Northdown Systems
The Business Compliance Experts

Eight Steps to ISO27001:2013 Certification

Note: activities overlap and do not rely upon the completion of the previous step (except Step 8).

Step1: Initiating the ISMS Project

- Purchase a copy of the ISO27001 standard
- Obtain Senior Management commitment for the project
- Identify the project team and other required resources
- One-day workshop to understand the end-to-end process

Step 2: Defining the ISMS Project

- Executive workshop – define the ISMS scope, information security goals and objectives
- Understand any dependencies on other systems, define any exclusions
- Relationship to other regulatory, legislative or contractual requirements

Step 3: Documentation Preparation Phase

- Implement top-level information security policy, and specific supporting policies
- Implement other documentation and records required by the ISO27001 standard
- Define approach, documentation and records for undertaking risk management (steps 4 & 5)
- Define approach, documentation and records for data protection (GDPR compliance)
- Agree documentation and records for ensuring supply chain security compliance

Step 4: Risk Assessment Activities

- Implementation of risk assessment and risk treatment activities to meet ISO27001 standard
- Options for manual or cloud-based SaaS solution for undertaking risk assessments
- Provision of detailed training to asset owners and risk owners on chosen approach
- Workshop to identify information and supporting assets (and their relationships)

Step 5: Risk Treatment Activities

- Identification of unacceptable risks which are required to be treated
- Progression of unacceptable risks:
    - Risk reduction (e.g. change of approach, application of new security controls)
    - Risk transfer (e.g. pass the activity to an outsourced provider, insurance company)
    - Risk avoidance (cessation of the activity to remove the identified risks)
    - Risk acceptance (senior management acceptance of risks that cannot be treated)

Step 6: Training, Education and Culture Initiatives

- Preparation of information security and data protection training material
- Delivery of educational initiatives – e.g. workshops, webinars, surveys
- Training for contractors, third parties and any other personnel in scope of the ISMS
- Workplace assessment to identify security opportunities/weaknesses
- Optional: educational plan for GDPR/data protection activities

Step 7: Preparation for External Certification Assessment

- Introduction to UKAS audit organisation with preferential rates/scheduling
- Produce and validate Statement of Applicability (automatically produced by SaaS solution)
- Conduct of audit readiness assessment, and remediation of any identified shortcomings
- Conduct of initial internal audits / internal audit training for own personnel

Step 8: External Certification Audit

- Stage 1 assessment – management elements and ISO27001 standard compliance
- *(progress to Stage 2 if no major non-conformities, otherwise repeat of Stage 1)*
- Stage 2 assessment – delivery of information security in operational activities
- *(progress to certification award if no major non-conformities)*
- Certification awarded!

- Review, assessment and remediation of any non-conformities identified
- Workshop to progress from certification preparation to "business as usual" maintenance
- Optional ongoing risk assessment, supplier management and internal audit support

Other Related Services

- UK Data Protection Act 2018 / GDPR requirements:
    - ICO registration, data protection policy, privacy notices etc.
    - Inventory of personal data, security of data, data retention schedule
    - Data protection training for personnel, contractors and third parties
    - Data Protection Impact Assessments
    - GDPR compliance within the supply chain
    - Data subject rights processes and supporting records
    - Data breach monitoring and reporting protocols

- Implementation of related standards, e.g.
    - ISO9001 (Quality Management)
    - ISO27017 (Security of Cloud Services), ISO27018 (Personal Data in Cloud Services)
    - Cyber Essentials and Cyber Essentials Plus
    - Specialist, sector-specific standards – e.g. Government MCSS, PCI DSS

- Security testing (e.g. vulnerability scanning, penetration testing)

- Northdown Systems' audit services:
    - Internal audits
    - Second-party assessments (e.g. with suppliers of products and services)
    - Third-party assessments (IRCA-qualified Lead Auditors)
    - Supplier and third-party due diligence assessments

- "Virtual CISO" and "Virtual DPO" services

