

Informationen.Daten.Sicherheit.

Unter dem Dach des Competence Center Informationen.Daten.Sicherheit. bündelt die DQS ihr themenspezifisches Fachwissen und Engagement rund um Informationssicherheit und Datenschutz. Dabei bietet das Competence Center Leistungen für alle Unternehmensgrößen und Branchen an. Neben der international anerkannten Managementsystemnorm ISO/IEC 27001 und Auditierungen gemäß dem IT-Sicherheitskatalog liegt ein weiterer Schwerpunkt auf den vielfältigen gesetzlichen Anforderungen rund um die EU-Datenschutz-Grundverordnung und das neue Bundesdatenschutzgesetz.



Das Competence Center verfolgt intensiv die aktuellen Herausforderungen am Markt und entwickelt Lösungen für die Auditierung, Zertifizierung und Reifegradermittlung. Durch das breit gefächerte Angebot unterschiedlicher Normen sowie speziell auf die Bedürfnisse der Organisationen zugeschnittener Auditierungen gewährleisten wir einen ganzheitlichen Blick auf die Einhaltung einzelner Standards und deren optimale Verzahnung miteinander. Akkreditierungen und Zulassungen für alle maßgeblichen Regelwerke stehen weltweit für Kompetenz und Zuverlässigkeit.

Themenspezifische Normen und gesetzliche Vorgaben

ISO/IEC 27001 – Informationssicherheits-Management

Es vergeht kaum ein Tag, an dem sich nicht zahllose Medien mit Cyber Crime, Wirtschaftsspionage und ungewolltem Know-how-Abfluss in Unternehmen befassen – und mit den ebenso zahlreichen Fragen, wie sich sensible Informationen schützen lassen. Mit der Einfachheit des modernen Datentransfers und dem oftmals sorglosen Umgang durch eine Fülle von Nutzern wird schnell vergessen, wie leicht es auch Unbefugte haben, an bedeutende Unternehmenswerte zu gelangen. Auch der alltägliche Datenverlust durch Ausfall von Hardware, Unkenntnis oder vergessene Unterlagen bergen Risiken in sich.

Erfolgreiche Unternehmen nutzen die Struktur und die Transparenz moderner Managementsysteme, um Bedrohungen aufdecken und den Einsatz zeitgemäßer Sicherheitssysteme gezielt steuern zu können. Die bevorzugte Basis zur Einführung eines ganzheitlichen Informationssicherheits-Managementsystems (ISMS) ist die internationale Norm ISO/IEC 27001. Mit der Revision von 2013 wurde das Thema Informationssicherheit als bedeutendes strategisches Element hervorgehoben und avancierte damit endgültig zur „Chefsache“.

Nachhaltiger Geschäftserfolg durch Informationssicherheit

Der präventive Managementsystemansatz führt nachweislich zu einer Reihe von Vorteilen:

- Aufrechterhaltung der Geschäftskontinuität
- Sicherung der Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität
- Etablierung eines strikten Risikomanagementprozesses
- Fortlaufende Verbesserung Ihres Sicherheitsniveaus
- Einhaltung relevanter Compliance-Anforderungen
- Vertrauensbildung gegenüber interessierten Parteien
- Mehr Handlungs- und Rechtssicherheit, Reduzierung von Haftungsrisiken
- Kostenersparnis durch Vermeidung von Sicherheitsvorfällen

ISO/IEC 27001 orientiert sich im Aufbau und der Herangehensweise an der nunmehr verbindlichen Grundstruktur für alle neuen, prozessorientierten Managementsystemnormen. Dies bietet Ihnen die Möglichkeit der einfachen Integration eines Informationssicherheits-Managementsystems in ein bereits bestehendes Managementsystem, z. B. nach ISO 9001.

ISIS12 – Informationssicherheit für den Mittelstand und die Verwaltung

Für klein- und mittelständische Unternehmen und Kommunen bietet das kompakte, pragmatische Zertifizierungsschema ISIS12 eine gute Alternative zur Norm ISO/IEC 27001.

ISIS12 wurde vom Netzwerk Informationssicherheit für den Mittelstand* entwickelt. Die Einführung vollzieht sich in 12 Schritten, die vergleichsweise einfach nacheinander bearbeitet werden können. Begleitet wird die Einführung durch das „Handbuch zur effizienten Gestaltung von Informationssicherheit im Mittelstand“ und ein praxisorientiertes Softwaretool. Vielfach ist eine bundeslandspezifische Förderung der Kosten für eine Zertifizierung möglich. Die Zertifizierung erfolgt exklusiv durch die DQS.

Informationssicherheit in handlichen Päckchen

- Geprüftes Informationssicherheitsniveau
- Darstellung Ihrer Verlässlichkeit und Transparenz hinsichtlich der Einhaltung von Informationssicherheitsanforderungen
- Steigerung Ihrer Prozess- und Ergebnisqualität sowie der damit einhergehenden Reputation
- Stärkeres Sicherheitsbewusstsein Ihrer Mitarbeiter, Führungs- und Leitungskräfte

ISIS 12

* www.isis12.de, www.it-sicherheit-bayern.de

ISO 22301 – Business Continuity Management

Die Aufrechterhaltung kritischer Geschäftsprozesse in Ausnahmesituationen – das ist das Ziel eines ganzheitlichen Business Continuity Managementsystems (kurz: BCM). Derartige Ausnahmezustände können sich jederzeit und überall ereignen. Datenverlust, Stromausfall, Rohstoffknappheit oder Umweltkatastrophen – jedes dieser Ereignisse kann eine Organisation in ihrer Existenz bedrohen. Die international anerkannte Norm ISO 22301 liefert dazu den Rahmen für die Einführung und Zertifizierung. Das DQS-Audit stellt dabei exakt jene Aspekte in den Mittelpunkt, die für den Fortbestand Ihrer Organisation im Fall der Fälle überlebenswichtig sind.



THE AUDIT COMPANY

Datenschutz – Einhaltung rechtlicher und kundenspezifischer Anforderungen

EU-Datenschutz-Grundverordnung (DS-GVO) und Bundesdatenschutzgesetz (BDSGneu)

Der Umgang mit personenbezogenen Daten ist seit jeher eine heikle Angelegenheit, vor allem seit moderne Technik deren massenhafte Verarbeitung möglich macht. Für Privatpersonen ist der Schutz dieser Daten ein elementares Grundrecht. Diesen Stellenwert des Datenschutzes unterstreicht der europäische Gesetzgeber künftig mit Bußgeldern von bis zu 20 Millionen Euro oder vier Prozent vom weltweiten Konzernumsatz.

Die neue DS-GVO trat am 25. Mai 2016 europaweit in Kraft – und ist mit einer Frist von zwei Jahren von allen Unternehmen und öffentlichen Stellen, die personenbezogene Daten verarbeiten, verbindlich umzusetzen. In Deutschland wird die Verordnung durch die enthaltenen Öffnungsklauseln zusammen mit dem BDSGneu umzusetzen sein. Aufgrund der Kürze der Zeit bis zur Umsetzung am 25. Mai 2018 ist für alle Betroffenen eine frühzeitige Kenntnis der neuen Anforderungen wichtig, insbesondere damit noch fehlende Datenschutzprozesse umgesetzt und etwaige Korrekturen an bestehenden Prozessen vorgenommen werden können.

Wer die Herausforderungen kennt, kann auf sie reagieren

Die Nichterfüllung der gesetzlichen Neuerungen birgt ein enorm hohes Risikopotenzial – hinsichtlich finanzieller Strafen wie auch für die Reputation Ihres Unternehmens. Machen Sie Datenschutz frühzeitig zu Ihrem Compliance-Thema und beugen Sie möglichen Verstößen vor.

▪ **Prozessaudit der Systematik zur Erreichung der rechtlichen Anforderungen**

Lassen Sie sich die Wirksamkeit Ihrer Systematik zur Erreichung der rechtlichen Anforderungen durch die DQS bestätigen.

▪ **Datenschutz-Check**

Auditierung Ihrer bereits umgesetzten Maßnahmen zur Einhaltung des Datenschutzes / Reifegradbestimmung.

▪ **Datenschutzaudit**

Auditierung Ihres Datenschutzmanagementsystems auf Basis des BDSGneu sowie den Anforderungen der relevanten Abschnitte von ISO/IEC 27001 und des Datenschutz-Risikomanagementsystems analog zu ISO/IEC 27005.

IT-Sicherheit für Kritische Infrastrukturen gemäß BSI-KritisV

Das IT-Sicherheitsgesetz (IT-SIG) und die BSI-Kritisverordnung (BSI-KritisV) schaffen seit 2015 einen Rahmen zur Verbesserung der Sicherheit informationstechnischer Systeme von Betreibern sogenannter Kritischer Infrastrukturen (KRITIS). Sie sind demnach verpflichtet, ein Mindestsicherheitsniveau an IT-Sicherheit einzuhalten und erhebliche IT-Sicherheitsvorfälle an das Bundesamt für Sicherheit in der Informationstechnik (BSI) zu melden. Die Zuordnung der betroffenen Unternehmen und Anlagen erfolgt in sieben Sektoren: Energie, Informationstechnik und Telekommunikation, Wasser und Ernährung sowie Transport und Verkehr, Finanz- und Versicherungswesen und Gesundheit. Die DQS ist als Prüfstelle anerkannt; eine Reihe ihrer Auditoren haben die Prüfverfahrenskompetenz nach § 8a BSI-Gesetz nachgewiesen und sind beim BSI gelistet.

www.bsi.bund.de

Sektor Energie: Informationssicherheit für Netzbetreiber

Um die Sicherheit informationstechnischer Systeme im Sektor Energie zu erhöhen, veröffentlichte die Bundesnetzagentur 2015 den IT-Sicherheitskatalog. Dieser fordert gemäß §11 Abs. 1a Energiewirtschaftsgesetz (EnWG) von Energienetzbetreibern grundsätzlich die Umsetzung eines vollumfänglichen Informationssicherheits-Managementsystems (ISMS) gemäß ISO/IEC 27001. Die Anforderungen an das ISMS werden durch die des IT-Sicherheitskatalogs erweitert. Hinzu kommen Erweiterungen der ISO/IEC TR 27019, die sich auf spezifische Besonderheiten des Energiesektors beziehen.

Das ISMS ist unter Beachtung der Erweiterungen gemäß der Anforderungen des Konformitätsbewertungsverfahrens der BNetzA vom Netzbetreiber einzuführen und durch eine DAkkS akkreditierte Zertifizierungsstelle wie der DQS zertifizieren zu lassen. Stichtag ist der 31. Januar 2018.

Nachweis für den sicheren Betrieb von Energieversorgungsnetzen

- Das DQS-Zertifikat nach der „Trilogie“ ISO/IEC 27001, ISO/IEC TR 27019 und den Anforderungen des IT-Sicherheitskatalogs ist der verbriefte Nachweis für die Wirksamkeit Ihrer Sicherheitsmaßnahmen.

Alles, was uns bewegt.

www.dqs.de

Das Spektrum unserer Leistungen (Auszug)

Qualitätsmanagement	ISO 9001 Qualitätsmanagement	Prozessaudit Qualitätsmanagement		
Informationssicherheit	ISO 27001 Informationssicherheit	ISIS 12 KMU und Verwaltung	Prozessaudit Informationssicherheit	Prozessaudit IT-Safety & Security
KRITIS/ IT-Sicherheitskatalog	IT-SiKat Netzbetreiber	BSI-Kritisv gemäß §8a (3) BSIG	Störungsmanagement	
Datenschutz gemäß BDSG und DS-GVO	Datenschutzaudit	Datenschutz-Check	Datenschutz- Prozessaudit	
Unternehmensrisiken, Risikomanagement	ISO 22301 Business Continuity Management	Risikomanagement	Compliance-Audit	
Umwelt- und Energiemanagement	ISO 14001 Umweltmanagement	ISO 50001 Energiemanagement	Auditierung gemäß gesetzl. Anforderungen: SpaEFV, EEG	
Arbeits- und Gesundheitsschutz	ISO 45001 BS OHSAS 18001	DIN SPEC 91020 Betriebliches Gesundheitsmanagement		
Automotive, Transport	IATF 16949 QM-Automobilzulieferer	ISO/IEC 15504 (SPICE)	EN 9100ff Luft- und Raumfahrt	ISO/TS 22163 IRIS
Logistik	TAPA Frachtsicherheit	Qualified Carrier Qualifizierter Frachtführer		
Sonstiges	IT-Sicherheit im Krankenhaus BSI-KritisV	Lieferantenmanagement	u.v.a.m. www.dqs.de	

DQS. THE AUDIT COMPANY.

Als Deutschlands erste Managementsystem-Zertifizierungsstelle wurde die DQS GmbH 1985 durch die DGQ und das DIN gegründet. Heute ist sie eine 100%ige und zugleich die größte Tochtergesellschaft der DQS Holding GmbH – und damit Teil der international agierenden DQS Gruppe. Mit mehr als 200 Mitarbeitern in der Zentrale Frankfurt am Main steuert die DQS GmbH die Hälfte der weltweit 59.000 Zertifikate und hält rund 100 Akkreditierungen und Zulassungen für national und international anerkannte Normen sowie zahlreiche branchen- oder verbandsspezifische Regelwerke.

Weltweit sind 2.500 Auditoren für Sie im Einsatz, an über 100.000 Tagen im Jahr. Und: Sie alle verbindet das gleiche Verständnis und Anspruchsniveau, niedergelegt in der „DQS Good Audit Practice“. Aufgrund des bedeutenden Anwendungsbereiches achtet die DQS streng darauf, nur branchenerfahrene Auditoren im Zertifizierungsverfahren einzusetzen. Mit diesem Expertenwissen auf Augenhöhe und der Bündelung einzelner Audits zu einem zeitlich abgeschlossenen Auditierungsprozess bieten wir Ihnen nachhaltigen Mehrwert.