CERTIKIT
Compliance made easy

ISO/IEC 27701
Implementation Guide

ISO/IEC 27701 Toolkit: Version 1

Contents

Tables

1 Toolkit support

The CertiKit ISO/IEC 27701 toolkit includes 75+ 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), 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 ISO27701 standard.

1.4 Exclusive access to customer discussion group

Complying to the ISO27701 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.

2 Introduction

This concise guide takes you through the process of implementing the ISO/IEC 27701 international standard for privacy information management using the CertiKit ISO/IEC 27701 Toolkit. It provides a recommended route to certification against the standard starting from a position where the organization has already implemented (and possibly become certified to) the ISO/IEC 27001 information security standard. Indeed, certification to ISO/IEC 27701 is not an option on its own – ISO/IEC 27001 is a necessary prerequisite to ISO/IEC 27701. This point will become increasingly clear as we go through the ISO/IEC 27701 standard and begin to understand its structure.

Of course, every organization is different and there are many valid ways to embed the disciplines of information privacy. 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 privacy; the important thing is that you end up with a Privacy Information Management System (PIMS) that is relevant and appropriate for your specific organization’s needs.

3 The ISO/IEC 27701 Standard

The ISO/IEC 27701 international standard for "Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines" was published by the ISO and IEC in 2019. ISO/IEC 27701 specifies the requirements that your PIMS will need to meet in order for your organization to become certified to the standard. The requirements in ISO/IEC 27701 are amendments and additions to those of the ISO/IEC 27001 information security standard and its supporting guidance, ISO/IEC 27002.

There are many other documents published within the ISO/IEC 27000 series and they provide useful supporting (and in some cases essential) information for organizations going for ISO/IEC 27701 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 27001 - Information technology — Security techniques — Information security management systems — Requirements
- ISO/IEC 27002 – Information technology – Security techniques – Code of practice for information security controls
- 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

It's worth pointing out that, although useful, none of these are required reading for certification to the ISO/IEC 27701 standard (except perhaps ISO/IEC 27001) so if you are limited in time and budget, just a copy of ISO/IEC 27701 itself will suffice (although if you haven't purchased the standard yet, we would recommend you look at our *ISO27701 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 27701 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 privacy risks and achieving compliance with relevant privacy legislation, such as the GDPR (General Data Protection Regulation).

Sections 0 to 4 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.

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 (see section 2.5 below for more on this within ISO27701). 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). Since the introduction of the High-Level Structure for ISO standards 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? Privacy impact assessments – what was assessed, 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 privacy according to the ISO/IEC 27701 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 a PIMS 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 27701 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 27701 Toolkit comes in….

4 The CertiKit ISO27701 Toolkit

The CertiKit ISO27701 Toolkit (referred to within this document simply as "the Toolkit") provides an array of useful documents which provide a starting point for the different areas of the standard. The documents are in Microsoft Office 2010® format and consist of Word documents, Excel workbooks, PowerPoint presentations and Project plans.

To open and edit the documents you will need to use the relevant Microsoft application at version 2010 or later. For the Microsoft Project file, we have provided the same content in an Excel spreadsheet also, for people who do not use Microsoft Project.

4.1 How the documents work

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. These can all be changed very easily using the various tools in Microsoft Word, including themes, styles and colour palettes. 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 the document properties (see *CERTIKIT ISO27701 Toolkit Completion Instructions* for details of how to do this, and how to change the look of the documents using themes etc.).

Each document starts with an "Implementation Guidance" section which describes its purpose, the specific clauses of the 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 some 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. Do not 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.

4.2 Last words before you begin

The remainder of this guide will take you through what you may need to do in each area and show how the various items in the CertiKit ISO27701 Toolkit will help you to meet the requirements quickly and effectively.

As we have 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 the Toolkit 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 we think you might need to know to achieve compliance. There are many great books available about information privacy generally and we recommend that, if you have time, you invest in a few and supplement your knowledge as much as possible.

But perhaps our single most important piece of advice would be to read the ISO27701 standard itself. There is really no replacement for going straight to the source document if you want to understand what it's all about. So, by all means, listen to what other people tell you about it, but try to take some time out to go to a coffee shop or somewhere equally comfortable, and read the thing from beginning to end (or at the very least, the relevant clauses). We believe you will not regret it. Enough said.

4.3 Where to start

Relevant Toolkit documents

- *ISO27701 Gap Assessment Tool*
- *Assessment Evidence*
- *CERTIKIT ISO27701 Toolkit Index*
- *Privacy Introduction Presentation*

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

- *ISO27701 Enhanced Gap Assessment Tool*

Before embarking on a project to achieve conformity (and possibly certification) to the ISO/IEC 27701 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 PIMS afterwards) will be successful and without it there is a danger that the PIMS will not be taken seriously by the rest of the organization, and the resources necessary to make it work may not be available.

The first questions top management are likely to ask about a proposal to become certified to the ISO/IEC 27701 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 ISO27701 Toolkit provides certain resources.

The *ISO27701 Gap Assessment Tool* is an Excel workbook that breaks down the sections of the ISO/IEC 27701 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 tool includes a variety of tables and charts 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 *ISO27701 Enhanced Gap Assessment Tool* goes several steps further than the default gap assessment by breaking down the text of the ISO/IEC 27701 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 *ISO27701 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 ISO27701 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 *Privacy Introduction Presentation* is provided in the Toolkit for

this purpose. Note that budgetary proposals should include the costs of running the PIMS 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).

4.4 A suggested project plan

Relevant Toolkit documents

- *ISO27701 Project Plan (MS Project)*
- *ISO27701 Project Plan (Excel)*
- *ISO27701 Project Initiation Document*
- *ISO27701 Progress Report*
- *Certification Readiness Checklist*
- *Meeting Minutes*

Having secured top management commitment, you will now need to plan the implementation of your PIMS. 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 *ISO27701 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 ISO27701 Toolkit provides a Microsoft Project® plan as a starting point for your project (reproduced in Excel for non-Project users). 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.

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.

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 ISO27701 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 PIMS 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.

4.5 How the rest of the guide is structured

The remainder of this guide will take you through the sections of the ISO/IEC 27701 standard one by one, explaining what you may need to do in each area and showing how the various items in the CertiKit ISO27701 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 a PIMS 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 privacy and we recommend that, if you have time, you invest in a few and supplement your knowledge as much as possible.

5 Implementing the ISO/IEC 27701 Standard

5.1 Section 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 a PIMS; this is relevant and important when understanding where the auditor is coming from in discussing what might be called the "spirit" of the PIMS. 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.

5.2 Section 1: Scope

This section refers to the scope of the standard rather than the scope of your PIMS. The fact that this standard is an extension to ISO/IEC 27001 and ISO/IEC 27002 is explained. It also mentions 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.

5.3 Section 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 27701 there are four listed which include the other standards from the ISO/IEC 27000 family that this one is closely related to, and an existing privacy-related standard, ISO/IEC 29100. Certainly ISO/IEC 27001 will be essential in understanding how ISO/IEC 27701 expands that standard into the area of privacy.

There are no requirements to be met in this section.

5.4 Section 3: Terms and definitions

Only two additional terms are defined in this section, and the reader is referred to a combination of ISO/IEC 27000 and ISO/IEC 29100 for the rest.

There are no requirements to be met in this section.

5.5 Section 4: General

This section describes how the rest of ISO/IEC 27701 is laid out and how it maps onto the ISO/IEC 27001 and ISO/IEC 27002 standards which it extends. It's worth spending some time to fully understand how ISO/IEC 27701 works, as it is not always immediately obvious to the reader. The main point is to recognise the difference between requirements, which are audited against, and guidance which is not. In ISO standards, requirements are stated using the word "shall" and guidance generally uses the word "should". For example:

*The organization **shall** determine its role as a PII controller (including as a joint PII controller) and/or a PII processor.*

And:

*The organization **shall** identify and document the specific purposes for which the PII will be processed.*

Are both requirements. The first relates to the management system and the second is a control. If these requirements have not been met, a nonconformity may be raised during an audit.

However,

*The organization **should** ensure that the use of mobile devices does not lead to a compromise of PII.*

And:

*Roles and responsibilities for the processing of PII **should** be determined in a transparent manner.*

Are both guidance and so are recommended, but still optional, and a nonconformity can't be raised against them at an audit (although an observation might be made perhaps).

Note: CertiKit has had this interpretation confirmed by the British Standards Institute (BSI).

Other words may be used in an ISO standard and their accepted meaning is as follows:

- "Shall" indicates a requirement;
- "Should" indicates a recommendation;
- "May" indicates a permission;
- "Can" indicates a possibility or a capability.
- Information marked as "NOTE" is for guidance in understanding or clarifying the associated requirement.

Let's take each of the clauses of the ISO/IEC 27701 standard and look at what it covers and whether it contains requirements (which are audited) or guidance (which is not audited).

Clause 5 describes how the ISO/IEC 27001 management system must be adapted to cater for privacy as well as information security. These are requirements. Note that there are in fact only two parts of the management system that require specific adaption – context and planning, although there is also a need to look at all areas to include privacy considerations within them.

Clause 6 provides additional privacy-related guidance for the controls set out in Annex A of the ISO/IEC 27001 standard, and which are more fully described in the accompanying code of practice, ISO/IEC 27002. These are recommended enhancements to the control set and may be considered to be guidance.

Clause 7 sets out guidance for the additional controls for controllers which are listed in Annex A of ISO/IEC 27701. These controls are over and above those from Annex A of ISO/IEC 27001. However, this is guidance only.

Clause 8 explains similar guidance for the additional controls for processors. Again, this is guidance, not requirements.

Annex A contains a table setting out the additional controls for PII controllers. These controls may or may not be applicable in the same way as the controls in Annex A of ISO/IEC 27001 may or may not be applicable (and as detailed in the Statement of Applicability for ISO/IEC 27001). Where applicable, these controls may be considered as requirements. The guidance for these is contained in Clause 7 above.

Annex B contains a table setting out the additional controls for PII processors. Again, their applicability needs to be determined and documented as they may not all apply. Where applicable, these controls may be considered as requirements. The guidance for these is contained in Clause 8 above.

The main point to repeat at this time is that certification to an ISO standard is all about requirements and controls. The guidance does not form part of these requirements and is not audited against. So, if your organization is looking to become certified to ISO/IEC 27701 (having already been certified to ISO/IEC 27001) then the areas to focus on are:

- Clause 5
- Annex A
- Annex B

... because these contain the requirements and the controls. Clauses 6, 7 and 8 give guidance in the same way as ISO/IEC 27002 gives guidance for ISO/IEC 27001. To be clear, for information security an organization becomes certified to ISO/IEC 27001 because that contains the requirements. An organization does not become certified to ISO/IEC 27002 because that only has guidance. It's the same for ISO/IEC 27701; stick to the requirements and controls parts when preparing for certification and don't feel that you must do everything that is stated in the guidance sections (although if it's appropriate and you can, then by all means go for it).

Annexes C, D and E provide a cross-reference of ISO/IEC 27701 onto ISO/IEC 29100 (privacy framework), the GDPR (the EU General Data Protection Regulation) and the two standards ISO/IEC 27018 (protection of PII in the cloud) and ISO/IEC 29151 (code of practice for PII protection).

Annex F gives a little more detail about how the current wording in ISO/IEC 27001 should be adapted to refer to privacy also.

Lastly in this section, the standard tries to clarify what is meant by the term "customer" in varying scenarios.

5.6 Section 5: PIMS-specific requirements related to ISO/IEC 27001

Relevant Toolkit documents:

- *PIMS Extensions to Existing ISMS*
- *Risk Assessment and Treatment Process*
- *Applicable Privacy Legislation*
- *Privacy Awareness Presentation*
- *ISO27001 and ISO27701 Statement of Applicability*
- *Internal Audit Checklist*

Since we are now including privacy within our management system, ISO27701 states that the term "information security" within ISO27001 should be extended to read "information security and privacy" wherever it is used. This is explained in more detail in Annex F of ISO27701 where examples are given such as "information security policy" becoming "information security and privacy policy". A search of the ISO/IEC 27001:2013 standard shows that the term "information security" is used 177 times (although four of these are in the bibliography) so it's quite a far-reaching change. This has the effect of widening the scope of the requirements of the ISO27001 standard to cover privacy also, so you'll need to be able to show that privacy is considered in all areas of your existing ISMS (Information Security Management System), thus extending it to be a PIMS (Privacy Information Management System) also. The term ISPMS (Information Security and Privacy Management System) has been used in some quarters to describe the combined management system, but it has yet to be seen whether this catches on within the industry.

What this means in practice is that documents within your existing ISMS that have "information security" in the title may need to be renamed to include "and privacy". For example, your existing *Information Security Roles Responsibilities and Authorities* document could become *Information Security and Privacy Roles Responsibilities and Authorities*. The content will need to be updated too so that references to information security include privacy also. Some documents will need to be expanded to consider privacy-specific issues

in addition to information security ones. The main areas in which these amendments may result in additional content within your existing ISMS documentation are the following:

- 4. Context of the organization (see Clause 5.2 of ISO27701)
    - PII (Personally Identifiable Information) controller and processor roles
    - Internal and external issues related to privacy
    - Further interested parties and their requirements
    - Scope clarification to include processing of PII
- 5. Leadership
    - Information security (and privacy) policy
    - Expand objectives to include privacy
    - Additional communication topics related to privacy
    - Commitment to satisfy applicable privacy requirements
    - Commitment to continual improvement of the PIMS
    - Additional roles, responsibilities and authorities for privacy
- 6. Planning (see Clause 5.4 of ISO27701)
    - Include privacy risks within risk assessments
    - Consider controls from ISO27701 Annex A and B when identifying risk treatment
    - Expand the statement of applicability to cover ISO27701 controls
    - Establish objectives for privacy
- 7. Support
    - Identify resources for privacy
    - Establish competence requirements and training needs for privacy
    - Conduct privacy awareness training
    - Add privacy-related issues to internal and external communication
- 8. Operation
    - Implement privacy processes
    - Plans should include privacy-related activities
- 9. Performance evaluation
    - Monitoring and measuring for privacy effectiveness
    - Internal audits covering privacy (and ISO27701)
    - Management reviews to include privacy issues
- 10. Improvement
    - Privacy-related nonconformities and corrective action
    - Identify privacy improvements

Most of these changes will be enhancements to existing documentation, rather than creating new ones and will require a managed exercise to take each document in turn and “upgrade” it for privacy.

What we provide in the Toolkit is a mixture of complete replacement documents and extracts of text to be added to existing ISMS documentation. These documents and extracts

refer to the CertiKit ISO27001 Toolkit, but if that toolkit has not been used to create the existing ISMS, then they should also provide enough information to decide where in your current documentation set the additional information should be placed.

5.7 Section 6: PIMS-specific guidance related to ISO/IEC 27002

Relevant Toolkit documents:

- *None*

This clause in the ISO/IEC 27701 standard provides PIMS-specific implementation guidance for a total of thirty-two of the 114 controls set out in ISO/IEC 27002 code of practice, which are of course the same controls that are listed in Annex A of the ISO/IEC 27001 requirements standard. Remember that these thirty-two items are guidance, not requirements, so a nonconformity should not be raised at audit if your organization doesn't have them in place within your PIMS. Treat this additional guidance in the same way as you treated the guidance in ISO/IEC 27002 during your project to implement the requirements of the ISO/IEC 27001 standard. From experience, it's fair to say that some organizations try to follow such guidance very carefully, whereas others make no reference at all to the content of ISO/IEC 27002 (but still become successfully certified to ISO/IEC 27001 nonetheless). This guidance exists to aid your interpretation of the Annex A controls within ISO/IEC 27001 and provide a fuller explanation of what they could mean in differing circumstances. The ISO/IEC 27001 Annex A reference controls for which additional guidance is provided in ISO/IEC 27701 are shown in Table 1 (note that the references used in this table are from ISO/IEC 27001 Annex A, not the ISO/IEC 27701 standard).

CONTROL GROUP	CONTROL	BRIEF SUMMARY OF ISO27701 PIMS-SPECIFIC GUIDANCE
A.5 Information security policies	A.5.1.1 Policies for information security	Policy commitment to terms of legislation and contracts with regard to PII.
A.6 Organization of information security	A.6.1.1 Information security roles and responsibilities	Appoint a data protection officer, or similar.
	A.6.2.1 Mobile device policy	Be careful with PII on mobile devices.
A.7 Human resource security	A.7.2.2 Information security awareness, education and training	Make employees aware of the consequences of PII breaches.
A.8 Asset management	A.8.2.1 Classification of information	Explicitly consider PII as part of the classification scheme.
	A.8.2.2 Labelling of information	Ensure everyone can recognize PII.

CONTROL GROUP	CONTROL	BRIEF SUMMARY OF ISO27701 PIMS-SPECIFIC GUIDANCE
	A.8.3.1 Management of removable media	Encrypt PII on removable media where possible.
	A.8.3.2 Disposal of media	Dispose of media containing PII securely.
	A.8.3.3 Physical media transfer	Implement secure procedures for PII transfer.
A.9 Access control	A.9.2.1 User registration and de-registration	Ensure compromised password situations are considered.
	A.9.2.2 User access provisioning	Be clear about customer responsibilities for access management in a cloud hosting environment.
	A.9.4.2 Secure log-on procedures	Provide secure logon facilities for customer-controlled user accounts.
A.10 Cryptography	A.10.1.1 Policy on the use of cryptographic controls	Provide information to customers about use of encryption for PII.
A.11 Physical and environmental security	A.11.2.7 Secure disposal or reuse of equipment	Ensure deleted PII is inaccessible when media are reused.
	A.11.2.9 Clear desk and clear screen policy	Restrict the printing of PII.
A.12 Operations security	A.12.3.1 Information backup	Ensure backups meet relevant requirements for PII processing.
	A.12.4.1 Event logging	Record access to PII via event logs.
	A.12.4.2 Protection of log information	Restrict access to log information that may contain PII.
A.13 Communications security	A.13.2.1 Information transfer policies and procedures	Ensure transfer rules for PII are enforced.
	A.13.2.4 Confidentiality or nondisclosure agreements	Ensure confidentiality agreements are in place for employees handling PII.
A.14 System acquisition, development and maintenance	A.14.1.2 Securing application services on public networks	Encrypt PII transmitted over insecure networks.
	A.14.2.1 Secure development policy	Ensure privacy by design and by default in system development and design.
	A.14.2.5 Secure system engineering principles	Ensure privacy by design and by default in systems/and or components that process PII.
	A.14.2.7 Outsourced development	Ensure privacy by design and by default in outsourced systems/and or components that process PII.
	A.14.3.1 Protection of test data	Don’t use PII for testing; if unavoidable, implement mitigating controls.
A.15 Supplier relationships	A.15.1.2 Addressing security within supplier agreements	Ensure agreements with suppliers acting as PII processors are compliant with relevant legislation.

CONTROL GROUP	CONTROL	BRIEF SUMMARY OF ISO27701 PIMS-SPECIFIC GUIDANCE
A.16 Information security incident management	A.16.1.1 Responsibilities and procedures	Make sure that PII breach management and notification obligations are met.
	A.16.1.5 Response to information security incidents	Ensure that PII breach investigation, recording, reporting and notification obligations are met. The interface between processor and controller should also be addressed.
A.18 Compliance	A.18.1.1 Identification of applicable legislation and contractual requirements	Identify potential legal sanctions with regard to PII processing.
	A.18.1.3 Protection of records	Retain previous versions of policies such as privacy policy when they are updated.
	A.18.2.1 Independent review of information security	Processors should provide customers with evidence of independent audit where appropriate.
	A.18.2.3 Technical compliance review	Include PII considerations when undertaking technical reviews.

Table 1: Additional guidance for ISO27001 Annex A controls

An auditor might reasonably expect much of this guidance to be in place already as part of the established ISMS, as PII is but a subset of the information processed within the organization. However, there are certainly specific areas that are new from ISO/IEC 27701, such as the appointment of a data protection officer, privacy by design and by default, and the notification obligations associated with legislation covering PII.

5.8 Section 7: Additional ISO/IEC 27002 guidance for PII controllers

Relevant Toolkit documents:

- *None*

This clause of the ISO/IEC 27701 standard provides more information about the additional controls for PII controllers that are laid out in Annex A of the same standard (not to be confused with Annex A of the ISO/IEC 27001 standard). The same comments apply as before, in that this is guidance and not requirements, so the clause should be read as helpful expansion of the specific controls in Annex A. The guidance is lengthy, so we don't cover it in any detail here; suffice to say that if you don't understand a control in Annex A then look here for more help.

5.9 Section 8: Additional ISO/IEC 27002 guidance for PII processors

Relevant Toolkit documents:

- *None*

This clause fulfils the same purpose as Clause 7, but for the controls for PII processors set out in Annex B of the ISO/IEC 27701 standard. Just to be extra clear, this is also guidance.

5.10 Annex A: PIMS-specific reference control objectives and controls (PII Controllers)

And so we come to the additional thirty-one controls for PII controllers which form the major part of the extra work in creating a PIMS to work alongside your existing ISMS. Although an organization may not be a PII processor, it would be relatively unusual for it not to be a PII controller, as it is difficult to run any kind of organization without needing to process some form of PII, for example that of employees. These controls should be thought of as an extension to the list of reference controls at Annex A of the ISO/IEC 27001 standard. The same principles apply, in that each of the controls may or may not be relevant to your organization and its processing of PII. This decision is required to be documented in the statement of applicability, along with an indication as to whether the control has been implemented. Within the Toolkit, we have provided a combined *ISO/IEC 27001 and 27701 Statement of Applicability* which lists all of the controls from Annex A of ISO/IEC 27001 and those from Annexes A and B of ISO/IEC 27701. The controls are grouped into four areas:

1. A.72 Conditions for collection and processing
2. A.73 Obligations to PII principals
3. A.74 Privacy by design and privacy by default
4. A.75 PII sharing, transfer and disclosure

Let's take each of these areas in turn and discuss what's required to implement the controls within them.

5.10.1 A.72 Conditions for collection and processing

Relevant Toolkit documents:

- *PII Analysis Procedure*
- *Legitimate Interest Assessment Procedure*
- *PII Controller-Processor Agreement Policy*
- *PII Processor Assessment Procedure*

- *Letter to Processors*
- *Privacy Impact Assessment Process*
- *Privacy Impact Assessment Report*
- *Records of Processing Activities*
- *PII Analysis Form*
- *PIA Questionnaire*
- *PII - Initial Questionnaire*
- *Legitimate Interest Assessment*
- *Consent Request Form*
- *Contract Review Tool*
- *PII Processor Assessment*
- *Privacy Impact Assessment Tool*

The eight controls in this area deal with how and why the PII is collected, including the lawful basis that is used under the relevant legislation that applies to it. If that basis is consent, then the methods used to signify consent and the records of it having been given are covered. The need to conduct a privacy impact assessment (also commonly referred to as a data protection impact assessment) for new and changed processing is set out. Relationships with PII processors and those situations where a joint controller situation applies must be defined, including in contractual terms where appropriate. Lastly, the keeping of records of processing required to meet the applicable legislation is prescribed.

5.10.2 A.73 Obligations to PII principals

Relevant Toolkit documents:

- *Privacy Notice Procedure*
- *Website Privacy Policy*
- *CCTV Policy*
- *PII Principal Request Procedure*
- *PII Principal Request Register*
- *Privacy Notice Planning Form - PII Principal*
- *Privacy Notice Planning Form - Other Source*
- *PII Principal Request Form*
- *PII Principal Request Rejection*
- *PII Principal Request Charge*
- *PII Principal Request Time Extension*

This is a significant set of controls covering the provision of clear privacy information to PII principals and how their rights under applicable data protection legislation will be exercised. These rights are embodied in laws such as the GDPR and typically consist of the right to:

- Modify or withdraw consent
- Object to processing

- Access their PII and have it corrected or erased if appropriate
- Be provided with a copy of their PII

Procedures for handling such requests (usually within set timeframes) need to be in place. Obligations surrounding the use of automated decision-making, for example using an algorithm, must be complied with.

5.10.3 A.74 Privacy by design and privacy by default

Relevant Toolkit documents:

- *Records Retention and Protection Policy*
- *Privacy and Data Protection Policy*

This set of nine controls deals with methods surrounding the design of processes and systems so that privacy is considered from the outset, and as a key part of the way they work. These are related to the basic principles of much of the relevant legislation, which requires that:

- No more PII is collected than is necessary for the processing
- The processing is no more than is necessary to achieve the objective
- The PII is kept up to date
- PII is minimised and anonymised where possible
- The data is retained for no longer than necessary
- Appropriate safeguards are in place to protect PII

5.10.4 A.75 PII sharing, transfer and disclosure

Relevant Toolkit documents:

- *Procedure for International Transfers of PII*
- *Records of PII Disclosures*
- *Records of PII Transfers*

The smallest of the control groups in Annex A, this set of four controls covers the requirement to ensure that transfers of PII between countries are covered by a relevant justification, such as an EU adequacy decision (in the case of the GDPR) or appropriate standard contractual clauses. It also requires that a list is maintained of the countries to which PII may be transferred by the organization, and records of such transfers. Account must be taken of the potential need to liaise with these third parties in the fulfilment of requests from PII principals to exercise their rights over their data. Lastly, records must be kept of disclosures of PII to third parties such as law enforcement organizations.

5.11 Annex B: PIMS-specific reference control objectives and controls (PII Processors)

This annex lists the eighteen controls that are relevant to an organization acting as a PII processor. Not all organizations will be taking this role, so some or all of these controls may not be relevant. As for Annex A, the idea is that the organization defines those controls that apply using a statement of applicability. The controls fall into the same four areas as for Annex A:

1. B.82 Conditions for collection and processing
2. B.83 Obligations to PII principals
3. B.84 Privacy by design and privacy by default
4. B.85 PII sharing, transfer and disclosure

We will look at each of these areas for processors in the following sections.

5.11.1 B.82 Conditions for collection and processing

Relevant Toolkit documents:

- *PII Processor Policy*
- *Records of Processing Activities*
- *Processor Employee Confidentiality Agreement*

The six controls in this section are mainly concerned with the contractual nature of the relationship between the PII controller and the processor. The contract must cover how the processor will help the controller to fulfil its relevant privacy obligations, and the purpose of the processing stated in the contract must be the only form of processing that is undertaken with that data. Using the data for marketing purposes is generally not allowed unless it is confirmed that the consent of the PII principal has been obtained. A further control encourages the processor to keep an eye on the legality of the processing it is being asked to do, and to let the controller know if there may be a problem. Good communication is also prescribed so that the controller has all the information it needs from the processor to be able to show that it is staying compliant. Lastly, the processor must keep appropriate records of the processing it carries out on behalf of the controller.

5.11.2 B.83 Obligations to PII principals

Relevant Toolkit documents:

- *None*

The single control in this section states that the processor must help the controller to meet its obligations to PII principals, consisting mainly of their rights under relevant legislation, including access, erasure and objection to processing.

5.11.3 B.84 Privacy by design and privacy by default

Relevant Toolkit documents:

- *Processor Security Controls*

These three controls cover the processor's obligation to ensure that temporary files holding PII are subject to a documented retention policy, that the controller's PII can be transferred or disposed of at the controller's request, and that PII is transmitted by the processor over secure links with appropriate controls.

5.11.4 B.85 PII sharing, transfer and disclosure

Relevant Toolkit documents:

- *Customer PII Transfer Policy*
- *PII Disclosure Procedure*
- *Records of Processor PII Transfers*
- *Records of Processor PII Disclosures*
- *Sub-Processor Agreement*

These final eight processor controls largely deal with similar issues as those for the controller, namely the international transfer of PII and the disclosure of it to third parties. The key is communication and consultation with the controller (i.e. the processor's customer) both to keep them informed and to allow them to take part in decision-making.

Three controls also cover the use and further engagement of subcontractors (often also referred to as sub-processors), specifically ensuring that the controller is aware of the subcontractors used and has a chance to object to any new or changed engagements that don't meet their requirements.

6 Advice for the audit

6.1 Choosing an auditor

If your organization wishes to become certified to the ISO/IEC 27701 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 ISO/IEC 27001 (which is a prerequisite) then it makes sense to use the same auditing company for ISO/IEC 27701, if they can provide that service.

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.

6.1.1 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 (probably) 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 people 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 (e.g. your customers or regulators) may simply not believe you.

6.1.2 Third-party certification

So instead, you may decide to get a third party to assess 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 (to use an

information security analogy) 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 27701").

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.

6.1.3 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.

6.2 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 the *ISO27701 Gap Assessment Tool* within the Toolkit as a guide to your readiness, but don't expect to be 100% compliant before going for Stage One.

6.3 Preparing for audit day

Once you feel you are ready to be visited by the auditor for either the Stage One or Stage Two then there are a number of sensible preparations to take to make the best impression from the start. For an onsite audit, 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 he/she 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 PIMS is ready. This means knowing where all of 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 your data protection officer or individual process managers 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 privacy-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.

6.4 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 sometimes doesn't happen so don't worry if you don't get one). Despite the appearance of power, auditing is actually 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 is purely a matter of going through the requirements of the ISO/IEC 27701 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 does not 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 or process 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 done, or no management reviews held.

A minor nonconformity is a lower-level issue that does not affect the operation of the PIMS as a whole but means that one or more requirements have not been met. Examples could be that an improvement has not been evaluated properly, a procedure has not been carried out as specified or a privacy risk assessment does not follow the documented process.

Some auditors take note of a third level of item often called an “observation” or an “opportunity for improvement”. These are not nonconformities and so do not 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 his 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.

6.5 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 a PIMS 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 PIMS 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 PIMS 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 PIMS are maintained. Plans can get out of date very quickly so the performance evaluation side of the PIMS 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 PIMS to stay up to date.

7 Conclusion

This implementation guide has taken you through the process of positioning your organization to achieve certification to the ISO/IEC 27701 standard, supported by the CertiKit ISO27701 Toolkit. Hopefully, you will have seen that most of what is involved is applied common sense, even if the standard does not always make it sound that way!

Implementing the requirements of a standard such as ISO/IEC 27701 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 the Toolkit is of value in clarifying what needs to be done and speeding up the process of privacy compliance.

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