Eine Veröffentlichung des ISACA Germany Chapter e.V.

Prüfungsleitfaden IT-Compliance

ISACA Germany Chapter

dpunkt.verlag

Prüfungsleitfaden IT-Compliance

Herausgeber:
ISACA Germany Chapter e.V.
Storkower Straße 158
10407 Berlin
www.isaca.de
info@isaca.de

Autorenteam:
- David Zaißmann, CISA (Genoverband e.V.)
- Diana Nestler, CISA (SONNTAG IT Solutions GmbH & Co. KG)
- Ioannis Karamitros, CIA (Ioannis Karamitros Consulting)
- Prof. Dr. Michael Klotz (Hochschule Stralsund)
- Oliver Dax, CISA (Genoverband e.V.)
- Uwe Brinkmann, CISA (Sparkassenverband Niedersachsen)

Fotocredit:
Shutterstock: 1686839911©Sashkin

Stand: Dezember 2025 (Final nach Review und Überarbeitung durch die ISACA-Fachgruppe IT-Compliance)

Inhaltsverzeichnis

Vorwort

Die Informationstechnologie (IT) ist zu einem integralen Bestandteil jeder modernen Organisation geworden, von kleinen Start-ups bis zu globalen Konzernen. Sie ermöglicht nicht nur effiziente Geschäftsprozesse, sondern treibt Innovationen voran und eröffnet neue Möglichkeiten für Wachstum und Wettbewerbsvorteile. Die Vorteile der Nutzung von IT sind unbestreitbar, doch gleichzeitig bringen neue Technologien auch Herausforderungen mit sich, nicht zuletzt im Bereich der Compliance. Die Sicherstellung der IT-Compliance ist essenziell, um die Integrität, Vertraulichkeit und Verfügbarkeit von Informationen zu gewährleisten und gleichzeitig gesetzliche Anforderungen und regulatorische Standards zu erfüllen. Dies ist keine optionale Aufgabe, sondern eine grundlegende Verpflichtung für jedes Unternehmen, das sich den rechtlichen, ethischen und operativen Risiken bewusst ist, die mit einer mangelnden Compliance einhergehen können.

Die Überprüfung der IT-Compliance durch gezielte Prüfungsfragen ist ein unverzichtbarer Bestandteil dieses Prozesses. Sie ermöglicht es Unternehmen, ihre Systeme und Prozesse kritisch zu hinterfragen, potenzielle Schwachstellen aufzudecken und effektive Kontrollmechanismen zu implementieren. Prüfungsfragen dienen nicht nur der Bewertung der aktuellen Compliance-Praktiken, sondern fördern auch die kontinuierliche Verbesserung und Weiterentwicklung der IT-Governance und der Sicherheitsmaßnahmen.

Die Autorinnen und Autoren

Die Fachgruppe »IT-Compliance«

In Unternehmen ist die Informationstechnologie kontinuierlich mit neuen gesetzlichen Vorgaben, Standards und internen Regelungen konfrontiert. Dies stellt Führungskräfte und Mitarbeiter vor die Herausforderung, stets aktuell informiert zu bleiben.

Die Schwerpunkte der Fachgruppe »IT-Compliance« liegen auf dem Berufsbild des IT-Compliance-Managers sowie der Gestaltung der IT-Compliance-Funktion und deren Schnittstellen innerhalb von Unternehmen. Sie nimmt aktiv Stellung zu aktuellen Entwicklungen im Bereich der IT-Compliance und strebt danach, die Compliance-Landschaft nachhaltig zu beeinflussen. Durch die Erarbeitung von Arbeitspapieren und Leitfäden, die kostenfrei für Mitglieder zugänglich sind, fördert die Fachgruppe Wissen, Innovation und praktische Unterstützung in der IT-Compliance.

Um den größtmöglichen Nutzen aus dem Prüfungsleitfaden zu ziehen, sollte dieser in Verbindung mit dem Leitfaden »IT-Compliance« [Schmidt et al. 2021] gelesen werden.

Für an einer Mitarbeit Interessierte bietet die Fachgruppe »IT-Compliance« die Möglichkeit, über die Funktionsmail *FG-IT-Compliance@isaca.de* Kontakt aufzunehmen und sich aktiv einzubringen.

Diana Nestler
ISACA Germany Chapter e.V.
Leiterin ISACA-Fachgruppe IT-Compliance

Jutta Zilian
ISACA Germany Chapter e.V.
Stellv. Leiterin ISACA-Fachgruppe IT-Compliance

Danksagung

Die Grundlage des Prüfungsleitfadens bildet der bereits im Jahr 2021 erschienene Leitfaden »IT-Compliance« der Fachgruppe IT-Compliance.

Der Dank gilt den Autorinnen und Autoren des Leitfadens, die diesen Prüfungsleitfaden erst ermöglicht haben:
David Zaißmann, CISA (Genoverband e.V.)
Diana Nestler, CISA (SONNTAG IT Solutions GmbH & Co. KG)
Ioannis Karamitros, CIA (Ioannis Karamitros Consulting)
Prof. Dr. Michael Klotz (Hochschule Stralsund)
Oliver Dax, CISA (Genoverband e.V.)
Uwe Brinkmann, CISA (Sparkassenverband Niedersachsen)

1 Erläuterungen zum Prüfungsleitfaden

Der vorliegende »Prüfungsleitfaden IT-Compliance« stellt ein Instrument dar, das Unternehmen dabei unterstützt, ihre IT-Systeme und -Prozesse im Einklang mit regulatorischen Anforderungen, internen Richtlinien und branchenspezifischen Standards zu halten. Er bietet eine umfassende Sammlung von Fragen, die darauf abzielen, die Einhaltung verschiedener Compliance-Anforderungen systematisch zu bewerten.

Bei einem IT-Compliance-Management-System (IT-CMS) eines Unternehmens handelt es sich in der Regel nicht um ein eigenständiges System, das unabhängig und als »Silo« in der IT implementiert wird. Vielmehr hat sich die Ausgestaltung des IT-CMS an den Rahmenbedingungen des unternehmensweiten Compliance-Management-Systems zu orientieren. Dies gilt für alle Komponenten des IT-CMS. Beispielsweise sollten IT-Compliance-Ziele aus den Compliance-Zielen des Unternehmens abgeleitet bzw. in eine hierarchische Zielpyramide des Unternehmens integriert werden.

Der Leitfaden ist thematisch entlang zentraler Elemente der IT-Compliance aufgebaut, die eine strukturierte und praxisnahe Bewertung ermöglichen. Den Einstieg bildet die schriftlich fixierte Ordnung (sfO), in der die formalen Grundlagen des IT-CMS festgelegt sind. Hierzu zählen insbesondere die Definition zentraler Begriffe, die Etablierung einer Aufbauorganisation nach dem Drei-Linien-Modell sowie die Dokumentation von Zuständigkeiten, Verantwortlichkeiten und Prozessen. Die sfO bildet die Basis für alle weiteren Elemente des IT-CMS und dient als Referenzrahmen für dessen Umsetzung und Steuerung.

Die Compliance-Kultur und Awareness-Maßnahmen bilden das weiche Fundament eines wirksamen IT-CMS. Dieses Themenfeld beleuchtet, inwieweit Werte, Haltungen und Verhaltensweisen im Unternehmen in Bezug auf Compliance gefördert und gelebt werden. Besondere Aufmerksamkeit gilt dabei dem »Tone at the Top« sowie der Kommunikation relevanter Inhalte über Schulungen, Awareness-Kampagnen und interne Informationsformate.

Die Pflege eines Normenregisters und die Ableitung von Anforderungen an die IT beschäftigen sich mit der strukturierten Erhebung, Dokumentation und Umsetzung externer und interner Vorgaben. Hierbei geht es darum, regulatorische Anforderungen systematisch zu erfassen, Verantwortlichkeiten zu definieren und Handlungsanweisungen abzuleiten, die für die Einhaltung von IT-Compliance entscheidend sind. Ein aktuelles, gepflegtes Normenregister bildet dafür das zentrale Steuerungsinstrument.

In der Steuerung und dem Monitoring des IT-Compliance-Risikos und der IT-Compliance-Level liegt der Fokus auf der kontinuierlichen Überwachung und Bewertung bestehender Risiken und Maßnahmen. Es wird geprüft, ob ein strukturiertes Risikomanagement besteht, geeignete Kontrollen etabliert sind und ob der Grad der Zielerreichung mittels definierter Kennzahlen (KPIs) messbar gemacht wird. Auch die Integration in bestehende Überwachungssysteme wie Informationssicherheits-Managementsysteme oder Datenschutz wird hier betrachtet.

Der Umgang mit Non-Compliance und der Einsatz von Korrekturmaßnahmen beschäftigt sich mit der Frage, wie das Unternehmen mit festgestellten Regelverstößen umgeht. Im Vordergrund stehen Meldewege, Ursachenanalysen, Dokumentation von Verstößen und getroffene Reaktionen – von der Sanktionierung bis zur Anpassung bestehender Maßnahmen zur Erhöhung der Akzeptanz und Wirksamkeit.

Die Berichterstattung im Kontext der IT-Compliance widmet sich der systematischen Aufbereitung und Weitergabe relevanter Informationen an das Management und andere zentrale Stellen. Die Qualität der Berichte, die Regelmäßigkeit, der Informationsgehalt sowie Schnittstellen zu anderen Managementsystemen stehen hier im Fokus.

Abschließend adressiert der kontinuierliche Verbesserungsprozess (KVP) die Frage, ob und wie das IT-CMS regelmäßig überprüft, angepasst und weiterentwickelt wird. Dazu gehören Rückmeldeschleifen aus internen und externen Prüfungen, Reifegradmodelle, die Umsetzung von Lessons Learned sowie eine fortlaufende Optimierung der Strukturen und Inhalte auf Basis der Praxisanforderungen.

Der Prüfungsleitfaden ist so strukturiert, dass er Prüfern und Auditoren eine klare und systematische Methode zur Bewertung der IT-Compliance bietet. Er enthält bewusst eine Vielzahl von Detailfragen, die darauf ausgelegt sind, spezifische Aspekte der IT-Compliance eingehend zu beleuchten. Jedoch sind sie nicht für jedes Unternehmen gleichermaßen relevant. Daher ist es erforderlich, dass jedes Unternehmen eine Auswahl der Fragen trifft, die am besten den eigenen Gegebenheiten und Anforderungen entspricht.

Dies stellt sicher, dass alle relevanten Bereiche der IT-Compliance berücksichtigt werden und die Prüfung die tatsächlichen Bedürfnisse des Unternehmens erfüllt. Es ist wichtig zu beachten, dass der Leitfaden keinen Anspruch auf Vollständigkeit erhebt. Er sollte als Ausgangspunkt betrachtet werden, der nach Bedarf ergänzt und angepasst werden kann. Bei Rückfragen oder Unklarheiten sollte auf die Autoren dieses Prüfungsleitfadens zugegangen werden, um Unterstützung und zusätzliche Klärungen zu erhalten.

2 Schriftlich fixierte Ordnung (sfO) – Rahmenbedingungen und Aufbauorganisation eines IT-Compliance- Management-Systems

Teil eines IT-CMS ist die schriftliche Fixierung der Strukturen, Prozesse und Richtlinien. Diese »schriftlich fixierte Ordnung« (sfO) ist für die Implementierung und Aufrechterhaltung eines effektiven IT-CMS grundlegend und erforderlich. Sie dient als Referenz für das gesamte IT-Compliance-Management und beschreibt den Rahmen für die Umsetzung von Compliance-Maßnahmen in der IT-Umgebung.

Sie stellt sicher, dass die grundlegenden Parameter und Leitlinien, innerhalb derer das IT-CMS operiert, bestimmt sind. Die Aufgabenverteilung sowie die Verantwortlichkeiten für die Umsetzung des IT-CMS könnten (bzw. sollten) sich an dem etablierten Drei-Linien-Modell orientieren.

Die Eingliederung der IT-Compliance in die hierarchische Ordnung des Unternehmens bedeutet die Übertragung von IT-Compliance-Aufgaben sowie eine entsprechende Zuweisung von Befugnissen und Verantwortung. Es geht hierbei nicht nur um die Einrichtung einer Abteilung oder einer Stelle mit der Bezeichnung »IT-Compliance« bzw. die Einrichtung einer Position »IT-Compliance-Manager«. Vielmehr ist für die Sicherstellung von IT-Compliance eine umfangreiche Zusammenarbeit zu organisieren, die über unterschiedliche hierarchische Ebenen von der Unternehmensleitung bis auf die operative Ebene zentrale und dezentrale Strukturen verbinden und hierbei auch organisatorische Schnittstellen zwischen IT-Funktion und Fachabteilungen klären muss.

Eine der wesentlichen Voraussetzungen ist die Sicherstellung der erforderlichen personellen Ausstattung zur Erreichung bzw. Aufrechterhaltung von IT-Compliance. Dies bezieht sich nicht allein auf die Ressourcen einer IT-Compliance-Funktion, sondern ist für alle Organisationseinheiten und Unternehmensteile entsprechend den zugewiesenen Aufgaben mit zu berücksichtigen.

2.1 Rahmenbedingung

#	Prüfungsfrage	Grundlagen und Verweise
1	Existiert im Unternehmen in der schriftlich fixierten Ordnung (sfO) eine Definition für den Begriff der IT-Compliance und wird diese auch regelmäßig überprüft? Wird die Richtlinie im Unternehmen für alle Mitarbeiter zugänglich veröffentlicht und kommuniziert?	Leitfaden IT-Compliance, Abschnitt 2.2 und 5.5
2	Orientiert sich das IT-CMS an anerkannten Standards?	Leitfaden IT-Compliance, Abschnitt 7.1; IDW PS 980 [IDW PS 980 n.F.]; DIN ISO 19600[1] [DIN ISO 19600: 2016]; COBIT 2019 (implizit)
3	Umfasst der Regelungsbereich des IT-CMS auch die Anforderungen relevanter Stakeholder?	Leitfaden IT-Compliance, Kapitel 4 und Abschnitt 7.2
4	Ist in der Definition sichergestellt, dass IT-Compliance auch bei Dienstleistern relevant ist und berücksichtigt werden muss?	Leitfaden IT-Compliance, Abschnitte 4.1, 4.2 und 7.3
5	Ist eine regelmäßige Überprüfung der Angemessenheit und Aktualität der sfO im Bereich IT-Compliance geregelt und beschrieben?	Leitfaden IT-Compliance, Abschnitt 7.6; ISO 9001; ISO/IEC 27001 [DIN EN ISO/IEC 27001:2024]; ITIL; COBIT

1 Din ISO 19600 wurde zurückgezogen und 2021 durch ISO 37301 [ISO 37301:2021] ersetzt.

2.2 Aufbauorganisation

#	Prüfungsfrage	Grundlagen und Verweise
1	Sind die Schnittstellen zwischen IT-Compliance und anderen Funktionen (bspw. Auslagerungsmanagement) sowie Schnittstellen zu Managementsystemen transparent geregelt?	Leitfaden IT-Compliance, Abschnitt 6.1
2	Ist die Schnittstelle IT-Compliance zu Corporate Compliance klar geregelt? (Dies ist insbesondere bei Unternehmensgruppen zu prüfen.)	Leitfaden IT-Compliance, Abschnitt 7.1
3	Sind die Verantwortlichkeiten innerhalb der IT-Compliance-Funktion/2nd Line geregelt und dokumentiert (Aufgaben, Rollenprofile, Kompetenzen, Berichtswege)? *Hinweis:* *bspw. Chief Compliance Officer und dezentraler Compliance Officer*	Leitfaden IT-Compliance, Abschnitt 6.1
4	Sind die Verantwortlichkeiten innerhalb der 1st Line ausreichend geregelt? (z. B. dezentrale Compliance-Beauftragte mit bereichsbezogener Verantwortung, Compliance-Experten) *Hinweis:* *Es gibt nicht die eine Aufbauorganisation und Struktur. Es gilt, die definierten Aufgaben wahrnehmen zu können, zudem hat die Unternehmensgröße Einfluss auf die Struktur.*	Leitfaden IT-Compliance, Abschnitt 6.1
5	Sind Compliance-Themen an ein Gremium zu richten bzw. existiert ein Compliance-Gremium? Ist sichergestellt, dass dieses Gremium eingebunden wird? *Hinweis:* *Diese Funktion könnte auch ein bestehendes Gremium (z. B. IT-Risiko- und Sicherheitsgremium) übernehmen.*	Leitfaden IT-Compliance, Abschnitt 6.1
6	Sind Aufgaben, Verantwortlichkeiten und Kompetenzen für das Gremium/die Gremien geregelt?	Leitfaden IT-Compliance, Abschnitt 6.1
7	Gibt es für aktuelle und künftige Handlungsfelder angemessene organisatorische Regelungen, die die Berücksichtigung von Compliance-Fragen sicherstellen, und sind diese hinreichend dokumentiert?	Leitfaden IT-Compliance, Abschnitte 7.3 und 7.6
8	Sind die Anforderungen in den Stellenbeschreibungen für das Compliance-Management sachgerecht ausgestaltet (qualitativer Aspekt sowie Unabhängigkeit, Kompetenz und organisatorische Stellung)?	Leitfaden IT-Compliance, Abschnitte 6.1, 6.2 und 7.2
9	Ist eine ausreichende personelle und technische Ausstattung sichergestellt, um IT-Compliance einhalten zu können (quantitativer Aspekt)?	Leitfaden IT-Compliance, Abschnitte 6.1, 6.2 und 7.2
10	Werden die Mitarbeiter schriftlich zur Einhaltung der Compliance-Vorgaben verpflichtet? Gibt es eine entsprechende Anforderung?	Leitfaden IT-Compliance, Abschnitte 4.3 und 5.1

3 Compliance-Kultur und Awareness

Die Compliance-Kultur ist als weicher Mechanismus der IT-Governance Grundlage für die Angemessenheit und Wirksamkeit des CMS und schafft die Basis für ein regelkonformes Verhalten. Sie bildet im Zusammenspiel mit den Awareness-Maßnahmen das Fundament für sämtliche Aktivitäten zur Erfüllung der Compliance-Ziele. Ausdruck der Compliance-Kultur sind die Grundeinstellungen und Verhaltensweisen der Unternehmensleitung im Umgang mit Compliance-Risiken und die Art und Weise, wie die Unternehmensleitung die zentralen Unternehmenswerte in der Organisation verankert ([IDW PS 980 n.F.], Tz. 27). Bestandteil einer solchen Kultur ist die laufende Kommunikation zu aktuellen Themen und Erkenntnissen aus dem Bereich der IT-Compliance. Adressaten dieser Kommunikation sind alle Unternehmensmitglieder, aber auch externe Stakeholder, wie z. B. Geschäftspartner, Kunden oder Aufsichtsinstitutionen.

In der Vergangenheit waren Compliance-Verstöße in vielen Fällen auf eine unzureichende Compliance-Kultur zurückzuführen. Sehr wichtig für eine effektive Compliance-Kultur ist die Bedeutung, die die Unternehmensleitung der Regeltreue und der Regelbefolgung beimisst. Hierbei kommt es insbesondere auf den »Tone at the top«, an, also das individuelle Verhalten und die persönlichen kommunizierten Grundeinstellungen der Mitglieder der Unternehmensleitung. Jedoch ist nicht allein durch die Vermittlung von Werten und die Erstellung von Dokumentationen gewährleistet, dass die gewünschte Kultur in der IT auch gelebt wird. Daher sollte Compliance Gegenstand regelmäßiger Mitarbeiterschulungen und fortbildungen sein. Dabei werden die Compliance-Themen im Regelfall nicht nur in separaten Präsenzveranstaltungen oder Onlineseminaren behandelt, sondern sind eingebunden in artverwandte Awareness-Maßnahmen aus den Bereichen Informationssicherheit oder Datenschutz.

3.1 Compliance-Kultur

#	Prüfungsfrage	Grundlagen und Verweise
1	Werden Aussagen zur Bedeutung und zum Stellenwert der IT-Compliance in der Compliance-Kultur getroffen? Welche Aussagen sind das?	Leitfaden IT-Compliance, Abschnitt 7.2
2	Stellen Sie fest, ob das Unternehmen Anforderungen an die Compliance-Kultur in der sfO festgelegt hat? *Hinweis:* *Mindestinhalte für die Compliance-Kultur sind u. a.:* ◗ *Umgang mit Fraud-Vorfällen* ◗ *Sanktionsmaßnahmen (bei Gesetzesverstößen oder Verstoß gegen interne Regelungen)* ◗ *Hinweisgebersystem*	Leitfaden IT-Compliance, Abschnitt 7.2
3	Werden die Mitarbeiter und das Management nachvollziehbar über die Inhalte der Compliance-Kultur und Konsequenzen der Nichteinhaltung informiert? *Hinweis: Form der Information* ◗ *Rundschreiben, Anweisung, Bestätigungsschreiben* ◗ *Veröffentlichung der Nachvollziehbarkeit (bspw. Liste der Schulungsteilnehmer)*	Leitfaden IT-Compliance, Abschnitt 7.2
4	Sind Mechanismen (bspw. technische Tools) im Einsatz, die die Compliance-Kultur unterstützen?	Leitfaden IT-Compliance, Abschnitt 7.2

3.2 Awareness

#	Prüfungsfrage	Grundlagen und Verweise
1	Bestehen Regelungen für die Durchführung von Schulungs- und Awareness-Maßnahmen und sind diese beschrieben?	Leitfaden IT-Compliance, Abschnitt 7.2
2	Gibt es ein mehrjähriges, fortgeschriebenes Schulungs- und Awareness-Programm, um relevante Zielgruppen hinsichtlich der Einhaltung der Compliance zu sensibilisieren?	Leitfaden IT-Compliance, Abschnitt 7.2
3	Werden bei diesen Programmen zielgruppen- und risikoorientierte Schulungen, ausgerichtet an den grundlegenden Handlungsfeldern und Inhalten des Compliance-Leitbildes, berücksichtigt?	Leitfaden IT-Compliance, Abschnitt 7.2
4	Wurden vorgesehene Schulungen regelmäßig und nachvollziehbar gemäß der Planung umgesetzt?	Leitfaden IT-Compliance, Abschnitt 7.2
5	Gibt es Nachweise hinsichtlich der Teilnahme an Schulungsmaßnahmen?	Leitfaden IT-Compliance, Abschnitt 7.2
6	Wird der Erfolg der Schulungs- und Awareness-Maßnahmen gemessen?	Leitfaden IT-Compliance, Abschnitt 7.2

4 Pflege eines Normenregisters und Ableitung von Anforderungen an die IT

Wesentlicher Bestandteil eines IT-CMS ist die systematische Identifizierung, Erhebung und Umsetzung von Anforderungen an die IT aus Regelwerken. Ihre sachgerechte und strukturierte Behandlung und Beachtung sind durch einen wirksamen Prozess sicherzustellen. Zur Identifizierung dienen hierbei interne und externe, personelle und/oder technische Quellen. Aus diesen werden relevante IT-Compliance-Anforderungen abgeleitet und hinsichtlich ihrer Bedeutung für die IT analysiert. Hierauf aufbauend sind konkrete Handlungsanweisungen und Maßnahmen zu definieren, sodass die Einhaltung von Anforderungen an die IT sichergestellt ist. Bestehende Prozesse und deren Dokumentationen sind auf Handlungsbedarf zu überprüfen und zu aktualisieren.

#	Prüfungsfrage	Grundlagen und Verweise
1	Liegt eine Klassifikation der Normen und Standards vor, die in das Compliance-Management eingebunden werden sollen und sind diese im Einklang mit der Definition, den Rahmenbedingungen von IT-Compliance und der Stakeholder-Analyse?	Leitfaden IT-Compliance, Kapitel 5
2	Wer ist für die Identifizierung, Einführung und Überwachung der Normen und Standards im Unternehmen zuständig? Ist die Zuständigkeit angemessen geregelt (bspw. Verantwortungsmatrix, Stellenbeschreibung)? Werden hierfür Tools eingesetzt?	Leitfaden IT-Compliance, Abschnitt 7.3
3	Liegt ein aktuelles, vollständiges und hinreichend gepflegtes Register vor, in dem die zu berücksichtigenden internen und externen Normen und Standards aufgeführt sind? Ist aus diesem Register der weitere Umsetzungs- und Handlungsbedarf ersichtlich? Ist dieses Normenregister für relevante Organisationseinheiten im Rahmen ihrer Verantwortlichkeiten im Zugriff? *Hinweis:* *Zur Ableitung des Umsetzungsbedarfs wären z. B. folgende Informationen im Register zu hinterlegen:* ◗ *Risikobewertung und abgeleiteter Umsetzungsbedarf (Definition einer Priorisierung)* ◗ *Änderung/Verschärfung* ◗ *Schadensausmaß*	Leitfaden IT-Compliance, Kapitel 5
4	Bestehen Regelungen für die Ableitung von Handlungsanweisungen aus Normen und ist dieser Prozess beschrieben? Wurden relevante Organisationseinheiten bzw. Fachbereiche in den Ableitungsprozess einbezogen?	Leitfaden IT-Compliance, Abschnitt 7.3
5	Findet eine Stakeholder-Identifikation statt, die regelmäßig aktualisiert und in der Stakeholder-Analyse nachgehalten wird? Wurden die Anforderungen der Stakeholder in einer Art und Weise aufbereitet und dokumentiert, sodass eine sinnvolle Operationalisierung/Umsetzung im Rahmen des CMS erfolgen kann?	Leitfaden IT-Compliance, Kapitel 4
6	Wurden konkrete und verständliche Handlungsanweisungen vollständig und nachvollziehbar aus den Normen abgeleitet und ist die Rückführung auf die Norm gewährleistet, um den Compliance-Status zu ermitteln?	Leitfaden IT-Compliance, Abschnitt 7.3

5 Steuerung und Monitoring des IT-Compliance-Risikos und der IT-Compliance-Level

Das Management der IT-Compliance und der identifizierten Risiken sowie deren Behandlung kann als Ausbalancierung zwischen Compliance-Anforderungen und wirksamer Umsetzung korrespondierender Maßnahmen verstanden werden. Verändern bzw. verschärfen sich die Anforderungen oder erreichen die implementierten Maßnahmen nicht ihre Wirkungsziele, wird diese Balance gestört und es entsteht Non-Compliance. Dieses IT-Compliance-Risiko gilt es, permanent zu überwachen und angemessen zu steuern, um damit auch die Umsetzung der Compliance-Ziele zu gewährleisten.

Die Steuerung und Messung identifizierter IT-Compliance-Risken zielt darauf ab, den Grad der Konformität bewerten zu können, den Status des IT-Compliance-Risikos zu überwachen und sich einen Überblick zu verschaffen, ob die Vorgaben zu IT-Compliance eingehalten werden.

5.1 IT-Compliance-Risiko

#	Prüfungsfrage	Grundlagen und Verweise
1	Wie sind die Prozesse und Schnittstellen definiert, damit die IT-Compliance-Risiken in das unternehmensweite Risikomanagement einfließen? Ist im Risikomanagement z. B. eine Risikoklasse Compliance-Risiko definiert (i.d.R. Teil des operationellen Risikos)?	Leitfaden IT-Compliance, Abschnitte 2.4 und 7.4
2	Werden die identifizierten IT-Compliance-Risiken nachvollziehbar und vollständig erhoben und mit den Kriterien aus dem Risikomanagement bewertet und priorisiert?	Leitfaden IT-Compliance, Abschnitte 2.4 und 7.4
3	Wie wird sichergestellt, dass erkannt wird, wenn einzelne (unkritische) Compliance-Risiken zusammenwirken und in einem relevanten Risiko kumulieren? Werden hierbei Auswirkungen auf andere Compliance-Bereiche angemessen beurteilt und berücksichtigt?	Leitfaden IT-Compliance, Abschnitte 2.4 und 7.4
4	Wurden bei der Risikobewertung die erforderlichen Risikoeigentümer und weitere fachliche Expertise (wie juristische Beratung) mit eingebunden? Sind Schäden, Verstöße, Bußgelder, Beinahverluste bekannt – in der Regel zu einem Handlungsfeld –, die in die Bewertung einfließen?	Leitfaden IT-Compliance, Abschnitte 2.4 und 7.4
5	Werden Compliance-Risiken der IT hinreichend im Risikoreporting gewürdigt?	Leitfaden IT-Compliance, Abschnitte 2.4 und 7.4

5.2 Steuerung und Messung

#	Prüfungsfrage	Grundlagen und Verweise
1	Existiert ein Compliance-Plan, aus dem Fristen und Überwachungsaktivitäten der Compliance-Managementfunktion ersichtlich werden?	Leitfaden IT-Compliance, Abschnitt 7.5
2	Sind hinreichende Prozesse und Kontrollen implementiert, die sicherstellen, dass offene Maßnahmen, Sicherheitsereignisse und Ergebnisse des Schwachstellenmanagements rechtzeitig abgestellt werden, um das Compliance-Level nach einer Feststellung schnellstmöglich zu optimieren? *Hinweis:* *Beispielsweise sollten kritische Schwachstellen oder Ergebnisse aus dem Penetrationstest zeitnah geschlossen werden.*	Leitfaden IT-Compliance, Abschnitt 7.5
3	Hat das Unternehmen einen Prozess zur Überwachung und Messung des IT-Compliance-Status implementiert und dokumentiert? Wie stellt dieser Monitoring-Prozess sicher, dass die Vorgaben aus IT-Compliance, die das Unternehmen einzuhalten hat, vollumfänglich berücksichtigt werden (z. B. durch einzelne Kontrollen)?	Leitfaden IT-Compliance, Abschnitt 7.5
4	Ist unter Berücksichtigung der Kapazitäten der IT-Compliance-Funktion die Überwachungstiefe und -spanne ausreichend, um eine belastbare Aussage über den Compliance-Status treffen zu können? Bezieht der Monitoring-Prozess Ergebnisse anderer Prüfungen mit ein, um z. B. getätigte Aussagen der Fachbereiche zu plausibilisieren oder auch in die eigene Bewertung mit aufzunehmen?	Leitfaden IT-Compliance, Abschnitt 7.5
5	Ist die Aggregation der Ergebnisse der Messungen und Überprüfungen über alle Handlungsfelder der IT-Compliance hinweg nachvollziehbar und aussagekräftig (z. B. bei einem aggregierten Score)? Liefert das Berichtswesen an das Management über diese Aggregation alle erforderlichen Informationen, damit das Management das IT-Compliance-Risiko sachgerecht einschätzen kann?	Leitfaden IT-Compliance, Abschnitt 7.5
6	Eine Compliance-Funktion allein kann den Compliance-Status nicht überprüfen. Wie sind weitere 2nd-Line-Funktionen und die operative IS-Einheit in den Überwachungsprozess eingebunden? Haben diese selbst hinreichende Überwachungs- und Überprüfungsmechanismen implementiert, um den Compliance-Status der eigenen herausgegebenen Anforderungen zu überwachen? *Hinweis:* *Das Access & Identity Management regelt den grundsätzlichen Umgang mit Berechtigungen und privilegierten Zugriffen. Die Fachabteilungen stehen hier primär in der Verantwortung, für die eigenen Systeme (kritische) Berechtigungen zu identifizieren, zu dokumentieren und nach AIM-Prinzipien, wie z. B. »need to know«, zu vergeben. Das Access & Identity Management steht hier in der Verantwortung, die Einhaltung dieser Vorgaben zu überwachen und im Reporting den Status z. B. an den Informationssicherheitsbeauftragten oder an die Compliance-Funktion zu berichten.*	Leitfaden IT-Compliance, Abschnitt 7.5

→

#	Prüfungsfrage	Grundlagen und Verweise
7	Wurden in den strategischen Vorgaben zum CMS entsprechende Ziele formuliert und mit Leistungsindikatoren (KPI) operationalisiert, um den Grad der Zielerreichung fortlaufend messen zu können? Sind aussagekräftige Kennzahlen definiert worden, ausgerichtet an den Zielen von Compliance, die für die Beurteilung des Compliance-Levels herangezogen werden können?	Leitfaden IT-Compliance, Abschnitt 7.5
8	Sind die Ergebnisse der Messung bzw. des Überwachungsprozesses mit einer Kritikalitätsskala (Auswirkungsskala) verbunden, sodass die Unternehmensleitung, abhängig vom Ergebnis, regelmäßig bzw. ad hoc alarmiert wird?	Leitfaden IT-Compliance, Abschnitt 7.5
9	Stellt der Dienstleistersteuerungsprozess sicher, dass die Vorgaben an IT-Compliance hinreichend bzw. wirksam bei den Dienstleistern umgesetzt werden?	Leitfaden IT-Compliance, Abschnitte 2.6, 4.2, 7.4, 7.5

6 Umgang mit Non-Compliance und Einsatz von Korrekturmaßnahmen

Abweichungen von festgelegten Compliance-Vorgaben können immer wieder aus unterschiedlichen Gründen auftreten, sind jedoch für sich genommen in der Regel noch kein Anzeichen dafür, dass das IT-CMS insgesamt ineffektiv ist. Gerade die Aufdeckung von Non-Compliance ist Aufgabe des IT-Compliance-Systems. Entscheidend ist ein zielführender Umgang mit festgestellten Compliance-Verstößen. Erkannte Abweichungen stellen u. a. eine Grundlage dar, das vorhandene System zu korrigieren und weiter zu verbessern.

#	Prüfungsfrage	Grundlagen und Verweise
1	Gab es im Prüfungszeitraum IT-Compliance-Verstöße?	Leitfaden IT-Compliance, Abschnitt 7.7; ISO 19600
2	Welche Meldewege (Eingangskanäle) sind definiert und dokumentiert, die sicherstellen, dass Compliance-Verstöße rechtzeitig identifiziert und an die Compliance-Funktion gemeldet werden? Welches Format der Meldung (elektronisch, Mail, MS Office etc.) ist festgelegt? Sind im Rahmen des Prozesses die Verantwortlichkeiten definiert? Ist dieser Prozess hinreichend im Unternehmen kommuniziert bzw. bekannt? *Hinweis:* *Vorgaben aus der Informationssicherheit sind hierbei zu berücksichtigen.*	Leitfaden IT-Compliance, Abschnitt 7.7
3	Ist geregelt, bei welchen Verstößen eine Kommunikation nach außen erfolgt?	Leitfaden IT-Compliance, Abschnitt 7.7
4	Bei bewussten Verstößen: Werden die Gründe für die Nichtakzeptanz der IT-Compliance-Regelungen untersucht?	Leitfaden IT-Compliance, Abschnitt 7.7
5	Findet eine Ursachenanalyse statt und wird diese hinreichend dokumentiert, um sicherzustellen, dass der Eintritt von weiteren Compliance-Verstößen mit gleicher oder ähnlicher Ursache vermieden wird?	Leitfaden IT-Compliance, Abschnitt 7.7
6	Wird überprüft, ob Compliance-Verstöße weitere Non-Compliance begünstigen?	Leitfaden IT-Compliance, Abschnitt 7.7
7	Welche Eskalationsstufen sind für wiederholte IT-Compliance-Verstöße vorgesehen?	Leitfaden IT-Compliance, Kapitel 7.7
8	Erfolgt neben einer Sanktionierung auch eine Untersuchung, ob Compliance-Maßnahmen angemessen sind bzw. durch Anpassungen eine höhere Akzeptanz erreicht werden kann, ohne das Risiko wesentlich zu erhöhen?	Leitfaden IT-Compliance, Abschnitt 7.7
9	Welche technischen organisatorischen Maßnahmen hat das Unternehmen umgesetzt, sodass mögliche Compliance-Verstöße verhindert oder reduziert werden?	Leitfaden IT-Compliance, Abschnitt 7.7
10	Werden Kosten-Nutzen-Analysen in Bezug auf die Wirtschaftlichkeit einzelner Maßnahmen durchgeführt? Werden in diesem Zusammenhang die Kosten für Maßnahmen zur Verhinderung von Non-Compliance den möglichen Kosten bei einer erwarteten Häufigkeit von Verstößen gegenübergestellt? Werden nach einem IT-Compliance-Verstoß Untersuchungen zur erwarteten Häufigkeit ähnlicher Verstöße vorgenommen und die Kosten für technische Maßnahmen zur Verhinderung eines solchen Verstoßes analysiert?	Leitfaden IT-Compliance, Abschnitt 7.7
11	Werden die aus Verstößen und Analysen abgeleiteten Entscheidungen (Behandlung oder Akzeptanz) angemessen dokumentiert? Gibt es klare Anforderungen aus dem Prozess der Maßnahmenbehandlung?	Leitfaden IT-Compliance, Abschnitt 7.7

7 Berichterstattung zur IT-Compliance

Im IT-CMS ist eine umfassende Berichterstattung von entscheidender Bedeutung. Sie gewährleistet Transparenz und Verantwortlichkeit. Durch präzise Datenerfassung, aussagekräftige Berichterstellung und effektive Kommunikation an relevante Stakeholder kann sichergestellt werden, dass Compliance-Richtlinien eingehalten werden. Konsistenz, Genauigkeit und zeitnahe Updates sind dabei unerlässlich, um einen effizienten Überblick zu gewährleisten. Eine Kommunikation der IT-Compliance-Risiken, des IT-Compliance-Status und eines etwaigen Handlungsbedarfs an die Unternehmensleitung sowie Bereitstellung relevanter Informationen für weitere zentrale Managementsysteme (z. B. zentrales Risikomanagement) und für weitere Fachbereiche ist sicherzustellen.

#	Prüfungsfrage	Grundlagen und Verweise
1	Ist vorgesehen und beschrieben, regelmäßig und anlassbezogen über den Stand und die Einhaltung der Compliance-Vorgaben zu berichten? *Hinweis:* *Mindestinhalte bei der Regelung zur Berichterstattung:* ◗ *Aktualität und Umsetzungsstand von Normen/Regelung* ◗ *Verantwortlichkeiten, Status der IT-Compliance im Unternehmen (bspw. Prozessreifegrad)* ◗ *Eingetretene Compliance-Verstöße und Status* ◗ *Aktivitäten Compliance-Beauftragter (Audits, KVP etc.) und Ergebnisse* ◗ *Handlungsbedarf und Entscheidungen, die von der Geschäftsführung eingefordert werden* ◗ *Ausblick* *Hinweis:* *Kriterien zur Anforderung der Regelung:* ◗ *Regelmäßig: Jahresbericht* ◗ *Anlassbezogen: ad hoc bei Verstößen oder nach Abschluss der Bearbeitung der Verstöße* ◗ *Wie werden Daten (bspw. Risiken, Auditberichte) aus dem IT-CMS in andere Managementsysteme (bspw. ISMS, Datenschutz, zentrales Risikomanagement) übertragen? Sind die Adressaten hinreichend festgelegt worden?*	Leitfaden IT-Compliance, Abschnitte 4.3, 6.3, 7.5 und 7.6
2	Bestehen Regelungen zum regelmäßigen Reporting der IT-Compliance-Risiken? *Hinweise zu Inhalten:* *Dies kann auch mit Berichtswesen aus Punkt 1 zusammengefasst werden.* ◗ *Aggregationslevel* ◗ *Angaben zum Compliance-Risiko* ◗ *Top-Ten-Handlungen/korrektive Handlungen aktuell* ◗ *Schnittstellen zu anderen Prüfungen*	Leitfaden IT-Compliance, Abschnitte 4.3, 6.3, 7.5 und 7.6
3	Ist die Berichterstattung entsprechend den Vorgaben erfolgt? *Hinweis:* *Einsichtnahme in die entsprechenden Berichte im Prüfungszeitraum*	Leitfaden IT-Compliance, Abschnitte 4.3, 6.3, 7.5 und 7.6

8 Der kontinuierliche Verbesserungsprozess des IT-CMS

Ein wesentliches Ziel des kontinuierlichen Verbesserungsprozesses (KVP) ist es, die Eignung, Angemessenheit und Effektivität des IT-CMS regelmäßig zu überprüfen, um die Eintrittswahrscheinlichkeit für eine Nichtkonformität zu verringern und um Maßnahmen zu definieren, die die IT-Compliance-Prozesse und Aktivitäten optimieren.

#	Prüfungsfrage	Grundlagen und Verweise
1	Richtet sich der KVP an Standards und Governance-Referenzmodellen aus (ISO 9001, ISO 27001, ITIL, COBIT)?	Leitfaden IT-Compliance, Abschnitt 7.6
2	Berücksichtigt der KVP alle Teilprozesse des IT-CMS und werden diese laufend hinsichtlich ihres Umsetzungsstands bewertet (bspw. in Form eines Reifegradmodells)? *Hinweis:* ◗ *Die Effektivität der eigenen Managementkontrollen (auch die IT-Compliance-Funktion sollte Kontrollen implementiert haben)* ◗ *Die Angemessenheit und Aktualität von Richtlinien zu IT-Compliance und zugehörige Arbeitsanweisungen* ◗ *Die Zielerreichung der IT-Compliance-Ziele und den Umsetzungsgrad der Compliance-Planung* ◗ *Die Optimierung des Compliance Universe durch die Überprüfung der Handlungsfelder*	Leitfaden IT-Compliance, Abschnitt 7.6
3	Werden im Rahmen des KVP Ergebnisse und Maßnahmen aus (externen) Prüfungen zeitnah und vollständig berücksichtigt?	Leitfaden IT-Compliance, Abschnitt 7.6
4	Erfolgen bei festgestellter Non-Compliance entsprechende Anpassungen des IT-CMS?	Leitfaden IT-Compliance, Abschnitte 7.6 und 7.7

9 Zusammenfassung

Die Zukunft der Prüfung von IT-Compliance steht vor mehreren Herausforderungen und Chancen, die sich aus der fortschreitenden Digitalisierung und der sich wandelnden regulatorischen Landschaft ergeben. Ein zentraler Aspekt wird die Integration neuer Technologien sein, die traditionelle IT-Infrastrukturen transformieren. Cloud Computing, künstliche Intelligenz (KI), das Internet der Dinge (IoT) und Big Data Analytics sind Beispiele für Technologien, die Unternehmen zunehmend nutzen, um ihre Geschäftsprozesse zu optimieren. Diese Technologien bieten enorme Vorteile, bringen jedoch auch neue Risiken und Herausforderungen für die Compliance mit sich. Ein weiterer wichtiger Trend ist die zunehmende Globalisierung der Geschäftstätigkeiten, die zu komplexeren Compliance-Anforderungen führt. Unternehmen müssen sich auf unterschiedliche rechtliche Rahmenbedingungen in verschiedenen Ländern einstellen und sicherstellen, dass ihre IT-Systeme und -Prozesse weltweit den jeweiligen Standards entsprechen. Darüber hinaus wird erwartet, dass die Zusammenarbeit zwischen Regulierungsbehörden und Unternehmen intensiver wird. Regulierungsbehörden werden vermehrt auf technische Expertise angewiesen sein, um angemessene Richtlinien und Vorschriften zu entwickeln, die den sich ständig weiterentwickelnden technologischen Landschaften gerecht werden. Daher erachten wir es als unerlässlich, dass ein IT-CMS regelmäßig Bestandteil der Prüfungen ist.

Der Prüfungsleitfaden dient als grundlegende Orientierung zur Prüfung eines IT-CMS. Aufgrund der sich schnell ändernden regulatorischen Anforderungen ist die Überprüfung auf Aktualität der zugrunde gelegten Rahmenbedingungen unerlässlich. Neue Gesetze und Vorschriften im Bereich Datenschutz, Cybersicherheit und Compliance werden Auswirkungen auf die Prüfungsmethoden haben und eine Anpassung der Fragestellungen und Bewertungskriterien erforderlich machen.

10 Quellenverzeichnis

[DIN EN ISO/IEC 27001:2024] Informationssicherheit, Cybersicherheit und Datenschutz – Informationssicherheitssysteme – Anforderungen (ISO/IEC 27001:2022); deutsche Fassung EN ISO/IEC 27001:2023, 2024.

[DIN ISO 19600:2016] Compliance-Managementsysteme – Leitlinien (ISO 19600:2014), deutsche Fassung der ISO 19600:2014, Ausgabedatum 2016-12.

[IDW PS 980 n.F.] Institut der Wirtschaftsprüfer in Deutschland (Hrsg.): IDW PS 980 n.F. Prüfungsstandard: Grundsätze ordnungsmäßiger Prüfung von Compliance-Management-Systemen, Stand: 09.2022.

[ISO 37301:2021] Compliance-Managementsysteme – Anforderungen mit Leitlinien zur Anwendung, 2021.

[Schmidt et al. 2021] Schmidt, H. A.; Dors, A.; Kretschmann, C.; Nestler, D.; Meissner, D.; Untucht, G.; Karamitros, I.; Zilian, J.; Klotz, M.; Kunzewitsch; M.; Dax, O.; Loos, P.; Purder, S.: Leitfaden IT-Compliance, 2012, online verfügbar unter: *https://www.isaca.de/images/Publikationen/Leitfaden/Leitfaden%20IT-Compliance%20Grundlagen.pdf* (letzter Abruf 26.06.2025).