

Legislation Outlook

February 2022

This monthly legislation briefing is a **supplement** to your Activ Comply service to help you to **plan ahead** for maintenance of your ISO 14001, ISO 45001, ISO 50001 and ISO 27001 systems. In addition to giving you advance warning about important legislation that will affect your compliance with the standards, we'll provide news, newly-published guidance and government consultations that you might find useful, as well as any other significant legislation beyond the scope of the standards listed that will potentially impact your organisation. Unlike other services, we only report items of value: we don't waste your time on items such as an increase in administrative fees or changes that only affect enforcement agencies.

When legislative changes are announced with short notice (<1 month) they are not reported here. All changes are automatically delivered direct into your [Activ Comply](#) system as they come into effect so you can be confident that you are always 100% up to date.

This month, we see the publication of environmental legislation affecting our larger clients, in addition to some interesting ISO/IEC 27002-related news.

Upcoming Standard-Related Legislation

ISO 14001

Companies (Strategic Report) (Climate-related Financial Disclosure) Regulations 2022

These [Regulations](#) come into force on 6 April 2022 to require certain companies to provide climate-related financial disclosures in their strategic report. The following information will need to be included in the strategic reports of affected companies:

- a description of the company's governance arrangements in relation to assessing and managing climate-related risks and opportunities;
- a description of how the company identifies, assesses, and manages climate-related risks and opportunities;
- a description of how processes for identifying, assessing, and managing climate-related risks are integrated into the company's overall risk management process;
- a description of the principal climate-related risks and opportunities arising in connection with the company's operations, and the time periods by reference to which those risks and opportunities are assessed;
- a description of the actual and potential impacts of the principal climate-related risks and opportunities on the company's business model and strategy;
- an analysis of the resilience of the company's business model and strategy, taking into consideration different climate-related scenarios;
- a description of the targets used by the company to manage climate-related risks and to realise climate-related opportunities, and of performance against those targets; and
- a description of the key performance indicators used to assess the progress against the targets that are used to manage climate-related risks and realise climate-related opportunities, and of the calculations on which those key performance indicators are based.

The requirement applies to the following companies, provided they have more than 500 employees:

- traded companies (those with shares that carry rights to vote at general meetings, and are trading on a UK regulated market or an EU regulated market);
- banking companies (those with permission under Part 4A of the Financial Services and Markets Act 2000 to accept deposits);
- authorised insurance companies (those with permission under Part 4A of the Financial Services and Markets Act 2000 to effect or carry out contracts of insurance);
- companies carrying out insurance market activity (i.e. a regulated activity relating to contracts of insurance written at Lloyd's);
- companies which have securities admitted to trading on the Alternative Investment Market; and
- high turnover companies (those which do not fall within another category but which have a turnover of more than £500 million per annum).

Limited Liability Partnerships (Climate-related Financial Disclosure) Regulations 2022

These [Regulations](#) come into force on 6 April 2022 to require certain limited liability partnerships (LLPs) to provide climate-related financial disclosures in their strategic report or their energy and carbon report. The required disclosures are identical to those set out in the Companies (Strategic Report) (Climate-related Financial Disclosure) Regulations 2022 (see above).

The requirement applies to the following LLPs, provided they have more than 500 employees:

- traded LLPs (those whose transferable securities are trading on a UK regulated market);
- banking LLPs (those with permission under Part 4 of the Financial Services and Markets Act 2000 to accept deposits); and
- LLPs with an annual turnover of more than £500 million per annum.

ISO 45001

Mines (Amendment) Regulations (Northern Ireland) 2022

These [Regulations](#) come into force on 21 March 2022 and amend the Mines Regulations (Northern Ireland) 2016 to reduce the Workplace Exposure Limit (WEL) for respirable crystalline silica below ground in coal mines from 0.3mg/m³ to 0.1mg/m³.

Remember: short-notice changes to legislation are not reported in this briefing; all changes are delivered direct into your Activ Comply system as they come into effect.

ISO 9001 Internal Auditor Online Training Course (2 days)

February 21/22, 2022



[Learn More](#)



News

ISO 27002 Updated

A new edition of ISO 27002 has been approved. The third edition, expected to be published either later this month or in early March, is titled 'ISO/IEC 27002 Information security, cybersecurity and privacy protection – Information security controls', and includes significant changes to the previous edition.

The standard has been significantly reorganised, with the 14 clauses in the second edition being reduced to just four – organisational controls, people controls, physical controls and technological controls.

The controls themselves have also seen extensive changes, with 11 new controls being introduced to align with current technology and best practice. The new controls are shown in the table below:

Organisational Controls	Physical Controls	Technological Controls
Threat intelligence	Physical security monitoring	Configuration management
Information security for use of cloud services		Information deletion
ICT readiness for business continuity		Data masking
		Data leakage prevention
		Monitoring activities
		Web filtering
		Secure coding

There are also important changes within the existing controls, with around half of the old controls being combined with others where they were inseparable in practice or closely related., resulting in 24 'merged controls'. The remaining controls have all been retained from the previous edition, but now contain up-to-date guidance. In all, the new standard contains 93 controls, as opposed to the previous edition's 114, with the aim of this reduction being to simplify implementation.

Another notable change is the introduction of 'Attributes'. Each control has five attributes associated with it, and each control's attributes have been assigned a particular 'value' from a predetermined selection, as set out in the table below:

Attributes	Values
Control type	Preventative, detective, corrective
Information security properties	Confidentiality, integrity, availability
Cybersecurity concept	Identify, protect, detect, respond, recover
Operational capabilities	Aligned to clauses in the second edition
Security domains	Governance and ecosystem, protection, defence, resilience

The use of these attributes is not mandatory, they have been designed as a tool to help organisations filter and organise the controls to suit their particular context.

There is likely to be a two year transition period following publication of the new standard, but this has yet to be confirmed, with Annex A of ISO/IEC 27001 being updated to reflect these changes in due course.

ISO 13485 Awareness Online Training Course

February 15, 2022



[Learn More](#)



Consultations

Cyber Resilience

The Department for Digital, Culture, Media & Sport has issued a [consultation](#) setting out new proposed laws to improve the cyber resilience of organisations which are important to the UK economy, such as managed IT providers. The proposals build on the current legal requirements in the Network and Information Systems (NIS) Regulations 2018 by looking to bring additional critical providers of digital services into the NIS regulatory framework and future-proofing the NIS Regulations so that they can adapt to potential changes in threat and technological developments.

The consultation closes on 10 April 2022.

Mandatory Digital Waste Tracking

The Department for Environment, Food & Rural Affairs has issued a [consultation](#) seeking views on proposals for the implementation of a mandatory digital waste tracking service across the UK. The proposals include:

- what waste will be tracked;
- what information should be recorded;
- when this information should be recorded;
- different ways to record the information;
- what the enforcement consequences might be if the information isn't recorded as required; and
- charges for the operation and maintenance of the waste tracking service.

The consultation closes on 15 April 2022.

Waste Carrier, Broker and Dealer System Reform

The Department for Environment, Food & Rural Affairs has issued a [consultation](#) seeking views on proposals to improve the waste carrier, broker and dealer system in England. The plans include:

- moving from a registration to a permit-based system;
- enhancing background checks needed to operate as a waste carrier, broker or dealer;
- introducing a technical competence requirement for waste carriers, brokers and dealers;
- making it easier for regulators to enforce against non-compliant operators; and
- making it harder for un-registered operators to find work.

The consultation closes on 15 April 2022.

[Invite](#) someone else to subscribe to this Briefing



Like to know more?

0333 301 9003
legal@myactiv.co.uk
www.activcomply.co.uk

Coming Soon: Audit Manager
/ Watch the Video / etc

Text here