability management will in most cases mean patching and this may be enough to meet the control requirement, but it is always worth looking at running a vulnerability scanner (both within and outside of your network) on a regular basis to check your exposure. Consider also your approach to vulnerabilities that you find and those that are reported to you, if you write your own software.

There is no strict requirement for penetration testing to be carried out regularly, but this is always an option if budgets allow. ISO/IEC 27002:2022 goes into some detail on this control, which is worth a read if you have the guidance standard available.

4.4.9 A.8.9 Configuration management

Relevant Toolkit documents

- *Configuration Management Policy*
- *Configuration Management Process*
- *Configuration Standard Template*

Many breaches occur due to the incorrect configuration of hardware or software rather than the exploitation of vulnerabilities, so this control (new in the 2022 control set) is well worth your time. Look at each of the components of your infrastructure (including user endpoints) and determine how they should be configured for best security. Implementation of these standard configurations may be achieved by the use of software tools (often cloud-based) which allow a profile to be defined and applied remotely. In many environments (including popular cloud ones) checking tools can find incorrect configurations and make automated adjustments to close off vulnerabilities, so reducing the human effort required.

4.4.10 A.8.10 Information deletion

Relevant Toolkit documents

- *Information Deletion Policy*

In essence, this control is about housekeeping of your PII (personally identifiable information) so that it is not kept beyond the time it is useful and legally acceptable. This may involve the scheduled deletion of data in situ but also the secure disposal of removable

storage containing data for example by disk shredding. You will need to be able to show to an auditor that the record retention timeframes stated in your *Records Retention and Protection Policy* are actually enacted in reality so that data is deleted on time.

4.4.11 A.8.11 Data masking

Relevant Toolkit documents

- *Data Masking Policy*
- *Data Masking Process*

This control may apply if your organization has a need to provide PII (perhaps to a third party) in a form where the identities of the individuals concerned has been hidden. The main techniques involved are anonymization and pseudonymization, but others such as encryption may also be relevant. This is quite a specialist area and the techniques must be used effectively to avoid the possibility of reidentification of the PII principals.

4.4.12 A.8.12 Data leakage prevention

Relevant Toolkit documents

- *Data Leakage Prevention Policy*

If you have sensitive data that is relatively easily identifiable, perhaps from its format such as credit card numbers, then data leakage prevention tools may be able to help in protecting that data from being stolen. The implementation of this control is likely to revolve around the installation and configuration of software with this purpose and its applicability will depend on the nature and value of the information at risk.

4.4.13 A.8.13 Information backup

Relevant Toolkit documents

- *Backup Policy*

The starting point for this control is to create a topic-specific policy which sets out the overall approach to information backup. This is likely to reflect measures that are already in place, as backup is a fundamental building block of common ICT management practice. There is an opportunity to spot data that is currently not being backed up adequately and perhaps to introduce better testing of backups.

A frequent area of concern is the extent to which cloud service providers back up customer data, and how that information is retrieved in the event of an issue.

4.4.14 A.8.14 Redundancy of information processing facilities

Relevant Toolkit documents

- *Availability Management Policy*

In essence, redundancy means having at least two of something, whether it's a server or a datacentre, and in the past this has been expensive to achieve. However, with the growth of cloud computing, most providers allow for data to be spread across multiple availability zones with very little effort. Your efforts in this area should be informed by the conclusions from your business impact analysis (see control *A.5.30 ICT readiness for business continuity*) and the priorities that establishes.

4.4.15 A.8.15 Logging

Relevant Toolkit documents

- *Logging and Monitoring Policy*

Logs are incredibly useful in the event of a breach, but only if they are available and their integrity has not been compromised. You will need to look at where logs are generated, and how they can be configured to record the information you are interested in. The management of event logs is made much easier using software tools and there are many available, including some open-source ones. An effective method of protecting the logs so that a hacker can't get at them must be in place, and many software tools address this issue. The key is to be able to detect any exception situations within the mass of log data (which is almost impossible manually) and react to them appropriately. Many tools now make use of artificial intelligence and machine learning to help with this.

4.4.16 A.8.16 Monitoring activities

Relevant Toolkit documents

- *Monitoring Policy*

A new control with the 2022 version of ISO/IEC 27001, if applicable you will be required to make use of monitoring software that is capable of detecting unusual or suspicious behaviour within your infrastructure and if possible, take actions to block it. Such intrusion detection systems have been available for some time and are increasing in their sophistication. An auditor may want to see alerts generated by the monitoring system and trace through the actions taken as a result of them.

4.4.17 A.8.17 Clock synchronization

Relevant Toolkit documents

- *This control is addressed by documents in other folders - See Toolkit Index*

In the event of a breach the synchronization of clocks to a standard time source is absolutely vital if the trail of the attacker is to be traced accurately. When configuring systems and associated devices this can seem like an afterthought, but a strict policy must be enforced to ensure that an appropriate time source is used in all cases.

4.4.18 A.8.18 Use of privileged utility programs

Relevant Toolkit documents

- *Privileged Utility Program Register*

If your technical environment includes software utilities that allow the user to bypass logging on to an application and interact directly with items such as a database then you will need to control access to them. The first step will be to identify such programs, document them, for example in a register, and then to understand their capabilities and therefore level of risk. The ways in which access can be restricted will vary, from preventing their installation to keeping logon details secure.

4.4.19 A.8.19 Installation of software on operational systems

Relevant Toolkit documents

- *Software Policy*

Application software requires upgrading periodically perhaps to keep it on a supported release, or to obtain additional functionality, or to apply program and security fixes. The way in which upgrades should be applied must be defined both at the overview policy level and specifically as detailed procedures for each relevant system. These procedures should cover the testing to be carried out beforehand, the technical details of how the upgrade is to be installed and the post-installation testing. The upgrade should be carried out under the control of the change management function, with appropriate authorisations and planning for actions such as backout of the change.

4.4.20 A.8.20 Networks security

Relevant Toolkit documents

- *Network Security Policy*

A comprehensive network diagram is the best starting point in satisfying the control requirements in this section. This needs to cover not only internal networks but also links with external third parties and an appreciation of the data transferred via the networks will help to identify the need for encryption and transfer agreements to be in place.

Use of a reliable network management tool will help to monitor the network for availability and allow remote configuration where required. Standard configurations of network devices should be used as described in control *A.8.9 Configuration management*.

4.4.21 A.8.21 Security of network services

Relevant Toolkit documents

- *Network Services Agreement*

This control refers to network services provided by third parties, including managed networks, and point services such as firewalls and intrusion detection systems. Tender documents for new systems will need to show consideration of information security issues, including how data transmitted over the Internet will be protected, for example using strong encryption. Other requirements and controls in the area of supplier management are also relevant here, with regular performance reviews and issue and change management.

4.4.22 A.8.22 Segregation of networks

Relevant Toolkit documents

- *This control is addressed by documents in other folders - See Toolkit Index*

Once networks reach a certain size it may make sense to split them into sub-nets based on attributes such as who uses them and the classification of information they typically carry. If your organization is small this may not apply as there isn't sufficient scope for segregation. There are various ways to achieve the separation of network traffic, for example using VLANs on routers and switches, or more explicitly using firewalls between network segments.

4.4.23 A.8.23 Web filtering

Relevant Toolkit documents

- *Web Filtering Policy*

This is another new control that has been introduced in the latest version of the ISO/IEC 27001 standard, although it refers to something that has been a staple control in most ICT environments for many years. User access to websites should be monitored and filtered according to defined rules which block any sites that are not desirable for one or more reasons, such as illegal content or known hosts of malicious content. Often such functionality is provided as part of an anti-malware solution, or it may be achieved using a specialist appliance on the network.

4.4.24 A.8.24 Use of cryptography

Relevant Toolkit documents

- *Cryptographic Policy*

Although the standard only refers to policies for cryptography and key management, you will probably need to ensure that accurate procedures (and ideally automated policies) are developed and used for common cryptography-related tasks such as encrypting the hard disks of laptops. As the use of encryption grows, especially in a cloud environment, it will become harder to manage the variety of keys used and the consequences of losing a key can be severe, so it is important to get this right.

In a cloud environment, make full use of available services such as KMS (Key Management Service) on AWS to simplify the use of encryption and remember that as far as regulators are concerned, breaches of encrypted personal data are in many cases not reportable, as long as the key stays safe.

4.4.25 A.8.25 Secure development life cycle

Relevant Toolkit documents

- *Secure Development Policy*

If your organization develops its own software, then this control will certainly apply. In some ways, this control acts as a directory for some of the other controls within Annex A, as it defines in overview the areas that need to be covered to ensure that the code produced is as secure as possible. These areas include the separation of development, test and production environments, secure coding, access to source code and security testing.

4.4.26 A.8.26 Application security requirements

Relevant Toolkit documents

- *Requirements Specification*

This control entails the involvement of someone with good security knowledge during the requirements definition phase of a project, such as a new software development or an acquisition of a COTS (commercial off the shelf) application. This is an opportunity to consider security from the start, rather than try to retrofit it after the fact. The kinds of requirements areas that should be considered may include the classification of the information involved, privacy considerations, data storage and transmission, logging and input validation, amongst others.

4.4.27 A.8.27 Secure system architecture and engineering principles

Relevant Toolkit documents

- *Principles for Engineering Secure Systems*

When designing information systems, a set of guiding principles should be adopted which encourage the creation of secure environments by default. These principles can vary widely and can be established by the organization itself or taken from an external source such as NIST (National Institute for Science and Technology). At a basic level, principles could be as simple as:

- Defence in depth
- Privacy by design
- Security by default
- Least privilege
- Adopt zero trust

The applicability of this control and the depth into which it requires definition will depend upon the size of your organization's infrastructure and the types of system being implemented.

4.4.28 A.8.28 Secure coding

Relevant Toolkit documents

- *Secure Coding Policy*

An organization that has a software development function will want to write code that introduces as few vulnerabilities as reasonably possible, whilst achieving their objectives. This will require activities to be carried out before, during and after coding and the specifics

will depend on the languages and other technologies adopted. As well as establishing the basic principles used, detailed advice should be sought from relevant vendors for writing secure code using their products. There are a number of independent third parties, such as OWASP, who can also provide advice.

4.4.29 A.8.29 Security testing in development and acceptance

Relevant Toolkit documents

- *Acceptance Testing Checklist*

For organizations in the software development business an auditor would expect to see code changes tightly controlled and effective segregation of duties in place (for example developers cannot promote code directly to production). However, modern development approaches such as continuous integration continuous deployment (CI/CD) in a cloud environment make the automation of security checks essential and the use of available tools such as AWS CodePipeline will probably be expected by the auditor.

The scope of security testing should include security functions, secure coding and secure configurations, and be well defined and structured.

4.4.30 A.8.30 Outsourced development

Relevant Toolkit documents

- *This control is addressed by documents in other folders - See Toolkit Index*

When the development of code is outsourced, there is a need to contractually ensure that the third party provider has in place the same kinds of controls as are set out in Annex A. This will involve some detailed due diligence work in the appointment of the supplier in the first place and regular checks that the promised controls are being successfully implemented. On receipt of the outputs, the organization must perform appropriate testing and security checks to satisfy themselves that the code is of the required quality.

4.4.31 A.8.31 Separation of development, test and production environments

Relevant Toolkit documents

- *Secure Development Environment Guidelines*

Although this control is obviously applicable in a situation where an organization develops their own code, it may also be relevant where packaged applications are used and there is a separate test and production (and perhaps training) environment. The main requirement is

the protection of the production environment from accidental or deliberate corruption. Generally, the various environments will be hosted either on physically separate servers or on discrete virtual domains and the interactions between them will be carefully managed.

4.4.32 A.8.32 Change management

Relevant Toolkit documents

- *Change Management Process*

Change management is a mature discipline that has been the cornerstone of frameworks such as ITIL (Information Technology Infrastructure Library) for many years. The key to implementing a successful process that doesn't introduce unacceptable barriers is to scale the degree of control according to the size of the organization and the criticality of the systems involved. At the lower end, a basic process of recording and discussing change may suffice whilst at the more complex end a formal process supported by effective workflow will be more suitable. The main points will be to ensure that changes are identified in the first place, and then planned, assessed, authorised and communicated.

4.4.33 A.8.33 Test information

Relevant Toolkit documents

- *This control is addressed by documents in other folders - See Toolkit Index*

The selection of test data can be a bit of an art if all possible situations are to be catered for. For this reason, it is common practice to copy data from the production environment to the development or test ones. This control addresses the need to manage this process and protect personally identifiable information, where it is involved, using techniques such as data masking. Levels of access to test environments may need to be the same as those to the production environment, to prevent the exposure of live data by the back door.

4.4.34 A.8.34 Protection of information systems during audit testing

Relevant Toolkit documents

- *This control is addressed by documents in other folders - See Toolkit Index*

Auditing activities can have a detrimental effect on operational systems if they are not timed and managed appropriately. It is important to plan audits in conjunction with management so that it is clearly understood in advance what will be happening, and any potential impact identified. Rather than give the auditor direct access to a system, it may be

advisable to provide access by proxy where an administrator uses the system under guidance from the auditor.

5 Advice for the audit

5.1 Choosing an auditor

If your organization wishes to become certified to the ISO/IEC 27001 standard, it will need to undergo a two-stage process performed by a suitable external auditing body. Before this, you will need to select your auditing body and, in most countries, there are a variety of options. If you are already certified to a different international standard such as ISO 9001 then it usually makes sense to use the same auditing company for ISO/IEC 27001, if they can provide that service. Increasingly, multi-standard audits will become commonplace as the effects of the Annex SL revisions are felt (see section 1.1 The ISO/IEC 27001 standard).

There are many companies that offer certification audits and your choice will obviously depend upon a variety of factors including where in the world you are based. However, there are a few general things you need to be aware of before you sign up with any auditor.

5.1.1 Self-certification

The first is to emphasize the fact that ISO standards are not legal documents; the creation, maintenance and adoption of ISO standards is a voluntary exercise that is co-ordinated by the ISO. Yes, ISO owns the copyright and sells standards for cash both directly and through third parties but be assured that you won't be breaking any laws if you don't quite implement a standard in full. And the same goes for declaring compliance with ISO standards. You have a choice.

You could simply tell everyone you deal with that you meet the requirements of an ISO standard. That's it – no audit fees or uncomfortable visits from men in suits. Just say that you comply. The trouble with this is that if everyone did it, there would be no way of telling the difference between good organizations that really had done it properly and less conscientious ones that just paid the standard lip service. It only takes a few bad apples to spoil it for everybody. The people that matter to you (for example your customers or regulators) may simply not believe you.

5.1.2 Third-party certification

So instead, you may decide to get a third party to test your implementation of a standard and testify that you've done it properly. This is where Registered Certification Bodies (RCBs) come in. An RCB is a company that has the expertise and resources to check that you do indeed meet the requirements of the standard and is willing to tell others that you do. But hold on, how do your customers know that the RCB itself can be trusted to have done a good job of the audit?

What's needed is another organization that is trusted to check the auditors and make sure that they are doing a good job. But how do we know they can be trusted? And so on. What we end up with is a chain of trust like the way that Public Key Infrastructure works. At this point we need to introduce you to a few important definitions:

Certification: This is what happens when you are audited against a standard and you (hopefully) end up with a certificate to put on the wall (as in "we are certified to ISO/IEC 27001").

RCB: A Registered Certification Body is basically an auditing company that has been accredited to carry out certification audits and issue a certificate to say you are compliant with a standard. Some operate in a single country and some in a lot of countries. This is what you, as an organization wanting to become certified, need to choose.

Accreditation: This is what the auditors go through to become an RCB and allow them to carry out certification audits.

OK, now we've got those definitions out of the way we need to talk about who does the accrediting. There are basically two levels, international and national.

IAF: Based in Quebec, Canada, the International Accreditation Forum is the worldwide body that represents the highest level of trust concerning accreditation of RCBs. They have lots of strict rules that national accreditation bodies must agree to, embodied in a charter and a code of conduct. All the national accreditation bodies are members of the IAF.

ANAB: As if there weren't enough acronyms in the world, here we have an acronym within an acronym. ANAB stands for the ANSI-ASQ National Accreditation Board. ANSI is the American National Standards Institute and deals with standards in the USA. ASQ is the American Society for Quality and although based in the USA, has a more international reach than ANSI. Put them together and you get ANAB which is the national accreditation body for the USA and therefore a member of the IAF.

UKAS: The United Kingdom Accreditation Service is the body in the United Kingdom that accredits RCBs. It is effectively the UK representative of the IAF.

JAS-ANZ: The Joint Accreditation Service of Australia and New Zealand is the IAF member for these countries.

DAC: The Dubai Accreditation Department is a government department that accredits RCBs within the United Arab Emirates.

Other IAF Members: There are over 60 other members of the IAF which provide accreditation services for their respective countries and a full list can be found on the IAF website so when you have a moment why not look up the member organization for your country.

The core message here is that whichever RCB you choose to carry out your certification audit, make sure they are accredited by the IAF member for your country. For the UK that means UKAS-accredited, the USA ANAB-accredited and so on. Most auditing companies display the logo of the organization that they are accredited by prominently on their website so it should be easy to tell.

5.1.3 Choosing between accredited RCBs

You've checked that the audit companies you're considering are accredited, but what other factors come into play when making your decision? In our experience asking the following questions will help you to choose:

Which standards do they audit? Check the RCB has the capability to audit the standard you are going for and, if so, how many customers they have for that standard. How long have they been auditing the standard and how many qualified people do they have?

Do they cover the geographical areas you need? There's no point in considering an RCB that can't cover the geographical area(s) you need. This is particularly relevant if you need to have more than one office audited, possibly in different countries. They may cover one country but not another. It's worth checking whether they feel an onsite visit is needed to all the offices in scope before you dismiss them.

How long will it take? Officially there is a formula that should be used when calculating how many days an audit should take. This considers variables such as number of locations and employees and which standards are involved. However, there is some flexibility in how the formula is applied so you may get differing estimates from RCBs on how many days will be needed, which will obviously affect the cost.

How much will it cost? This follows on from the question about time as most RCBs charge by the hour or day, but rates can vary significantly so a longer audit could be cheaper. Consider the ongoing certification fees as well as the cost for the stage one and stage two audits.

What is their availability? Auditors are generally busy people so if you're in a hurry to get your organization certified then their availability will be an important factor. How soon can they do a stage one and when can they come back for the stage two?

What is their reputation? Even amongst accredited RCBs, there are more and less well-known names. Since a lot of the reason for going for certification is to gain credibility with your customers and perhaps regulators, consider which RCB would carry most weight with them.

How good is their administration? A lot of the frustration we see with RCBs is not due to the quality of their auditors but their administration processes. You need an auditing company that will arrange the audits professionally and issue your certificate promptly,

providing additional materials to help you advertise your certification. When you contact them initially, do they return your call and sound knowledgeable?

Do they use contract auditors? Many RCBs use auditors that are not directly employed by them, which is not necessarily a problem, but it would be useful to understand how much continuity you will have with the individuals that carry out your audits. Try to avoid having to describe what your company does to a new auditor every visit as this soaks up time that you are paying for.

Do they have experience of your industry? Some RCBs and auditors specialize in certain industries and build up a strong knowledge of the issues relevant to their customers. This can be helpful during the audit as basic industry concepts and terms will be understood and time will be saved. Check whether they have audited similar organizations in your industry.

Making a good choice based on the above factors can't guarantee that the certification process will run smoothly, but by having a good understanding of the accreditation regime and by asking the right questions early on you will have given yourself the best chance possible to have a long and happy audit relationship.

Having agreed a price, your chosen external auditor will contact you to arrange the Stage One review. This is essentially a documentation review and a "getting to know you" discussion where the exact scope of potential certification is decided. Based on the Stage One, the external auditor will make a recommendation about your readiness for the Stage Two – the certification audit itself. It used to be common for there to be at least a three-month gap between the Stage One and the Stage Two visits, but this is less often the case nowadays and the two can be quite close together if desired.

5.2 Are we ready for the audit?

Deciding when to ask the external auditor in for the Stage One visit is a matter of judgement on your part. If you invite them in too early, they will simply tell you you're not ready and this can have a detrimental effect on team morale (and possibly cost you more money for further visits). If you leave it longer the danger is that you're extending the timescale to certification unnecessarily. We suggest you use a combination of the *ISO/IEC 27001 Gap Assessment Tool* and the *Certification Readiness Checklist* within the Toolkit as a guide to your readiness, but don't expect to be 100% compliant before going for Stage One. A more appropriate figure is probably 90% or so but it does depend on which areas are not yet complete.

Before arranging the Stage One you should have completed the following:

- Information security policy
- Risk assessment and treatment plan
- Implemented most (but not necessarily all) of your information security controls
- Conducted user awareness training
- Internal audits of all areas of the standard

- At least one management review (ideally more)

Not having any of the above available would probably mean that the Stage One visit is inconclusive in terms of judging your readiness for the Stage Two i.e. the auditor would tell you just weren't ready yet.

5.3 Preparing for audit day

Once you feel you're ready to be visited by the auditor for either the Stage One or Stage Two, there are sensible preparations to take to make the best impression from the start. Firstly, make sure that the visit is confirmed, provide directions and check the time of arrival of the auditor(s). If appropriate, inform reception that they will be coming, get an identity badge prepared and reserve a parking space. Book a room for the auditor's use (more if there is a team) and ensure that refreshments will be available, including lunch if possible. You will be needing to show documents and discuss them, so some form of large screen or projector will be useful.

For a remote audit, ensure that the online meeting tool you are going to use is agreed and that everyone involved knows how to use it, including how to share the screen to show the auditor some documented information. Check that microphones and cameras work and that the area behind each participant (in view of the camera) is appropriate. If technology such as a mobile phone is going to be used to perform a virtual walkaround of the offices, then test that first too.

Once the basic arrangements are in place you need to ensure that whoever is going to act as the auditor's guide around the ISMS is ready. This means knowing where all the relevant documents are and how each of the requirements is met within the documents. Supporting information such as HR and training records should also be available if required. Anyone who might be able to help the auditor such as managers and support staff should be on standby and everyone who is planned to talk to the auditor should be prepared.

There is no substitute for practice so conduct a mock audit beforehand if you can and identify any improvements needed before the day. Having obvious signs of information security-related activity on display at your location does no harm; this could be performance charts or posters for raising awareness on the walls.

It's all about showing the auditor that you are a professional organization that is in control; you may be surprised how little the auditor feels they need to look at if the overall impression they are getting is very positive.

5.4 During the audit

The auditor should have provided an audit plan which will set out the structure of the audit, including areas to be reviewed, people to be met and timings (this often doesn't happen so

don't worry if you don't get one). Despite the appearance of power, auditing is quite strictly regulated so the auditor will have specific things they need to do, in a specific format, starting with an opening meeting and ending with a closing meeting. Do what you can to make it easy for them by providing access to the relevant documents and resources as quickly and smoothly as possible.

Basically, all the auditor is doing is the same exercise as you did yourself when you performed (and repeated) the gap assessment. It's purely a matter of going through the requirements of the ISO/IEC 27001 standard and asking to be shown how you meet them. The auditor will need to record the evidence they have been shown, including any relevant references such as document titles and versions. They may also want to see the relevant procedures etc. in action which may mean reviewing the records you keep and possibly talking to the people who perform the procedures.

If the auditor finds something that doesn't conform to the requirements of the standard, they will raise a "nonconformity". These can be major or minor and, as the names suggest, these vary in importance.

A major nonconformity may be raised if there is a significant deviation from the standard. This is often due to a complete section not really having been addressed, or something important that has been documented but there is no evidence that it has been done. Examples might be if no internal auditing has been carried out, no risk assessment completed, or no management reviews held.

A minor nonconformity is a lower-level issue that doesn't affect the operation of the ISMS but means that one or more requirements have not been met. Examples could be that an improvement has not been evaluated properly, a control has not been implemented as planned or a risk assessment doesn't follow the documented process.

Some auditors take note of a third level of item often called an "observation". These are not nonconformities and so don't affect the result of the audit but may be useful for improvement purposes.

Once the audit has been completed the auditor will write up the report, often whilst still on site (or on the same day in the case of a remote audit). They will then tell you the result of the audit and go through any nonconformities that have been raised. Certification to the standard is conditional upon any nonconformities being addressed and upon the higher-level body that regulates the auditors agreeing with their recommendations. This can take a while to process so, even if you have no nonconformities, officially your organization is not certified yet.

You will need to produce an action plan to address the nonconformities and if this is accepted and they are closed off, you will then become certified and the certificate will be issued for a period of three years. During this time, there will be annual surveillance visits followed at the three-year mark by a recertification audit.

5.5 After the audit

There is usually a huge amount of pressure built up before the audit and once it's over the relief can be enormous. It's very easy to regard the implementation of an ISMS as a one-off project that is now over. But the auditor will be back within the next twelve months to check that you have carried on running the ISMS as required, so you can't afford to relax too much.

Certification is really a starting point rather than a result and hopefully as time goes by your ISMS will mature and improve and start to provide more and more value to the organization. However, you may find that the resources that were made available for the implementation now start to disappear and you need to ensure that the essential processes of the ISMS are maintained. Plans can get out of date very quickly so the performance evaluation side of the ISMS in particular will become very important; make sure you continue with the management reviews, exercising and testing controls and internal audits and this should drive the rest of the ISMS to stay up to date.

6 Conclusion

This implementation guide has taken you through the process of putting an ISMS in place for your organization, supported by the CertiKit ISO/IEC 27001 Toolkit. Hopefully, you will have seen that most of what's involved is applied common sense, even if the standard doesn't always make it sound that way!

Implementing a management system such as ISO/IEC 27001 is always a culture change towards becoming more proactive as an organization and, with the day-to-day reactive pressures of delivering a product or service, it can sometimes seem daunting. However, we hope you will find that it's well worth the effort as you come to the gradual realization that it's really the only effective way of doing it.

We wish you good luck in your work and, as always, we welcome any feedback you wish to give us via feedback@certikit.com.