ISO27001 Services

Contents

3 ISO27001 base activity phases

4 Phase 1 – Gap analysis

5 Phase 2 – Implementation support

ISO27001 base activity phases

LRQA Nettitude firmly believe in operating good security as the foundation of our offerings so have broken down the 27001 certification and the certification process into a number of distinct activities.

We support your journey to certification, from initial gap analysis through to certification audits and ongoing activities such as internal auditing and management reviews.

Activities are broken down into three phases, and we can provide a tailored approach to fit your organisation's requirements.

ISO27001 base activity phases		
Phase 1 **Gap analysis**	**Phase 2** **Implementation support**	**Phase 3** **Ongoing support**
• Management workshop • ISMS review • Security control assessment • Implementation roadmap provided	All or a selection of items required identified in phase 1: • Risk approach & assessment • Internal audit • Third-party risk management • Policy creation • Training and awareness • Continued control assessment • Management review facilitation	All or a selection of the following based upon your resources: • Certification audit on-site assistance • Third-party risk management • Management review facilitation • Policy review • Training and awareness

Phase 1 – Gap analysis

ISO/IEC 27001:2022 management workshop

Getting started is often the most challenging step, usually through a misunderstanding of the ISO/IEC 27001:2013 standard and its purpose.

This workshop is designed for top level management, decision makers and risk owners – people who need an input into the scope.

We spend the day demystifying the standard into Specific, measurable, achievable, , relevant, and time bound (SMART) activities and objectives which can be incorporated into either a project or within business as usual activities. It will make the standard accessible and sow the seeds for engaging the rest of your organisation.

If you are running alternative security or compliance regimes, such as PCI DSS, it will demonstrate how the work you are already doing can be incorporated into your ISO/IEC 27001:2022 ISMS for quick wins and ensure that other activities are not isolated for enterprise security.

The completion of this management workshop will produce an ISMS scope of certification document. This document can then be used as part of clause 4 of the standard, and onwards, within your management review and other related processes.

Information security management system (ISMS) review

This review is aimed at the elements of the standard which form the core requirements and is, again, focused at top management, decision makers and risk owners.

It will determine how compliant your organisation is with clauses 4 to 10 in ISO/IEC 27001:2022 and provide you with a roadmap to achieving full compliance. The roadmap will be tailored to suit your organisation and align with your objectives, so that the scope of your ISMS meets your corporate business strategy and reinforces that your scope of certification is correct.

Security control review

Our consultants will use a combination of substantive and compliance methods to assess your security controls against the ISO/IEC 27001 Annex A Controls, with the help of ISO/IEC 27002:2017.

This review will look across your entire organisation to provide you with an indication of your security posture and risk levels which you are currently exposed to.

It will also provide you with the ability to create SMART activities/objectives to address those risks.

Your creation of the Statement of Applicability (for clause 6) will also be an output from this review as well as the creation of your implementation roadmap.

Phase 2 – Implementation support

Risk management

Risk management is at the heart of ISO/IEC27001:2013.

In conjunction with our consultants, a risk management system incorporating the requirements of the standard will be developed which fits your organisation both in terms of size and complexity. This will incorporate into your ISMS and provides the necessary documented information for a risk assessment process including information security risk assessment and risk treatment which are required for certification alongside your Statement of Applicability.

Third-party risk service

Third-party risk management is crucial for safeguarding your data and meeting the ISO 27001 standard. It helps identify and mitigate potential vulnerabilities from external partners, ensuring robust security and adherence to regulations.

Our consultants will work with you to determine your third parties' risk levels (RLs) and design an assessment process to harvest and manage these.

We can then support you in this area by completing those risk assessments on your behalf and reporting back any risks to a risk owner, within your organisation, and suggested remediation activities.

Internal audit service

Internal auditing serves as a cornerstone for maintaining the integrity and effectiveness of your information security management system. By conducting regular internal audits, you not only identify areas for improvement but also ensure alignment with ISO 27001 standards and regulatory requirements.

If your organisation lacks the internal expertise to conduct audits, our consultants can conduct them for you. Our team can seamlessly step in to perform thorough internal audits on your behalf, ensuring compliance with clause 9.2 of ISO 27001 and fostering a culture of continuous improvement. With our assistance, you can confidently navigate the audit process, identify improvement opportunities, and maintain your commitment to information security excellence..

As your familiarity with the standard and processes improve, you may choose to bring this in-house or simply retain LRQA Nettitude to deliver this core element of the standard on your behalf.

CREST

VA | PEN TEST | STAR Intelligence-led PT | STAR Threat intelligence | CSIR | SOC | OVS

PCI Security Standards Council™
QUALIFIED SECURITY ASSESSOR

PCI Security Standards Council™
APPROVED SCANNING VENDOR

CYBER ESSENTIALS

ISO 9001 ISOQAR REGISTERED
ISO 27001 ISOQAR REGISTERED
Cert No. 23208

ISO 14001:2004 REGISTERED FIRM

Get in touch

Visit **www.nettitude.com** for more information
or email enquiries to **solutions@nettitude.com**

UK Head Office
1 Trinity Park
Bickenhill Lane
Birmingham
B37 7ES

Americas
810 Seventh Avenue
Suite 1110
New York
NY 10019

Asia Pacific
460 Alexandra Road
#15-01
mTower
Singapore 119963

Europe
Fidiou 9
Athina
106 78
Greece

LRQA NETTITUDE