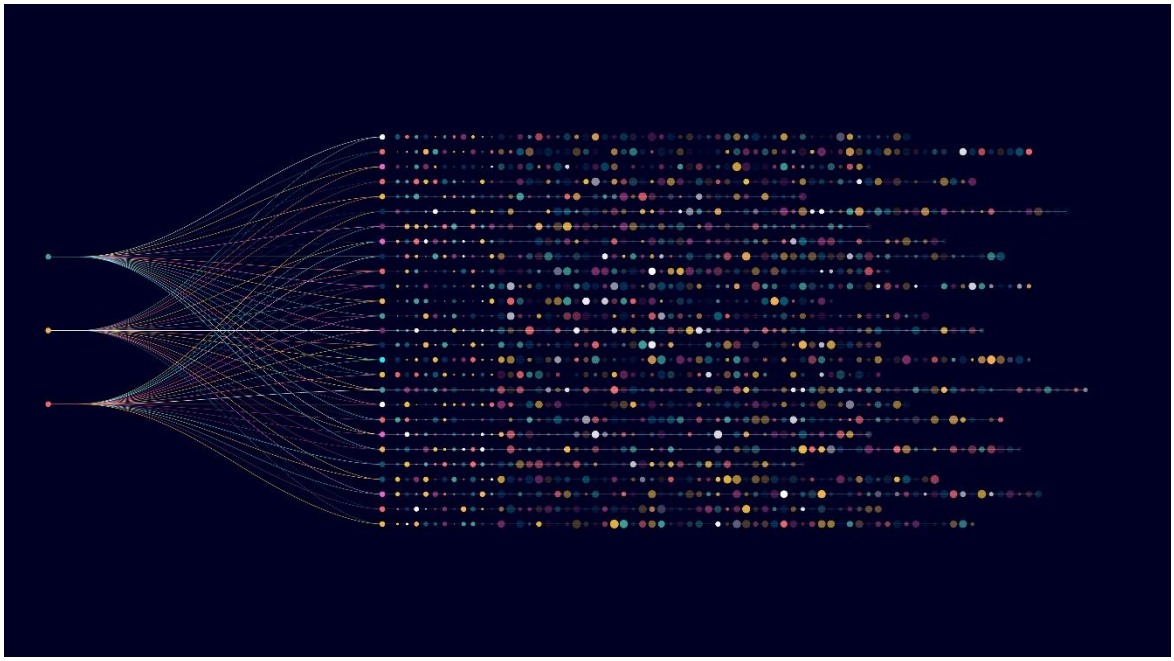
ISO22301:2019 Overview and Guidance

Introduction

The ISO 22301 standard details the requirements for a Business Continuity Management System (BCMS) and the aim of this standard is to help organisations review and identify threats to their ongoing operations and to prepare and test arrangements to ensure business can continue or recover from these threats, whether internal or external, with as little impact to ongoing operations as possible.

The current version of the standard, ISO 22301:2019, is structured following Annex SL and therefore the clauses are very similar to the structure of ISO 9001 and other Annex SL standards. The standard requires a clearly defined organisational structure with roles and responsibilities defined with the involvement and commitment from top management.



Business Continuity Management

A business impact analysis and risk assessment is required to demonstrate that risks have been considered and evaluated and the impact they could have on normal operational activities are considered.

Business continuity strategies and solutions then need to be prepared to address the risks to normal business operations. A programme of testing and checking is also required to demonstrate that all risks have been identified and that adequate prevention and recovery systems are in place and effective.

Business impact assessment should consider all business-critical functions and consideration of what unplanned events / disruptive incidents could affect these critical functions.

Meeting the requirements of this standard requires that an effective Business Continuity Management System (BCMS) has been prepared and that adequate business continuity plans and arrangements are in place with evidence that these plans are reviewed and tested on an ongoing basis. Business Continuity objectives should also be set and monitored.

There are quite specific documentation requirements for this standard including business impact analysis and risk assessments.

Two of the key requirements of the standard are for companies to have a **business impact analysis** and a **risk assessment** in place. The business impact analysis required consideration of the types of **impact** that certain events could have on operational activities – and pair those with resources and dependencies which are required to support those functions.

Once such factors have been identified – the business shall identify then select **continuity strategies** which consider all options (before / during / after) disruption. The **risk assessment** is to assist with assessing the risks of disruption to the organisations activities and prioritise the most major risks – pairing those with solutions.

Procedures and Testing

As well as identification of risks and continuity strategies – they are also requirements to develop **procedures, plans** and to also **test the responses** to any disruptive events. Procedures are required to inform staff of the steps to be taken during a disruption and to ensure that the correct roles and responsibilities have been assigned in terms of what must be done when normal systems are disrupted. Plans are required and these must include the purpose, scope and objectives as well as responsible persons within the organisation – procedures may be referenced or included as part of these plans.

Exercise programme – requirements that arrangements for business continuity are tested. Tests must be conducted that are consistent with the objectives for continuity that are set and are able to validate that continuity plans, procedures and staff are all adequate.

Key areas that organisations must consider to comply with this standard are as follows:

- Business continuity policy and other key documentation
- Actions to address risks and opportunities
- Business continuity objectives and planning to achieve them

- Business impact analysis and risk assessment
- Business continuity strategy
- Business continuity plans and procedures
- Evaluation of business continuity documentation and capabilities

ISO22301:2019 Certification Audit

During an audit – the auditor(s) will be looking for objective evidence that each clause in the standard has been met and complied with.

As well as reviewing all the relevant clauses there are various other things you can prepare and have in place prior to the audit;

- Completed and up-to-date management review
- Completed internal audit(s) relating to business continuity
- Documented information regarding business continuity arrangements
- Evidence of roles clearly identified
- Evidence of staff awareness of business continuity
- Business continuity objectives and planning to achieve them
- Business impact analysis and risk assessment
- Business continuity strategy
- Business continuity plans and procedures

Presenting evidence during the audit

For guidance on the audit process and how to prepare for the audit and an overview of the audit plan and the certification audit process please review the **Certification Audit Guidance** which is available **online here**.

In an audit involving a site visit, the auditor will likely just view evidence in person, whilst asking questions, a site tour may also be conducted. For remote audits it is often requested that photographs / videos are submitted as evidence.

Further support

- Management system documentation & resources: **isomanaged.com/alphazdocuments**
- Remote support: **isomanaged.com/iso-consultancy-support**
- ISO Consultancy: **isoassured.co.uk/iso-consultancy**