

**iapp**



# **CIPM WISSENSFUNDUS UND PRÜFUNGSVORLAGE**

VERSION 4.2.0

GÜLTIG AB: 1. Sept. 2025

# IAPP WISSENSFUNDUS FÜR DEN CIPM

## VERSTÄNDNIS DES WISSENSFUNDUS DER IAPP

Der Hauptzweck des Wissensfundus besteht in der Dokumentation der Kenntnisse und Fähigkeiten, die in der Zertifizierungsprüfung bewertet werden. Die Bereiche entsprechen dem, was ein Datenschutzexperte zum Nachweis seiner Kompetenz im jeweiligen Bereich wissen und können sollte.

Der Wissensfundus enthält außerdem die Zahlen zur Prüfungsvorlage, mit denen die Mindest- und Höchstzahl der Prüfungsfragen aus jedem Bereich angegeben wird.

Der Wissensfundus wird von den Fachexperten entwickelt und gepflegt, die den Prüfungsausschuss für die einzelnen Zertifizierungsbezeichnungen und den Ausschuss für das Prüfungsschema bilden. Der Wissensfundus wird jedes Jahr überprüft (und gegebenenfalls aktualisiert). Änderungen werden in den jährlichen Prüfungsaktualisierungen berücksichtigt und den Kandidaten mindestens 90 Tage vor dem Erscheinen neuer Prüfungsinhalte mitgeteilt.

## KOMPETENZEN UND LEISTUNGSKENNZAHLEN

Wir stellen den Wissensfundus als eine Reihe von Kompetenzen und Leistungsindikatoren bereit.

Kompetenzen sind Bündel miteinander verbundener Aufgaben und Fähigkeiten, die einen breiten Wissensbereich bilden.

Leistungsindikatoren sind die einzelnen Aufgaben und Fähigkeiten, die die breitere Kompetenzgruppe bilden. Mit den Prüfungsfragen wird die Beherrschung der Leistungsindikatoren durch den Datenschutzbeauftragten bewertet.

## WELCHE ARTEN VON FRAGEN WERDEN IN DER PRÜFUNG GESTELLT?

Für den Zertifizierungskandidaten sind die Leistungsindikatoren Anhaltspunkte für die Tiefe der Kenntnisse, die für den Kompetenznachweis erforderlich sind. Die Verben, mit denen die Aussagen zu den Fähigkeiten und Aufgaben beginnen (identifizieren, beurteilen, umsetzen, definieren), signalisieren das Komplexitätsniveau der Prüfungsfragen und finden ihre Entsprechung in der Bloomschen Taxonomie (siehe nächste Seite).

## ANAB-AKKREDITIERUNG

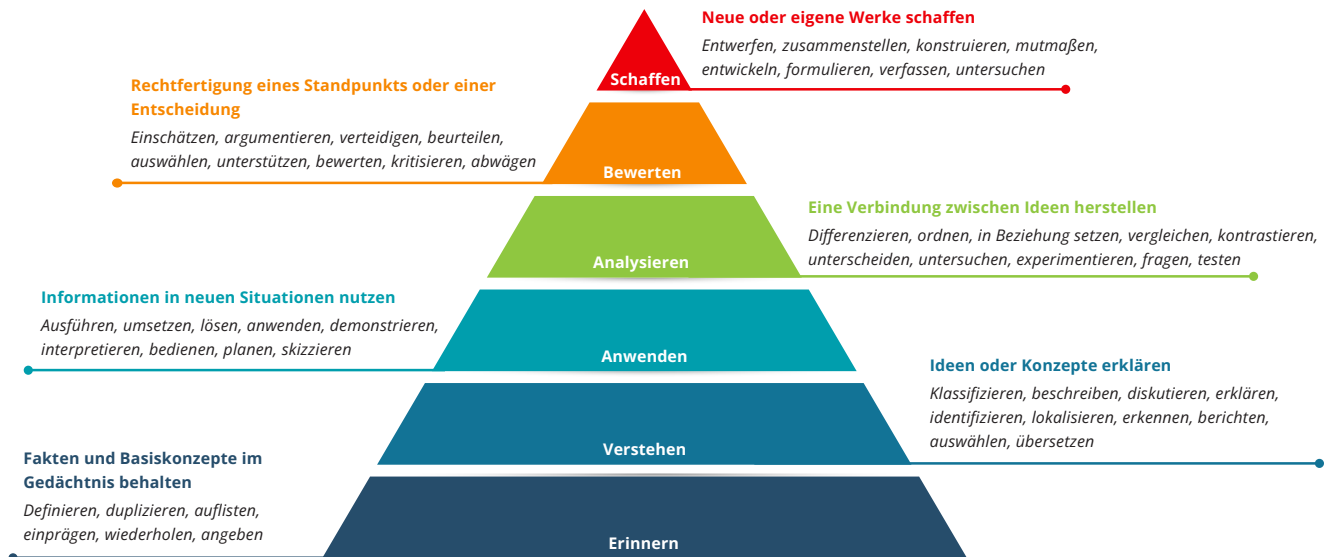
Die CIPM-, CIPP/E-, CIPP/US- und CIPT-Zertifikate der IAPP sind von der folgenden Organisation akkreditiert: **ANSI National Accreditation Board (ANAB) nach der Norm der Internationalen Organisation für Normung (ISO) 17024: 2012.**

ANAB ist eine international anerkannte Akkreditierungsstelle, die Zertifizierungsprogramme bewertet und akkreditiert. Diese erfüllen strenge Standards.

Die Akkreditierung ist eine enorme Anerkennung für die Qualität und Integrität der Zertifizierungsprogramme der IAPP, die:

- zeigt, dass die IAPP-Zertifizierungen einen globalen, von der Industrie anerkannten Maßstab erfüllen.
- sicherstellt, dass die IAPP-Zertifikate weltweit einheitlich, vergleichbar und zuverlässig sind.
- die Integrität schützt und die Gültigkeit des IAPP-Zertifizierungsprogramms sicherstellt.
- Arbeitgebern, Arbeitnehmern, Kunden und Dienstleistern weltweit nachweist, dass IAPP-zertifizierte Fachleute über die erforderlichen Kenntnisse, Fertigkeiten und Fähigkeiten für ihre Aufgaben verfügen.

# IAPP WISSENSFUNDUS FÜR DEN CIPM



## Beispiele für zurückgezogene Fragen aus verschiedenen Bereichen zum Erinnern/Verstehen:

- Welche der folgenden Definitionen ist die richtige für datenschutzfreundliche Technologien (Privacy-Enhancing Technologies)?
- Für welche Art von Tätigkeit gilt die kanadische Charter of Rights and Freedoms?
- Welche EU-Institution ist ermächtigt, neue Rechtsvorschriften zum Datenschutz vorzuschlagen?
- Wer ist für den Erlass von Vorschriften im Rahmen des Fair Credit Reporting Act (FCRA) und des Fair and Accurate Credit Transactions Act (FACTA) zuständig?

Die Antworten auf diese Fragen sind Tatsachen, die nicht bestritten werden können.

## Beispiele für zurückgezogene Fragen aus verschiedenen Bereichen zum Erinnern/Verstehen:

- Welche der folgenden Fragen stellt für einen Verantwortlichen in der Europäischen Union die **größte** Herausforderung dar, wenn es keine klar definierten vertraglichen Bestimmungen gibt?
- Welches der folgenden Beispiele würde eine Verletzung der räumlichen Privatsphäre darstellen?
- Wie lässt sich am **besten** sicherstellen, dass alle Interessenvertreter die gleichen Grundkenntnisse über die Datenschutzprobleme einer Organisation haben?
- Wenn die Informationstechnologie-Entwickler ursprünglich die Standardeinstellung für Kundenkreditkartendaten auf „Nicht speichern“ gesetzt hätten, wäre diese Maßnahme gemäß welchem Konzept erfolgt?

Die Antwort auf diese Frage muss auf Faktenwissen und einem Verständnis beruhen, das die Anwendung, Analyse und/oder Beurteilung der angebotenen Optionen ermöglicht, um die beste Antwort zu wählen.

# IAPP WISSENSFUNDUS FÜR DEN CIPM

MIN. MAX.

## Bereich I – Datenschutzprogramm: Entwurf des Rahmens

14 18

**Bereich I – Datenschutzprogramm: Entwurf eines Rahmens** dokumentiert die vorbereitenden Aufgaben zur Schaffung einer soliden Grundlage für das Datenschutzprogramm, den Zweck des Programms und die Verantwortlichkeiten für das Programm. Er konzentriert sich auf die Einführung eines Datenschutzprogramms im Einklang mit der Datenschutzstrategie der Organisation; Da jede Organisation ihre eigenen Bedürfnisse hat, kann das Modell von Organisation zu Organisation variieren.

### KOMPETENZEN

### LEISTUNGSINDIKATOREN

4 6 I.A	Definition des Programmmumfangs und Entwicklung einer Datenschutzstrategie	Identifizierung der Quelle, Arten und Verwendungszwecke von personenbezogenen Daten im Unternehmen
		Verständnis des Geschäftsmodells, der Betriebsumgebung des Unternehmens und der Risikobereitschaft
		Auswahl des geeigneten Governance-Modells
		Definition der Struktur des Datenschutzteams
		Ermittlung von Interessenvertretern und internen Partnern
4 6 I.B	Kommunikation der Vision und des Leitbilds des Unternehmens	Interne und externe Sensibilisierung für das Datenschutzprogramm des Unternehmens
		Sicherstellung eines angemessenen Zugangs zu rollenspezifischen Richtlinien und Verfahren für die Mitarbeiter
		Schaffung eines gemeinsamen Verständnisses der Begriffe zum Thema Datenschutz innerhalb der gesamten Organisation
5 7 I.C	Angabe der für das Programm geltenden Gesetze, Vorschriften und Normen	Erfassung territorialer, sektoraler und branchenspezifischer Verordnungen, Gesetze, Verfahrensregeln und/oder Selbst-zertifizierungsmechanismen
		Verständnis der potenziellen Auswirkungen von Verstößen auf Unternehmens- und/oder individueller Ebene
		Kenntnis des Geltungsbereichs und der Befugnisse von Aufsichtsbehörden
		Kenntnis der Auswirkungen auf den Datenschutz und den territorialen Geltungsbereich, wenn anderen Ländern mit abweichenden Datenschutzgesetzen Geschäfte abgewickelt oder Niederlassungen gegründet werden
		Kenntnis der Datenschutzrisiken durch die Nutzung von KI im Geschäftsumfeld

MIN.	MAX.	Bereich II – Datenschutzprogramm: Einführung einer Governance von Datenschutzprogrammen
------	------	--

12	16	<b>Bereich II – Datenschutzprogramm: Einführung einer Governance von Datenschutzprogrammen</b> Sie legt fest, wie die Datenschutzanforderungen in der gesamten Organisation in allen Phasen des Datenschutzes-Lebenszyklus umgesetzt werden sollen. Der Bereich konzentriert sich auf die Rollen, Zuständigkeiten und Schulungsanforderungen der verschiedenen Interessenvertreter sowie auf die Strategien und Verfahren, mit denen die kontinuierliche Einhaltung der Vorschriften gewährleistet werden soll.
----	----	---

## KOMPETENZEN

## LEISTUNGSINDIKATOREN

6	8	II.A	Erstellung von Richtlinien und Prozessen, die in allen Phasen des Lebenszyklus des Datenschutzprogramms befolgt werden müssen	Auswahl eines geeigneten Organisationsmodells sowie Festlegung von Verantwortlichkeiten und Berichtsstruktur je nach Organisationsgröße
				Definition von Richtlinien, die für die von der Organisation verarbeiteten Daten geeignet sind, unter Berücksichtigung der rechtlichen und ethischen Anforderungen
				Ermittlung der Erfassungspunkte unter Berücksichtigung von Transparenz und Fragen der Datenqualität bei der Datenerfassung
				Erstellung eines Plans für den Umgang mit Datenschutzverletzungen
				Erstellung von Plänen für Beschwerdeverfahren und Prozesse und Verfahren im Zusammenhang mit den Rechten der Betroffenen
				Erstellung von Richtlinien und Verfahren zur Datenaufbewahrung und -vernichtung
1	3	II.B	Klärung der Rollen und Zuständigkeiten	Definition der Rollen und Verantwortlichkeiten des Datenschutzteams und der Interessenvertreter
				Definition von Rollen und Zuständigkeiten beim Management von Datenfreigaben und -offenlegungen für interne und externe Zwecke
				Definition der Rollen und Verantwortlichkeiten für die Reaktion auf Datenschutzverletzungen nach Funktionen, einschließlich der Interessenvertreter und ihrer Rechenschaftspflicht gegenüber verschiedenen internen und externen Partnern (z. B. Erkennungsteams, IT, HR, Anbieter, Aufsichtsbehörden, Aufsichtsteams)



# IAPP WISSENSFUNDUS FÜR DEN CIPM

2	4	II.C	Festlegung von Datenschutz-Kennzahlen für Überwachung und Governance	Erstellung von Kennzahlen nach Zielgruppen und/oder Identifizierung der Zielgruppen für Kennzahlen mit klaren Prozessen, die Zweck, Wert und Berichterstattung von Kennzahlen beschreiben
				Kenntnis des Zwecks, der Arten und des Lebenszyklus von Audits bei der Bewertung der Effektivität von Kontrollen in allen Abläufen, Systemen und Prozessen der Organisation
				Einrichtung von Überwachungs- und Durchsetzungssystemen zur Beobachtung von Änderungen des Datenschutzrechts in verschiedenen Rechtsordnungen, um eine kontinuierliche Angleichung zu gewährleisten
1	3	II.D	Einführung von Schulungs- und Sensibilisierungsmaßnahmen	Entwicklung gezielter Schulungen für Mitarbeiter, Führungskräfte und Auftragnehmer und Sensibilisierungsmaßnahmen in allen Phasen des Datenschutz-Lebenszyklus zur Sicherstellung der Compliance

# IAPP WISSENSFUNDUS FÜR DEN CIPM

MIN. MAX.

## Bereich III – Betriebslebenszyklus des Datenschutzprogramms: Beurteilung der Daten

12 16

**Bereich III – Betriebslebenszyklus des Datenschutzprogramms: Beurteilung der Daten** umfasst die Identifizierung und Minimierung von Datenschutzrisiken und die Beurteilung der Auswirkungen auf den Datenschutz im Zusammenhang mit den Systemen, Prozessen und Produkten eines Unternehmens. Die frühzeitige Behebung potenzieller Probleme trägt dazu bei, ein solideres Datenschutzprogramm zu entwickeln.

### KOMPETENZEN

### LEISTUNGSINDIKATOREN

3	5	III.A	Dokumentation der Data-Governance-Systeme	Zuordnung von Datenbeständen, -flüssen, -lebenszyklen und Systemintegrationen
				Abgleich der Richtlinien mit internen und externen Anforderungen
				Durchführung einer Gap-Analyse hinsichtlich geltender Gesetze und/oder anerkannter Standards
1	3	III.B	Beurteilung der Auftragsverarbeiter und Drittanbieter	Identifizierung und Beurteilung der Risiken von Outsourcing von personenbezogenen Daten (z. B. vertragliche Anforderungen und Regeln für internationale Datenübermittlungen)
				Durchführung von Bewertungen auf der am besten geeigneten Funktionsebene innerhalb der Organisation (z. B. Beschaffung, Innenrevision, Informationssicherheit, physische Sicherheit, Datenschutzbehörde)
0	2	III.C	Beurteilung der physischen und umgebungsbezogenen Kontrollen	Identifizierung der operativen Risiken physischer Standorte (z. B. Rechenzentren und Büros) und physischer Kontrollen (z. B. Aufbewahrung und Vernichtung von Dokumenten, Mediansanierung und -entsorgung und Gerätesicherheit)
3	5	III.D	Beurteilung der technischen Maßnahmen	Ermittlung der operativen Risiken der digitalen Verarbeitung (z. B. Server, Speicher, Infrastruktur und Cloud)
				Überprüfung und Einschränkung der Nutzung und Aufbewahrung personenbezogener Daten
				Bestimmung des Speicherorts der Daten, einschließlich grenzüberschreitender Datenströme
2	4	III.E	Bewertung von Risiken im Zusammenhang mit gemeinsam genutzten Daten bei Fusionen, Übernahmen und Veräußerungen	Durchführung von Due-Diligence-Prüfungen
				Bewertung von vertraglichen Verpflichtungen und Verpflichtungen zur gemeinsamen Nutzung von Daten, einschließlich Gesetzen, Vorschriften und Normen
				Abgleich von Risiken und Kontrollen

# IAPP WISSENSFUNDUS FÜR DEN CIPM

MIN. MAX.

## Bereich IV – Betriebslebenszyklus des Datenschutzprogramms: Schutz personenbezogener Daten

9 13

**Bereich IV – Betriebslebenszyklus des Datenschutzprogramms: Schutz personenbezogener Daten** umreißt, wie Datenbestände im Verlauf ihrer Nutzung durch die Implementierung wirksamer Datenschutz- und Sicherheitskontrollen und -technologien geschützt werden können. Die Daten müssen auf allen Ebenen des Unternehmens physisch und virtuell sicher sein, unabhängig von Größe, geografischem Standort oder Branche.

### KOMPETENZEN

### LEISTUNGSINDIKATOREN

4	6	IV.A	Anwendung von Informationssicherheitspraktiken und -richtlinien	Klassifizierung der Daten nach dem geltenden Klassifizierungsschema (z. B. öffentlich, vertraulich, eingeschränkt)
				Verständnis des Zwecks und der Grenzen der verschiedenen Kontrollen
				Identifizierung von Risiken und Implementierung geeigneter Zugriffskontrollen
				Implementierung geeigneter technischer, administrativer und organisatorischer Maßnahmen zur Minderung etwaiger Risiken
1	3	IV.B	Integration der wichtigsten Grundsätze von Privacy by Design (PbD)	Einbindung des Datenschutzes in den gesamten Systementwicklungsprozess (System Development Life Cycle, SDLC)
				Integration des Datenschutzes in alle Geschäftsprozesse
				Verständnis der Prinzipien und Ziele von „Privacy by Design“
3	5	IV.C	Anwendung der Unternehmensrichtlinien für die Datennutzung und Gewährleistung der Durchsetzung technischer Maßnahmen	Überprüfung der Einhaltung von Richtlinien zur Sekundärnutzung der Daten
				Überprüfung der Anwendung von Sicherheitsvorkehrungen wie z. B. Richtlinien, Verfahren und Lieferantenverträge
				Sicherstellung, dass Zugriffskontrollen und Datenklassifizierungen angemessen und wirksam sind
				Zusammenarbeit mit Datenschutzexperten, um technische Maßnahmen für Verfremdung, Datenminimierung, Sicherheit und andere Technologien zum Schutz der Privatsphäre zu ermöglichen



# IAPP WISSENSFUNDUS FÜR DEN CIPM

MIN. MAX.

## Bereich V – Betriebslebenszyklus des Datenschutzprogramms: Aufrechterhaltung des Datenschutzprogramms

7 9

**Bereich V – Betriebslebenszyklus des Datenschutzprogramms: Aufrechterhaltung des Datenschutzprogramms** umfasst Einzelheiten darüber, wie das Datenschutzprogramm mit einschlägigen Kennzahlen und Prüfverfahren aufrechterhalten wird. Während eine Organisation die Verwaltungszyklen für ihr Datenschutzprogramm durchläuft, muss sichergestellt werden, dass alle Prozesse und Verfahren effektiv funktionieren und auch in Zukunft reproduzierbar sind.

### KOMPETENZEN

### LEISTUNGSINDIKATOREN

1 3 V.A	Verwendung von Kennzahlen zur Messung der Leistung des Datenschutzprogramms	Bestimmung geeigneter Messgrößen für verschiedene Ziele (z. B. Trendentwicklung, ROI, Widerstandsfähigkeit des Unternehmens)
		Analyse der gesammelten Daten und Verknüpfung mit Programmzielen und Compliance-Maßnahmen (durchgeführte PIAs, Antwortraten auf Rechteanfragen, Beschwerdevolumen, Kennzahlen zu Datenschutzverletzungen)
1 3 V.B	Audit des Datenschutzprogramms	Auswahl geeigneter Überwachungsformen anhand der Programmziele (z. B. Audits, Kontrollen, Unterauftragnehmer)
		Vollständiges Compliance-Monitoring durch die Überprüfung von Datenschutzrichtlinien, -kontrollen und -standards, auch im Vergleich zu Industriestandards sowie rechtlichen und/oder gesetzlichen Änderungen
3 5 V.C	Verwaltung der kontinuierlichen Beurteilung des Datenschutzprogramms	Durchführung von Risikobewertungen für Systeme, Anwendungen, Prozesse und Aktivitäten
		Verständnis des Zwecks und des Lebenszyklus der einzelnen Beurteilungsverfahren (z. B. PIA, DSFA, TIA, LIA, PTA)
		Umsetzung von Risikominderung und Kommunikation mit internen und externen Interessenvertretern nach Fusionen, Übernahmen und Veräußerungen

MIN. MAX. **Bereich VI – Betriebslebenszyklus des Datenschutzprogramms: Reaktion auf Anfragen und Vorfälle**

10 14 **Bereich VI – Betriebslebenszyklus des Datenschutzprogramms: Reaktion auf Anfragen und Vorfälle** dokumentiert die Aktivitäten, die mit der Reaktion auf Datenschutzvorfälle und den Rechten der betroffenen Personen verbunden sind. Organisationen müssen dafür sorgen, angemessene Verfahren für Informationsanfragen, Datenschutzrechte und Reaktionen auf Vorfälle einzurichten, die sich nach den entsprechenden territorialen, sektoralen und branchenspezifischen Gesetzen und Vorschriften richten.

## KOMPETENZEN

## LEISTUNGSINDIKATOREN

5	7	VI.A	Reaktion auf Auskunftsverlangen und Datenschutzrechte betroffener Personen	Sicherstellen, dass die Datenschutzhinweise und -richtlinien transparent sind und die Rechte der betroffenen Personen klar zum Ausdruck bringen
				Einhaltung der Datenschutzrichtlinien der Organisation zur Einwilligung (z. B. Widerruf der Einwilligung, Berichtigungsanträge, Einwände gegen die Verarbeitung, Zugang zu Daten und Beschwerden)
				Verständnis und Einhaltung der Gesetzgebung in Bezug auf die Rechte der Betroffenen auf Kontrolle über ihre persönlichen Daten
3	5	VI.B	Einhaltung der betrieblichen Verfahren zum Umgang mit und zur Reaktion auf Vorfälle	Verständnis und Umsetzung von Verfahren zur Behandlung und Reaktion auf Vorfälle (z. B. Beurteilung, Eindämmung, Wiedergutmachung)
				Kommunikation mit den Interessenvertretern unter Einhaltung der rechtlichen, globalen und geschäftlichen Anforderungen
				Führung eines Vorfallregisters und zugehöriger Nachweise für den Vorfall
1	3	VI.C	Beurteilung und Änderung des aktuellen Vorfallreaktionsplans	Durchführung von Überprüfungen nach einem Vorfall, um die Wirksamkeit des Plans zu verbessern
				Implementierung von Änderungen, um die Wahrscheinlichkeit und/oder die Auswirkungen künftiger Verstöße zu verringern