

AWS Leitfaden zur Entscheidungsfindung

# Auswahl eines AWS Cloud-Governance-Dienstes



# Auswahl eines AWS Cloud-Governance-Dienstes: AWS Leitfaden zur Entscheidungsfindung

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Die Marken und Handelsmarken von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, die geeignet ist, die Kunden zu verwirren oder Amazon in einer Weise herabzusetzen oder zu diskreditieren. Alle anderen Marken, die nicht Eigentum von Amazon sind, sind Eigentum ihrer jeweiligen Inhaber, die mit Amazon verbunden oder nicht verbunden oder von Amazon gesponsert oder nicht gesponsert sein können.

# Table of Contents

Leitfaden zur Entscheidungsfindung ..... 1

Einführung in die AWS Cloud-Governance ..... 1

Verstehen ..... 2

Erwägen ..... 4

Klicken Sie auf ..... 6

Verwenden Sie ..... 9

Erkunden ..... 14

Dokumentverlauf ..... 15

..... xvi

# Auswahl eines AWS Cloud-Governance-Dienstes

## Den ersten Schritt machen

Zweck	Finden Sie heraus, welche AWS Cloud-Governance-Dienste für Ihr Unternehmen am besten geeignet sind.
Letzte Aktualisierung	23. Dezember 2024
Abgedeckte Dienstleistungen	<ul style="list-style-type: none"><li>• <a href="#">AWS Artifact</a></li><li>• <a href="#">AWS Audit Manager</a></li><li>• <a href="#">CloudFormation</a></li><li>• <a href="#">AWS CloudTrail</a></li><li>• <a href="#">AWS Config</a></li><li>• <a href="#">AWS Control Tower</a></li><li>• <a href="#">AWS Organizations</a></li><li>• <a href="#">AWS Security Hub CSPM</a></li><li>• <a href="#">AWS Service Catalog</a></li><li>• <a href="#">AWS Systems Manager</a></li><li>• <a href="#">AWS Trusted Advisor</a></li></ul>

## Einführung in die AWS Cloud-Governance

Cloud-Governance besteht aus einer Reihe von Regeln, Prozessen und Berichten, mit deren Hilfe Sie Ihre AWS Cloud Nutzung an Ihren Geschäftszielen ausrichten können.

Dies deckt die Sicherheit ab, indem Strategien für mehrere Konten sowie kontinuierliche Überwachungs- und Kontrollrichtlinien ermöglicht werden. Es deckt die Einhaltung von Vorschriften ab, indem Prüfungen, Berichte und Problembehebungen automatisiert werden. Es deckt den Betrieb ab, indem es unternehmensweit Kontrollen anwendet. Es deckt das Identitätsmanagement ab, indem es das Identitäts- und Zugriffsmanagement in großem Umfang zentralisiert. Es deckt die Kosten, indem es Nutzungsberichte und die Durchsetzung von Richtlinien erleichtert. Und es deckt die

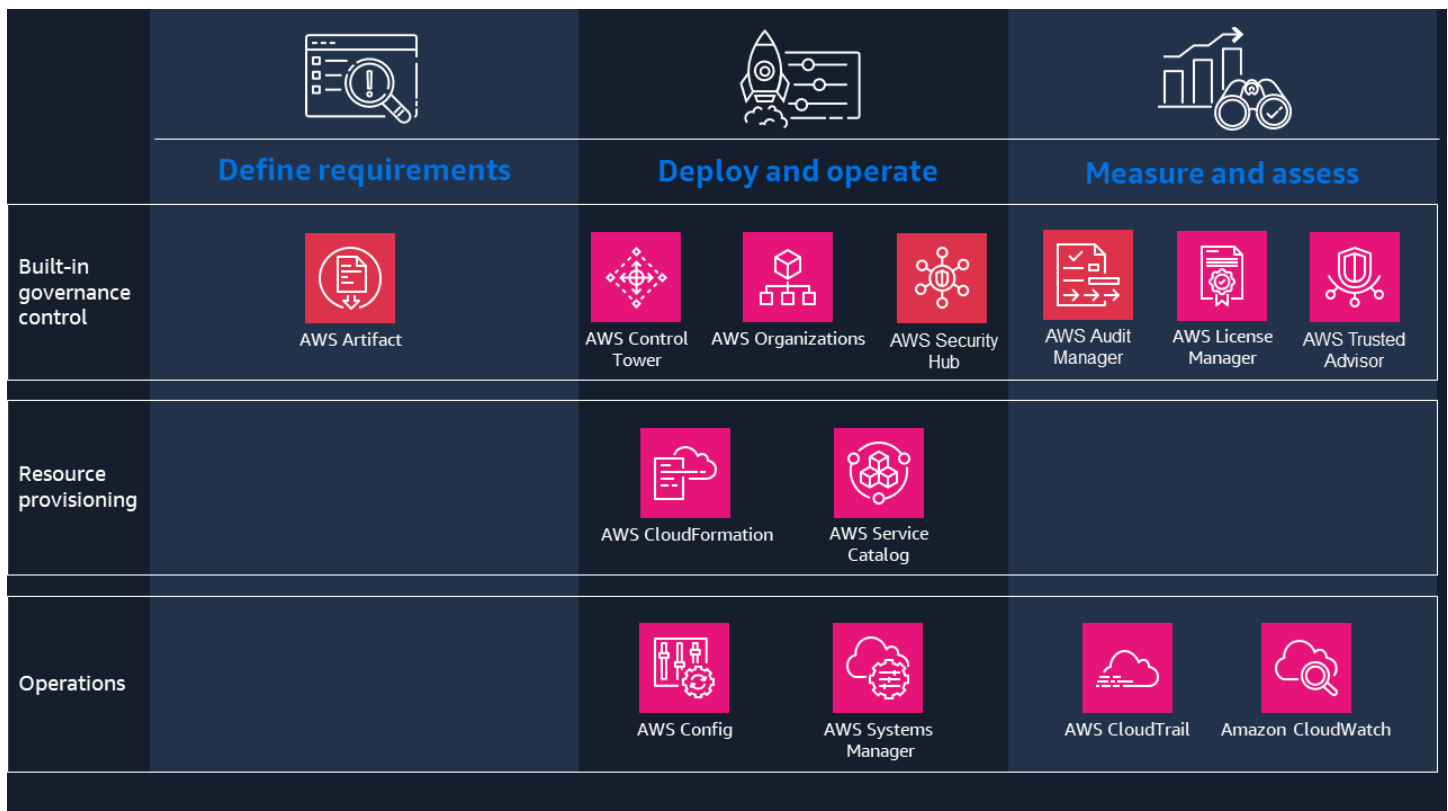
Widerstandsfähigkeit ab, indem es hilft, Bewertungen und Tests zur Validierung in CI/CD Pipelines zu integrieren.

Wir bieten eine Reihe von Services, die Sie bei der Einrichtung, Verwaltung, Überwachung und Kontrolle der Nutzung von Konten, Diensten und Ressourcen in der Cloud unterstützen und so bewährte Methoden für Cloud-Governance implementieren.

Der Leitfaden soll Ihnen bei der Entscheidung helfen, welche AWS Cloud-Governance-Dienste für Ihr Unternehmen am besten geeignet sind, um die betriebliche Widerstandsfähigkeit zu stärken, die Kosten zu optimieren und Kontrollen einzurichten, um Vorschriften oder Unternehmensstandards einzuhalten und gleichzeitig die Entwicklungsgeschwindigkeit aufrechtzuerhalten und Innovationen zu beschleunigen.

[Dieses Video ist ein sechsminütiger Abschnitt einer Präsentation, in der bewährte Verfahren für Cloud-Governance vorgestellt werden.](#)

## Verstehen Sie AWS Cloud-Governance



Das vorherige Diagramm zeigt, wie Cloud-Governance auf mehreren Ebenen aufbaut AWS-Services, die es Ihnen ermöglichen, Ihre Governance-Anforderungen zu definieren, Ihre Systeme

bereitzustellen und zu betreiben sowie deren Leistung zu messen und zu bewerten. Die Services bieten integrierte Governance-Kontrolle, Ressourcenbereitstellung zur Anpassung an Ihre Governance-Richtlinien und Betriebstools, die Sie bei der Überwachung und Verwaltung Ihrer Umgebung unterstützen.

Durch die Nutzung von AWS Cloud-Governance-Diensten können Sie sicherstellen, dass Ihre Cloud-Nutzung Ihren Geschäftszielen entspricht. Insbesondere ermöglichen sie es Ihnen, die Geschwindigkeit und Flexibilität für Entwickler zu verbessern, in einem dynamischen regulatorischen Umfeld zu agieren, Fusionen und Übernahmen zu rationalisieren und die betriebliche Widerstandsfähigkeit zu stärken:

- Verbessern Sie die Geschwindigkeit und Flexibilität für Entwickler — Erschließen Sie schnell neue Umgebungen, APIs indem Sie sicherstellen, dass Ihre Entwickler nicht auf wochenlange Bereitstellungszyklen warten müssen, und beschleunigen Sie die Bereitstellung der Pipeline. CI/CD Finden und verhindern Sie Fehler frühzeitig im Softwarebereitstellungsprozess, indem Sie vorgefertigte Kontrollen und Regeln sowie infrastructure-as-code Vorlagen für die effiziente Bereitstellung gemeinsamer Ressourcen verwenden.
- Arbeiten Sie in einem dynamischen regulatorischen Umfeld — Schaffen Sie stets gültige Grenzen, um den Zugriff auf Daten zu schützen und zu kontrollieren AWS, Ihre Compliance-Anforderungen zu kodifizieren und die Bewertung Ihrer Ressourcenkonfigurationen in Ihrem gesamten Unternehmen zu automatisieren.
- Optimieren Sie Fusionen und Übernahmen — Migrieren Sie Workloads schneller, indem Sie eine sichere, gut strukturierte Umgebung mit mehreren Konten einrichten. Zentralisieren Sie die Kontoerstellung, weisen Sie Ressourcen zu, gruppieren Sie Konten und wenden Sie Governance-Richtlinien und -Kontrollen einfach und schnell an. Verfolgen Sie einen programmatischen Ansatz für die Verwaltung mehrerer Konten in großem Maßstab.
- Stärkung der betrieblichen Belastbarkeit — Richten Sie schnell eine sichere, gut strukturierte und belastbare Umgebung mit mehreren Konten ein. Führen Sie Bewertungen Ihrer Workloads durch, um potenzielle Schwächen im Zusammenhang mit der Ausfallsicherheit aufzudecken. Führt automatisierte Prüfungen anhand von fünf Schlüsselbereichen durch — Kostenoptimierung, Leistung, Sicherheit, Fehlertoleranz und Servicebeschränkungen — und erhält Empfehlungen, anhand derer Sie bekannte Best Practices befolgen können.
- Kosten optimieren — Visualisieren, verstehen und verwalten Sie Kosten und Nutzung im Laufe der Zeit. Analysieren Sie kontinuierlich die Ressourcennutzung, identifizieren Sie nicht ausgelastete Ressourcen und beenden Sie ungenutzte Ressourcen.

Bewährte Methoden für Cloud-Governance können effektiv in die Einrichtung und den Betrieb Ihrer Workloads integriert werden. AWS Interoperable Services helfen Ihnen dabei, eine konsistente, zentralisierte Verwaltung Ihres IT-Bestands zu erreichen, einschließlich Produkten AWS von Drittanbietern. Breite und Tiefe der Kontrollen AWS-Services helfen Ihnen dabei, sich ändernde regulatorische Anforderungen zu erfüllen und Sicherheitsrisiken zu minimieren.

## Berücksichtigen Sie die AWS Kriterien für Cloud-Governance

Im folgenden Abschnitt werden einige der wichtigsten Kriterien beschrieben, die bei der Auswahl einer Cloud-Governance-Strategie zu berücksichtigen sind. Insbesondere werden die verschiedenen Arten von Cloud-Umgebungen, Kontrollsystemen und Möglichkeiten zur Unterstützung durch Entwickler erörtert, die für Ihr Unternehmen und Ihre Geschäftsziele relevant sein könnten.

### Multi-account strategy

Was es ist: Die Implementierung von Best Practices für Cloud-Umgebungen hängt von der Einführung einer sicheren Strategie für mehrere Konten ab. Verwenden Sie Konten als Bausteine und gruppieren Sie sie in [Organisationseinheiten \(OUs\)](#), z. B. grundlegende Konten OUs für Sicherheit und Infrastruktur und zusätzliche OUs für Sandboxing und Workloads.

Warum das wichtig ist: Eine Strategie für mehrere Konten sorgt für natürliche Grenzen und Isolation in Ihrer Cloud-Umgebung. Dies wiederum ermöglicht es Ihnen, Kontingente und Kontolimits zu verwalten, die Bereitstellung und Anpassung von Konten zu automatisieren und das Prinzip der geringsten Rechte anzuwenden, indem Sie den Zugriff auf Ihr Verwaltungskonto einschränken. Es ermöglicht Transparenz, sodass Sie Benutzeraktivitäten und Risiken in Ihrer gesamten Umgebung verfolgen können. Ihre Multi-Account-Strategie bildet die Grundlage, auf der Sie für Migrationsprojekte oder organisatorische Veränderungen wie Fusionen und Übernahmen aufbauen können.

Wird verwendet [AWS Organizations](#), um mehrere AWS-Konten zu einer Organisation zu konsolidieren, die Sie verwenden können, um Ressourcen zuzuweisen, Konten zu gruppieren und Governance-Richtlinien anzuwenden.

Verwenden Sie es [AWS Control Tower](#) als zusätzlichen Orchestrierungsservice, der Ihnen hilft AWS Organizations, Ihren Bestand zu strukturieren und die Steuerung OUs Ihrer AWS Umgebung mit mehreren Konten zu erweitern.

## Controls management best practices

Was es ist: Die Implementierung von Best Practices für das Kontrollmanagement kann eine Reihe von Ansätzen beinhalten. Detective Controls catch Ressourcen ab, die gegen definierte Sicherheitsrichtlinien verstoßen. Präventive Kontrollen schützen die Sicherheitsstandards, indem sie bestimmte Aktionen blockieren. Und die proaktive Kontrolle scannt Ressourcen, bevor sie bereitgestellt werden, verhindert, dass nicht konformer Code bereitgestellt wird, und weist Entwickler an, diese Fehler zu beheben. Dank der Interoperabilität können AWS-Services Sie Ihren gesamten IT-Bestand, einschließlich Produkten von Drittanbietern, zentral steuern AWS und kontrollieren, wenn Sie neue Märkte erschließen.

Warum das wichtig ist: Bewährte Methoden für das Kontrollmanagement ermöglichen es Ihnen, Kontrollen in großem Umfang programmgesteuert zu implementieren und die Einhaltung von Vorschriften automatisch zu konfigurieren oder Verstöße zu beheben. Dies ist besonders wichtig, wenn Ihr Unternehmen in einer regulierten Branche tätig ist, z. B. im Gesundheitswesen, in den Biowissenschaften, im Finanzdienstleistungssektor oder im öffentlichen Sektor, wo spezifische regulatorische Rahmenbedingungen gelten oder bestimmte Unternehmensstandards oder Anforderungen an die Datenresidenz und digitale Souveränität eingehalten werden.

Erwägen Sie Möglichkeiten zur Orchestrierung mehrerer, AWS-Services um die Sicherheits- und Compliance-Anforderungen Ihres Unternehmens zu gewährleisten [AWS Control Tower](#), indem Sie Konfigurationseinstellungen verwenden, definieren und Abweichungen davon erkennen, die AWS Nutzung und die Einhaltung von Vorschriften und Industriestandards verwenden [AWS Config](#) und überprüfen. [AWS Audit Manager](#)

## Cloud governance for developers

Was es ist: Die Implementierung von Best Practices für Cloud-Governance für Entwickler kann die Verwendung von Infrastructure as Code (IaC) zur Sicherstellung der Wiederholbarkeit und Konsistenz ihrer Arbeit sowie die Einrichtung von Prozessen zur Erkennung von Sicherheitslücken umfassen.

Warum das wichtig ist: Dies hilft Teams, schnell voranzukommen und gleichzeitig Vertrauen in ihre Governance-Prozesse zu haben. Es bietet Entwicklern eine zentrale Informationsquelle, die für den gesamten Stack bereitgestellt werden kann, eine Infrastruktur, die sie replizieren, erneut bereitstellen und für neue Zwecke verwenden können, die Möglichkeit, die Versionierung von Infrastruktur und Anwendungen gemeinsam zu kontrollieren, und eine Auswahl an Self-Service-Aktionen.



Cloud-Governance für Entwickler kann auch die Erkennung von Sicherheitslücken im Code beinhalten. Dies hilft ihnen, die Codequalität zu verbessern, kritische Probleme zu identifizieren, konsistente Release-Pipelines sicherzustellen und Projekte mit Blueprints zu starten.

[Überlegen Sie, wie Sie Buildern vorab genehmigte infrastructure-as-code Vorlagen und entsprechende IAM-Richtlinien zur Verfügung stellen könnten, die festlegen, wer, wo und wie sie verwendet werden können, indem Sie einen AWS-Service ähnlichen Service Catalog verwenden.](#)

## Scalability and flexibility

Was es ist: Entscheiden Sie sich dafür AWS-Services , dass Ihre Cloud-Governance-Maßnahmen nahtlos mit Ihrer Infrastruktur mitwachsen und sich an sich ändernde Anforderungen anpassen können. Überlegen Sie, wie und wie schnell Ihr Unternehmen wachsen wird.

Warum das wichtig ist: Wenn Sie Skalierbarkeit und Flexibilität berücksichtigen, können Sie sicherstellen, dass Ihre Cloud-Governance-Vereinbarungen robust und reaktionsschnell sind und dynamische Geschäftsumgebungen unterstützen können.

Um Ihnen eine schnelle Skalierung zu ermöglichen, AWS Control Tower orchestriert es die Funktionen mehrerer anderer [AWS-Services](#) Systeme, einschließlich AWS Organizations und AWS IAM Identity Center, um eine landing zone in weniger als einer Stunde aufzubauen. Control Tower richtet Ressourcen in Ihrem Namen ein und verwaltet sie.

AWS Organizations ermöglicht es Ihnen, die Ressourcen von [mehr als 40 Diensten](#) über mehrere Konten hinweg zu verwalten. Dies gibt einzelnen Anwendungsteams die Flexibilität und Transparenz, um Cloud-Governance-Anforderungen zu verwalten, die für ihre Arbeitslast spezifisch sind, und bietet ihnen gleichzeitig Transparenz für zentralisierte Teams.

## Wählen Sie einen AWS Cloud-Governance-Dienst

Jetzt kennen Sie die Kriterien, anhand derer Sie Ihre Cloud-Governance-Optionen bewerten werden, und können entscheiden, welcher AWS Cloud-Governance-Dienst für Ihre Unternehmensanforderungen am besten geeignet ist. In der folgenden Tabelle wird hervorgehoben, welche Dienste für welche Umstände optimiert sind. Verwenden Sie sie, um den Service zu ermitteln, der für Ihr Unternehmen und Ihren Anwendungsfall am besten geeignet ist.

Art des Anwendungsfalls	Wann würden Sie es verwenden?	Empfohlener Service
Anforderungen definieren	Um AWS Sicherheits- und Compliance-Dokumente auf Abruf herunterzuladen.	<a href="#">AWS Artifact</a>
Bereitstellung und Betrieb	Um die Cloud-Bereitstellung mit Infrastruktur als Code zu beschleunigen.	<a href="#">AWS CloudFormation</a>
	Um Ihre idealen Konfigurationseinstellungen darzustellen und zu erkennen, ob AWS Ressourcen davon abweichen.	<a href="#">AWS Config</a>
	Um mehrere in Ihrem Namen einzurichten und AWS-Services zu orchestrieren und Ihnen dabei zu helfen, die Sicherheits- und Compliance-Anforderungen Ihres Unternehmens zu erfüllen.	<a href="#">AWS Control Tower</a>
	Um mehrere AWS-Konten zu einer Organisation zu konsolidieren, die Sie verwenden können, um Ressourcen zuzuweisen, Konten zu gruppieren, Governance-Richtlinien anzuwenden und zentral und skalierbar zu verwalten.	<a href="#">AWS Organizations</a>
	Um automatisierte und kontinuierliche Prüfungen anhand der Regeln einer	<a href="#">AWS Security Hub CSPM</a>

Art des Anwendungsfalls	Wann würden Sie es verwenden?	Empfohlener Service
	Reihe unterstützter Sicherheitsstandards durchzuführen.	
	Um Entwicklern vorab genehmigte infrastructure-as-code Vorlagen und entsprechende IAM-Richtlinien zur Verfügung zu stellen, die festlegen, wer, wo und wie sie verwendet werden können.	<a href="#">Service Catalog</a>
	Um eine sichere end-to-end Verwaltung von Ressourcen in AWS und in Multicloud- und Hybridumgebungen zu ermöglichen.	<a href="#">AWS Systems Manager</a>
Messen und Beurteilen	Um die AWS Nutzung zu prüfen und das Risiko und die Einhaltung von Vorschriften und Industriestandards zu bewerten.	<a href="#">AWS Audit Manager</a>
	Um die Betriebs- und Risikoprüfung, Unternehmensführung und Einhaltung Ihrer AWS-Konto Vorschriften zu ermöglichen.	<a href="#">AWS CloudTrail</a>
	Um Ihre AWS Ressourcen und die Anwendungen, auf denen Sie laufen, AWS in Echtzeit zu überwachen.	<a href="#">Amazon CloudWatch</a>

Art des Anwendungsfalls	Wann würden Sie es verwenden?	Empfohlener Service
	Um Softwarelizenzen von Anbietern zentral in AWS und in Ihren lokalen Umgebungen zu verwalten.	<a href="#">AWS License Manager</a>
	Um Nutzung und Konfiguration anhand von Best Practices zu bewerten.	<a href="#">AWS Trusted Advisor</a>

## Verwenden Sie einen AWS Cloud-Governance-Dienst

Sie sollten jetzt genau wissen, was die einzelnen AWS Cloud-Governance-Dienste tun und welche für Sie geeignet sein könnten.

Um zu erfahren, wie Sie die einzelnen verfügbaren AWS Cloud-Governance-Dienste nutzen können, und um mehr über sie zu erfahren, haben wir einen Weg bereitgestellt, um zu untersuchen, wie die einzelnen Dienste funktionieren. In den folgenden Abschnitten finden Sie Links zu ausführlicher Dokumentation, praktischen Tutorials und anderen Ressourcen, die Ihnen den Einstieg erleichtern.

### AWS Artifact

- Erste Schritte mit AWS Artifact

Laden Sie Sicherheits- und Compliance-Berichte herunter, verwalten Sie rechtliche Vereinbarungen und verwalten Sie Benachrichtigungen.

[Erkunden Sie den Leitfaden“](#)

- Verwaltung von Vereinbarungen in AWS Artifact

Verwenden Sie den, AWS-Managementkonsole um Vereinbarungen für Ihr Konto oder Ihre Organisation zu überprüfen, zu akzeptieren und zu verwalten.

[Erkunden Sie den Leitfaden“](#)

- Bereiten Sie sich auf ein Audit in AWS Teil 1 vor — AWS Audit Manager, AWS Config, und AWS Artifact

Nutzen Sie AWS-Services Dienste, um die Erfassung von Nachweisen zu automatisieren, die bei Audits verwendet werden.

[Lesen Sie den Blog“](#)

## AWS Audit Manager

- Erste Schritte mit AWS Audit Manager

Aktivieren Sie Audit Manager mithilfe der AWS-Managementkonsole, der Audit Manager API oder der AWS CLI.

[Erkunden Sie den Leitfaden“](#)

- Tutorial für Prüfungsverantwortliche: Eine Bewertung erstellen

Erstellen Sie eine Bewertung mithilfe des Audit Manager Sample Framework.

[Beginnen Sie mit dem Tutorial“](#)

- Tutorial für Delegierte: Überprüfung eines Kontrollsatzes

Prüfen Sie einen Kontrollsatz, der Ihnen von einem Audit-Verantwortlichen in Audit Manager zur Verfügung gestellt wurde.

[Fangen Sie mit dem Tutorial an“](#)

## AWS CloudTrail

- Eventverlauf anzeigen

Überprüfen Sie die AWS API-Aktivität in Ihrem AWS-Konto für Dienste, die Folgendes unterstützen CloudTrail.

[Fangen Sie mit dem Tutorial an“](#)

- Erstellen Sie einen Pfad, um Verwaltungsereignisse zu protokollieren

Erstellen Sie einen Pfad, um Verwaltungsereignisse in allen Regionen zu protokollieren.

[Fangen Sie mit dem Tutorial an“](#)

## AWS Config

- AWS Config features

Erkunden Sie die Funktionen von zur Ressourcenverfolgung von AWS Config, von Konfigurationsverläufen und Snapshots bis hin zu anpassbaren Regeln und Konformitätspaketen.

[Erfahren Sie mehr über die Anleitungen“](#)

- Wie AWS Config funktioniert

Erfahren Sie mehr darüber AWS Config, wie der Service Ressourcen erkennt und nachverfolgt und Konfigurationselemente über verschiedene Kanäle bereitstellt.

[Erkunden Sie den Leitfaden“](#)

- Workshop zu Risiko und Compliance

Automatisieren Sie AWS Config Steuerungen mithilfe von AWS Managed Config Rules.

[Erkunden Sie den Workshop“](#)

- AWS Config Rule Development Kit-Bibliothek: Regeln in großem Maßstab erstellen und anwenden

Verwenden Sie das Rule Development Kit (RDK), um eine benutzerdefinierte AWS Config Regel zu erstellen und sie zusammen mit dem RDKLib bereitzustellen.

[Lesen Sie den Blog“](#)

## AWS Control Tower

- Erste Schritte mit AWS Control Tower

Erfahren Sie, wie Sie Ihre landing zone mit der AWS Control Tower Konsole einrichten oder APIs.

[Erkunden Sie den Leitfaden“](#)

- AWS Control Tower Workshop zum Thema Kontrollmanagement

Erfahren Sie, wie Sie die Governance in Ihrer Umgebung mit mehreren Konten einrichten können, um sie an AWS bewährten Verfahren und gängigen Compliance-Frameworks auszurichten.

#### [Erkunden Sie den Workshop“](#)

- Modernisierung der Kontoverwaltung mit Amazon Bedrock und AWS Control Tower

Richten Sie ein Konto für Sicherheitstools ein und nutzen Sie generative KI, um den Einrichtungs- und Verwaltungsprozess zu beschleunigen. AWS-Konto

#### [Lesen Sie den Blog“](#)

- Aufbau einer gut strukturierten Umgebung mit AWS GovCloud (US) AWS Control Tower

Richten Sie Ihre Verwaltung in den AWS GovCloud (US) Regionen ein, einschließlich der Steuerung Ihrer AWS Workloads mithilfe von Organisationseinheiten () OUs und. AWS-Konten

#### [Lesen Sie den Blog“](#)

## AWS Organizations

- Erste Schritte mit AWS Organizations

Erfahren Sie, wie Sie mit der Nutzung beginnen können AWS Organizations, einschließlich der Überprüfung von Terminologie und Konzepten, der Verwendung der konsolidierten Fakturierung und der Anwendung von Unternehmensrichtlinien.

#### [Erkunden Sie den Leitfaden“](#)

- Eine Organisation erstellen und konfigurieren

Erstellen Sie Ihre Organisation und konfigurieren Sie sie mit zwei AWS Mitgliedskonten.

#### [Fangen Sie mit dem Tutorial an“](#)

- Organisieren Sie Ihre AWS Umgebung mithilfe mehrerer Konten

Erfahren Sie, wie Sie mithilfe mehrerer Anwendungen Ihre Geschäftsanwendungen und -daten isolieren und verwalten und alle AWS Well-Architected Framework-Säulen optimieren AWS-Konten können.

#### [Lesen Sie das Whitepaper“](#)

- Dienste, die funktionieren mit AWS Organizations

Erfahren Sie, welche AWS-Services Dienste Sie zusammen nutzen können AWS Organizations und welche Vorteile die Nutzung der einzelnen Dienste auf unternehmensweiter Ebene bietet.

[Erkunden Sie den Leitfaden“](#)

- Best Practices for Organizational Units with AWS Organizations

Informieren Sie sich ausführlich über die empfohlene Architektur von AWS Best Practices für den Aufbau Ihrer Organisation und finden Sie Beispiele für die Organisationsstruktur und spezifische Implementierungsbeispiele.

[Lesen Sie den Blog“](#)

- Erzielung betrieblicher Exzellenz mit gestalterischen Überlegungen für AWS Organizations SCPs

Erfahren Sie, SCPs wie Sie den Zugriff auf AWS-Services und die bereitgestellten Ressourcen für mehrere innerhalb eines Unternehmens erstellte Konten kontrollieren können.

[Lesen Sie den Blog“](#)

## AWS Security Hub CSPM

- Aktivieren AWS Security Hub CSPM

AWS Security Hub CSPM Mit AWS Organizations oder in einem eigenständigen Konto aktivieren.

[Erkunden Sie den Leitfaden“](#)

- Regionsübergreifende Aggregation

Aggregieren Sie AWS Security Hub CSPM Ergebnisse aus mehreren AWS-Regionen Aggregationsregionen in einer einzigen Aggregationsregion.

[Erkunden Sie den Leitfaden“](#)

- AWS Security Hub CSPM Werkstatt

Erfahren Sie, wie Sie die Sicherheitslage Ihrer AWS Umgebungen nutzen AWS Security Hub CSPM , verwalten und verbessern können.



[Erkunden Sie den Workshop“](#)

- Drei wiederkehrende Security Hub Hub-Nutzungsmuster und wie man sie einsetzt

Erfahren Sie mehr über die drei häufigsten AWS Security Hub CSPM Nutzungsmuster und wie Sie Ihre Strategie zur Identifizierung und Verwaltung von Ergebnissen verbessern können.

[Lesen Sie den Blog“](#)

## Erkunden Sie die Ressourcen zur AWS Cloud-Governance

### Architekturdiagramme

Sehen Sie sich Referenzarchitekturdiagramme an, die Sie bei der Entwicklung Ihrer Sicherheits-, Identitäts- und Governance-Strategie unterstützen.

[Erkunden Sie Architekturdiagramme](#)

### Whitepapers

In Whitepapers finden Sie weitere Einblicke und bewährte Verfahren zur Auswahl, Implementierung und Nutzung der Sicherheits-, Identitäts- und Governance-Services, die am besten zu Ihrem Unternehmen passen.

[Entdecken Sie Whitepapers](#)

### Lösungen

Verwenden Sie diese Lösungen, um Ihre Sicherheits-, Identitäts- und Governance-Strategie weiterzuentwickeln und zu verfeinern.

[Lösungen erkunden](#)

# Dokumentverlauf

In der folgenden Tabelle werden die wichtigen Änderungen an diesem Entscheidungsleitfaden beschrieben. Für Benachrichtigungen über Aktualisierungen dieses Handbuchs können Sie einen RSS-Feed abonnieren.

Änderung	Beschreibung	Datum
<a href="#">Erste Veröffentlichung</a>	Der Leitfaden wurde zuerst veröffentlicht.	4. Oktober 2024

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.