[Company] : Implementation Checklist

Classification: Internal

PRE IMPLEMENTATION PREPARATION

Session	Documents	What needs to be done	Guidance	WHO	WHEN?	Completed?
	LEARNING CONTEXT					
1	Get a copy of the ISO 27001 Standard	You need to purchase a copy of the actual standard.				NO
1	Everything you need to know to get started	Watch the video of common questions and background. Everything you need to know to get started.	Video: https://youtu.be/PKhTlpVI0KU			NO
1	ISO 27001 and Pack Orientation - ISO 27001 Gap Analysis and ISO 27001 Audit	Watch the video on pack orientation that covers Gap Analysis and Audit approaches	Video: https://youtu.be/SKgZskF4z9I			NO
1	The ISO 27001 Standard Walkthrough - Part 1	Watch the first video that walks you through the standard and what is required	Video: https://youtu.be/B8j0hvdRPho			NO
1	The ISO 27001 Standard Walkthrough - Part 2	Watch the second video that continues the walk through of the standard and what is required	Video: https://youtu.be/MSpKCTeBmeI			NO

BRAND YOUR DOCUMENTS

Session	Documents	What needs to be done	Guidance	WHO	WHEN?	Completed?
	ALL DOCUMENTS					
2	All documents	Brand your documents with your company name and logo	It can make sense to leave branding until the last stage before your version 1 release are there are header and footer elements that need to change and this can reduce the amount of times that you do it. It will depend on who is getting access to the documents, if it is a core small team this approach can work to save time. If you have a larger organisation and to show professional deployment then doing now and updating is the was to go.			NO

ASSIGN YOUR TEAM

Session	Documents	What needs to be done	Guidance	WHO	WHEN?	Completed	Reviewed, Approved and Minuted at Management Review Meeting?
	Information Security Management System						
2	Information Security Roles Assigned and Responsibilities	Work out who is doing what and complete the assigned roles document	Video: https://youtu.be/dLHZ_TNX_kQ Document: https://hightable.io/iso-27001-clause-5-3-organisational-roles-responsibilities-and-authorities/ Document: https://hightable.io/iso-27001-clause-7-1-resources-essential-guide/			NO	

2	Information Security Management System Document Tracker	The Information Security System Document Tracker is the list of documents that make up ISO 27001 (this list) and you need to allocate an owner to each one that is responsible for it and completing it.				NO	
2	ISMS Annex A Controls - Accountability Matrix	The ISMS Annex A Controls accountability matrix is the list of required controls that the business has to implement that is the annex to the standard. Having decided which control set you are being audited against, and ideally for both control sets, go through and add the name of the person that is going to implement and be responsible for the control.	Document: https://hightable.io/iso-27001-clause-7-1-resources-essential-guide/			NO	

DOCUMENT YOUR POLICIES

Session	Documents	What needs to be done		WHO	WHEN?	Completed	Reviewed, Approved and Minuted at Management Review Meeting?
	Policies						
2	IS 01 Information Security Policy	The policies are what good looks like. You are going to follow this guide: In basic terms, allocate the policy to the person that knows the area covered, get them to review it and change it as per the guide. Approve it at the management review meeting and communicate it to all staff seeking evidence that they have read it and accept it.	Video: https://www.youtube.com/watch?v=saSUOkf7ppE Document: _02 - Getting Started Guide - How to Deploy and Implement the Policies			NO	
2	IS 02 Access Control Policy					NO	
2	IS 03 Asset Management Policy					NO	
2	IS 04 Risk Management Policy					NO	
2	IS 05 Information Classification and Handling Policy					NO	
2	IS 06 Information Security Awareness and Training Policy					NO	
2	IS 07 Acceptable Use Policy					NO	
2	IS 08 Clear Desk and Clear Screen Policy					NO	
2	IS 09 Mobile and Teleworking Policy					NO	
2	IS 10 Business Continuity Policy					NO	
2	IS 11 Backup Policy					NO	
2	IS 12 Malware and Antivirus Policy					NO	
2	IS 13 Change Management Process					NO	
2	IS 14 Third Party Supplier Security Policy					NO	
2	IS 15 Continual Improvement Policy					NO	
2	IS 16 Logging and Monitoring Policy					NO	
2	IS 17 Network Security Management Policy					NO	
2	IS 18 Information Transfer Policy					NO	
2	IS 19 Secure Development Policy					NO	
2	IS 20 Physical and Environmental Security Policy					NO	
2	IS 21 Cryptographic Key Management Policy					NO	
2	IS 22 Cryptographic Control and Encryption Policy					NO	
2	IS 23 Document and Record Policy					NO	
2	IS 24 Significant Incident Policy and Collection of Evidence					NO	

2	IS 25 Patch Management Policy					NO	
2	HR and other Policies	There are other policies that you need to run your business. These are policies required by other disciplines such as HR and as such are outside of the scope of the toolkit being professions in their own right. Make sure you have copies of all business policies that you need, that they are marked up appropriately, reviewed and signed off. Examples can include Anti Bribery, Parental Leave, Grievance etc.				NO	

TRAIN EVERYONE

Session	Documents	What needs to be done	Guidance	WHO	WHEN?	Completed	Reviewed, Approved and Minuted at Management Review Meeting?
	Training and Awareness						
2	Get a training tool - not provided	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 pre built modules, have tests and quizzes built it 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.				NO	
2	1 The Governance Framework	This overview explains how the governance framework fits together and how ISO 27001 fits in. It forms part of awareness training that we would give when we start and engagement.	Video: https://youtu.be/PKhTIpVI0KU			NO	
2	2 Introduction to Information Security	This is a basic communication presentation. Complete the required sections and use it as part of your communications to the company. People need to know, especially for the audit, where are the policies, how to raise and incident, who is responsible for information security. They will also be asked when they were last trained and in what.				NO	

DOCUMENT WHO YOU ARE AND WHAT YOU HAVE

Session	Documents	What needs to be done	Guidance	WHO	WHEN?	Completed	Reviewed, Approved and Minuted at Management Review Meeting?
	Context of Organisation						
2	Organisation Overview	Complete the Organisation Overview.	Video: https://youtu.be/iwSr-LloQ6Y Document: https://hightable.io/iso-27001-clause-4-1-understanding-the-organisation-and-its-context/			NO	
2	Context of Organisation	Complete the Context of Organisation.	Video: https://youtu.be/asYMhvFw7-U 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/			NO	
2	Documented ISMS Scope	Define and document the scope of the information security management system	Video: https://youtu.be/5RXi_8INtgg Document: https://hightable.io/iso-27001-clause-4-3-determining-the-scope-of-the-information-security-management-system/			NO	
3	Legal and Contractual Requirements Register	With the help of legal counsel complete the legal and contractual requirements register.	Video: https://youtu.be/kxEh3OBPRUQ			NO	

3	Physical and Virtual Assets Register	Complete or have an asset register of every physical and virtual device that can process, store or transmit data.	Video: https://youtu.be/ScQyCcX_q6g			NO	
3	Statement of Applicability	Confirm with the certification body which control set you will be assessed with then complete the statement of applicability deciding which controls are applicable to you. It may be that you complete both versions, there is no harm in it.	Video: https://youtu.be/aqFYZ7GPRMg			NO	
3	Data Asset Register	Complete or have a data asset register for all data stores and data items that you have. Consider the use of a Data Protection ROPA.	Video: https://youtu.be/U17JzWO_UNY			NO	
3	Software License Assets Register	Complete the Sofware Licenses Assets Regsiter					
3	Third Party Supplier Register	Complete the supplier register for suppliers and if you have a massive list you can priorities the suppliers that are in scope for the certification to narrow the list down. This needs completing with no gaps and you need actual copies of contracts and copies of certifications if you rely on them (the ISO 27001 certificate)				NO	
3	Supplier Contracts	You need copies of in date supplier contracts that include information security clauses for the products or services you have bought from them,				NO	
3	Supplier Security Certificates	You need ISO 27001 certificates or similar for suppliers to show you have checked that they are doing the right thing for security. If you do not then you have a lot of work to do on supplier audits.				NO	

DOCUMENT YOUR INFORMATION SECURITY SYSTEM

Session	Documents	What needs to be done	Guidance	WHO	WHEN?	Completed	Reviewed, Approved and Minuted at Management Review Meeting?
	Information Security Management System						
3	The Information Security Management System	Complete the Information Security Management System Document	Video: https://youtu.be/xpqSsc2qOAg Document: https://hightable.io/iso-27001-clause-4-4-information-security-management-system/			NO	
3	Information Security Objectives	Complete the Information Security Objectives Document. You need to decide on the objectives for the information security management system.					
3	Information Security Manager Job Description	This is a reference document - no action needed other than review and know you have it				NO	
3	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.	Video: https://youtu.be/GjO3xtzUksM Document: https://hightable.io/iso-27001-clause-5-3-organisational-roles-responsibilities-and-authorities/ Document: https://hightable.io/iso-27001-clause-7-1-resources-essential-guide/			NO	
3	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.	Video: https://youtu.be/iqQ5w9IBIDg			NO	
3	Management Review Team Minutes - Template	These are the draft templated minutes. You will need to ensure that the objectives that you have set in the document 'Information Security Management System' are also contained in the Information Security Policy AND that you have them in the Management Review Team Meeting minutes template and all minutes you create.				NO	

3	Information Security Measures Report (you have to create this)	For the objectives you have defined you have decided what you are going to measure. It could be machine patching, machine antivirus, staff training - what ever you are measuring create a report that you can populate each month to track your measures.				NO	

CREATE YOUR PLANS

Session	Documents	What needs to be done	Guidance	WHO	WHEN?	Completed	Reviewed, Approved and Minuted at Management Review Meeting?
	Plans						
4	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 small audits each month or one / two large audits. Plan what is right for you and your business. Once planned ensure you follow the plan and conduct the audits.				NO	
4	ISMS Management Plan	The changes to the ISMS need to be evidenced as being managed and planned so you will complete the ISMS Management Plan that documents when you will perform routine updates, reviews and changes.					
4	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)	Document: https://hightable.io/iso-27001-clause-7-4-communication-essential-guide/			NO	

CONDUCT YOUR RISK REVIEW

Session	Documents	What needs to be done	Guidance	WHO	WHEN?	Completed	Reviewed, Approved and Minuted at Management Review Meeting?
	Risk Management			WHO	WHEN?		
4	Risk Review Meeting	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.				NO	
4	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	Document: https://hightable.io/iso-27001-risk-assessment-guide/ 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			NO	

IMPLEMENT YOUR OPERATIONAL PROCESSES

Session	Documents	What needs to be done	Guidance	WHO	WHEN?	Completed	Reviewed, Approved and Minuted at Management Review Meeting?
	Operational Processes						

4	Operations Manual	You need to write your operational processes. This is something that we cannot pre do for you as every business is different. The Operations Manual has pre populated headings for common processes so you 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 is the process steps if it fails? Often these simple exceptions are missed and auditor will easily pick up on it.				NO	
4	Implement and Evidence Operational Processes	Once the process is written, 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.				NO	

PLAN AND CONDUCT YOUR BUSINESS CONTINUITY

Completed	Documents	What needs to be done	Guidance	WHO	WHEN?	Completed	Reviewed, Approved and Minuted at Management Review Meeting?
	BPC and DR						
5	1. Business Impact Assessment	Document your systems, locations and teams and follow the guide to prioritise them.				NO	
5	2. Business Impact Analysis Exec Summary	Summaries your business impact assessment in an nice summary				NO	
5	3. Business Continuity Objectives and Strategy	Set the objectives and strategy for your business continuity				NO	
5	4. Business Continuity Plan	Create you business continuity plan and put in place disaster recovery documents				NO	
5	5. Business Continuity Incident Action Log	This is an operational template that you can use in the event of an incident. If you have online ticketing, help desk etc then you may not need this, just embed the contents into existing digital processes.				NO	
5	6. Post Incident Review Form	This is an operational template that you can use after an incident has occurred. You would always update the Incident and Corrective Action Log no matter what.				NO	
5	7. 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.				NO	
5	8. 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.				NO	

CONDUCT YOUR INTERNAL AUDIT

Completed	Documents Plans and Logs	What needs to be done	Guidance	WHO	WHEN?	Completed	Reviewed, Approved and Minuted at Management Review Meeting?
6	Audit Template ISO 27001 2013 and 2022 Version	Using the template and the step by step guide provided conduct your internal audits and follow the process.	Document: https://hightable.io/how-to-conduct-an-iso-27001-internal-audit/ Video: https://youtu.be/FnfCzTbLVdk			NO	
6	Audit Report - Template	Complete an Audit Report high level summary of the audit conducted with findings.	Document: How to Conduct an Internal Audit			NO	
6	Incident and Corrective Action Log	Update the incident and corrective action log and follow the continual improvement process as a result of the audit.	Document: How to Continual Improvement			NO	

HOLD YOUR MANAGEMENT REVIEW MEETING

Completed	Documents Management Review Meeting	What needs to be done	Guidance	WHO	WHEN?	Completed	Reviewed, Approved and Minuted at Management Review Meeting?
7	Management Review Meeting ONE	Create a folder for the management review meeting. Create the management review meeting agenda from the template. In the 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. Minute the meeting and keep a record. Update your document tracker document.	Document: How to Conduct a Management Review Team Meeting.docx			NO	

COMMUNICATE YOUR NEW INFORMATION SECURITY MANAGEMENT SYSTEM

Completed	Documents Information Security Management System	What needs to be done	Guidance	WHO	WHEN?	Completed	Reviewed, Approved and Minuted at Management Review Meeting?
7	The ISMS	Communicate as appropriate to the company that the new information security management system exists and where it is. Consider different communication methods and potentially targetted communications. Update your communocation plan and keep a record of it.				NO	