Cybersecurity

ISO/IEC 27001:2022

Checklist

LRQA

Use our checklist and find out if you are sufficiently prepared for certification.

This ISO 27001:2022 compliance checklist is a valuable tool to help you assess your Information Security Management System (ISMS) and pinpoint any areas that may require attention before your certification or transition audit. The checklist is organised in accordance with ISO 27001:2022 requirements and covers the following key areas:

- **The context of your organisation**
- **Needs and expectations of interested parties**
- **Leadership and commitment**
- **Risks and opportunities**
- **Risk treatment**

By utilising this checklist, you can easily select a response and provide comments for each requirement, which will assist you in gaining a comprehensive understanding of all aspects of your ISMS.

LRQA

Section 01
The context of your organisation

ISO 27001:2022, which follows the Annex SL High Level Structure, emphasises the importance of conducting a thorough analysis of your organisation's context before designing and implementing an ISMS. This analysis is crucial in determining the specific needs and requirements of your organisation and, ultimately, in ensuring the effectiveness of your ISMS. By taking the time to fully understand the context in which your business operates, you can create a more tailored and effective ISMS that addresses your unique risks and opportunities.

You can use this interactive checklist to mark any requirements you've completed and add any relevant comments.

- [ ] You have identified the external factors that can influence your ISMS and your ability to achieve the desired results.
- [ ] You have identified the internal factors that can influence your ISMS and your ability to achieve the desired results.
- [ ] You have considered the contextual factors (internal and external) when defining and documenting the scope, and when planning your ISMS.
- [ ] Changes to contextual factors are reviewed periodically during the Management Review.

Section 02
Needs and expectations of interested parties

According to ISO 27001:2022, an ISMS must take into account the needs and expectations of interested parties and how they can impact the desired outcomes. This is essential for determining the scope of the system, from operational to strategic, and aligning it with the organisation's business objectives. The organisation should assess the understanding and expectations of all parties under their control and involve them in the system's effective operation.

- [ ] You have identified the needs and expectations of all those under the organisation's control, including other interested parties, and have identified which of these could be considered legal requirements.
- [ ] You have considered the needs and expectations of the interested parties when planning your ISMS and defining and documenting the scope.
- [ ] Those under the organisation's control were consulted when you determined the needs and expectations of the interested parties, and these needs and expectations are periodically reviewed by management.
- [ ] You have identified the interested parties, in addition to those under the organisation's control, who can influence your ISMS and your ability to achieve the desired outcome.

Section 03
Leadership and commitment

ISO 27001:2022 includes specific requirements around how top management should demonstrate leadership and the role of employees in the ISMS. Senior managers can assign certain tasks while still being ultimately accountable. Their active and proactive participation helps to align the ISMS with the company's business, ensuring consistency between the information security policy, business objectives, and corporate strategy.

- [ ] Senior managers are directly involved in promoting the ISMS by communicating the importance of complying with the system, and supporting the company functions, so they contribute to the system's effectiveness.

- [ ] The Information security policy includes commitments to meet information security requirements and continually improve the ISMS, as well as information security objectives (or a framework for setting them).

- [ ] You have defined, communicated, and documented the authorities and responsibilities of the relevant roles within the ISMS.

Section 04
Risks and opportunities

ISO 27001:2022 mandates that the ISMS be designed to effectively address both risks and opportunities related to the organisation's context and interested parties, within the scope of the system. This means that the organisation must assess risks and opportunities in terms of whether the management system can achieve its goals and objectives. This assessment should go beyond just information security threats and compliance with data protection regulations, and should result in a plan to manage unacceptable risks and capitalise on identified opportunities. The effectiveness of these actions should be reviewed regularly.

- [ ] You have determined the risks and opportunities related to the expected outcomes of the ISMS.
- [ ] When identifying risks and opportunities, you have considered the organisation's overall business strategy and objectives, internal and external contextual factors, needs and expectations of the interested parties, the lifecycle of information within the organisation and the scope of the ISMS.
- [ ] Risks and opportunities are considered in the context of defining information security objectives, planning the management system, determining needs for monitoring and measuring, and management reviews.

Section 05
Risk Treatment

ISO 27001:2022 requires an organisation to establish and implement a risk treatment plan. This plan should be effective in selecting the appropriate treatment methods and monitoring their effectiveness. To ensure the proper selection of controls, they should be compared against the best practices outlined in Annex A of ISO 27001:2022. The risk treatment plan should be approved and accepted by the identified risk owners.

- [ ] You have put in place a process to select appropriate risk treatment options.
- [ ] You have put in place processes to determine the organisational, people, physical and technical controls necessary to implement the treatment options.
- [ ] You have compared the controls to Annex A and verified that no controls are missing.
- [ ] You have produced a Statement of Applicability, justifying the inclusion and exclusion of controls.
- [ ] You have gained the permission of risk owners for the risk treatment plan.

Our ISO 27001 training and audit services

Training

Build your knowledge of ISO 27001 with a range of courses designed for different experience levels – delivered via multiple learning styles.

View courses

Gap analysis

An optional service where one of our expert auditors will help you identify any critical, high-risk, or weak areas of your system prior to your transition audit.

Certification and transition assessment

We assess your ISMS in line with the requirements of ISO 27001:2022 – with a particular focus on Annex A controls and how they impact your system.

Integrated assessments

If you have implemented multiple management systems, you could benefit from an integrated audit and surveillance programme, which is more efficient and cost-effective.

Why choose LRQA?

Local and global

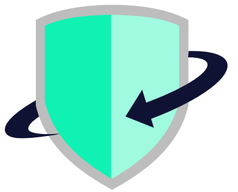
We're everywhere you are. With more than 300 highly qualified auditors and 250 dedicated cybersecurity specialists worldwide, we can provide a local service with a globally consistent dedication to excellence. Our people are technical experts with in-depth knowledge of information and cyber security risks, challenges, standards, regulations and frameworks.

Flexible delivery

In most cases, all our ISO 27001 training and certification services can be delivered on-site or remotely using safe and secure technology. If you opt for our remote delivery methods, you'll receive the same high-quality service with several added benefits, including flexibility, fast delivery and access to global expertise.

History of firsts

We were the first to receive UKAS accreditation to deliver certification services for a range of standards across the globe. We continue to be instrumental in developing a variety of specific standards and frameworks across different sectors.



Beyond compliance

Our award-winning cybersecurity experts help you stay one step ahead of sophisticated cyber threats with advanced services that give a first line of defence and response to all threats and vulnerabilities.

Working with you to target every aspect of cybersecurity

Our deep experience in assurance, combined with award-winning cybersecurity services and threat-led intelligence enable us to deliver bespoke insights into – and protection from – the unique threats facing your business. Keeping you one step ahead of cyber risk, today tomorrow and beyond.

We provide audit, training and certification services against the world's leading international standards and schemes, complemented by our advanced cybersecurity services. We work collaboratively with your business – helping you to identify the specific threats you face and build strategies to mitigate them. We work with you to certify your systems, identify vulnerabilities and help prevent attacks and incidents that could impact your brand integrity, finances and operations.

Information security

Our compliance and certification services help you protect business-critical information and demonstrate internationally recognised best practices.

ISO 27001, ISO 27701, ISO 27017, ISO 27018, CSA STAR

Find out more >

Operational resilience

Be ready to prevent, respond and recover from disruption with our certification, training and governance, risk and compliance services.

ISO 22301, ISO 20000-1, Cyber Essentials

Find out more >

Cyber threat protection

Stay one step ahead of cyber threats, with tailored solutions that provide a first line of defence and response to all types of cyber attacks.

Security Assurance Testing, Managed Security Services, Threat Intelligence, Incident Response

Find out more >

Discover ThreatWatcher

LRQA's ThreatWatcher service provides a managed assessment using advanced reconnaissance and analytics to identify previously unknown threats that could be used in a cyberattack. Security intelligence from ThreatWatcher can highlight weaknesses in user education and help to identify digital attack surface like never before. The service is delivered by our team of highly skilled and experienced Threat Intelligence analysts.

ThreatWatcher and ISO 27001:2022

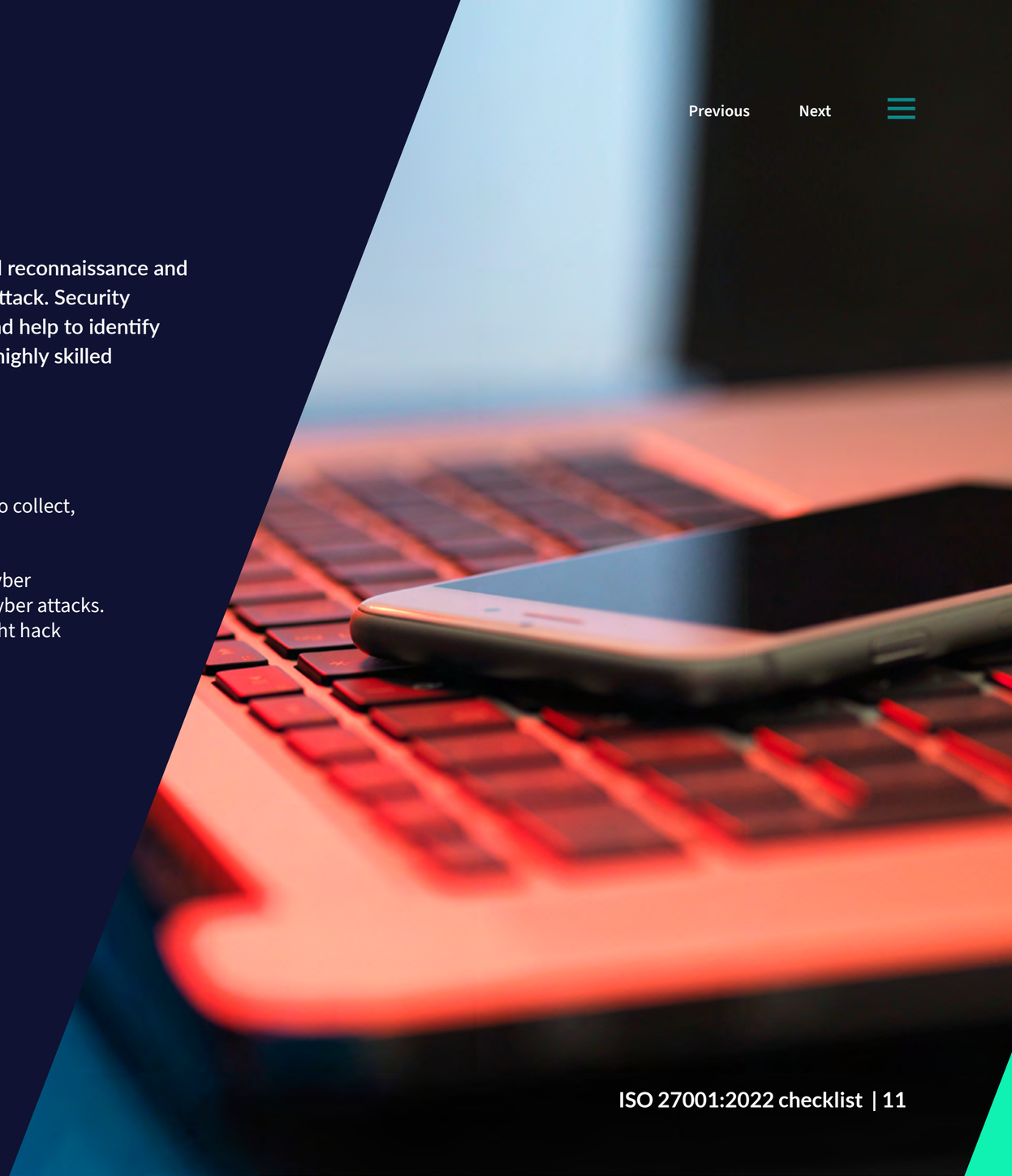
One of the organisational controls, A.5.7 Threat intelligence, requires organisations to collect, analyse and produce threat intelligence regarding information security threats.

The goal of this control is to provide organisations with a deeper understanding of cyber threats by collecting, analysing, and contextualising data about current and future cyber attacks. The control is also designed to help organisations understand how threat actors might hack them and inform companies about what types of data attackers are seeking.

ThreatWatcher provides these exact solutions, helping organisations demonstrate compliance with the new threat intelligence control.

Contact our experts for more information about ThreatWatcher and other LRQA cybersecurity services that can help demonstrate compliance with the requirements and controls introduced in ISO 27001:2022.

Find out more →



About LRQA:

LRQA is the leading global assurance partner, bringing together decades of unrivalled expertise in assessment, advisory, inspection and cybersecurity services.

Our solutions-based partnerships are supported by data-driven insights that help our clients solve their biggest business challenges. Operating in more than 150 countries with a team of more than 5,000 people, LRQA's award-winning compliance, supply chain, cybersecurity and ESG specialists help more than 61,000 clients across almost every sector to anticipate, mitigate and manage risk wherever they operate.

In everything we do, we are committed to shaping a better future for our people, our clients, our communities and our planet.

Get in touch

Visit **www.lrqa.com** for more information or email **cybersolutions@lrqa.com**

LRQA
460 Alexandra Road
mTower #15-01
Singapore 119963