ISO 27001: Safeguard your information

> 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.

What is ISO 27001?

ISO 27001 (Information technology – Security techniques – Information security management systems – Requirements) aims to ensure that adequate controls (addressing confidentiality, integrity and availability of information) are in place to safeguard the information of 'interested parties'. These include your customers, employees, suppliers and the needs of society in general.

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.

Accredited certification to ISO 27001 is a powerful demonstration of your organization's commitment to managing information security effectively.

This overview provides some practical guidance and advice to support your implementation of a certified ISMS.

Implementing an ISMS

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.

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

- **Awareness:** Participants should be aware of the need for security of 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 co-operative 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 organization, the starting point for implementing an ISMS is to obtain management commitment and support.

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

Planning for success

Just 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 recognize 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, but 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 in place this will provide a strong foundation for your ISMS.

We strongly recommend attending an LRQA training course, where you will be able to discuss information security issues with other delegates and your tutor.

Understanding the standard

It's important that you familiarize yourself with the standard, this includes understanding the criteria you have to meet. This will influence the overall structure of your ISMS and associated documentation.

The standard is in two parts:

- ISO 27002 is not a standard itself, but a code of practice that describes security objectives and 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 and against which your certification body will audit you during the certification assessment.

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

These processes are critical to the effective implementation of an ISMS. If your organization already operates an ISO 9001:2015 management system, these processes 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.

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 review provides the opportunity for top management to assess and understand how well the management system is operating and supporting 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, then the information assets covered by the scope can be identified, along with their value and owner.

ISMS policy

The requirements relating to the ISMS policy are addressed in both ISO 27001 (5.2) and ISO 27002. There are also references to the policy in other requirements of ISO 27001 and in Annex A, which provides an indication of what the policy should contain. For instance, the ISMS objectives have to be consistent with the ISMS policy. Other policies will be required to meet certain control objectives.

Risk assessment and risk management

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 effective. 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 considered to be 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, then document, a method of risk assessment. There are proprietary methods available, normally computer-based, such as CRAMM (CCTA Risk Analysis and Management Method).

Additionally, ISO 31000 - the international standard for risk management - can be utilized to develop a more organization specific method that addresses the complexity of information systems. The risk assessment process involves identifying and valuing the information assets. This valuation is not solely financial – it also takes into account other factors such as reputational damage or compromised regulatory compliance. This is where your context has an important influence.

The process should consider the threats and vulnerabilities and any 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.

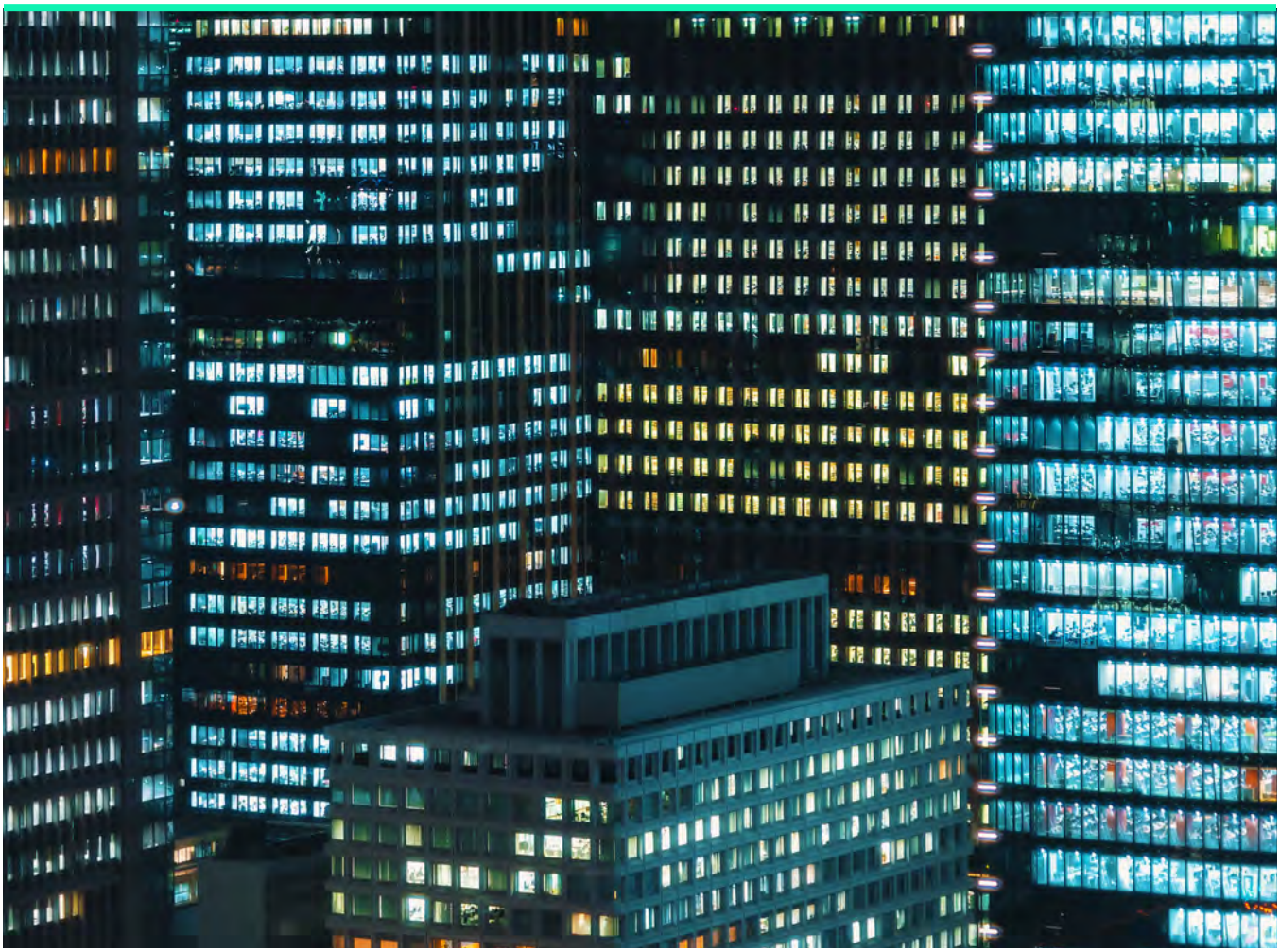
The identification of threats, vulnerabilities and their impacts must take into account the security environment. For example, the threat of denial of physical access to the premises is greater for an organization based on an industrial estate next to a petrochemical plant than it is for an office on 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 organization'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 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 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 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 organization accepting the risk should be aware of, and agree to accept, their obligations. Contracts with outsourcing organizations should address the appropriate security requirements.

The risk treatment plan is used to manage the risks by identifying the actions taken and planned, plus the timescales for the completion of outstanding actions. The plan should prioritize the actions and include responsibilities and detailed action plans.



Our ISO 27001 audit and training services

Our range of audit and training services are suitable for organizations of all sizes and locations, and can help you make the most of the standards.

Training

LRQA's range of training services supports your organization throughout your journey to ISO 27001 certification. We understand that each and every one of us learns differently. That's why we provide our training courses in multiple different formats from face -to-face and Virtual Classroom options through to eLearning.

Our range of ISO 27001 training courses include:

- Introduction to ISO 27001:2013
- ISO 27001:2013 Implementation
- ISO 27001:2013 Internal Auditor,
- Lead Auditor, Lead Auditor Conversion

Gap analysis

This auditor-delivered activity offers the opportunity to focus on critical, high-risk or weak areas of your system in order to create a certifiable system.

Wherever you are in the certification process – the scope can be defined by you.

Certification

This is typically a two-stage process consisting of a system appraisal and an initial audit, the duration of which is dependent on the size and nature of your organization.

When working with LRQA, organizations can, in many cases, choose to have their audits delivered remotely using safe and secure technology. This option provides the same high-quality service with several added benefits, including flexibility, fast delivery and access to global expertise

Surveillance

Once we've approved your ISMS, we carry out regular surveillance visits to ensure the ongoing effectiveness of your system. This gives you, and your top management, the assurance that your ISMS is on track and continually improving.

Integrated management system assessment

If you're looking to combine your organization's ISMS with an existing management system (such as quality you could benefit from a co-ordinated assessment and surveillance programme.

Why choose LRQA?

We're here to help negotiate a rapidly changing world, by working with you to manage and mitigate the risks you face. From compliance to data-driven supply chain transformation, it's our job to help you shape the future, rather than letting it shape you. We do this by delivering:

Strategic vision

Our technical know-how, sector expertise and innovative, forward thinking approach will help you meet the challenges of today – and become a safer, more secure, and sustainable organization tomorrow.

Technical expertise

Our people are sector experts. They bring with them a clear understanding of your specific challenges, standards and requirements – then deploy deep knowledge of certification, customized assurance, cybersecurity, inspection and training to help you meet them.

Global capability

Operating in more than 120 countries, recognized by over 50 accreditation bodies worldwide, and covering almost every sector, we can help you manage risk, drive improvement and build credibility with stakeholders around the globe.

Effective partnership

Every business is unique. That's why our experts work with you, to fully understand your needs and goals, and work out how we can best support them.

Fresh perspective

We have led the way in shaping our industry and continue to take every opportunity to collaborate with clients and pioneer new ideas, services and innovation.

LRQA offers a wide range of services against the world's leading information security standards.

- Training ✓
- Gap analysis ✓
- Certification ✓
- Integrated assessments ✓

YOUR FUTURE. OUR FOCUS.

About LRQA:

By bringing together unrivaled expertise in certification, customized assurance, cybersecurity, inspection and training, we've become a leading global assurance provider.

We're proud of our heritage, but it's who we are today that really matters, because that's what shapes how we partner with our clients tomorrow. By combining strong values, decades of experience in risk management and mitigation and a keen focus on the future, we're here to support our clients as they build safer, more secure, more sustainable businesses.

From independent third-party auditing, certification and training; to technical advisory services; to real-time assurance technology; to data-driven supply chain transformation, our innovative end-to-end solutions help our clients negotiate a rapidly changing risk landscape – making sure they're shaping their own future, rather than letting it shape them.

Get in touch

Visit **www.lrqa.com/us** for more information
866-971-LRQA
info-usa@lrqa.com

LRQA
1330 Enclave Parkway, Suite 200
Houston, TX 77077
United States