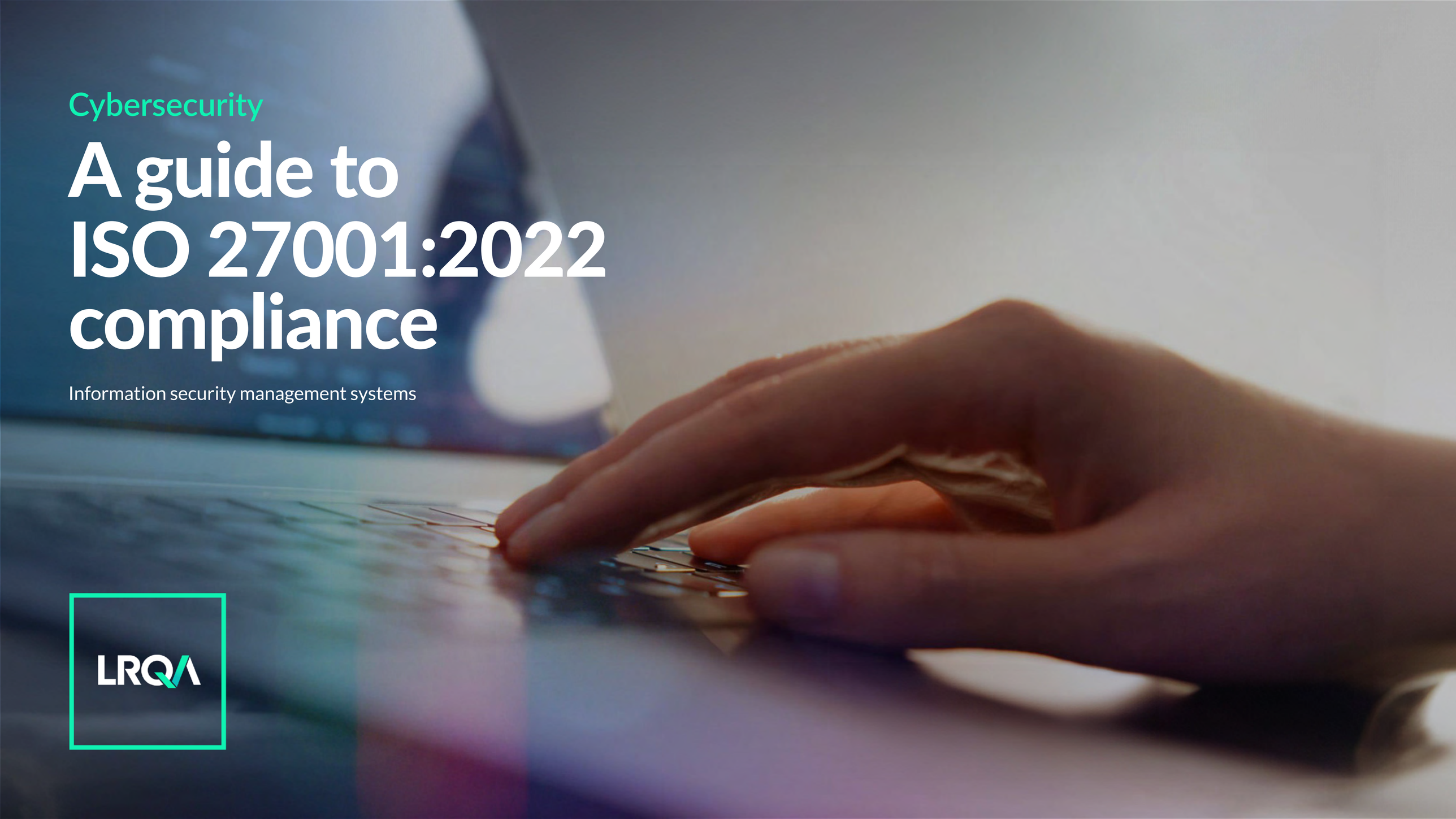


Cybersecurity

A guide to ISO 27001:2022 compliance

Information security management systems

LRQA

Contents

What is ISO 27001? 3

Introducing ISO 27001:2022 4

Implementing ISO 27001 6

Our ISO 27001 training and audit services 9

Why choose LRQA? 10

Working with you to target every aspect of cybersecurity 11

What is ISO 27001?

ISO/IEC 27001 is the international standard that specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS).

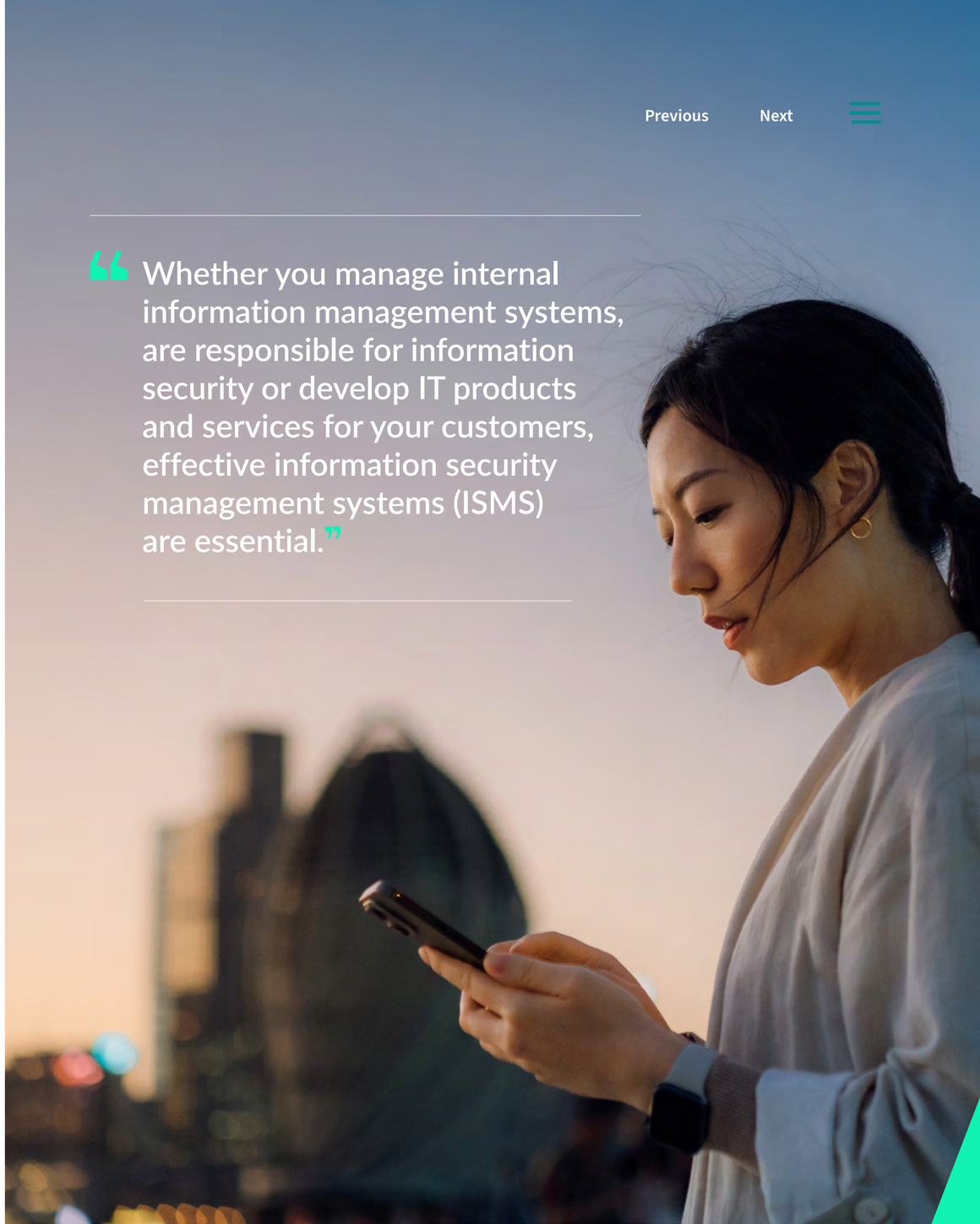
For any organisation – regardless of size or sector - ISO 27001 provides a strong foundation for a comprehensive information and cybersecurity strategy. The standard outlines a best practice ISMS framework to mitigate risks and safeguard business-critical data through identification, analysis and actionable controls.

Whether you manage internal information management systems, are responsible for information security or develop IT products and services for your customers - effective information security management systems are essential. Accredited ISO 27001 certification demonstrates that you have the processes and controls in place to defend your organisation's information – and that of your customers – against an increasingly complex threat landscape.

In addition to the normal commercial need to protect confidential information – such as intellectual property and pricing information – there are recent events in the regulatory and corporate governance fields that have placed ever more demanding requirements on the integrity of information.

An ISO 27001-compliant ISMS certified by LRQA gives you an independent and unbiased view regarding the appropriateness and effectiveness of your ISMS.

“Whether you manage internal information management systems, are responsible for information security or develop IT products and services for your customers, effective information security management systems (ISMS) are essential.”



Introducing ISO 27001:2022

Why was ISO 27001 updated?

In February 2022, ISO 27002:2022 – the standard which provides the best practice controls that organisations can implement to improve security – was updated.

A new version of ISO 27001 was also required to align the two standards. As a result, ISO 27001:2022 was published on 25 October 2022, and organisations with existing certification have until October 2025 to transition to the new version.

What is new in ISO 27001:2022?

The new version of the standard features the controls outlined by ISO 27002:2022 – which can be found in Annex A. This is the most significant change, and organisations need to revisit their risk assessment to determine whether updates or new risk treatments need to be implemented.

Annex A has now been restructured, featuring 93 controls instead of 114, split between 4 different themes:

- Organisational
- People
- Physical
- Technological

56 controls from the previous version have been merged into 24 in ISO 27001:2022, with 11 new controls added. On the surface, there is little change when comparing clauses 0-10 of the 2013 and 2022 versions of the standard. However, there have been changes to the structure, terminology and ordering of words that could impact how it is interpreted.

There are now **93** controls instead of **114**

In total there are **11** new controls

56 controls from ISO 27001:2013 have now been merged into 24 controls in ISO 27001:2022

Most controls are subject to some form of text change which could impact how the standard is interpreted and implemented

Controls are now split across four ‘new’ themes

Organisational	People	Physical	Technical
- 28 merged	- 2 merged	- 5 merged	- 21 merged
- 3 new	- 0 new	- 1 new	- 7 new

Introducing ISO 27001:2022

What's the impact on organisations with an ISO 27001:2013 certified ISMS?

Organisations with existing certification will have three years from the publication of ISO 27001:2022 to complete their transition – meaning it can take place no later than 31 October 2025.

If you're an existing LRQA client, you can now book your dedicated transition assessment, where one of our expert auditors will review your system against the requirements of ISO 27001:2022.

New organisation's can no longer be certified to ISO/IEC 27001:2013.

All certificate renewal audits to ISO/IEC 27001:2013 must be combined with a transition audit to move to the new standard.

All ISO/IEC 27001:2013 certificates must complete transition to the new standard before 31 October 2025 to avoid withdrawal of certificate.

If you seek certification against ISO 27001:2022, LRQA offers training and certification services delivered online or in person by information security experts. We work closely with you to meet your organisation's unique requirements, supporting you at every stage of your certification journey.

Implementing ISO 27001

ISO 27001 provides an ISMS framework for implementing best practices and principles using the Plan-Do-Check-Act (PDCA) cycle and management system processes covering:

Awareness: Participants should be aware of the need to secure information systems and networks.

Responsibility: All participants are responsible for the security of information systems and networks.

Response: Participants should act in a timely and cooperative manner to prevent, detect and respond to security incidents.

Risk assessment: Participants should conduct risk assessments.

Security design and implementation: Participants should incorporate security as an essential element of information systems and networks.

Security management: Participants should adopt a comprehensive approach to security management.

Reassessment: Participants should review and reassess the security of information systems and networks.

Adapted from the OECD Guidelines on Digital Security Risk Management

Getting started

Whatever the current state of your organisation, the starting point for implementing an ISMS is to obtain management commitment and support.

There is a requirement for the motivation and direction to come from top management. They must be actively engaged in ensuring the direction of the ISMS and its compatibility with your organisation's strategy, as well as owning key aspects such as the policy and objectives.

Planning for success

Like any project you take on, success is more likely if you develop a meaningful and realistic plan, measure performance against the plan and then are prepared to change it in the event of unforeseen circumstances.

The plan should recognise that developing the management system will require time, effort and adequate resources. Overall responsibility for information security lies with top management and often the IT department. Still, information security has a wider impact than just IT systems, including personnel, security, physical security and legal compliance.

ISO 27001 is aligned with ISO 9001:2015 – so if you already have a certified quality management system, this will provide a strong foundation for your ISMS. We strongly recommend attending an LRQA training course, where you can discuss information security issues with other delegates and your tutor.

Implementing ISO 27001

Understanding the standard

It is important that you familiarise yourself with the standard, this includes understanding the criteria you must meet. This will influence the overall structure of your ISMS and associated documentation.

The standard is in two parts:

- ISO 27002 is a reference document that describes security controls that may be selected and implemented to manage specific risks to information security.
- ISO 27001 is the management system specification that defines the requirements you need to address to implement an ISMS. Your certification body will audit your system in line with ISO 27001 during your certification audit.

The specification includes the common elements of all management systems; policy, leadership, planning, operation, management review and improvement. It also contains a section specifically aimed at identifying risks to your information and the selection of suitable controls and checks (Annex A).

Management processes

Management processes are critical to the effective implementation of an ISMS. If your organisation already operates an ISO 9001:2015 management system, these will be familiar to you. If this is the case, the most efficient way forward is often to integrate the information security requirements into your existing management system. If you are implementing these processes for the first time, consider the overall intent of these management requirements.

Top management are ultimately responsible for the effectiveness of the management system – obtaining their buy-in is crucial, and adequate resources should be allocated to the development, implementation and monitoring of the ISMS.

- Internal audits identify opportunities for improvement and verify that the management system is operating as intended.
- Management reviews allow top management to assess and understand how well the management system operates and supports the business.

Define the scope

It is essential that the logical and geographical scope of the ISMS is accurately defined so that the boundaries of your ISMS and security responsibilities can be identified. The scope should identify the people, places and information covered by the ISMS.

Once you have defined and documented the scope, the information assets covered by can be identified, along with their value and owners.

ISMS policy

The requirements relating to the ISMS policy are addressed in both ISO 27001:2022 (A.5.1) and ISO 27002. There are references to the policy in other requirements of ISO 27001 and in Annex A, which indicates what the policy should contain. For instance, the ISMS objectives must be consistent with the ISMS policy. Other policies will be required to meet certain control objectives.

Implementing ISO 27001

Risk assessment and risk management

The risk assessment is the foundation on which an ISMS is built. It provides the focus for the implementation of security controls and ensures that they are applied where they are most needed, are cost-effective and, just as importantly, are not applied where they are least impactful. The risk assessment helps to answer the question, 'How much security do we need?'

One of the key considerations of risk management is that risk needs to be considered in a positive and negative light. Risk is the effect of uncertainty on objectives, so it is vital in risk management that the opportunities for you to take advantage of are also considered.

The risk assessment involves all owners of information assets. You are unlikely to be able to conduct an effective risk assessment without them.

The first step is to decide on and then document a risk assessment method. There are proprietary methods available which are normally computer-based, such as CRAMM (CCTA Risk Analysis and Management Method).

Additionally, ISO 31000 - the international standard for risk management - can be utilised to develop a more organisation-specific method that addresses the complexity of information systems.

The risk assessment process can involve identifying and valuing the information assets. This valuation is not solely financial – it also considers other factors, such as reputational damage or compromised regulatory compliance. This is where your context has an important influence.

ISO 27005:2022 now also provides the option of event based risk assessment as an alternative to asset-based - this approach highlights the underlying concept that risks can be identified and assessed through an evaluation of events and consequences.

An asset-based process would consider threats, vulnerabilities and opportunities associated with the assets and their exploitation. Finally, you must determine the level of risk and identify the controls to be implemented to manage those risks.

The identification of threats, vulnerabilities and their impacts must consider the security environment. For example, the threat of denial of physical access to the premises is greater for an organisation based on an industrial estate next to a petrochemical plant than it is for an office in a small urban office park.

Risk treatment

The risk assessment identifies risk levels which are then compared to the acceptable level of risk determined by the organisation's security policy. Appropriate actions are taken to manage risks which are above the acceptance level, with the possible actions being:

- Implementing security controls selected from Annex A - or other sources relating to sector-specific or national best practices - to reduce the risk to an acceptable level. The risk level should be recalculated to confirm that the residual risk is below the acceptance level. The selected controls are recorded in the Statement of Applicability, which should be compared to Annex A and include the justification for the inclusion or exclusion of each control, status and traceability to the risk assessment.
- Accepting the risk in accordance with management's policy and criteria for risk acceptance. There may be instances where residual risk is above the acceptance level after an action has been taken, in which case the residual risk should also be subject to the risk acceptance process. A record of the management's acceptance of risk should be maintained.
- Removing the risk by changing the security environment. For example, installing secure applications where vulnerabilities have been identified in data processing applications or moving physical assets to a higher floor if there is a risk of flooding. Again, the residual risk should be recalculated following risk removal actions.
- Transferring the risk by taking out appropriate insurance or outsourcing the management of physical assets or business processes. The organisation accepting the risk should be aware of and agree to accept its obligations. Contracts with outsourcing organisations should address the appropriate security requirements.

The risk treatment plan manages the risks by identifying the actions taken and planned, plus the timescales for completing outstanding actions. The plan should prioritise the actions and include responsibilities and detailed action plans.

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

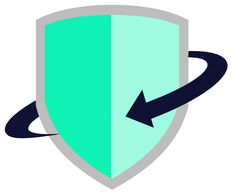
We're everywhere you are. With more than 300 highly qualified auditors and 250 dedicated cybersecurity specialists worldwide, we can provide a local service with a globally consistent dedication to excellence. Our people are technical experts with in-depth knowledge of information and cyber security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

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
1 Trinity Park
Bickenhill Lane
Birmingham
B37 7ES
United Kingdom

Care is taken to ensure that all information provided is accurate and up to date; however, LRQA accepts no responsibility for inaccuracies in or changes to information.