Key Requirements Checklist for Achieving ISO 9001 and ISO 27001 Certification

ISO 9001 and ISO 27001 share many of the same principles, with both focused on building strong management practices, managing risks, and driving continual improvement. ISO 9001 looks at quality across your organisation, while ISO 27001 is more focused on information security but the way you meet their requirements is often very similar. This checklist breaks down the key similarities whilst also highlighting the **differences between the two standards**.

British Assessment Bureau

AMTIVO

ISO 9001

		Complete?
1	Determine the **context** of the organisation, any **relevant interested parties** and the risks or **opportunities** relating to these.	☐
2	Define the **scope** of the Quality Management System (QMS) and the certification.	☐
3	Create documented **processes** that describe the organisation's operations, including any inputs, outputs and controls to ensure processes achieve their intended outcomes.	☐
4	Ensure senior management demonstrate **leadership**, provide sufficient resources and assign clear **responsibilities** across the organisation.	☐
5	Establish and communicate a **Quality Policy.**	☐
6	Establish and communicate measurable **quality objectives.**	☐
7	Control any **changes** to the QMS to ensure they are carefully planned before implementation.	☐
8	Establish a means of **document control** to ensure that only correct versions are in use.	☐
9	Identify any **infrastructure** and **equipment** used and establish a **maintenance/calibration programme**.	☐
10	Record what **skills, competencies** and **organisational knowledge** are required for each employee and how those have been obtained.	☐
11	Ensure product/service supply processes enable a **consistent product/service** to be delivered in accordance with **customer requirements.**	☐
12	Determine controls on **externally provided processes, products and services** to enable a consistent product/service to be delivered in accordance with customer requirements.	☐
13	Obtain **customer feedback.**	☐
14	Conduct **monitoring and measurement** to demonstrate the effective operation of processes.	☐
15	Conduct an **internal audit** and create an internal audit plan.	☐
16	Hold a **management review**, review key areas of the management system, record decisions, conclusions and actions agreed.	☐
17	Demonstrate how the QMS has been subject to **continual improvement.**	☐
18	Undergo an **external certification assessment** by an accredited certification body.	☐

ISO 27001

		Complete?
1	Determine the **context** of the organisation, any **relevant interested parties**, what elements of the **ISMS** will inform those interested parties and the risks or **opportunities** relating to these.	☐
2	Define the **scope** of the Information Security Management System (ISMS) and the certification.	☐
3	Create documented **processes** that describe the organisation's operations, including any inputs, outputs and controls to ensure processes achieve their intended outcomes.	☐
4	Ensure senior management demonstrate **leadership**, provide sufficient resources and assign clear **responsibilities** across the organisation.	☐
5	Establish and communicate an **Information Security Policy.**	☐
6	Establish and communicate measurable **information security objectives.**	☐
7	Control any **changes** to the ISMS to ensure they are carefully planned before implementation.	☐
8	Establish a means of **document control** to ensure that only correct versions are in use.	☐
9	Record what **skills and competencies** are required for each employee and how those have been obtained.	☐
10	Identify relevant **information assets**, assess their significance, their impacts on **CIA (confidentiality, integrity and availability)** and record the assessment on an **Asset and Risk Assessment Register**.	☐
11	Review the **information security controls** in place against the required **best practice controls** detailed in Annex A.	☐
12	Establish **controls** required to manage information security and achieve the information security objectives.	☐
13	Develop and implement a **comprehensive risk treatment plan** that outlines the actions required to address, manage, and mitigate the risks identified during the risk assessment process.	☐
14	Conduct **monitoring and measurement** to demonstrate the effective operation of processes.	☐
15	Conduct an **internal audit** and create an internal audit plan.	☐
16	Hold a **management review**, review key areas of the management system, record decisions, conclusions and actions agreed.	☐
17	Demonstrate how the ISMS has been subject to **continual improvement.**	☐
18	Undergo an **external certification assessment** by an accredited certification body.	☐