CHECKLIST ISO 27001 **IT SAFETY MANAGEMENT**

With our checklist, you can quickly and easily fnd out whether your business is properly prepared for certifcation as per ISO/IEC 27001 for an integrated information safety management system.

ISO/IEC 27001 certifcation – for an accurate assessment of your information safety management!

Te following questions are arranged according to the basic structure for management system standards. If you can answer a question with yes, mark it with a check. Tat way you can see instantly which areas of your company already comply with the requirements, and which areas require more work.

Context of the organization

- ☐ You have broken down the precise organization of your business (e.g. as an organizational diagram).
- ☐ You have defined the area of application for your ISMS (especially for stakeholders).
- ☐ You have drawn up a statement of applicability (SoA), which documents the decisions about implementation of measures, and the reasons for those decisions.
- ☐ You have conducted an environment analysis for the integration of the ISMS into the company.
- ☐ You have conducted a requirements analysis about the different interest groups (stakeholders).
- ☐ You have compiled an overview of all relevant legal, regulatory and contractual requirements that have an effect on your information safety strategy and the ISMS.

Management

- ☐ You have clearly defined and documented the business aims and requirements relating to the information safety policy at your company.
- ☐ You have defined a concrete information safety strategy.
- ☐ You have defined your “top management”; this group is responsible for controlling the ISMS of the organization to be protected and decides how resources are deployed.
- ☐ You have implemented an information security policy.

Planning ☐

- ☐ You have a documented risk assessment procedure.
- You have comprehensive documentation of the risk assessment process and the risk handling process/plan.
- ☐ You have all records and results from risk assessments and risk analyses.
- ☐ You have documented all records and results from risk handling.
- ☐ You have defined all the safety targets for your company and stakeholders.

Support ☐

- ☐ You have a communication plan or matrix for documenting all communications within the company that relate to information safety.
- You are able to provide the personnel and infrastructure required for the implementation and control of the ISMS.
- ☐ You have a strategy for handling documented information.
- ☐ You have created detailed role descriptions for employees who are affected by the ISMS (e.g. ISB and/or CISO or DSB) and documented all verification of their competences.
- ☐ You have created documentation for the awareness and training concept regarding the ISMS.
- ☐ You have training documents for the ISMS and proof that your employees have taken part in the relevant training measures.
- ☐ You have defined a procedure for internal and external communications.

Operation

- ☐ You have verification that the ISMS processes were executed correctly, and that the ISMS is controlled and its performance measured.
- You have documentation about internal audit programs and audit results.
- ☐ You have defined an incident response plan (IRP) that includes current contact lists and escalation plans.
- ☐ You have comprehensive documentation on the measuring structure for all KPIs (key performance indicators), as well as on the measurement results and the resulting management reports for escalation.
- ☐ Your documentation comprises behavioral rules in the event of safety-relevant irregularities, process descriptions and work instructions for securing proof, and reports about information safety incidents.
- ☐ You have proof of the types of non-compliance, of all implemented reactive measures, and of the results of all corrective measures.
- ☐ You have an overview of the results of risk assessment (e.g. risk assessment reports, risk key figures) and risk handling (e.g. control test reports, penetration test reports).

DEKRA Audit

Mail **audit@dekra.com**
Web **www.dekra.com/en/audit/**