

IMPLEMENTATION GUIDE

The ISO27001 People



INTRODUCTION

This guide is going to walk you through implementing the ISO 27001 Toolkit. At the end of this process, you will be ISO 27001 Stage 1 Ready and have an effective Information Security Management System (ISMS). Assuming you follow and complete the steps.

Whether you are a business implementing yourself or a consultant implementing for your clients this guide has your back.

If you have any questions, you can contact me at:

Stuart@hightable.io

<https://www.linkedin.com/in/stuartabarker/>

The ISO27001 People



RESOURCES TO HELP YOU

You have a wealth of resources to help you. An absolute feast of information. Over 20 years of knowledge and experience are now at your fingertips.

Video Guides

To implement ISO 27001 a set of video guides will walk you through everything you need to know and how to do it. There is an extensive YouTube channel, but you are best placed to start here:

<https://youtube.com/playlist?list=PLCHmT3D9hgL7jWTQUJNjy-1Tm2fMFlmvV>

ISO 27001 Guides

You have access to a wealth of blogs on ISO 27001 on the website.

- ISO 27001 Reference Guide: Clause by Clause: <https://hightable.io/iso-27001-reference-guide/>
- ISO 27001 ANNEX A Reference Guide: <https://hightable.io/iso-27001-annex-a-controls-reference-guide/>

The ISO27001 People



YOUR TABLE OF CONTENTS

IMPLEMENTAITON GUIDE..... 1

INTRODUCTION 2

RESOURCES TO HELP YOU 3

 Video Guides..... 3

 ISO 27001 Guides..... 3

YOUR TABLE OF CONTENTS 4

Audit Compliance Report..... 10

Document Builds..... 13

 Variables to Change..... 13

 GREEN Text..... 13





[Text in Brackets]..... 14

The Order in Which to Tackle the Pack 15

Brand the Pack 16

 When branding 16

Assign Your Team 17

 Assign Owners of Documents 17

 Complete: Information Security Assigned Roles and Responsibilities 18

 Complete: Information Security Management System Document Tracker..... 19

 Assign Owners of the ANNEX A Controls 20

 Update each document in the toolkit to assign the owner. 21

CHECK POINT 1 22

Document Who You Are and What You Have 23

 Organisation Overview 24

 Context of Organisation 25

 Documented Scope..... 26





Legal and Contractual Requirements Register 27

Physical and Virtual Asset Register 28

Data Asset Register 28

Software Licence Assets Register 30

Statement of Applicability 31

Third Party Supplier Register / Contracts / Security Certificates..... 32

CHECKPOINT 2 34

Document Your Information Security Management System..... 35

Information Security Objectives 36

The Information Security Management System Overview 37

Competency Matrix 38

Information Classification Summary..... 38

Information Security Measures Report..... 39

CHECKPOINT 3 40

Document Your Policies 41





CHECKPOINT 4 42

Conduct Your Risk Review 43

 Risk Review Meeting..... 43

 Risk Register 44

 Supporting Resources..... 44

CHECKPOINT 5 45

Create Your Plans 46

 Audit Plan 46

 Communication Plan 47

 Information Security Management System Plan 48

CHECKPOINT 6 49

Train Everyone. 50

CHECKPOINT 7 51

Implement and Test Business Continuity 52

 Business Impact Assessment 52





Business Impact Analysis Exec Summary 52

Business Continuity Objectives and Strategy 53

Business Continuity Plan 53

Disaster Recovery Scenario Plans..... 53

Disaster Recovery Tests 54

Business Continuity Desk Top Test 54

CHECKPOINT 8 55

Implement Your Operational Processes 56

 Operations Security Manual 57

 Implement and Evidence Operational Processes 58

CHECKPOINT 9 59

Conduct Your Internal Audit..... 60

CHECKPOINT 10 61

Hold Your Management Review Meeting 62

 Management Review Meeting ONE 62



CHECKPOINT 11 65

Communicate Your New Information Security Management System 66

Operate Your Information Security Management System 66

Prepare To Be Audited 67

Conclusion 70

Good Luck. You’ve got this. 71



Audit Compliance Report

The best place to start is in the audit folder. This is **folder 8**. The audit folder has 4 files, we will come back to that later, but for now the file that you want is called:

1b. Audit Template ISO 27002 2013 and 2022 Version PRE-MAPPED

We use the audit template to, well, conduct audits throughout the year as the working document. BUT this version is already pre mapped and pre completed to the pack that you have just bought. There are several tabs

- Front Sheet – the version control and document mark up
- Dashboard – the management level compliance report sheet,
- ISO 27001 ISMS - the *ISMS audit sheet* - 1 for each version of the standard
- Annex A – the *controls audit* sheet - 1 for each version of the standard

For now, you are going to go ahead and look at the *ISO 27001 ISMS* tab.

If you look at the *ISO 27001 ISMS* tab you will that is already mapped to the document pack. How fast was that?

The ISO27001 People



You have the ISO 27001 clause number, the title, the control objective and then the evidence columns. In the positive evidence column, we have recorded which documents you have that meet the control objective.

You will also see that you have a column on the far right called Guidance. For each clause you will see a link to a detailed blog specific to that clause.

So, you now have a document that lists all the control requirements of the ISMS and how the pack meets that requirement to make you compliant with a link to a specific blog on the requirements of that clause and how to meet it.

You also have this for both versions of ISO 27001, including the 2022 updated version.

In addition, you have it for the ISO 27001 Annex A/ ISO27002, including the 2022 updated version.

This is the bare minimum clearly but is the massive boost and time saver and

you can now see EXACTLY why you have the documents you have and which parts of the ISO 27001 ISMS standard they meet.

The ISO 27001 toolkit is not designed to specifically address the business controls that are required in the ANNEX A but now would be a good time to look at the

The ISO27001 People



ANNEX A tab audit sheet to see the list of all the *ANNEX A* controls that you will potentially require.

This is where you will record your audit results and it is a good idea to do a gap analysis of your business and record the findings.

The ISO27001 People



Document Builds

The documents are what good looks like. Overall, they will apply as is, with only certain areas requiring your input. You should read them, understand, and change them based on your needs, irrespective of the variables below. Remember they are designed to be highly customisable and flexible and be adaptable as you change and grow. But for guidance:

Variables to Change

There are variables within the documents that either require your attention, a change, an acceptance, or some information.

GREEN Text

Whilst all text should be considered for review, text that is in **GREEN** denotes that you have action to take or something to do. This text maybe an example, an instruction or text that requires you to confirm you do it. This is **GREEN** to draw your attention. Once you have made your change, added your information or to accept the text, set the text to BLACK.

There should be no **GREEN** text in a document when the time comes to sign off and release it.

[Text in Brackets]

[Text in Brackets] often refers to a place holder that requires your actual information.

They are self-explanatory. Make the change and remove the brackets so the text flows.

The ISO27001 People



The Order in Which to Tackle the Pack

Follow along in the **ISO 27001 Implementation Checklist**. Here you will find further guidance and you can mark off as you complete each step. It includes an automated management reporting dashboard to track your progress.

The order in which you tackle the pack is going to be based on the size of your organisation and your own experience and preference but a good order to tackle the pack based on experience is as follows.

The ISO27001 People



Brand the Pack

You are going to want to make the documents look like you. All the documents have standard mark-up such as version control and classification and it is recommended that you do not remove these elements from the pages to remain compliant. Of course, you can move them around, change the layout as needed.

When branding

- Update the logo to your company
- Change all occurrences of the place holder text [Company] with your company name.
- Change the font if applicable to your company font although based on experience this can be a ball ache and my advice is to leave as is.

The ISO27001 People



Assign Your Team

Even a small organisation of 1 or 2 people there are roles that need to be allocated.

In this step, like the Avenger's, you will Assemble.

Assign Owners of Documents

You want to assign owners to documents. Owners of documents are going to be responsible for completing the required documents, maintaining the documents, and reviewing the documents. Think of it this way, if someone was to ask about a particular document – who is the person that knows everything about it and what it covers? We are going to get audited at some point and you want to know exactly who to speak to about the document and its topic.

Getting this right is a key step. It will require agreement with the person that you assign ownership.

You *can* assign it to a team not a person. I advise against it and recommend assigning to a person. This is about accountability. In my experience assigning it to a team means no one is accountable, so no one maintains it, people in the team will not know about it, it will cause problems come the audit. Think, accountability.

Nothing focuses the mind like having your name on the document.



Complete: Information Security Assigned Roles and Responsibilities

Complete the following document:

2 The Information Security Management System / 2 Information Security Roles Assigned and Responsibilities

This document is a required document with place holders for key roles. Add the names of the people that are responsible and at this point consider who is on your Management Review Team. The Management Review Team is the oversight body that you will implement that has key responsibilities and meets to follow a structured, dictated agenda, for which we have provided a template. For now, complete this document.

How to video: https://youtu.be/dLHZ_TNX_kQ



Complete: Information Security Management System Document Tracker

Complete the following document adding in any other relevant documents that are missing:

*2. Information Security Management System / Information Security Management
System Document Tracker*

Maintain this document throughout your build. For now, do not worry about updating the version information until you have your first complete version 1 milestone pack. Just record the document owners.

The ISO27001 People





Assign Owners of the ANNEX A Controls

Annex A is the business controls. You will rely on the people in the business that run and manage those departments, functions, and controls to bring their areas of responsibility up to speed. Whilst Annex A implementation is part of the Stage 2 and not covered here, having the owners assigned is required. To have any kind of a chance you want accountability, to know who is responsible and as with the document assignment above, who the auditor is going to speak to about each control.

Complete: ISMS Annex A Controls - Accountability Matrix

2. Information Security Management System / ISMS Annex A Controls - Accountability Matrix

The ISMS Annex A Controls - Accountability Matrix is a great little document. It is a cut down version of a RACI matrix. You want to *complete at least column D* with the primary name of the primary person for the ANNEX A control.

You have both versions of the standard / controls, and it is recommended you complete this for both versions, even if you are not certifying against both control sets. The Annex A Controls are straight forward.



Update each document in the toolkit to assign the owner.

Every document in the toolkit has a place holder for the document owner. In each document replace the text in brackets – [Document Owner] – with the person that you have assigned and agreed as the document owner. You may want to consider using the persons job title rather than name.

The ISO27001 People



CHECK POINT 1

At this check point you now have

- A Branded Pack that is branded to your company
- Document owners assigned for the ISMS
- Control owners assigned for the ANNEX A Controls
- The required roles and responsibilities for the ISMS assigned
- The Management Review Team assigned
- An understanding of the requirements of ISO 27001 and how the pack addresses those requirements. Where to find that information.

The ISO27001 People



Document Who You Are and What You Have

In the last section you allocated owners to documents in the *Information Security Management System Document Tracker*.

Now is the time to go ahead and complete the documents.

Either assigning to the document owner or working with the document owner review each document, updating the variables (see section above) as required and filling in the required information.

To help you there are video guides provided on each significant document.

The ISO27001 People



Organisation Overview

1 Context of Organisation / 1 Organisation Overview

The organisation overview is straightforward information about you, that you already know about you. You may have it in different locations, or some of it, or none of it.

Now is the time to collate it into one document. We are making a link between who we are and the information security management system we have built.

When we built it, did we consider our business objectives? Our strategy? Our locations. Simple stuff but you want to draw a link and demonstrate it.

How to video: <https://www.youtube.com/watch?v=iwSr-LloQ6Y>

A guide to the organisation overview and more details: <https://hightable.io/iso-27001-organisation-overview/>

Document: <https://hightable.io/iso-27001-clause-4-1-understanding-the-organisation-and-its-context/>

The ISO27001 People



Context of Organisation

1 Context of Organisation / 2 Context of Organisation

Context of Organisation wants us to show that we have worked out who our interested parties are (our stakeholders), what their requirements are and again to show link between that and our information security management system. In addition, it talks about internal and external issues, which are in effect risks, so we record them here. We will show if we have considered it and it is NOT a risk. This is valid and great as auditors love to test us and check we have considered all possibilities. Here we can say, yes, we considered and for us, no it was not a risk. It will also show if we do in fact, YES, consider it a risk. If this is the case, make sure to include it in your risk register and to put the risk reference number here in this document. This creates the link between issues and risks that need to be managed.

How to video: <https://youtu.be/asYMhvFw7-U>

A guide to the context of organisation and more details: <https://hightable.io/context-of-organisation/>

Document: <https://hightable.io/iso-27001-clause-4-1-understanding-the-organisation-and-its-context/>



Document: <https://hightable.io/iso-27001-clause-4-2-understanding-the-needs-and-expectations-of-interested-parties/>

Documented Scope

1 Context of Organisation / 3 Documented ISMS Scope

Getting the scope right is absolutely key. It drives the complexity, the work you have to do, the costs and more. Take time to get this right. High level you want the scope to cover the products / services that you provide to customers that customers are asking for you to be certified for. It is customer driven.

How to video: https://youtu.be/5RXi_8INtgg

A guide to the ISO 27001 scope and more details and guidance:

<https://hightable.io/iso-27001-scope-statement/>

Document: <https://hightable.io/iso-27001-clause-4-3-determining-the-scope-of-the-information-security-management-system/>

The ISO27001 People



Legal and Contractual Requirements Register

1 Context of Organisation / 4 Legal and Contractual Requirements Register

You are expected to run your business in line with the laws and regulations of where you operate. Using the guidance of legal counsel complete the legal register. What you should note here is that whatever law or regulation you say applies to you, is fair game and in scope for your certification audit. People can fail on this. So, if you say it applies, before you go for certification, make sure that you do and can evidence you do. It is a massive catch all and one downside of the standard. Things like PAT testing, Fire Extinguishers, Data Protection all come in scope to catch you out if relevant laws apply to you. We are not lawyers; we cannot provide legal advice and we can answer this for you. You do have some examples but get this list from your legal counsel.

How to video: <https://youtu.be/kxEh3OBPRUQ>

A guide to the Legal and Contractual Requirements Register and more details and guidance: <https://hightable.io/how-to-create-and-use-a-legal-and-contractual-register/>



Physical and Virtual Asset Register

1 Context of Organisation / 5 Physical and Virtual Asset Register

You need a physical asset register which is actually a register of every device, both physical and virtual (if you have a VM environment) that can store, process, or transmit data. Of course, here we are looking at things that are in scope as defined in the scope statement. It will also include bring your own devices and user owned equipment that connects. For this we may not control it directly, but we do want to know about it and be able to control what it can access. The spreadsheet is the minimum information requirement. If you can get this information direct from a system, you do not have to also complete the spreadsheet. Being able to generate the reports from the systems is the ideal but if you cannot, the spreadsheet is the way to go. Potentially you will have a hybrid and use a combination.

How to video: https://youtu.be/ScQyCcX_q6g

A guide to the Physical Asset Register and more details and guidance:

<https://hightable.io/how-to-create-and-use-asset-register/>

Data Asset Register

1 Context of Organisation / 6 Data Asset Register



You need an asset register of all of your data assets. Now, ideally you have this already from your data protection implementations but if not, this template will meet the need. It is based on the GDPR best practice, and each field should be completed.

You identify your data assets and data stores by reviewing technical documentation, system documentation, process documentation, process mapping, brainstorming and just asking folks. If you have this information already, use that, if not, complete the data asset register.

You need a data asset register.

How to video: https://youtu.be/U17JzWO_UNY



Software Licence Assets Register

1 Context of Organisation / 7 Software License Assets Register

This has always been a requirement but as part of the 2022 update you are now explicitly looking at intellectual property and bringing software licenses directly under that you. You have an updated Intellectual Property Policy that directly references this, and this is a great and simple way to evidence your software licenses. Like everything else, if you already have something, and it meets the standard then you don't need this, clearly. Don't duplicate work. But if you don't have anything, then you will be expected to, and this is a great way to do it. Complete it.



Statement of Applicability

1 Context of Organisation / 8 Statement of Applicability

The statement of applicability is the list of controls that apply to your organisation, and it is a core mandatory document. The list of controls is taken from Annex A to the standard, which is also confusingly a standard called ISO 27002. You need to know the control list changed in 2022. You have both control lists as you will need to confirm with your certification body which control set you will be certified against. For now, and best proactive, complete both control sets.

It is simple to go through and set whether control applies or not, and if not put a compelling reason that is believable to an auditor as to why it does not apply. Set the review dates and consider if you need to make changes to the columns on why you need it.

How to video: <https://youtu.be/aqFYZ7GPRMg>

A guide to the Statement of Applicability and more details and guidance:

<https://hightable.io/statement-of-applicability-iso-27001/>



Third Party Supplier Register / Contracts / Security Certificates

6 Supplier Management / including Third Party Supplier Register

In information security we need to secure the supply chain. Our supply chain is one of our biggest risks and potential vulnerabilities. You will identify all the suppliers for the in-scope products and services and list them. You will add in the required details, and you will rank them for importance to your organisation and the assurance you have they are doing the right thing. We don't want to get into having to send questionnaires and audit companies, so we are going to place reliance on third party ISO 27001 or similar certifications. Guidance in the guidance tab allows you to rank and rate suppliers. For each supplier you need an in-date contract, with security clauses, that covers what you are buying AND you need a copy of the ISO 27001 or equivalent certificate for your assurance. You should be able to show both of these to an auditor.

If you have neither a contract nor a certificate, go ask for one. If they do not have a certificate, then you need to manage that via risk management by adding to the risk register and following the risk management process. This will likely include following the continual improvement process and adding it to the Incident and Corrective

The ISO27001 People



Action Log. Make sure there are NO GAPS in the third-party supplier register when you go for certification audit.

A guide to the Third-Party Supplier registers and more details and guidance:

<https://hightable.io/third-party-supplier-register/>

In the folder 01 Information Security Manager Guides is a detailed guide called: **How to Third Party Supplier Audit and Review**

The ISO27001 People



CHECKPOINT 2

At this check point you now have

- Documented and understood who you are
- Documented and understood what you have
- Set the scope for the ISO 27001 Management System
- Selected the first pass of the Annex A controls that apply to you
- Linked the information security management system to you

The ISO27001 People



Document Your Information Security Management System

In the last section you documented information about who you are. Now we are going to link that and tie that to the information security management system and we are going to document what our information security management system is.

The ISO27001 People



Information Security Objectives

2 Information Security Management System / Information Security Objectives

Objectives are the why. Why do you have the Information Security Management System. Why do you have ISO 27001.

Pay attention to the information security objectives. You should not need to change them for a first build but just double check them. You need to ensure that the objectives here are word for word the same in your information security policy and in your management review team meeting minutes that you track each month / set period you decide. Complete this document assigning people and the metrics and measures that you will put in place and track.

The ISO27001 People



The Information Security Management System Overview

*2 Information Security Management System / The Information Security Management
Overview*

This document sets a description of the information security management system. Complete it. Where videos and guides note this document includes Objectives also note these have now moved to their own standalone document as part of the 2022 upgrade for ease of management and this document has been updated to set out the process for setting objectives.

How to video: <https://youtu.be/xpqSsc2qOAq>

The ISO27001 People



Competency Matrix

2 Information Security Management System / Competency Matrix

For everyone involved in information security add them to the competency matrix and complete it. That is everyone in the roles and responsibilities matrix, the document tracker, and the accountability matrix as a minimum. If you have a third-party consultant helping, add them too. You are demonstrating that you have the resources with the required skills to operate and manage the information security management system and that you are managing where there are gaps.

How to video: <https://youtu.be/GjO3xtzUksM>

Information Classification Summary

2 Information Security Management System / Information Classification Summary

This is a reference document - no action needed other than review and know you have it. It is a summary of the information classification and handling policy, and you will communicate this to all staff as part of the implementation.

How to video: <https://youtu.be/iqQ5w9IBIDg>





Information Security Measures Report

(** you have to create this)

For the objectives you have defined, you have to decide what you are going to measure. We need to measure and report on a monthly basis metrics that are relevant to us that show that the information security management system is in control. These are most likely going to be outputs from, and the consequence of, annex A processes. For example, having patch management processes will likely result in a report of machines that are successfully patched and those that are not. This could be one measure. Another example could be the antivirus process which will likely result in a report of viruses that were caught and managed, or not, over a time period.

It could be machine patching, machine antivirus, staff training - whatever you are measuring create a report that you can populate each month to track your measures. Make sure each objective has measures you can track, and your report includes them. Keep historical records of the reports.

These reports are shared and minuted as part of the Management Review Meeting.



CHECKPOINT 3

At this check point you now have

- Documented and understood key components of your information security management system
- Set out your objectives for the information security management system
- Set out what your measures and monitors are going to be
- Ensured you have the required competence to run the information security management system on going

The ISO27001 People



Document Your Policies

Using and following the guide: **Getting Started – How to Deploy and Implement Policies**, complete the policy build.

The ISO27001 People



CHECKPOINT 4

At this check point you now have

- Documented policies that explain exactly what you do as an organisation for information security
- Approved, communicated, and had accepted by staff the information security policies

The ISO27001 People



Conduct Your Risk Review

ISO 27001 is a risk-based management system with risk management at its heart.

You need to complete your risk review meeting and complete your risk register and start your active risk management.

Risk Review Meeting

10 Meeting Minutes / Annual Risk Review Meeting - Template

The risk review meeting is a risk workshop that you conduct at least annually.

Arrange a meeting with the Management Review Team, invite anyone else that can add value. Work through any risks you have identified in the Context of Organisation document, review the example risks provided and then brainstorm any other risks that are appropriate to you. Minute the meeting and update the risk register.



Risk Register

5 Risk Management / ISMS Risk Register

Complete the risk register for your organisation. You can review the example risks that are provided to see if they apply. Make sure that:

- If you have issues in the Context of Organisation that say they are added to the risk register, that they are added to the risk register.
- That the risks identified in your risk review workshop meeting are on the risk register

You have a copy of the Risk Management Process document for ongoing risk management.

Supporting Resources

Document: <https://hightable.io/risk-register/>

Document: <https://hightable.io/risk-management-policy/>

Document: <https://hightable.io/iso-27001-clause-8-2-information-security-risk-assessment-essential-guide/>

Document: <https://hightable.io/iso-27001-clause-6-1-3-information-security-risk-treatment/>

Video: <https://youtu.be/eZdtSJzjNko>

The ISO27001 People



CHECKPOINT 5

At this check point you now have

- Conducted your risk review
- Updated your information security management as required based on the risk reviews
- Understood exactly what risks you are managing with the controls and risk management plans in place
- Effectively managing risk and able to communicate your risks

The ISO27001 People



Create Your Plans

We are going to plan and show that we have planned. Planning is part of managing.

Audit Plan

4 Plans and Logs / Audit Plan

You have to audit everything at least once annually and definitely before the certification audit. Plan your audits and document them including 12 months in advance. Be sure that everything is audited at least once, and some areas may need auditing more than once based on risk. You can do small audits each month or one / two large audits a year. Plan what is right for you and your business. Once planned ensure you follow the plan and conduct the audits.

Consider, if you find a non-conformity that goes into the continual improvement process and is entered on the incident and corrective action log for managing that it is likely that you would then schedule an audit of that area at a future date to check that the corrective action was effective. I would check this an auditor. This is not a consideration per se for a first build and certification audit, but it can be.



Communication Plan

4 Plans and Logs / Communication Plan

You have to communicate, plan and evidence it. Plan your communications and document them including 12 months in advance. Consider different communication types. Your meetings are a form of communication so include them (Management Review Meeting, Security Ops Meeting, Risk Review Meeting, Business Continuity meetings for example).

An auditor will check the plan and for complete communications expect to see evidence that it was completed. This can be meeting minutes, copies of emails, screenshots of SharePoint / Intranet posts.



Information Security Management System Plan

4 Plans and Logs / ISMS Management Plan

This is now an explicit requirement of the ISO 27001 standard as part of the 2022 update to plan the changes to the management system. It has always been done but we now evidence that we do it for audit purposes so complete the plan of when you will make the operational changes to the ISMS.

The ISO27001 People



CHECKPOINT 6

At this check point you now have

- Put in place your planning for the year

The ISO27001 People



Train Everyone.

You need to train everyone on at least on basic information security and data protection and you need to evidence that they understood and accepted it. This is one place where a tool will do the heavy lifting for you as they come with prebuilt modules, have tests and quizzes built in to demonstrate understanding and come with reports that show who has completed the training. You should make sure that everyone has completed the basic training before the certification audit, and you should plan in additional training for the next 12 months. Remember that the basic training should be conducted and evidenced at least annually.

The ISO27001 People



CHECKPOINT 7

At this check point you now have

- Trained and can evidence that you have trained everyone on information security and data protection
- Everyone has completed the training
- Set a plan for the future training requirements that you can evidence and show

The ISO27001 People



Implement and Test Business Continuity

9 Business Continuity / All documents

You need to implement the business continuity and disaster recovery. The documents here are self-explanatory. Business continuity is technically a standard in its own right called ISO 22301 but for now, complete the documents. You then need to run a test and evidence that you have keeping records.

Business Impact Assessment

Document your systems, locations and teams and follow the guide to prioritise them.

Business Impact Analysis Exec Summary

Summaries your business impact assessment in a nice summary

The ISO27001 People



Business Continuity Objectives and Strategy

Set the objectives and strategy for your business continuity.

Business Continuity Plan

Create your business continuity plan and put in place disaster recovery documents.

Disaster Recovery Scenario Plans

Work out common scenarios that may occur that would impact your business and its ability to operate and document what they might be, and the plans associated.

The ISO27001 People



Disaster Recovery Tests

Conduct tests of the scenarios recording evidence of the test. Evidence may be screen shots, screen recordings or output reports from systems. You have to have tested before going for certification.

Business Continuity Desk Top Test

9 Business Continuity / Business Continuity Desk Top Test

Conduct a desk top exercise that tests what the business will do in the face of a significant event.



CHECKPOINT 8

At this check point you now have

- Implemented, tested, and can evidenced Business Continuity that shows what the business is doing in the event of a significant event
- Implemented, tested, and can evidenced Disaster Recovery that shows what specific functions and / or technologies are doing in the event of a significant event for recovery.

The ISO27001 People



Implement Your Operational Processes

You need to write your operational processes. This is something that we cannot pre do for you as every business is different. We cannot write your software development process, or your HR hiring processes, or your HR off boarding, or your change because if we did, we would be telling you how to run your business. And you would just argue with us that what we were telling you was wrong, and you could not do it. Which would be correct. As you are all so very, very different. What you have are the policies on what you should do and the controls in the standard that set out what is expected of you but for the Annex A controls it is now time for you to write down HOW you do it and evidence it.

The ISO27001 People





Operations Security Manual

The Operations Security Manual is just one way to skin the cat. Smaller businesses like to have all of the processes and procedures in one document for ease. Some like to have separate documents for each process. And some like a hybrid approach. All of these are valid. You are not being measured here on the structure of your documents. Set them out in a way that works best for you.

The Operations Manual has prepopulated headings for common processes. You can use it. Or not use it.

You would need to add / remove from that list of processes. Then you need to write the how for how your processes work.

Tip: The policy documents say what you do so working through the policies you can write the processes for how you do it. This is down to your business and is straightforward.

Write simple process steps of what you do do, not what you think someone wants to hear. You will be audited on what you say you do.

The auditor will read the process and then say - show me that you do this.





Always include at least one exceptions step in your processes. An exception step is what you do if something common does not work. Imaging if a HR background check came back and failed. What are the process steps if it fails? Often these simple exceptions are missed, and auditor will easily pick up on it.

Implement and Evidence Operational Processes

Once the process is written, then you need to technically implement it. This may or may not take the most time. Implement each process. Then you need to be able to evidence the process before you do the internal audit and definitely before the external certification audit.

Implement and evidence the operation of operational processes.

This is where you MAY benefit from getting some expert help to fast track and save you some money.



CHECKPOINT 9

At this check point you now have

- Documented our annex a / business and operational processes
- Put in place the appropriate measures and monitors to ensure and evidence those processes are operating effectively

The ISO27001 People



Conduct Your Internal Audit

You need to have conducted an internal audit before you go for certification. There are guidelines that the audit should be conducted by someone independent of the area being audited. Often people use outside resource to run their internal audit program. Either way, conduct your audit, share the results and minute with the management review team. Ideally you will have no nonconformities as you have done a clean build, and everything should be working tickety boo.

*01 - Information Security Manager Guides / **How to Conduct an Internal Audit***

Conduct your audit and follow the document: **How to Conduct an Internal Audit**

Guide: <https://hightable.io/how-to-conduct-an-iso-27001-internal-audit/>

The ISO27001 People



CHECKPOINT 10

At this check point you now have

- Had independent verification that the Information Security Management System is implemented and operating effectively
- Had independent verification that the Annex A / business process are implemented and operating effectively
- Produced audit reports

The ISO27001 People



Hold Your Management Review Meeting

It may well be that you have been running management review meetings all this time during the build phase. That is the ideal. That is great. Pat self on back. Now is time to hold the first review meeting that we will use to formalise and sign off the mandatory aspects of the Information Security Management System.

Management Review Meeting ONE

Create a folder for the management review meeting.

Create the management review meeting agenda from the template.

In the agenda, in the section - documents relevant to meeting - list ALL the documents in the management system - all the documents here.

Create an agenda item for 'Review and Sign Off ISMS documents'.

Share the location of the documents before the meeting with the management review team and ask them to review them before the meeting.

In the meeting walk through them / seek approval that everyone agrees with them, and they can be signed off.

This includes the audit results and incident and corrective actions log.

Be sure to include your measures and update the section on objectives.

You will clearly have everything for the first pass - policies, risk register, plans ... everything.

At the conclusion of this meeting, you set all documents to version 1, and you set the last review date to the date of this meeting, and you set the version control to include the update that the document was reviewed and signed off at the management review meeting (and you include the date of it).

This is a fair chunk of admin, copy and paste but it gets you set for a stable version 1 of the ISMS, and you are Stage 1 ready and ISO 27001 certification ready.



Document Version Control

	Last Modified	Last Modified By	Document Changes
0.1	30-Mar-2021	Stuart Barker	Document first created
1.0	23-Jun-2021	Stuart Barker	Document Review and Sign Off at Management Review Meeting 23 June 2021.

Minute the meeting and keep a record. Now is the time to update and complete your document tracker document.

You have a document called: **How to Conduct A Management Review Team Meeting**. Follow it.



CHECKPOINT 11

At this check point you now have

- Had a mandatory management review meeting and followed the structured agenda
- Used the management review meeting as a mechanism to sign off the information security management system and minuted the meeting and decisions made.

The ISO27001 People



Communicate Your New Information Security Management System

Once you have signed off and set the baseline version control you are going to publish the documents and communicate to the business that they exist and where they are. Update your communication plan to reflect this.

Operate Your Information Security Management System

The ISO27001 People



We will cover in another guide how to manage the information security management system day in day out but in basic terms you will operate the processes you have implemented. You will run your management review meetings, review your measures, conduct your internal audits based on the plan, run your incident management process, run your continual improvement process.

Prepare To Be Audited

These are some high-level considerations before you go for audit. The audit is down to the auditor auditing you. You get good ones and bad ones. It is the luck of the draw.

Consider when you know the auditor's name checking them out on LinkedIn to get a feel for what their background is. Whatever it is, as a rule, that is what they will go to town on come the audit. Do they have a software development background, get your software development house in tip top order. Do they have a GDPR background? Then you better be sure your Data Protection is top notch. Networking background? ... you get the idea.

Ensure all your documents are up to date, that the version control matches, that all documents have been updated to show as a minimum a review in the last 12 months.



Ensure your processes are operating as expected and even though you have done, and internal audit now is a good time to double check before the auditor comes. Remember the audit is show and tell, don't trip yourself up by not checking and doubling checking before they come.

Ensure that those being audited are aware that they answer the questions asked and do not offer up any additional information that may get you in hot water. An auditor likes to pick a thread and watch in unravel. Do not give them threads to pluck.

Ensure that close to the audit you once again communicate to everybody, especially those being audited.

Where the information security policies are

How they raise and incident

Who is responsible for information security and who they would go to

Check that the machines of those being audited are patched, have up to date antivirus. Check and clear download folders and trash / waste bins. Have clean desktops.

Now is a good time to go into key systems and check admin accounts. Yes, you have done it, but do it again. Is there anyone in there that has left? Are there any generic accounts that should not be there?



If you have an office walk the floor and make sure you meet your clear desk policy.

Lock confidential data away, tidy up, don't have things that could raise questions lying around.

Make sure that you meet the legal requirements you say you do. Here are common things an auditor will check

- The cookie policy on your website
- They will run tracker checks on your website and see your policy matches
- They will check data protection registers such as the ICO website to see you are registered
- They will check fire extinguishers to check they are checked and in date
- They may check things like PAT testing of devices
- If you have them, they will check printer areas for print outs left around
- If you have them, they will check confidential waste bins, make sure the waste is IN them
- They will check things that you think, and you are right, are not relevant. If it is a law or regulation, it is fair game.





There are more tips, but these are the most common. Remember, you are PAYING THEM to audit you. They do not want you to fail. As a rule. So be confident, you have got this.

The worst case is they raise some issues and give you time to fix and then issue the certificate.

You basically have to have nothing in place and not be doing any of this guide and toolkit to fail. You are doing it, so, be cool.

Conclusion

You have now completed the build of your information security management system. You have branded the pack and made it your own. You have included and recorded key information. You have created policies that say what you do, if not just yet how you to do it.

As you move forward towards certification you are now going to build on the information security management system.

As with everything you can reach out to us for ad hoc guidance, adhoc pre checking, adhoc taking the audit guidance – whatever you need. If you need help – ask. We bill in half day blocks. We are here for you.



**Good Luck. You've got
this.**

The ISO27001 People

