SECURANCE
BE SURE

INDEPENDENT
CONSULTING
+ AUDIT
PROFESSIONALS

Schritt-für-Schritt-Anleitung

SOC 1 Compliance.

SOC 1 – Der Prüfungsstandard für Dienstleistungsorganisationen

Mit der Verlagerung von Geschäftsprozessen zu externen Dienstleistern stehen Unternehmen vor der Herausforderung, sicherzustellen, dass ihre Partner effektive und zuverlässige Kontrollen implementiert haben. **SOC 1** (International Standard on Assurance Engagements) bietet Unternehmen die Möglichkeit, eine umfassende Prüfung ihrer internen Kontrollen durchzuführen und nachzuweisen. Aber warum ist SOC 1 so wichtig?

Ihr Schlüssel zur internen Kontrollsicherheit

SOC 1 konzentriert sich auf die Überprüfung der internen Kontrollen von Dienstleistungsanbietern, um deren Eignung und Wirksamkeit zu bewerten. Dies schafft Vertrauen bei Kunden und Geschäftspartnern, die auf die Zuverlässigkeit und Sicherheit der ausgelagerten Prozesse angewiesen sind. Besonders für Unternehmen, die Geschäftstätigkeiten auslagern, ist SOC 1 ein entscheidender Nachweis über die Kontrolle der ausgelagerten Risiken.

Für wen ist SOC 1 relevant?

SOC 1 richtet sich an Dienstleistungsanbieter, die Geschäftsprozesse für andere Unternehmen übernehmen und nachweisen müssen, dass diese Prozesse sicher, zuverlässig und den geltenden Standards entsprechend ablaufen.

Zu den relevanten Branchen gehören:

- **Finanzdienstleister:** Banken, Versicherungen und Investmentfirmen, die Prozesse auslagern und hohe regulatorische Anforderungen erfüllen.
- **Rechenzentren und Cloud-Dienstleister:** Unternehmen, die IT-Infrastrukturen und -Dienstleistungen bereitstellen.
- **Shared Service Center:** Unternehmen, die zentrale Dienstleistungen wie Buchhaltung oder Personalwesen für andere Einheiten oder Konzerne übernehmen.

Die wichtigsten SOC 1 Kontrollbereiche – Grundlage der Prüfung

1. **Informationssicherheits- und Risikomanagement**: Schutz vor unbefugtem Zugriff durch strenge Sicherheitsmaßnahmen und Risikobewertung.
2. **Organisatorische Sicherheit**: Strukturen und Verantwortlichkeiten, die klare Sicherheitsrollen definieren.
3. **Konfigurationsmanagement**: Maßnahmen zur Sicherstellung, dass Systeme korrekt konfiguriert und gewartet werden.
4. **Personalmanagement**: Sicherheitsüberprüfungen und -richtlinien für Mitarbeiter.
5. **Physische und Umweltsicherheit**: Schutz von Rechenzentren und anderen kritischen Infrastrukturen.
6. **Systemadministration und Betrieb**: Überwachung und Pflege der laufenden IT-Operationen.
7. **Zugriffskontrollen**: Beschränkung des Zugriffs auf kritische Systeme und Daten.
8. **Vorfalls- und Problemmanagement**: Verfahren zur Behandlung und Lösung von Sicherheitsvorfällen.
9. **Änderungsmanagement**: Sicherstellung, dass alle Systemänderungen kontrolliert und dokumentiert werden.
10. **Business Continuity Management**: Pläne zur Sicherstellung des Geschäftsbetriebs im Falle von Notfällen.
11. **Schutz personenbezogener Daten**: Maßnahmen zur Einhaltung von Datenschutzvorgaben wie der DSGVO.
12. **Service-Level-Management**: Überwachung und Einhaltung von vertraglich vereinbarten Serviceleistungen.

5 gute Gründe für SOC 1

Vertrauensbildung und Compliance

- **Starke interne Kontrollen**: SOC 1 unterstützt Sie bei der Sicherstellung robuster interner Kontrollen, indem es eine gründliche Überprüfung Ihrer Prozesse und Systeme ermöglicht.
- **Reputation und Vertrauen**: Die SOC 1-Zertifizierung belegt Ihr Engagement für transparente und zuverlässige Geschäftsprozesse, was das Vertrauen von Kunden und Geschäftspartnern stärkt.
- **Risikomanagement**: SOC 1 hilft Ihnen, Risiken in ausgelagerten Prozessen zu identifizieren und zu minimieren, wodurch Sie Ihre Risikomanagementpraktiken verbessern können.
- **Effizienzsteigerung**: Der Zertifizierungsprozess deckt Ineffizienzen in Prozessen auf und unterstützt Sie bei der Optimierung, was langfristig zu Kostenersparnissen führt.
- **Kombinierte Compliance:** SOC 1 bietet eine solide Grundlage für die Einhaltung weiterer Standards, wie beispielsweise SOC 2 oder BSI C5 und erleichtert die Integration von zusätzlichen Vorschriften.

Das interne Kontrollsystem

Sicherheit, Compliance und Geschäftserfolg im Fokus

Ein **Internes Kontrollsystem (IKS)** ist für Unternehmen in der Finanzdienstleistungsbranche, in Rechenzentren, bei Cloud-Anbietern und Shared Service Center unerlässlich, um Sicherheitsanforderungen zu erfüllen, Risiken effektiv zu managen und regulatorische Vorgaben einzuhalten.

Effizientes Risikomanagement und erhöhte Sicherheit

Als Dienstleistungsanbieter müssen Sie sicherstellen, dass Sie sensible Daten Ihrer Kunden umfassend schützen. Ein IKS hilft dabei, Sicherheitsrisiken zu identifizieren und durch präventive Maßnahmen zu minimieren. Dazu gehören strikte Zugriffsregeln, Verschlüsselungen und eine kontinuierliche Überwachung der IT-Systeme. Das IKS reduziert das Risiko von Vorfällen wie Datenverlust oder Cyberangriffen, indem es Sicherheitskontrollen automatisiert und standardisiert.

Einhaltung von Compliance-Vorgaben: Mehr als nur eine Pflicht

Unternehmen, die nach dem SOC 1-Standard zertifiziert werden möchten, müssen strenge Compliance-Anforderungen erfüllen und wirksame Sicherheitskontrollen implementieren. Ein Internes Kontrollsystem (IKS) unterstützt dabei, diese Kontrollen in den täglichen Betriebsprozessen zu integrieren und sicherheitsrelevante Prozesse zu dokumentieren. Dies gewährleistet Transparenz und Nachvollziehbarkeit für Kunden, einschließlich der Einhaltung von Vorschriften wie der DSGVO.

Effiziente Steuerung von Prozessen für Cloud-Dienste

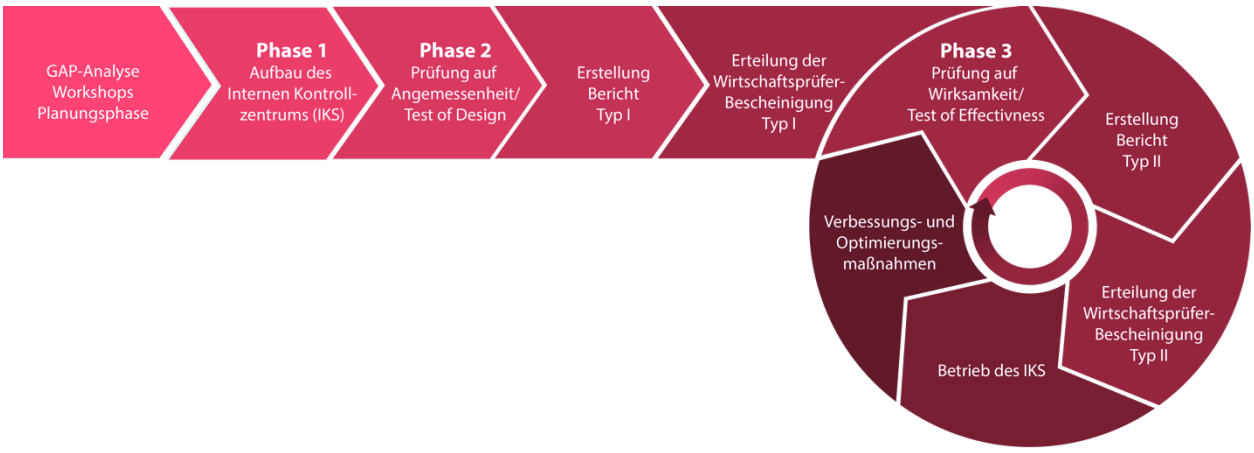
Neben der Einhaltung von Compliance-Vorgaben unterstützt ein IKS die effektive Kontrolle und Steuerung der internen Betriebsprozesse. Es überwacht die Verfügbarkeit von Diensten und stellt sicher, dass diese jederzeit funktionsfähig sind. Bei Störungen oder sicherheitsrelevanten Vorfällen ermöglicht das IKS eine schnelle Reaktion, um Ausfallzeiten zu minimieren. Es gewährleistet zudem die Integrität der Datenverarbeitung und schützt vor Manipulationen.

Schutz vor Betrug und Missbrauch

Ein wirksames IKS bietet nicht nur Schutz vor externen Bedrohungen, sondern auch vor internen Risiken wie Betrug oder Missbrauch. Durch die klare Zuweisung von Verantwortlichkeiten und die Etablierung transparenter Prozesse werden mögliche Schwachstellen minimiert. Beispielsweise verhindert ein IKS, dass unbefugte Mitarbeiter auf kritische Systeme zugreifen oder Änderungen an wichtigen Daten vornehmen können. Dadurch wird gewährleistet, dass die Integrität der Systeme und Daten jederzeit gewahrt bleibt.

SOC 1 Prüfung und Testierung

Der iAP-Step-by-step-Ansatz



GAP-Analyse, Workshops & Planung

Zu Beginn der SOC 1-Zertifizierung bewerten wir den Zustand Ihres internen Kontrollsystems (IKS). In einem gemeinsamen Workshop definieren wir den Geltungsbereich der Zertifizierung und identifizieren die relevanten Risiken und Kontrollziele für Ihre Dienstleistungsprozesse. Basierend auf den Ergebnissen wird ein detaillierter Plan erstellt, der die notwendigen Maßnahmen und Meilensteine sowie die Vereinbarungen mit dem Management festlegt.

PHASE 1. Aufbau und Implementierung des internen Kontrollsystems (IKS)

Risikobewertung, Prozesse & Kontrollen

Wir führen Interviews, um Risiken in Ihren Prozessen zu identifizieren und erfassen die wesentlichen Informationen innerhalb Ihrer Organisation. Auf Basis dieser Ergebnisse dokumentieren wir die bestehenden Kontrollmaßnahmen und erfassen diese in einer Kontrollmatrix nach den Anforderungen von SOC 1. Wir beraten proaktiv bei der Implementierung fehlender Kontrollen, einschließlich Prozessbeschreibungen, und sichern die Abdeckung der Anforderungen Ihrer Kunden zu.

Systembeschreibung

Ein zentraler Bestandteil des SOC 1-Berichts ist die Systembeschreibung. Diese umfasst die wesentlichen Prozesse, Strukturen und Kontrollen Ihres Unternehmens, die für die Zertifizierung relevant sind. Gemeinsam mit Ihnen bereiten wir den allgemeinen Abschnitt des Berichts vor.

Vorprüfung

Nach der Implementierung der Kontrollen führen wir eine Vorprüfung ('Walkthrough') durch. Während der Vorprüfung werden die Kontrollmaßnahmen getestet und mögliche Problembereiche vor der endgültigen Prüfung identifiziert. Während dieser Phase stellen Sie uns die erforderlichen Dokumentationen und Nachweise zur Verfügung.

Die Bearbeitungszeit der Phase 1 beträgt je nach Engagement und Verfügbarkeit der Mitarbeiter zwischen acht und zwölf Wochen. Die erforderliche Verfügbarkeit der zuständigen Mitarbeiter wird auf zwei bis drei Tage pro Woche während dieses Zeitraums geschätzt.

PHASE 2. Prüfung auf Angemessenheit (Typ I)

Prüfung

In der Prüfung bewerten wir, ob die implementierten Kontrollen so gestaltet sind, dass sie die Anforderungen des SOC 1-Standards erfüllen. Wir analysieren die implementierten Richtlinien, Verfahren und Sicherheitsmechanismen Ihrer Organisation. Dies umfasst Sicherheitsmaßnahmen, Zugriffskontrollen, Datenverschlüsselung und andere relevante Schutzmaßnahmen. Diese Phase führt zur Erstellung des SOC 1 Typ I-Berichts.

Die Bearbeitungszeit der Phase 2 beträgt je nach Engagement und Verfügbarkeit der Mitarbeiter zwischen vier bis sechs Wochen. Die erforderliche Verfügbarkeit der Mitarbeiter wird auf etwa zwei Tage pro Woche während dieses Zeitraums geschätzt.

Berichterstellung und Erteilung der Wirtschaftsprüferbescheinigung

Abschließend wird der SOC 1 Typ I-Bericht, bestehend aus den Standard- und gegebenenfalls zusätzlichen Abschnitten, erstellt. Dieser enthält unter anderem die Management-Erklärung, eine Beschreibung des Systems und die implementierten Kontrollen. Falls relevant, werden auch Kontrollen von Sub-Dienstleistern berücksichtigt. Den Entwurf des Berichts besprechen wir mit Ihnen im Detail.
Als Ergebnis erhalten Sie die Bescheinigung des Wirtschaftsprüfers über die Angemessenheit der Kontrollstruktur Ihres SOC 1-Systems zu einem bestimmten Stichtag.

Betrieb des IKS

Nachdem das interne Kontrollsystem (IKS) implementiert ist, überwachen und betreiben Sie es kontinuierlich. Sie stellen sicher, dass alle Kontrollen ordnungsgemäß durchgeführt werden und das

System an neue Anforderungen oder Veränderungen angepasst wird. Dies umfasst die regelmäßige Überprüfung und Einhaltung der festgelegten Richtlinien und Verfahren.

Verbesserungs- und Optimierungsmaßnahmen

Basierend auf den laufenden Überwachungen identifizieren Sie Bereiche zur Verbesserung und setzen Optimierungsmaßnahmen um. Sie passen bestehende Kontrollen an, führen neue Kontrollmechanismen ein und bieten Schulungen an, um die Wirksamkeit des Systems zu steigern. Das Ziel ist es, die Kontrollen kontinuierlich zu verbessern und ihre Effektivität zu maximieren.

PHASE 3. Prüfung auf Wirksamkeit (Typ II)

Prüfung

Nach einem bestimmten Zeitraum – in der Regel sechs Monate - evaluieren wir die Wirksamkeit Ihres implementierten internen Kontrollsystems (IKS), indem wir alle etablierten SOC 1-Kontrollen detailliert testen. Wir prüfen anhand Ihrer Dokumentationen und Nachweise, ob die Kontrollen wirksam sind, also gemäß den definierten Anforderungen funktionieren und die festgelegten Ziele erreichen. Wir dokumentieren alle Beobachtungen und bewerten die Effektivität der Maßnahmen.

Die Bearbeitungszeit der Phase 3 beträgt je nach Engagement und Verfügbarkeit der Mitarbeiter zwischen vier bis sechs Wochen. Die erforderliche Verfügbarkeit der Mitarbeiter wird auf etwa zwei Tage pro Woche während dieses Zeitraums geschätzt.

Berichterstellung und Erteilung der Wirtschaftsprüferbescheinigung

Nach Abschluss der Prüfung erstellen wir einen umfassenden Bericht, der die Ergebnisse zusammenfasst und die Wirksamkeit und Funktionsfähigkeit der Kontrollen bescheinigt. Wir besprechen den Entwurf des Berichts mit Ihnen, um sicherzustellen, dass alle relevanten Aspekte berücksichtigt sind.
Als Ergebnis erhalten Sie die Bescheinigung des Wirtschaftsprüfers über die Wirksamkeit der Kontrollstruktur Ihres SOC 1-Systems über den Prüfzeitraum.

Die SOC 1 -Konformität

Die SOC 1-Konformität wird durch den SOC 1-Bericht eines zugelassenen Wirtschaftsprüfers nachgewiesen, der entweder als Typ I (Angemessenheit der Kontrollen) oder Typ II (Wirksamkeit der Kontrollen über einen Prüfungszeitraum) ausgestellt wird. Ein solcher Bericht ist nicht zeitlich festgelegt, aber um die Konformität zu gewährleisten, müssen Unternehmen regelmäßig, in der Regel jährlich, Prüfungen durch eine Wirtschaftsprüfungsgesellschaft durchführen lassen. Dabei wird sichergestellt, dass die internen Kontrollsysteme weiterhin angemessen sind und ordnungsgemäß funktionieren, insbesondere in Bezug auf die ausgelagerten Prozesse und Dienstleistungen.

Der Bericht

SOC 1 Audits zur Qualitätssicherung

Ein SOC 1-Bericht bietet eine umfassende Bewertung der internen Kontrollen und Prozesse einer Organisation, insbesondere in Bezug auf ausgelagerte Dienstleistungen. Er beginnt mit der Erklärung der Unternehmensleitung, in der bestätigt wird, dass die relevanten Kontrollen ordnungsgemäß implementiert und wirksam sind. Der Bericht enthält zudem die Bewertung eines unabhängigen Wirtschaftsprüfers, der den Umfang der Prüfung, die geprüften Systeme und Kontrollen sowie sein abschließendes Urteil darlegt. Weiterhin beschreibt der Bericht detailliert die internen Prozesse und Kontrollen, die implementiert wurden, um die wesentlichen Risiken der ausgelagerten Dienstleistungen zu adressieren. Zusätzlich werden Informationen bereitgestellt, die für Kunden und Partner von Interesse sein könnten und zur besseren Transparenz beitragen.

Type I Bericht

Der Prüfer untersucht, ob die Kontrollen zu einem bestimmten Zeitpunkt vorhanden und angemessen konzipiert und mit hinreichender Sicherheit geeignet sind, die zuvor definierten Kriterien einzuhalten.

Type II Bericht

Ein SOC 2 Type II-Bericht bewertet die Eignung des Designs und die Existenz der Kontrollen sowie deren operative Wirksamkeit über einen definierten Zeitraum von mindestens sechs Monaten. Der externe Prüfer führt eine detaillierte Prüfung der internen Kontrollen der Organisation durch und überprüft, ob alle Kontrollen gemäß den vordefinierten Prozessen und Verfahren wirksam sind.

Der SOC 1-Bericht als Marketinginstrument

Ihr Schlüssel zu höherem Vertrauen und Wettbewerbsvorteilen

SAE 3402-Berichte sind ein kraftvolles Marketinginstrument, das Organisationen als vertrauenswürdige Partner positioniert. Durch die umfassende Dokumentation spezifischer Kontrollen und Sicherheitspraktiken gemäß den SOC 1-Anforderungen vermittelt der Bericht ein klares Bild der internen Kontrollsysteme eines Unternehmens. Dies ermöglicht es, sich klar von Wettbewerbern abzugrenzen und gezielt auf die individuellen Bedürfnisse der Kunden einzugehen. Da SOC 1-Berichte in vielen Branchen als wesentliche Norm anerkannt sind, riskieren Unternehmen ohne solchen Bericht, bedeutende Geschäftsmöglichkeiten zu verpassen und ihre Marktchancen zu schmälern.

RISIKO-EXCELLENZ

Verbessert die Qualität des Risikomanagements und stärkt das interne Kontrollrahmenwerk.

PROFESSIONALITÄT

Unterstützt die Professionalisierung interner Prozesse und Verfahren, wodurch Effizienz und Effektivität gesteigert werden.

MÖGLICHKEITEN

Schafft neue Geschäftsmöglichkeiten und stärkt bestehende Kundenbeziehungen durch erhöhte Sicherheit und Transparenz.

ANERKANNT

SOC 1 ist weithin anerkannt und gilt als umfangreiche Prüfung der Kontrollaktivitäten einer Dienstleistungs-organisation.

VERTRAUEN SCHAFFEN

Erfüllt das Kriterium der Bestätigung durch einen unabhängigen Dritten und stärkt das Vertrauen bei Kunden und Partnern.

SPART ZEIT

Reduziert den Aufwand, indem Partnern und Kunden Fragen effizient beantwortet werden, wodurch die Notwendigkeit entfällt, umfangreiche IT-Fragebögen auszufüllen.

Securance + iAP

Zwei starke Partner

Als führendes Kompetenzunternehmen hat **Securance** seit 2004 über 1.000 Prüfungen durchgeführt und betreut Kunden in 25 Ländern weltweit. Das Unternehmen mit Sitz in Utrecht (Niederlande) wurde mit dem Ziel gegründet, Unternehmen durch die komplexen Bereiche der Sicherheit und Cybersicherheit zu navigieren.
„Um diese Mission zu erreichen, müssen wir bahnbrechende Innovationen im Risikomanagement einführen, die Effizienz durch Automatisierung optimieren, ein vielfältiges globales Team aufbauen und einen positiven Beitrag zu den Gemeinschaften leisten, denen wir dienen, um nachhaltiger und transparenter zu werden."

Durch unsere Partnerschaft mit Securance seit 2024 bündeln wir unsere Stärken und etablieren uns als zuverlässige Assurance-Partner mit internationaler Expertise.

Die iAP - Independent Consulting + Audit Professionals GmbH mit Sitz in Berlin ist ein konstruktiver IT-Assurance Partner für Wirtschaftsprüfer und Unternehmen. Seit rund 20 Jahren sind wir erfolgreich im deutschen Markt tätig und haben bundesweit mehr als 800 Projekte erfolgreich für unsere Kunden abgeschlossen:
„Unsere fachliche Arbeitsweise ist digital und interdisziplinär. Ehrgeiz, Professionalität und Präzision prägen unser Tun. Als Dienstleister und Partner legen wir großen Wert auf Fairness, Vertrauen und Verlässlichkeit. Wir auditieren mit Bedacht und denken stets lösungsorientiert im Sinne unserer Mandanten und Partner."

Für unsere Kunden bedeutet die Verbindung zwischen **iAP** und **Securance**:

- **Großes Expertenteams**
- **Breite Kompetenzen für Informationssicherheit und Interne Kontrollsysteme**
- **Internationale Präsenz**
- **Globales Denken mit lokalem Know-how**
- **Integrierte Umsetzung mit umfassenden Risikomanagement**

„Gemeinsam sind wir fest davon überzeugt, dass Ihr Unternehmen seine Effizienz erhöhen und seine Risiken minimieren kann, wenn sich die Verfolgung spezifischer Standards für Prüfberichte in Verbindung mit robusten Cybersicherheitsmaßnahmen nahtlos in Ihre strategischen Ziele und Bestrebungen einfügt!"

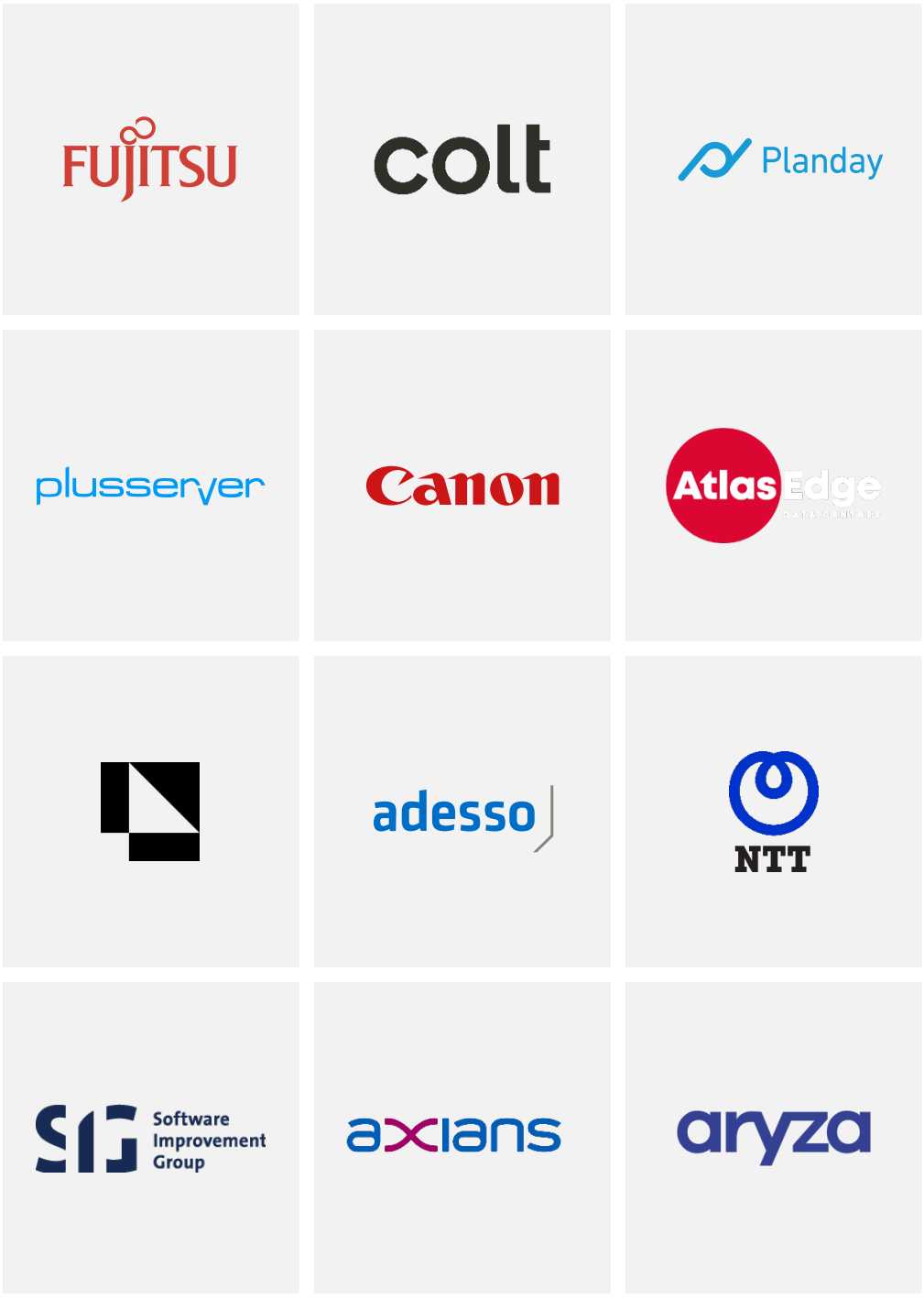
Investieren Sie in Effizienz, Wertschöpfung und Partnerschaft

- **Durchführung von Risikoanalysen**
- **Unterstützung beim Aufbau von Internen Kontrollsystemen**
- **Planung von Projekten**
- **Vorbereitung von Systembeschreibungen**
- **Durchführung von Readiness Assessments**

Die Implementierung von Internen Kontrollsystemen erfordert eine effektive Planung, die Einbindung der Führungsebene, eine gründliche Analyse von Prozessen sowie zuverlässige Ressourcen und ein solides Projektmanagement.
Wir arbeiten nach den höchsten professionellen Standards und haben umfassende Erfahrung im Umgang mit anspruchsvollen Zeitangaben. Wir leben unsere professionellen Standards und liefern stets höchste Qualität, während wir kontinuierlich bestrebt sind, die Bedürfnisse unserer Kunden zu erfüllen.
Dank unserer flachen Organisationsstruktur und effizienten Kommunikationswege können wir schnell auf Ihre Anforderungen reagieren. Wenn Sie sich für uns entscheiden, wählen Sie nicht nur eine professionelle Organisation, sondern auch einen persönlichen Ansatz. Effektives Projektmanagement, unsere Erfahrung bei dem Aufbau von internen Kontrollsystemen und unser professionelles Auftreten sind unserer Meinung nach das Fundament für herausragende Ergebnisse.
Wir sind der Überzeugung, dass ein gutes Verständnis, klare Kommunikation und Expertise entscheidend sind, um Ihnen als unseren Kunden einen Mehrwert zu bieten. Auf dieser Grundlage werden wir Sie über relevante Änderungen in regulatorischen Anforderungen, gesetzlichen Vorschriften und anderen wichtigen Entwicklungen informieren.

Unsere zufriedenen Kunden

Referenzen



SECURANCE
BE SURE

INDEPENDENT
CONSULTING
+ AUDIT
PROFESSIONALS

Securance Ltd.

63-66 Hatton Garden
London EC1N 8LE, UK
+44 20 351 446 56
www.securance.co.uk

Securance BV

Reactorweg 47
3542 AD Utrecht
+31 30 280 08 88
www.securance.nl

iAP GmbH

Josef-Orlopp-Str.54
10365 Berlin
+49 30 439 716 860
www.audit-professionals.de