CHECKLISTE – IT-SICHERHEIT AUF EINEN BLICK

Die wichtigsten Aspekte zur IT-Sicherheit im Überblick

ID	AKTIVITÄT	STATUS		
I	**INFORMATIONSSICHERHEITSMANAGEMENTSYSTEM (ISMS)**			
01	Ist in Ihrer Organisation ein organisationsweites Informationssicherheitsmanagementsystem (ISMS) etabliert und in Betrieb?	OK	KO	N/A
02	Sind Verantwortlichkeiten in Bezug auf das etablierte ISMS ihrer Organisation klar definiert und konkreten Personen zugewiesen?	OK	KO	N/A
03	Wurde in Ihrer Organisation vom Top-Management eine Informationssicherheits-Policy in Kraft gesetzt und wird diese laufend aktualisiert?	OK	KO	N/A
04	Stehen für den Betrieb des ISMS Ihrer Organisation ausreichend personelle und finanzielle Ressourcen zur Verfügung?	OK	KO	N/A
05	Wird das ISMS Ihrer Organisation regelmäßig internen Audits unterzogen?	OK	KO	N/A
06	Wird das ISMS Ihrer Organisation regelmäßig einem Management-Review unterzogen?	OK	KO	N/A
07	Existiert in Ihrer Organisation ein Prozess zur laufenden Verbesserung des ISMS?	OK	KO	N/A
08	Sind Vermögenswerte (Assets) Ihrer Organisation gelistet und klassifiziert?	OK	KO	N/A
09	Sind in Ihrer Organisation laufende Risikoanalyseprozesse etabliert, um etwaige IT-Sicherheitsrisiken und deren Auswirkungen auf Vermögenswerte verlässlich und rechtzeitig zu identifizieren?	OK	KO	N/A
10	Sind in Ihrer Organisation laufende Risikomanagementprozesse etabliert, über die die adäquate Adressierung identifizierter IT-Sicherheitsrisiken sichergestellt ist?	OK	KO	N/A
II	**TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN**			
11	Existieren geeignete, dokumentierte Vorgaben für Mitarbeiterinnen und Mitarbeiter, die deren Verhalten am Arbeitsplatz zur Erhöhung der IT-Sicherheit regeln?	OK	KO	N/A
12	Werden Mitarbeiterinnen und Mitarbeiter laufend in Bezug auf die Relevanz und die Einhaltung relevanter und sie betreffender IT-Sicherheitsmaßnahmen geschult?	OK	KO	N/A
13	Existieren definierte und dokumentierte Vorgaben für den Einsatz von Fremdpersonal?	OK	KO	N/A
14	Existiert ein Konzept zur Kontrolle und zur Beschränkung des Zugriffs auf IT-Systeme der Organisation über geeignete Authentifizierungs- und Berechtigungssysteme und ist dieses Konzept organisationsweit umgesetzt?	OK	KO	N/A
15	Existiert ein Konzept zum Einsatz von kryptographischen Methoden und kryptographischen Schlüsselmaterials in der Organisation zum Schutz von Vermögenswerten und ist dieses Konzept organisationsweit umgesetzt?	OK	KO	N/A
16	Existiert ein Konzept zum Betrieb von IT-Services, das relevante Betriebsaspekte wie Monitoring, Datensicherung, Protokollierung, Change-Management oder auch Intrusion Detection und Prevention abdeckt und ist dieses Konzept organisationsweit umgesetzt?	OK	KO	N/A

17	Existiert ein Konzept für die Netzwerksicherheit und ist dieses organisationsweit umgesetzt?	OK	KO	N/A
18	Existiert ein Konzept für den sicheren Datenaustausch innerhalb der Organisation und mit Dritten?	OK	KO	N/A
19	Existiert ein Konzept zur sicheren Entwicklung, zum sicheren Betrieb und zur Wartung eigner IT-Lösungen, das den gesamten Lebenszyklus dieser IT-Lösungen geeignet abdeckt?	OK	KO	N/A
20	Sind sicherheitsrelevante Abhängigkeiten zu Dritten (Lieferanten) bekannt und sind notwendige Leistungen von Dritten über Verträge geeignet geregelt?	OK	KO	N/A
21	Existiert ein Konzept zum organisationsinternen Umgang mit Sicherheitsvorfällen?	OK	KO	N/A
22	Existiert ein Konzept zum Wiederanlauf kritischer IT-Lösungen nach einem Ausfall (Disaster Recovery) zur Aufrechterhaltung des Geschäftsbetriebs (Business Continuity)?	OK	KO	N/A
III	**PHYSISCHE MASSNAHMEN**			
23	Existiert ein Konzept zur Raum- und Gebäudesicherheit und entsprechen verwendete Räume und Gebäude der Organisation den Vorgaben dieses Konzepts?	OK	KO	N/A
24	Existieren geeignete Konzepte für Zutrittskontrolle, Einbruchsschutz und Perimeterschutz und sind diese Konzepte organisationsweit umgesetzt?	OK	KO	N/A
25	Existieren geeignete Brandschutzvorkehrungen und sind diese mit den Sicherheitsanforderungen der Organisation und ihrer Vermögenswerte abgestimmt?	OK	KO	N/A
26	Ist die Stromversorgung der Organisation durch Redundanzen oder andere Vorkehrungen ausreichend sichergestellt?	OK	KO	N/A
27	Entspricht die Stromversorgung und Leitungsführung den Sicherheitsanforderungen der Organisation und ihrer Vermögenswerte?	OK	KO	N/A
28	Sind Arbeitsplätze so gestaltet, dass der sichere Betrieb und die sichere Verwendung von IT-Lösungen sichergestellt ist?	OK	KO	N/A
29	Existieren Vorgaben zur sicheren Verwendung von (speziell mobilen) Endnutzergeräten vor allem auch in Bezug ihre Verwendung außerhalb der Organisation?	OK	KO	N/A