IKT-Risikokontrolle und Informationssicherheit

Auslagerung des Beauftragten
IKT-Risikokontrolle und Informationssicherheit
Stand Mai 2026



Expertenwissen zu geringen Kosten

Die Begleitung Ihres IKT-Risikomanagementrahmens und Informationssicherheitsmanagements orientiert sich an den einschlägigen BSI-Standards zur Informationssicherheit sowie den ISO-Standards 27001 und 27002. Damit erfüllt Ihre Bank die Anforderungen der MaRisk und von DORA.

Die Herausforderung

Für Kreditinstitute besteht mit den Mindestanforderungen an das Risikomanagement (MaRisk „AT 7.2 Technisch-organisatorische Ausstattung") sowie von DORA die Notwendigkeit, IT-Systeme und IT-Prozesse sicher zu gestalten.

Bei der Ausrichtung verweist die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) auf die gängigen Standards für Informationssicherheit nach BSI-Grundschutz oder ISO 27001 und das auf dessen Basis einzurichtende Informationssicherheitsmanagement.

Organisatorische und technische Maßnahmen sind die Grundlagen, um ein angemessenes Sicherheitsniveau durch Einführung eines IKT-Risikomanagementrahmens und Informationssicherheitsmanagements zu erreichen. Wie ein geeignetes Managementsystem für Informationssicherheit genau aussieht, wird dabei in hohem Maße von der Größe und Infrastruktur des Unternehmens bestimmt.

Die Lösung: Auslagern

Wir helfen Ihnen, den IKT-Risikomanagementrahmen und das Informationssicherheitsmanagement als Teil des gesamten Risikomanagements sinnvoll zu etablieren, die vielfältigen gesetzlichen Anforderungen zu erfüllen und Daten als Vermögenswerte der Bank ausreichend zu den Grundwerten der Verfügbarkeit, Integrität und Vertraulichkeit abzusichern.

Unsere Erfahrung zeigt, dass eine Optimierung des IKT-Risikomanagementrahmens und des Informationssicherheitsmanagements oftmals die Informationssicherheit effektiver verbessert als Investitionen in die Sicherheitstechnik. Maßnahmen, die ursprünglich der Verbesserung der Informationssicherheit dienen, können sich auch außerhalb des Sicherheitszusammenhangs positiv auswirken und als gewinnbringend erweisen.

info@dz-cp.de
www.dz-cp.de

Unsere Leistungen

Der Beauftrage IKT-Risikokontrolle und Informationssicherheit der DZ CompliancePartner GmbH unterstützt Ihr internes Informationssicherheitsteam bei folgenden Aufgaben:

- Übernahme der Funktion und der Aufgaben des Beauftragten IKT-Risikokontrolle Informationssicherheit und seines Stellvertreters
- Erstellung des Informationssicherheitskonzepts einschließlich
  - Strukturanalyse
  - Schutzbedarfsanalyse
  - Dokumentation der Umsetzung von Sicherheitsmaßnahmen
- Einrichtung einer optimalen Organisationsstruktur für Informationssicherheit
- Erstellung, Implementierung und Aktualisierung von zielgruppengerechten Informationssicherheitsleitlinien und -anweisungen
- Abgrenzung von den Verantwortungsbereichen des Rechenzentrums
- Integration der Mitarbeiter in den Sicherheitsprozess
- Schulung der Mitarbeiter zur Informationssicherheit
- Koordination sicherheitsrelevanter Projekte
- Managementreporting und -bewertungen
- Bearbeitung von Sicherheitsvorfällen und Entwicklung von Lösungsvorschlägen

Ihre Vorteile

Einfach

- Sie erhalten praxisorientierte Lösungsvorschläge.
- Die Umsetzungsmaßnahmen sind mit Blick auf die gestellten Anforderungen angemessen.

Effektiv

- Ihr IKT-Risikomanagementrahmen und Informationssicherheitsmanagement wird effektiv und zuverlässig umgesetzt. Es erfüllt die Anforderungen der MaRisk AT 7.2 und von DORA auf Basis IT-Grundschutz (BSI) und ISO 27001. Bei Volksbanken Raiffeisenbanken wird darüber hinaus das Handbuch Ordnungsmäßigkeit der Rechenzentrale erfüllt.
- Sie profitieren vom Einsatz eines Anwendungstools zur Informationssicherheit
- Sie profitieren von dem Know-how erfahrenen Bankpraktikern im Umfeld der Kreditgenossenschaften.
- Sie profitieren von der objektiven Sicht und neutralen Bewertung unserer Spezialisten. Wir unterstützen Ihre betrieblichen Ziele.

Effizient

- Effiziente Dokumentation des Informationssicherheitskonzepts
- Sie profitieren von den Synergieeffekten eines Mehrmandantenanbieters.
- Sie senken den Aufwand Ihrer Internen Revision und bei der Abschlussprüfung. Ihre Kosten sinken spürbar im Vergleich.

Auf unsere Kompetenz verlassen sich deutschlandweit über 100 Kunden.

ANSPRECHPARTNER



Benjamin Wellnitz
Bereichsleiter IKT-Compliance
E-Mail: benjamin.wellnitz@dz-cp.de



Björn Blechenberg
Bereichsleiter Vertrieb,
E-Mail: vertrieb@dz-cp.de

IKT-Risikokontrolle und Informationssicherheit

Beratung zum Informationssicherheitskonzept
Stand Mai 2026

Risikokontrollfunktion inside DORA konform

Step by Step zum Informationssicherheitskonzept

Die Begleitung Ihres IKT-Risikomanagementrahmen und Informationssicherheitsmanagements orientiert sich insbesondere an den einschlägigen BSI-Standards zur Informationssicherheit sowie den ISO-Standards 27001 und 27002.

Die Herausforderung

Informationssicherheit ist niemals ein fixer Zustand, der – einmal erreicht – sich nicht mehr ändert: Sowohl der Informationssicherheitsprozess als auch die IT-Systme unterliegen einem Lebenszyklus, der beständig überprüft und angepasst werden muss.

Die Lösung: Auslagern

Mit unserer modularen Sicherheitskonzeption werden Sie in einzelne Phasen des Informationssicherheitsprozesses bedarfsorientiert unterstützt.

Lebenszyklus des IT-Sicherheitskonzepts nach Deming (PDCA-Modell)

PLAN Planung und Konzeption

- Wahl einer Methode zur Risikobewertung
- Klassifikation von Risiken bzw. Schäden
- Risikobewertung
- Strategieentwicklung zur Behandlung von Risiken
- Wahl von Informationssicherheitsmaßnahmen

DO Umsetzung

- Realisierungsplan für das Informationssicherheitskonzept
- Umsetzung der Informationssicherheitsmaßnahmen
- Überwachung und Steuerung der Umsetzung
- Aufbau Notfallvorsorge und Behandlung von Sicherheitsvorfällen
- Schulung und Sensibilisierung

CHECK Erfolgskontrolle, Überwachung

- Detektion von Informationssicherheitsvorfällen im laufenden Betrieb
- Überprüfung der Einhaltung von Vorgaben
- Überprüfung der Eignung, Wirksamkeit und Effizienz von Informationssicherheitsmaßnahmen
- Management-Berichte

ACT Optimierung

- Beseitigung von Fehlern
- Verbesserung von Informationssicherheitsmaßnahmen

info@dz-cp.de
www.dz-cp.de

Unsere Leistungen

Wir unterstützen Sie bei allen Schritten zur Erstellung und Pflege des Informationssicherheitskonzepts:

- IT-Strukturanalyse (schützenswerte Informationen, Geschäftsprozesse und IT-Strukturen)
- Risikobewertung durch Schutzbedarfsanalyse
- Ableitung konkreter Informationssicherheitsmaßnahmen aus dem identifizierten Schutzbedarf und der Risikobewertung
- Ggf. ergänzende Risikoanalyse und ergänzende Maßnahmen für Schutzobjekte mit hohem Schutzbedarf
- Konsolidierung und Umsetzung der Informationssicherheitsmaßnahmen
- Realisierungs- und Fälligkeitsplanung
- Verantwortlichkeitsplanung
- Risikoorientierte Umsetzungsreihenfolge
- Aktualisierungsmechanismus

Ihre Vorteile

- Sie schonen Ihre betrieblichen Ressourcen.
- Sie bestimmen bedarfsorientiert über den Einsatz unserer Leistungen.
- Sie erhalten praxisorientierte Lösungsvorschläge.
- Die Umsetzungsmaßnahmen sind mit Blick auf die gestellten Anforderungen angemessen.
- Sie profitieren vom Einsatz eines Anwendungstools zur Informationssicherheit
- Sie profitieren von dem Know-how erfahrener Bankpraktiker im Umfeld der Kreditgenossenschaften.
- Sie profitieren von der objektiven Sicht und neutralen Bewertung unserer Spezialisten.
- Effiziente Dokumentation des Informationssicherheitskonzepts.

ANSPRECHPARTNER



Benjamin Wellnitz
Bereichsleiter IKT-Compliance
E-Mail: benjamin.wellnitz@dz-cp.de



Björn Blechenberg
Bereichsleiter Vertrieb,
E-Mail: vertrieb@dz-cp.de

Datenschutz

Auslagerung des Beauftragten Datenschutz
Stand Mai 2026

Sicherheit in einem sensiblen Thema

Die Herausforderung

Seitdem die EU Datenschutz-Grundverordnung (DSGVO) Gültigkeit besitzt, wächst die Unsicherheit in den Unternehmen. Die möglichen Sanktionen bei Nichteinhaltung des Datenschutzes haben sich vervielfacht und Sanktionen werden – das zeigt das europäische Ausland – schon wesentlich früher verhängt als vor 2018.

Wenn in Ihrem Betrieb mehr als 19 Beschäftigte auf personenbezogene Daten zugreifen, sind Sie verpflichtet einen Datenschutzbeauftragten zu benennen. Das ist aber meist gar nicht so einfach. Der Datenschutzbeauftragte benötigt, um seine Aufgabe richtig wahrnehmen zu können, nicht nur Fachkenntnisse im Datenschutz, sondern auch tiefgehende Kenntnisse in der IT und in der unternehmenseigenen Organisation. Zudem ist er ständig fortzubilden. Das bindet personelle Ressourcen.

Die Lösung: Auslagern

Wir decken alle Belange des Datenschutzes ab, von der Information Ihrer Mitarbeiter bis zur Kontrolle technischer Datenschutzmaßnahmen. Unsere Spezialisten besitzen technisches Know-how und umfangreiche Kenntnisse in allen gesetzlichen Grundlagen.

So können Sie sicher sein, dass alle Themenfelder im Datenschutz effektiv und effizient bearbeitet werden.

Leistungen des Beauftragten Datenschutz

Anforderungen
durch Gesetze, Vorschriften, neue Technologien, Projekte, Menschen mit Fragen und Problemen

Input	**Beauftragter Datenschutz**	**Output**
recherchieren		beraten
informieren		realisieren
bewerten		informieren
		schulen

DZ CompliancePartner

info@dz-cp.de
www.dz-cp.de

Unsere Leistungen

- Kontinuierliche Beratung und Unterstützung zur Sicherstellung des Datenschutzes
- Kontrollen zur Zulässigkeit der Verarbeitung personenbezogener Daten
- Kontrollen zur Wahrung der Rechte Betroffener
- Prüfung der erforderlichen technischen und organisatorischen Maßnahmen
- Schulung und Unterrichtung der Mitarbeiter
- Entwicklung von Richtlinien zur betrieblichen Umsetzung des Datenschutzes
- Mitwirken bei neuen IT-Projekten: Berücksichtigung des Datenschutzes im Sinne des „Datenschutz by Design und by Default“ und Durchführung von Datenschutz-Folgenabschätzungen
- Führung der Datenschutzdokumentation für IT-Verfahren
- Regelmäßige Berichte an Vorstände bzw. Geschäftsführung und betroffene Geschäftsbereiche
- Unterstützung Ihres Auslagerungsmanagements
- Regelmäßige Abstimmung mit den Regionalverbänden und Aufsichtsbehörden

Ihre Vorteile

Einfach

- „Datenschutz mit Augenmaß“: Wir fokussieren uns auf die wirklich relevanten Themen.

Effektiv

- Effektive und zuverlässige Umsetzung der Aufgaben des Datenschutzbeauftragten.
- Sie profitieren von unserer Unvoreingenommenheit gegenüber der Sache und dem Betrieb.
- Sie vermeiden innerbetriebliche Interessenkonflikte.
- Sie vermeiden Imageschäden und bauen Vertrauen auf.

Effizient

- Sie vermeiden das Risiko interner Kosten zur Schadensbehebung.
- Sie vermeiden das Risiko externer Kosten durch Schadensersatz und Strafen.
- Sie senken Ihre Kosten: Keine Aus- und Weiterbildung.
- Ihre Mitarbeiter können sich ihren Hauptaufgaben widmen.

Auf die Kompetenz unserer Datenschutzspezialisten zählen bereits über 190 Kunden. Damit sind wir einer der größten Dienstleister im Datenschutzmanagement.

ANSPRECHPARTNER



Benjamin Wellnitz
Bereichsleiter IKT-Compliance
E-Mail: benjamin.wellnitz@dz-cp.de



Björn Blechenberg
Bereichsleiter Vertrieb,
E-Mail: vertrieb@dz-cp.de

Datenschutz

CheckUp Datenschutz
Stand Mai 2026

Neutrale Bewertung, konkrete Optimierungsvorschläge

Jedes Unternehmen, das mit sensiblen Daten umgeht, muss dafür sorgen, dass seine Maßnahmen zum Schutz dieser Daten stets auf dem neuesten Stand sind.

Die Herausforderung

Die Datensicherheit ist zunehmend Gefährdungen ausgesetzt, die das Unternehmen allein oft nur schwer oder erst spät erkennen kann. Dies sind zum Beispiel:

- Unzureichende Absicherung der Datenverarbeitung
- Verletzung der Vertraulichkeit
- Unzulässige Datenweitergabe
- Verfälschung von Daten

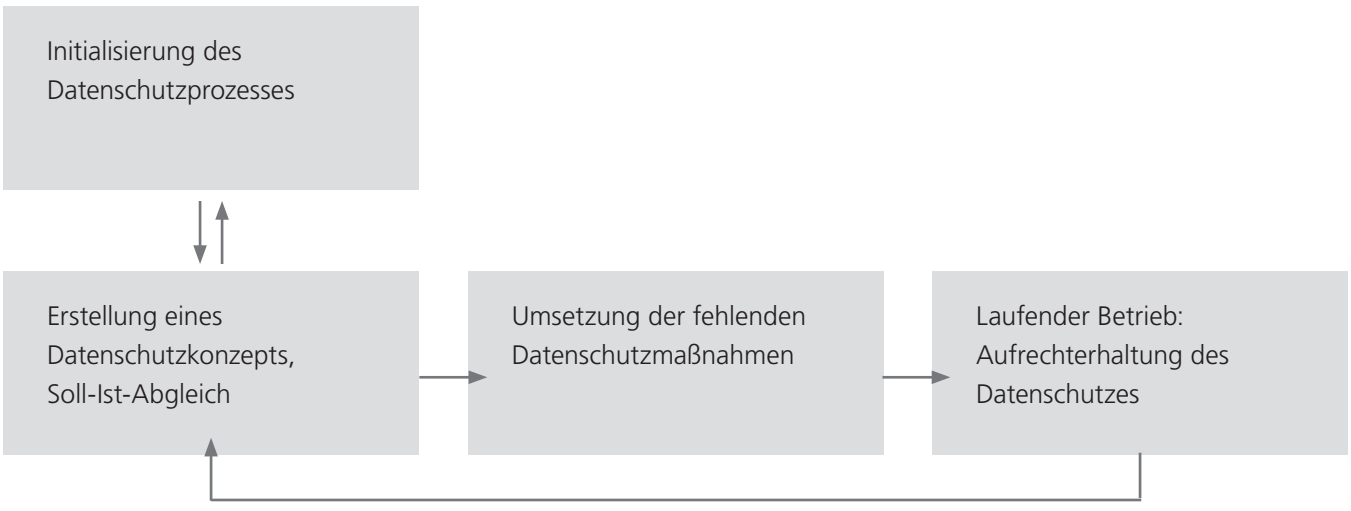
Die Lösung: Datenschutz CheckUp

Unser Datenschutz CheckUp bietet Ihnen:

- Vollständige Prüfung und neutrale Bewertung Ihres aktuellen Datenschutzniveaus
- Konkrete Vorschläge zur Optimierung
- Klare Rechtssicherheit

Die Datenschutzexperten der DZ CompliancePartner setzen gesetzliche Vorschriften in effektive und wirtschaftlich vertretbare Verfahrensweisen und Verfahrensregeln um. Ihre Datenschutzbestimmungen werden objektiv geprüft.

Datenschutzprozess



DZ CompliancePartner

info@dz-cp.de
www.dz-cp.de

Unsere Leistungen

Der Datenschutz CheckUp verläuft in drei Phasen und berücksichtigt den gesamten Datenschutzprozess.

Phase 1: Vorbereitung und Durchführung

Anhand von Unterlagen Ihres Hauses ermitteln wir Risiken und setzen Schwerpunkte für den CheckUp. Wir analysieren die vorhandenen Maßnahmen zum Datenschutz auf Schwachstellen und die Möglichkeiten zur Optimierung.

Phase 2: Optimierung

Wir beraten Sie vor Ort und empfehlen direkte Maßnahmen zur Optimierung Ihres Datenschutzes. Wir zeigen auch Mängel auf und erarbeiten mit Ihren Mitarbeitern konkrete Lösungsvorschläge.

Phase 3: Bericht

Im Rahmen einer Schlussbesprechung präsentieren wir Ihnen die Ergebnisse des CheckUp und deren Bewertung. Wir zeigen das Optimierungspotenzial auf und unterstützen Sie mit praxiserprobten Lösungsvorschlägen.

Ihre Vorteile

- Sie erhalten eine vollständige Prüfung und neutrale Bewertung des Status quo im betrieblichen Datenschutz.
- Mehr als eine reine Check-Untersuchung: Sie erhalten konkrete Vorschläge zur Optimierung.
- Vor-Ort-Beratung sind selbstverständlich.
- Ihr Datenschutzniveau wird durch den CheckUp-Bericht dokumentiert.
- Sie haben weniger Aufwand für die Interne Revision und bei der Abschlussprüfung.
- Ihr betrieblicher Datenschutzbeauftragte wird untestützt.
- Sie profitieren von dem Know-how eines Mehrmadantenanbieters.

Auf die Kompetenz unserer Datenschutzspezialisten zählen bereits über 190 Kunden.

ANSPRECHPARTNER



Benjamin Wellnitz
Bereichsleiter IKT-Compliance
E-Mail: benjamin.wellnitz@dz-cp.de



Björn Blechenberg
Bereichsleiter Vertrieb,
E-Mail: vertrieb@dz-cp.de

Notfallkonzeption

Punktuelle oder dauerhafte Unterstützung
Stand Mai 2026

MaRisk-konform und TÜV-zertifiziert

Nach MaRisk ist jede Bank verpflichet, „für alle kritischen Aktivitäten und Prozesse Vorsorge zu treffen". Die BaFin stellt heute konkrete Rahmenbedingungen zum gesamten Notfallmanagement des Instituts.

Die Herausforderung

Die einzelne Bank stößt bei der Notfallkonzeption schnell an ihre Grenzen, da hier Know-how in vielen Bereichen gefragt ist: In der Ablauforganisation etwa, wenn es um die Analyse der Geschäftsprozesse geht, oder im Gebäudemanagement, um Sofortmaßnahmen zu etablieren.

Die zeitgemäße Notfallkonzeption nach MaRisk fordert ein ganzheitliches Vorgehen, das sich am gesamten Geschäftsprozess orientiert. Es gilt, aus den einzelnen Teil-Notfallplänen ein Gesamtkonzept zu schmieden und dessen „Wirksamkeit und Angemessenheit" (MaRisk) regelmäßig durch Tests zu überprüfen.

Die Lösung:
Modulare, am Bedarf ausgerichtete Unterstützung

Unsere Notfallkonzeption ist modular aufgebaut: Abgeleitet von der Normalorganisation erstellen wir zu den Bereichen Krisenmanagement, Prozessfortführung, IT-Wiederanlauf und Sofortmaßnahmen zielgruppenorientierte Notfallhandbücher und halten diese aktuell. Die Grenzen zwischen Normal- und Notfallorganisation lassen sich so eindeutig erkennen und die Verantwortlichkeiten besser zuweisen.

Als erster deutscher Dienstleister wurden wir für unsere Notfallkonzeption mit dem TÜV-Siegel ausgezeichnet.

TÜV SAARLAND Geprüftes Notfallmanagement Systemprüfung
tuev-saar.de/TK45781

	Normalorganisation	Notfallorganisation
Vorstand	Strategien, Leitlinien, Policies	Strategien, Leitlinien, Policies
Leitungsebene	Risikomanagement	Krisenmanagement
Fachbereiche	Prozesssicherheit	Prozessfortführung
EDV-Management	IT-Verfügbarkeit	IT-Wiederanlauf
Gebäudemanagement	Schutzmaßnahmen	Sofortmaßnahmen
	IT-Sicherheitskonzept (ISME)	**Notfallkonzept**

DZ CompliancePartner

info@dz-cp.de
www.dz-cp.de

Unsere Leistungen

Wir erarbeiten einen Entwurf zu allen Notfalldokumenten. Die Übernahme von Musteränderungen in Ihre individuellen Notfallpläne wird technisch unterstützt und ist komfortabel durchzuführen.

- Elektronische Erfassung der Organisationseinheiten und Personen
- Auslieferung des Muster-Notfallplans in Form einer Lotus-Notes-Datenbank
- Unterstützung bei individueller Anpassung des Notfallplans
- Elektronischer Druck der zielgruppenbezogenen Handbücher

Basisversorgung

- Erfassung der bankspezifischen Infrastruktur in der Lotus-Notes-Datenbank „Stammdaten“
- Beratung und Verifizierung der Daten
- Notfallkonzept, das zielgruppenorientiert in Lotus-Notes-Datenbanken und verschiedenen Handbüchern ausgefertigt wird
- Zentrale Anpassung des Notfallkonzepts und der Notfalldatenbank

Zusatzleistungen

Wir bieten umfassende Unterstützung, damit Sie das Notfallkonzept komfortabel pflegen, die Handbücher mit geringstem Aufwand aktuell halten und die Anforderungen der MaRisk dauerhaft erfüllen können:

- Zentrale Aktualisierung des Notfallkonzepts und der Notfalldatenbank
- Musterübungsplan
- Vorbereitung, Begleitung, Auswertung und Dokumentation strukturierter Notfalltests
- Technische Unterstützung
- Schulung der Mitarbeiter

Ihre Vorteile

Unsere Beratung verbindet die Anforderungen aus über 40 Rechtsgrundlagen mit den praktischen Bedürfnissen Ihrer Bank. Auf Basis einer hocheffizienten Datenbanklösung liefern wir Ihnen zielgruppengerechte Notfalldokumente und -handbücher. So werden Ihre Mitarbeiter nur mit den Informationen konfrontiert, die sie im Ernstfall wirklich brauchen.

Mit der einmaligen Einführung des Notfallkonzepts ist es freilich nicht getan. Deshalb können wir als Zusatzleistung die Pläne regelmäßig aktualisieren und Sie bei der Durchführung strukturierter Notfalltests unterstützen. So ist dauerhaft gewährleistet, dass die Notfalldokumentationen und -maßnahmen auch greifen.

Sie profitieren von einer kostengünstigen und effizienten Lösung.

- Ihr Notfallkonzept ist immer auf dem neuesten Stand.
- Sie reduzieren den Prüfungsaufwand durch das zentrale Zertifizierungsaudit des TÜV

Über 100 Banken zählen bereits auf diesen geprüften Service.

ANSPRECHPARTNER



Benjamin Wellnitz
Bereichsleiter IKT-Compliance
E-Mail: benjamin.wellnitz@dz-cp.de



Björn Blechenberg
Bereichsleiter Vertrieb,
E-Mail: vertrieb@dz-cp.de