ISO 27001 Readiness Checkliste (D)

Sie erhalten im Rahmen der Bearbeitung der Checkliste schnell und einfach Auskunft darüber, ob Ihr Unternehmen bereits ausreichend für die Zertifizierung nach ISO 27001 für ein integriertes Informations-Sicherheitsmanagementsystem vorbereitet ist.

Der Aufbau der Fragen orientiert sich an Managementsystemnormen. Wenn Sie eine Frage nicht sicher positiv beantworten können, dann antworten Sie mit „Nein“. Nur wenn Sie alle Fragen mit „Ja“ beantworten können, besitzt ihr Unternehmen vermutlich bereits einen ausreichenden Reifegrad.

Gerne helfen wir Ihnen im Rahmen einer detaillierten GAP-Analyse dabei, herauszufinden, in welchen Bereichen Ihr Unternehmen die Anforderungen der ISO 27001 bereits vollumfänglich erfüllt und welchen Themen Sie sich noch zuwenden müssen.

Bereich	Frage	Ja/nein
Kontext der Organisation	Sie haben die genaue Organisation Ihres Unternehmens aufgeschlüsselt (z.B. als Organigramm).	
	Sie haben den Geltungsbereich Ihres ISMS (insbesondere für die Stakeholder) festgelegt.	
	Sie haben eine Liste mit Erklärungen zur Anwendbarkeit (engl.: Statement of Applicability: SoA) angelegt, in der die begründeten Entscheidungen zur nicht erforderlichen Umsetzung von Maßnahmen dokumentiert sind.	
	Sie haben eine Umfeldanalyse für die Einordnung des ISMS im Unternehmen durchgeführt.	
	Sie haben eine Anforderungsanalyse hinsichtlich der jeweiligen Interessengruppen (Stakeholder) durchgeführt.	
	Sie haben eine Übersicht aller relevanten gesetzlichen, regulatorischen und vertraglichen Anforderungen, die einen Einfluss auf die Informationssicherheitsstrategie und das ISMS haben, zusammengestellt.	
Führung	Sie haben die Geschäftsziele und Anforderungen im Zusammenhang mit der Informationssicherheitspolitik im Unternehmen klar definiert und dokumentiert.	
	Sie haben eine konkrete Informationssicherheitsstrategie festgelegt.	
	Sie haben das „Top-Management“ definiert, welches für die Steuerung des ISMS der zu schützenden Organisation verantwortlich ist und über den Ressourceneinsatz entscheidet.	
	Sie haben eine Informationssicherheitsleitlinie (engl. Information Security Policy) implementiert.	

Bereich	Frage	Ja/nein
Planung	Sie besitzen ein dokumentiertes Risikobewertungsverfahren.	
	Sie verfügen über eine umfassende Dokumentation zum Risikobeurteilungsprozess und Risikobehandlungsprozess/-plan.	
	Sie besitzen alle Aufzeichnungen und Ergebnisse von Risk Assessments bzw. Risikoanalysen.	
	Sie haben alle Aufzeichnungen und Ergebnisse von Risikobehandlungen dokumentiert.	
	Sie haben alle Sicherheitsziele für Ihr Unternehmen und Stakeholder definiert.	
Unterstützung	Sie verfügen über einen Kommunikationsplan bzw. -matrix für die Dokumentation aller Kommunikation im Unternehmen mit Bezug auf die Informationssicherheit.	
	Sie können die erforderlichen Personen und die Infrastruktur für die Umsetzung und Steuerung des ISMS zur Verfügung stellen.	
	Sie verfügen über eine Strategie für den Umgang mit dokumentierten Informationen.	
	Sie verfügen über eine Übersicht über alle relevanten Ressourcen (z.B. Budget, Personal).	
	Sie haben eine detaillierte Rollenbeschreibung von Mitarbeitern im Geltungsbereich des ISMS (z.B. ISB bzw. CISO oder DSB) angelegt und sämtliche Nachweise über deren Kompetenzen dokumentiert.	
	Sie haben eine Dokumentation zum Awareness- bzw. Schulungskonzept mit Bezug auf das ISMS angelegt.	
	Sie verfügen über Schulungsunterlagen zum ISMS und Nachweise über die Teilnahme Ihrer Mitarbeiter an jeweiligen Schulungsmaßnahmen.	
	Sie haben ein Verfahren zur internen und externen Kommunikation festgelegt.	

Bereich	Frage	Ja/nein
Betrieb	Sie besitzen Nachweise zur korrekten Ausführung der ISMS-Prozesse und für die Kontrolle und Leistungsmessung des ISMS.	
	Sie verfügen über Dokumentationen über interne Auditprogramme und Auditergebnisse.	
	Sie haben einen Incident Response Plan, inklusive aktueller Kontaktlisten und Eskalationspläne definiert.	
	Sie verfügen über eine umfangreiche Dokumentation der Messstruktur für alle KPIs (Key Performance Indikatoren) sowie über die Messergebnisse und die daraus abgeleiteten Managementberichte zur Eskalation.	
	Ihre Dokumentation umfasst Verhaltensregeln bei sicherheitsrelevanten Unregelmäßigkeiten, Prozessbeschreibungen und Arbeitsanweisungen für die Sicherung von Beweisen sowie Berichte von Informationssicherheits-Vorfällen.	
	Sie verfügen über Nachweise über die Art von Nichtkonformitäten sowie über sämtliche umgesetzte reaktive Maßnahmen und über die Resultate zu sämtlichen korrigierenden Maßnahmen.	
	Sie besitzen eine Übersicht über die Ergebnisse der Risikobewertung (z.B. Risikobewertungsberichte, Risikokennzahlen) und Risikobehandlung (z.B. Kontrolltestberichte, Penetrationstestberichte).	

ISO 27001 Readiness Checklist (E)

As part of the processing of the checklist, you will receive quick and easy information about whether your company is already sufficiently prepared for certification according to ISO 27001 for an integrated information security management system.

The structure of the questions is based on management system standards. If you can't answer a question positively with certainty, then answer "No". If you can answer "yes" to all questions, your organization probably already has a sufficient level of maturity.

As part of a detailed GAP analysis, we are happy to help you find out in which areas your company already fully meets the requirements of ISO 27001 and which topics you still have to address.

Range	Question	Yes/No
Context of the organization	You have the exact organization of your company broken down (e.g. as an organizational chart).	
	You have the scope of your ISMS (in particular for stakeholders).	
	You have a list of explanations of applicability (Engl.: Statement of Applicability, SoA), in which the justified decisions on the unnecessary implementation of measures are documented.	
	You have an environment analysis for the classification of the ISMS carried out in the company.	
	You have a requirements analysis with regard to the relevant stakeholders.	
	You have an overview of all relevant legal, regulatory and contractual requirements that an influence on the information security strategy and the ISMS.	
Management	You have defined the business objectives and requirements in the Context with information security policy in the Companies clearly defined and documented.	
	You have a concrete information security strategy set.	
	You have defined the "top management", which is used for the control of the ISMS of the organization to be protected is responsible and decides on the use of resources.	
	You have implemented an Information Security Policy.	
Planning	You have a documented risk assessment procedure.	
	You have comprehensive documentation to the risk assessment process and risk treatment process/plan.	
	You have all the records and results of Risk assessments or risk analyses.	
	You have all the records and results of Risk treatments documented.	
	You have all the security objectives for your company and Stakeholders defined.	

Range	Question	Yes/No
Support	You have a communication plan or matrix for the documentation of all communication in the company with regard to information security.	
	You can find the necessary people and the infrastructure for the implementation and control of the ISMS for Provide.	
	You have a strategy for dealing with documented information.	
	You have an overview of all relevant Resources (e.g. budget, personnel).	
	You have a detailed role description of Employees within the scope of the ISMS (e.g. ISB or CISO or DPO) and all evidence of their competences are documented.	
	You have a documentation for the awareness or awareness Training concept with reference to the ISMS.	
	You have training documents on the ISMS and Proof of the participation of your employees in the respective training measures.	
	You have defined a procedure for internal and external communication.	
Operation	You have evidence of the correct execution of the ISMS processes and of the control and performance measurement of the ISMS.	
	You have documentation of internal audit programs and audit results.	
	You have an Incident Response Plan, including Current contact lists and escalation plans defined.	
	You have extensive documentation of the Measurement structure for all KPIs (Key Performance Indicators) as well as the measurement results and the management reports derived from them on escalation.	
	Your documentation includes rules of conduct in the event of safety-relevant irregularities, process descriptions and work instructions for securing evidence as well as reports of Information Security Incidents.	
	They have evidence of the nature of non-conformities as well as all reactive Measures and the results of all corrective measures.	
	You have an overview of the results of the risk assessment (e.g. risk assessment reports, risk indicators) and risk treatment (e.g. control test reports, penetration test reports).	