Creditreform Compliance

Whitepaper Informations-sicherheit

Wie Unternehmen regulatorischen Anforderungen erfüllen, Risiken minimieren und Informationssicherheit strategisch umsetzen

Mit vielen Praxistipps und Beispielen

Informationssicherheit ist heute kein rein technisches Thema mehr. Sie ist ein integraler Bestandteil der Unternehmensführung, der Risikosteuerung und – je nach Branche – ein zentraler Baustein regulatorischer Compliance.

Informationssicherheit im Unternehmenskontext

Unternehmen sind inzwischen in nahezu allen Kernprozessen digitalisiert. Dies betrifft insbesondere die Finanzbuchhaltung und ERP-Systeme, Produktions- und Steuerungssysteme, Kunden- und Lieferantendatenbanken, Cloud-Infrastrukturen sowie digitale Kommunikationssysteme. IT übernimmt damit nicht mehr nur eine unterstützende Funktion, sondern ist geschäftskritisch für die Aufrechterhaltung operativer Prozesse und die Sicherstellung der Wertschöpfung.

Aus Sicht der Unternehmenssteuerung ist Informationssicherheit folglich ein wesentliches Element des internen Kontrollsystems (IKS) und des Risikomanagementsystems (RMS). Sie bildet die Grundlage für die Zuverlässigkeit der Finanzberichterstattung und ist zugleich ein Bestandteil ordnungsgemäßer Corporate Governance.

Spätestens seit regulatorischen Entwicklungen wie der NIS-2-Richtlinie und der DORA-Verordnung ist Informationssicherheit zudem kein freiwilliger Reifegradfaktor mehr, sondern für viele Unternehmen eine rechtliche Verpflichtung.

Aus Prüfersicht ist Informationssicherheit insbesondere im Hinblick auf die Ordnungsmäßigkeit der Buchführung, die Integrität von Daten, den Schutz vor Manipulationen sowie die Verlässlichkeit IT-gestützter Kontrollen von zentraler Bedeutung.

Informationssicherheit ist damit nicht lediglich ein IT-Thema, sondern ein wesentlicher Bestandteil der Unternehmenssicherheit und der unternehmerischen Steuerung insgesamt.

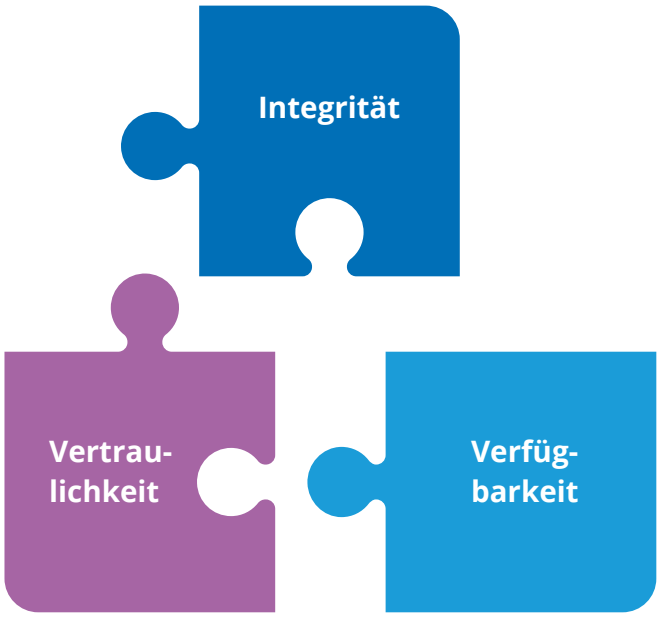
Was bedeutet Informationssicherheit?

Informationssicherheit schreibt den Schutz von Informationssystemen vor:

- Unbefugtem Zugriff
- Manipulation
- Datenverlust
- Ausfall
- Missbrauch

Kernziel ist die Sicherstellung der drei Schutzziele:

Schutzziel	Bedeutung	Management-Relevanz
Vertraulichkeit	Schutz vor unbefugter Einsicht	Datenschutz, Wettbewerb
Integrität	Schutz vor unbefugter Veränderung	Bilanzsicherheit
Verfügbarkeit	Sicherstellung der Nutzbarkeit	Geschäftskontinuität



Ergänzend werden heute häufig weitere Schutzziele berücksichtigt:

- Authentizität
- Verbindlichkeit
- Zurechenbarkeit
- Resilienz
- Nichtabstreitbarkeit

Wichtige Abgrenzung: Informationssicherheit vs. IT-Sicherheit

- ✔ IT-Sicherheit bezieht sich auf technische und organisatorische Schutzmaßnahmen für IT-Systeme.
- ✔ Informationssicherheit umfasst darüber hinaus auch physische und organisatorische Schutzmaßnahmen für Informationen allgemein.
- ✔ Cybersecurity fokussiert stärker auf externe Bedrohungen aus dem digitalen Raum.

In der Praxis werden diese Begriffe häufig synonym verwendet, fachlich sind sie jedoch differenziert zu betrachten.

Begriffsbestimmungen

Für eine saubere Governance-Struktur sind klare Definitionen erforderlich. Nur wenn zentrale Begriffe eindeutig und unternehmensweit einheitlich verstanden werden, können Verantwortlichkeiten klar zugeordnet und Risiken konsistent bewertet werden. Präzise Begriffsbestimmungen bilden daher die Grundlage für Transparenz, Nachvollziehbarkeit und regulatorische Belastbarkeit im Bereich der Informationssicherheit.

IT-Risiko

Risiko eines Schadens aus unzureichender IT-Sicherheit, Systemausfall oder Datenmanipulation.

Cyberangriff

Gezielter Versuch, Systeme oder Daten unbefugt zu kompromittieren.

ISMS (Informationssicherheits-Management-System)

Systematischer Ansatz zur Steuerung und kontinuierlichen Verbesserung der Informationssicherheit.

Technische und organisatorische Maßnahmen (TOMs)

Schutzmaßnahmen gem. DSGVO, z. B. Verschlüsselung, Zugriffskontrollen, Berechtigungskonzepte.

Business Continuity Management (BCM)

Sicherstellung der Fortführung kritischer Geschäftsprozesse im Krisenfall.

Regulatorische und prüfungsrelevante Standards

Informationssicherheit unterliegt einer Vielzahl von regulatorischen Rahmenwerken. Diese sind branchen- und größenabhängig unterschiedlich relevant.

Europäische Regulierung

NIS-2-Richtlinie

Verpflichtet wesentliche und wichtige Einrichtungen zur Implementierung von Cyber-Risikomanagementmaßnahmen.

DORA-Verordnung

Spezifisch für Finanzunternehmen: Anforderungen an ICT-Risikomanagement, Vorfallmeldung, Tests, Drittparteienrisiken.

Datenschutz-Grundverordnung

Technische und organisatorische Maßnahmen (TOMs) zum Schutz personenbezogener Daten.

Nationale Standards

IT-Grundschutz des BSI

Standardisiertes Rahmenwerk des BSI zur systematischen Implementierung und Zertifizierung eines Informationssicherheits-Managementsystems.

Deutsches Informationssicherheitsgesetz

Nationale gesetzliche Regelung zur Erhöhung der Cybersicherheit, insbesondere für Betreiber Kritischer Infrastrukturen (KRITIS) und Unternehmen mit besonderem öffentlichem Interesse.

Mindestanforderungen an das Risikomanagement

Aufsichtsrechtliche Vorgaben der Bundesanstalt für Finanzdienstleistungsaufsicht zur Ausgestaltung eines angemessenen Risikomanagementsystems in Finanzinstituten, einschließlich IT- und Auslagerungsrisiken.

Aus Prüfersicht steht nicht die technische Perfektion im Fokus, sondern:

- ✔ Durchführung angemessener Kontrollen
- ✔ Wirksamkeit dieser Kontrollen
- ✔ Angemessene Dokumentation
- ✔ Risikoorientierte Ausgestaltung

Internationale Standards

ISO/IEC 27001

Standard für ISMS.

COBIT

International anerkanntes Governance- und Kontrollrahmenwerk zur Steuerung und Überwachung der Informationstechnologie im Unternehmen.

NIST Cybersecurity Framework

Strukturierter Ansatz zur Identifikation, Bewertung und Steuerung von Cyber-Risiken.

Prüfungsrelevante Standards (JAP)

IDW PS 330

Prüfung von IT-Systemen im Rahmen der Abschlussprüfung.

IDW PS 261 n.F.

Konkretisiert die Anforderungen an die Prüfung von IT-gestützten rechnungslegungsbezogenen Prozessen und internen Kontrollen im Rahmen der Abschlussprüfung.

ISA 315

Identifikation und Beurteilung von Risiken wesentlicher falscher Darstellungen.

Warum Informationssicherheit entscheidend ist

Informationssicherheit ist entscheidend aus fünf Perspektiven:

1. Finanzielle Risiken

- Betriebsunterbrechungen
- Lösegeldzahlungen (Ransomware)
- Wiederherstellungskosten
- Reputationsschäden

2. Bilanzielle Auswirkungen

- Wertminderungen
- Rückstellungen
- Wiederherstellungskosten
- Offenlegungspflichten

3. Haftungsrisiken

Geschäftsleiter unterliegen Organisationspflichten.
Unzureichende Informationssicherheitsmaßnahmen:

- Organhaftung auslösen
- Compliance-Verstöße darstellen
- Aufsichtsrechtliche Sanktionen nach sich ziehen

4. Reputations- und Vertrauensverlust

Vertrauen ist ein immaterieller Vermögenswert. Cybervorfälle können nachhaltig marktwertrelevant sein.

5. Strategische Wettbewerbsfähigkeit

Informationssicherheit ist zunehmend Teil von Ausschreibungen und Lieferantenbewertungen.

Praktische Beispiele zur Informationssicherheit

Beispiel 1: Manipulation von Zahlungsdaten

In einem Unternehmen werden Änderungen an Kreditoren- oder Debitorenstammdaten ohne wirksames Vier-Augen-Prinzip vorgenommen. Dadurch besteht die Möglichkeit, dass Bankverbindungen unbemerkt manipuliert werden – sei es durch interne Akteure oder infolge eines kompromittierten Benutzerkontos.

Die Folge können Fehlüberweisungen auf betrügerische Konten, unmittelbare Liquiditätsabflüsse sowie aufwendige Rückabwicklungsverfahren sein. Neben dem direkten finanziellen Schaden entstehen erhebliche Reputationsrisiken sowie potenzielle Prüfungsfeststellungen im Rahmen der Jahresabschlussprüfung, da die Integrität rechnungslegungsbezogener Prozesse beeinträchtigt ist.

Beispiel 2: Ransomware-Angriff

Ein Unternehmen verfügt weder über eine konsequente Netzsegmentierung noch über regelmäßig getestete, physisch getrennte Offline-Backups. Im Falle eines erfolgreichen Ransomware-Angriffs werden zentrale Systeme, etwa ERP- oder Produktionssteuerungssysteme verschlüsselt und sind nicht mehr verfügbar.

Die unmittelbare Folge ist ein mehrtägiger Produktions- oder Betriebsstillstand mit erheblichen Umsatzausfällen. Hinzu kommen mögliche Vertragsstrafen, Wiederherstellungskosten, externe Forensikaufwendungen sowie regulatorische Meldepflichten, beispielsweise nach der NIS-2-Richtlinie. In besonders schwerwiegenden Fällen können bilanzielle Effekte und Offenlegungspflichten entstehen.

Beispiel 3: Unzureichende Zugriffskontrollen

Zugriffsrechte werden nach dem Ausscheiden von Mitarbeitenden nicht zeitnah entzogen oder regelmäßig überprüft. Ehemalige Beschäftigte oder nicht mehr autorisierte Personen behalten somit weiterhin Zugriff auf sensible Systeme und Datenbestände.

Dies eröffnet ein erhebliches Risiko für Datenabfluss, Manipulation geschäftskritischer Informationen oder missbräuchliche Transaktionen. Neben dem unmittelbaren Sicherheitsrisiko entstehen Compliance-Verstöße, etwa im Kontext der Datenschutz-Grundverordnung sowie potenzielle Schwächen im internen Kontrollsystem, die im Rahmen einer Abschlussprüfung als Kontrollmangel gewertet werden können.

Diese Beispiele zeigen: Informationssicherheit ist kein theoretisches Risiko, sondern operativ relevant.

Schritte zur erfolgreichen Umsetzung

Ein strukturierter Implementierungsansatz umfasst:

Governance etablieren

- Klare Verantwortlichkeiten
- Berichtslinien an Geschäftsleitung
- Integration in Risikomanagement

Risikoanalyse durchführen

- Identifikation kritischer Systeme
- Bewertung von Eintrittswahrscheinlichkeit und Schadenshöhe
- Priorisierung

Schutzmaßnahmen definieren

- Zugriffskontrollen
- Verschlüsselung
- Backup-Strategien
- Patch-Management
- Awareness-Schulungen

Dokumentation und Integration eines internen Kontrollsystems (IKS)

- Kontrollbeschreibungen
- Nachweisführung
- Testing-Zyklen

Monitoring und kontinuierliche Verbesserung

- Regelmäßige Audits
- Penetrationstests
- Incident-Management-Prozesse
- Lessons Learned

Informationssicherheit ist kein Projekt, sondern ein fortlaufender Prozess.

Fazit: Wieso Informationssicherheit für Unternehmen so wichtig ist

Informationssicherheit ist heute weit mehr als eine technische Disziplin. Sie ist ein zentrales Governance-Thema, ein prüfungsrelevanter Bestandteil des internen Kontrollsystems, eine regulatorische Verpflichtung und zugleich ein strategischer Erfolgsfaktor. Ihre Relevanz erstreckt sich von der operativen Prozesssicherheit über die Verlässlichkeit der Finanzberichterstattung bis hin zur Organverantwortung der Unternehmensleitung.

Unternehmen, die Informationssicherheit ausschließlich als Aufgabe der IT-Abteilung verstehen, unterschätzen ihre wirtschaftliche und haftungsrechtliche Tragweite. Eine isolierte, rein technische Betrachtung greift zu kurz und wird den Anforderungen moderner Regulierung, steigender Cyberrisiken und wachsender Prüfungsanforderungen nicht gerecht.

Demgegenüber schaffen Organisationen, die Informationssicherheit strukturiert, risikoorientiert und prüfungssicher implementieren, einen nachhaltigen Mehrwert.

Mehrwert

- **Operative Resilienz erhöhen**
  Erhöhte Handlungsfähigkeit und Widerstandsfähigkeit gegenüber operativen Herausforderungen
- **Regulatorische und haftungsrechtliche Risiken reduzieren**
  Minimierung rechtlicher Risiken und Erfüllung regulatorischer Anforderungen.
- **Verlässlichkeit stärken**
  KI-Lösungen können Arbeitsabläufe optimieren und verbessern
- **Vertrauensvorsprung schaffen**
  Messbare Fortschritte steigern das Vertrauen von Investoren, Geschäftspartnern und Aufsichtsbehörden

Aus Sicht eines Wirtschaftsprüfers ist daher klar: Eine belastbare, dokumentierte und wirksam implementierte Informationssicherheitsstruktur ist heute eine Grundvoraussetzung ordnungsgemäßer und zukunftsfähiger Unternehmensführung.

Jetzt handeln – Ihr Wettbewerbsvorteil durch Informationssicherheit

Die Regulierung der Informationssicherheit ist längst keine theoretische Perspektive mehr, sondern gelebte Realität in nahezu allen Branchen.
Unternehmen, die Informationssicherheit heute strategisch verankern und proaktiv umsetzen, verschaffen sich nicht nur regulatorische Sicherheit, sondern auch einen nachhaltigen Wettbewerbs- und Vertrauensvorsprung gegenüber weniger vorbereiteten Marktteilnehmern.

Unser Angebot für Sie:

- ✔ **Erstgespräch**
  Gemeinsames Kennenlernen und Einordnung Ihrer Ausgangssituation
- ✔ **Erstberatung**
  Analyse Ihres aktuellen Informationssicherheitsstatus und Compliance-Bedarfs
- ✔ **Maßgeschneiderte Compliance-Strategie**
  Entwicklung einer individuellen IT-Compliance-Roadmap
- ✔ **Richtlinien & Arbeitsanweisungen**
  Erstellung und Implementierung von Richtlinien und Arbeitsanweisungen für die Beschäftigten
- ✔ **Aufbau oder Optimierung eines ISMS**
  Aufbau eines ISMS sowie Integration in bestehende Governance- und Risikostrukturen
- ✔ **Schulungen & Sensibilisierung**
  Mitarbeiterschulungen zur Erfüllung regulatorischer Anforderungen und zur Reduktion menschlicher Risiken

AUSBLICK

Informationssicherheit entwickelt sich zunehmend zu einem strategischen Steuerungsinstrument und festen Bestandteil moderner Unternehmensführung. Regulatorische Anforderungen und Erwartungen von Geschäftspartnern sowie Prüfern steigen kontinuierlich und verlangen nach belastbaren, dokumentierten Sicherheitsstrukturen.

Unternehmen, die frühzeitig in eine risikoorientierte und wirtschaftlich tragfähige Sicherheitsarchitektur investieren, stärken nicht nur ihre Resilienz, sondern sichern sich einen nachhaltigen Vertrauens- und Wettbewerbsvorteil.

Sprechen Sie uns an und machen Sie IT-Compliance zu Ihrem Erfolgsfaktor!

Telefon: +49 2131 109-1089
info@creditreform-compliance.de
www.creditreform-compliance.de

Creditreform Compliance

INFORMATIONSSICHERHEIT FÜR IHR UNTERNEHMEN

Cyberrisiken minimieren, Sicherheit gewinnen, Anforderungen erfüllen

Creditreform Compliance Services begleitet Sie von der Betroffenheitsprüfung über die vollständige Umsetzung der regulatorischen Anforderungen bis zur prüfungssicheren Implementierung.

- ✓ Lassen Sie sich zur NIS-2-Richtlinie beraten
- ✓ Erfüllen Sie die Anforderungen der DORA-Verordnung
- ✓ Setzen Sie auf einen externen Informationssicherheitsbeauftragten
- ✓ Stärken Sie die Informationssicherheit Ihres Unternehmens beim Jahresabschluss

Praxisnah, strukturiert & rechtssicher.

Jetzt beraten lassen und Ihre Informationssicherheit optimieren

Creditreform Compliance