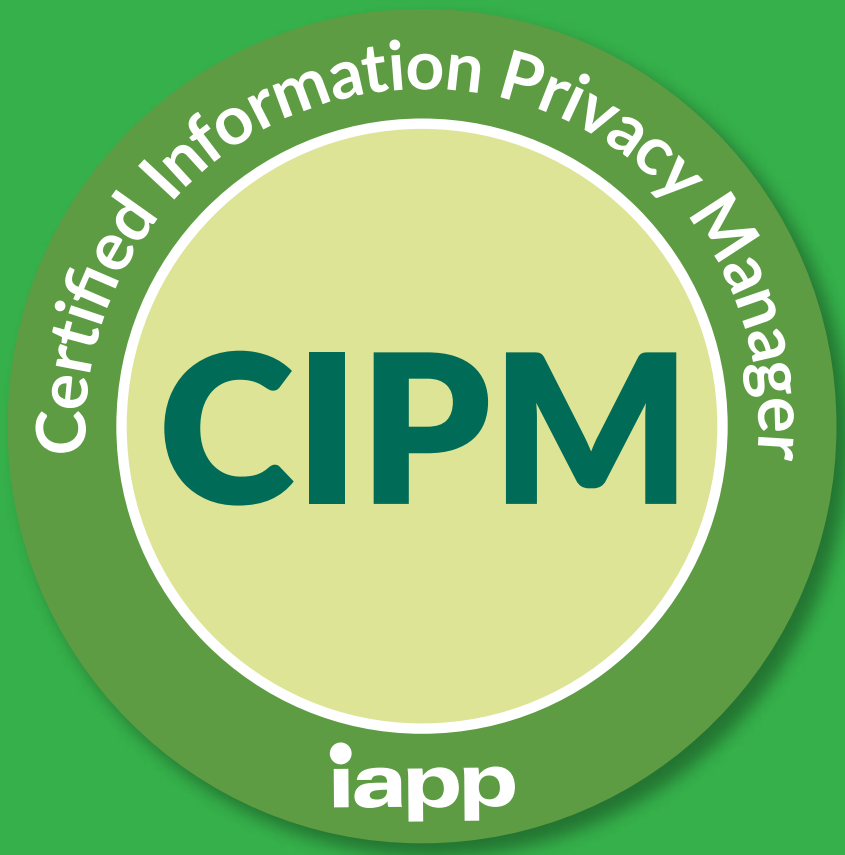
iapp



WISSENFUNDUS UND PRÜFUNGSVORLAGE FÜR DEN CIPM

VERSION 4.0.0

GÜLTIG AB: 02.10.2023

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

Im Gegensatz zum früheren Gliederungsschema unseres Wissensfundus stellen wir die Inhalte jetzt als eine Reihe von Kompetenzen und Leistungsindikatoren dar.

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

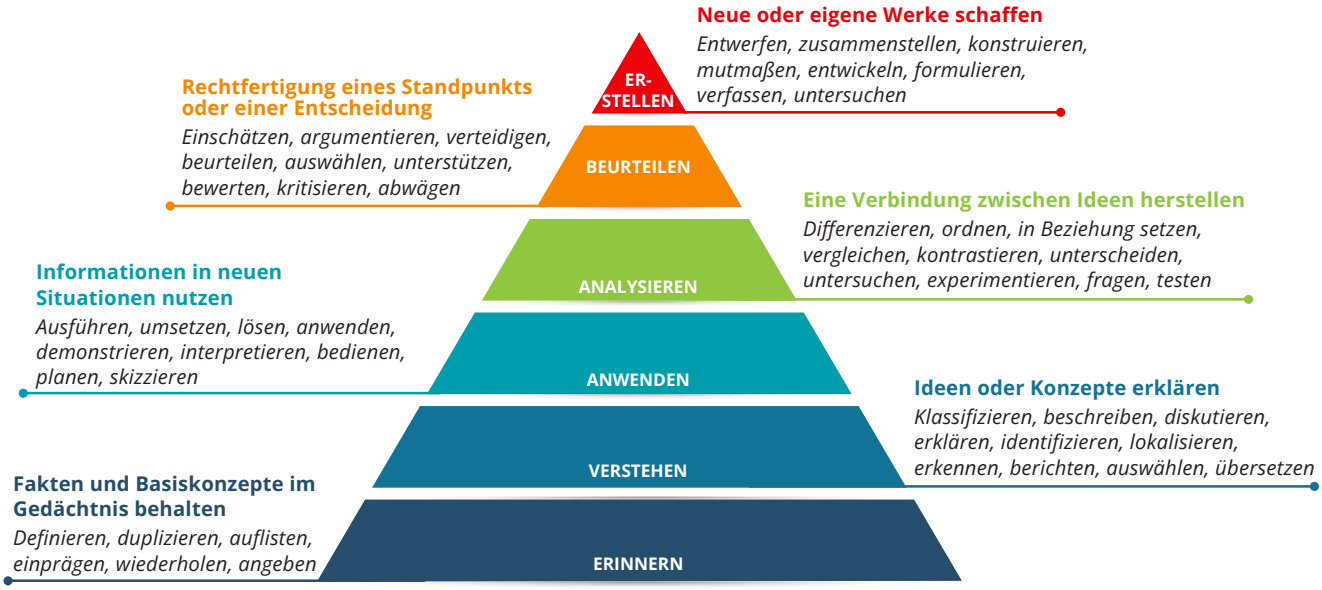
Die CIPM-, CIPP/E-, CIPP/US- und CIPT-Zertifikate der IAPP sind von der folgenden Organisation akkreditiert: **ANSI National Accreditation Board (ANAB) nach der Norm der Internationalen Organisation für Normung (ISO) 17024: 2012**.

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?
- 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 Anwenden/ Analysieren:

- 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.

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	Leistungskennzahlen
4	6	I.A	Definition des Programmumfangs und Entwicklung einer Datenschutzstrategie	Auswahl des geeigneten Governance-Modells
				Identifizierung der Quelle, Arten und Verwendungszwecke von personenbezogenen Daten im Unternehmen
				Zusammenstellung des Datenschutzteams
				Ermittlung von Interessenvertretern und internen Partnerschaften
4	6	I.B	Kommunikation der Vision und des Leitbilds der Organisation	Interne und externe Sensibilisierung für das Datenschutzprogramm des Unternehmens
				Sicherstellung eines angemessenen Zugangs zu rollenspezifischen Richtlinien und Verfahren für die Mitarbeiter
				Einführung eines Vokabulars für Datenschutzprogramme (z. B. Vorfall vs. Verletzung)
5	7	I.C	Angabe der für das Programm geltenden Gesetze, Vorschriften und Normen	Erfassung territorialer Verordnungen und/oder Gesetze
				Kenntnis der Geldbußen und Sanktionen bei Verstößen
				Kenntnis des Geltungsbereichs und der Befugnisse von Aufsichtsbehörden
				Datenschutzherausforderungen bei Geschäftstätigkeiten in oder mit Ländern, die ungenügende Datenschutzgesetze haben

MIN.	MAX.	Bereich II: Datenschutzprogramm: Einführung einer Governance von Datenschutzprogrammen		
12	16	**Bereich II – Datenschutzprogramm: Einführung einer Governance von Datenschutzprogrammen** 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		**Leistungskennzahlen**
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
				Festlegung gut durchdachter Richtlinien zur Datenverarbeitung in der Organisation und zur gemeinsamen Nutzung von Daten unter Berücksichtigung juristischer und ethischer Anforderungen
				Ermittlung der Erfassungspunkte unter Berücksichtigung von Transparenz und Integrität der Datenerfassung
				Erstellung eines Plans für den Umgang mit Verletzungen
				Erstellung eines Plans für die Bearbeitung von Beschwerden
1	3	II.B	Klärung der Rollen und Zuständigkeiten	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 Sicherheitsverletzungen nach Funktionen, einschließlich der Interessenvertreter und ihrer Rechenschaftspflicht gegenüber den Aufsichtsbehörden, der Koordinierung der Erkennungsteams (z. B. IT, physische Sicherheit, HR, Untersuchungsteams, Anbieter) und der Einrichtung von Aufsichtsteams.
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 in allen Phasen des Datenschutz-Lebenszyklus
				Schaffung kontinuierlicher Aktivitäten im Rahmen des Datenschutzprogramms (z. B. Aufklärung und Sensibilisierung, Überwachung der internen Einhaltung der Vorschriften, Programmsicherung, einschließlich Audits, Verfahren zur Bearbeitung von Beschwerden)

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	Leistungskennzahlen
3	5	III.A	Dokumentation der Data-Governance-Systeme	Zuordnung von Datenbeständen, -flüssen, -lebenszyklen und Systemintegrationen
				Abgleich der Richtlinien mit internen und externen Anforderungen
				Bestimmung des gewünschten Status und Durchführung einer Gap-Analyse zum Abgleich mit jeweiligem Standard oder Gesetz
1	3	III.B	Beurteilung der Auftragsverarbeiter und Drittanbieter´	Identifizierung der Risiken von Insourcing und Outsourcing von Daten, einschließlich vertraglicher 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, Mediensanierung und -entsorgung, Geräteforensik 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 personenbezogener Daten (z. B. rollenbasierter Zugang)
				Überprüfung und Festlegung von Fristen für die Aufbewahrung von Aufzeichnungen
				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

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		**Leistungskennzahlen**
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 organisatorischer Maßnahmen zur Minderung etwaiger Restrisiken
1	3	IV.B	Integration der wichtigsten Grundsätze von Privacy by Design (PbD)	Integration des Datenschutzes in den Systementwicklungsprozess (SDLC)
				Integration des Datenschutzes in die Geschäftsprozesse
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 administrativen Sicherheitsvorkehrungen wie z. B. Lieferanten- und Personalrichtlinien, Verfahren und Verträge
				Sicherstellung, dass Zugriffskontrollen für Mitarbeiter und Datenklassifizierungen aktiv sind
				Zusammenarbeit mit Datenschutzexperten, um technische Kontrollen für Verfremdung, Datenminimierung, Sicherheit und andere Technologien zur Verbesserung des Datenschutzes zu ermöglichen

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		**Leistungskennzahlen**
1	3	V.A	Verwendung von Kennzahlen zur Messung der Leistung des Datenschutzprogramms	Bestimmung geeigneter Messgrößen für verschiedene Ziele und Analyse der mithilfe von Kennzahlen gesammelten Daten (z. B. Trendentwicklung, ROI, Widerstandsfähigkeit des Unternehmens, PMM)
				Erfassung von Kennzahlen, um Schulungs- und Sensibilisierungsmaßnahmen mit der Verringerung von Datenschutzvorfällen zu verknüpfen, und kontinuierliche Verbesserung des Datenschutzprogramms auf Grundlage der erfassten Kennzahlen
1	3	V.B	Audit des Datenschutzprogramms	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
				Auswahl geeigneter Überwachungsformen anhand der Programmziele (z. B. Audits, Kontrollen, Unterauftragnehmer) und 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, DPIA, TIA, LIA, PTA)
				Umsetzung von Risikominderung und Kommunikation mit internen und externen Interessenvertretern nach Fusionen, Übernahmen und Veräußerungen
				Sicherstellung, dass die KI-Nutzung ethisch einwandfrei und unvoreingenommen ist, die Erwartungen an die Datenminimierung und Zweckbindung erfüllt und mit allen Vorschriften und/oder Datenschutzgesetzen im Einklang steht

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		**Leistungskennzahlen**
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 internationalen, bundesstaatlichen und einzelstaatlichen Gesetzgebung in Bezug auf die Rechte der Betroffenen auf Kontrolle über ihre persönlichen Daten (z. B. DSGVO, HIPAA, CAN-SPAM, FOIA, CCPA/CPRA).
3	5	VI.B	Einhaltung der betrieblichen Verfahren zum Umgang mit und zur Reaktion auf Vorfälle	Durchführung einer Risikobewertung des Vorfalls
				Durchführung von Eindämmungsmaßnahmen
				Bestimmung und Umsetzung von Wiedergutmachungsmaßnahmen
				Kommunikation mit den Interessenvertretern unter Einhaltung der rechtlichen, globalen und geschäftlichen Anforderungen
				Beauftragung des Datenschutzteams mit der Überprüfung der Fakten, der Festlegung von Maßnahmen und der Ausführung von Plänen
				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 weiterer Verstöße zu verringern