SECURANCE
BE SURE

INDEPENDENT
CONSULTING
+ AUDIT
PROFESSIONALS

Schritt-für-Schritt-Anleitung

BSI C5 + SOC 2 Compliance.

BSI C5 – Sicherheit und Compliance für Cloud-Dienste in Deutschland

Mit der Verlagerung geschäftskritischer Prozesse in die Cloud stehen Unternehmen vor der Herausforderung, ihre Daten sicher zu verwalten. Der **BSI C5-Standard** bietet Cloud-Anbietern und ihren Kunden eine klare Grundlage für den Nachweis der Einhaltung von Sicherheitsvorgaben und regulatorischen Anforderungen. Doch was macht diesen Standard so entscheidend?

Ihr Schutzschild für Cloud-Dienste

Der **BSI C5 (Cloud Computing Compliance Criteria Catalogue)** wurde vom Bundesamt für Sicherheit in der Informationstechnik entwickelt, um Cloud-Anbietern und -Nutzern ein strukturiertes System zur Bewertung und Dokumentation von Sicherheitsmaßnahmen zu bieten.

Wer profitiert von BSI C5? – Die relevanten Zielgruppen

BSI C5 ist maßgeschneidert für eine Vielzahl von Unternehmen, insbesondere für:

- **Cloud-Service-Provider (CSPs):** Anbieter von Public-, Private- oder Hybrid-Cloud-Lösungen, die hochsensible Daten und Geschäftsprozesse für ihre Kunden hosten;
- **Finanz- und Versicherungsdienstleister:** Unternehmen, die Daten in der Cloud speichern und strengen regulatorischen Anforderungen unterliegen;
- **Gesundheitswesen:** Cloud-Dienste im Gesundheitsbereich, die Patientendaten verarbeiten;
- **IT-Dienstleister:** Unternehmen, die Managed Services für sicherheitskritische Bereiche anbieten, müssen nachweisen, dass ihre Cloud-Infrastrukturen allen Anforderungen gerecht werden;
- **Regierungsbehörden:** Die C5-Konformität ist für öffentliche Institutionen ein wichtiges Kriterium bei der Auswahl von Cloud-Dienstleistern.

Die fünf zentralen Pfeiler des BSI C5

BSI C5 deckt fünf Schlüsselbereiche der Informationssicherheit ab, die sicherstellen, dass Cloud-Dienstleister höchste Sicherheitsstandards erfüllen:

1. **Informationssicherheitsmanagement:** Klare Richtlinien und Verantwortlichkeiten im Unternehmen.
2. **Zugangskontrollen:** Strenge Maßnahmen für den Schutz sensibler Daten.
3. **Notfall- und Vorfallmanagement:** Prävention und Reaktion auf Sicherheitsvorfälle.
4. **Betriebsprozesse und IT-Sicherheit:** Regelmäßige Sicherheitsupdates und physische Schutzmaßnahmen.
5. **Rechtliche Compliance:** Erfüllung gesetzlicher und vertraglicher Vorgaben.

SOC 2 – Der globale Sicherheitsstandard für IT- und Cloud-Dienstleister

Mit dem zunehmenden globalen Austausch von Daten und Diensten stehen Cloud-Anbieter vor der Herausforderung, internationale Sicherheitsanforderungen zu erfüllen. **SOC 2 (System and Organization Controls)** ist ein weltweit anerkannter Prüfstandard, der speziell für Unternehmen entwickelt wurde, die Daten verarbeiten und speichern. Aber warum ist SOC 2 so wichtig?

Ihr Schlüssel zur globalen Datensicherheit

SOC 2 baut auf den Trust Service Criteria auf und bietet Cloud-Anbietern eine umfassende Bewertung ihrer internen Kontrollen in Bezug auf Datensicherheit, Vertraulichkeit und Integrität. Besonders für Unternehmen, die international tätig sind, schafft eine SOC 2-Zertifizierung Vertrauen bei Kunden und Partnern.

Für wen ist dieser Standard relevant?

SOC 2 richtet sich an Cloud-Anbieter und Dienstleister, die international tätig sind und Kunden aus verschiedenen Branchen bedienen, wie:

- **IT-Dienstleister und SaaS-Anbieter:** Startups und etablierte Unternehmen, die Software-as-a-Service-Lösungen weltweit anbieten.
- **Finanz- und Versicherungsdienstleister:** Unternehmen, die Cloud-basierte Finanz- oder Versicherungsprodukte anbieten, profitieren von SOC 2.
- **Multinationale E-Commerce-Unternehmen:** Online-Plattformen, die sensible Zahlungs- und Kundendaten in globalen Cloud-Systemen verarbeiten.
- **Global agierende Technologieunternehmen:** Unternehmen, die weltweit Dienstleistungen erbringen und deren Kunden in verschiedenen Rechtsräumen tätig sind.

Die fünf Trust Service Kriterien – Eckpfeiler der SOC 2-Prüfung

1. **Sicherheit:** Schutz vor unbefugtem Zugriff durch strenge Sicherheitsmaßnahmen wie Firewalls und Verschlüsselung.
2. **Verfügbarkeit:** Sicherstellung der jederzeitigen Erreichbarkeit von Cloud-Diensten für Kunden und Geschäftspartner.
3. **Integrität der Verarbeitung:** Gewährleistung, dass Daten korrekt verarbeitet und gespeichert werden.
4. **Vertraulichkeit:** Maßnahmen zum Schutz sensibler Geschäftsdaten, um sicherzustellen, dass diese nur berechtigten Personen zugänglich sind.
5. **Datenschutz:** Einhaltung globaler Datenschutzrichtlinien wie der DSGVO.

Synergie von BSI C5 und SOC 2

Maximale Sicherheit und Compliance für Ihr Unternehmen

Umfassende Abdeckung von Sicherheits- und Datenschutzanforderungen
Die **BSI C5-Zertifizierung** ist speziell auf den deutschen und europäischen Markt ausgerichtet und stellt sicher, dass Ihre Sicherheits- und Datenschutzmaßnahmen den strengen Anforderungen der Datenschutz-Grundverordnung (DSGVO) entsprechen. Auf der anderen Seite bietet **SOC 2** einen international anerkannten Rahmen, der fünf Trust Service Criteria abdeckt: Sicherheit, Verfügbarkeit, Integrität der Verarbeitung, Vertraulichkeit und Datenschutz.
Die Kombination von BSI C5 und SOC 2 gewährleistet die Erfüllung sowohl lokaler als auch globaler Sicherheits- und Datenschutzanforderungen und ist besonders wertvoll für Unternehmen, die in verschiedenen Regionen agieren und eine internationale Kundenbasis bedienen.

Effiziente Einhaltung regulatorischer Anforderungen
Durch die Integration von BSI C5 und SOC 2 können Sie sicherstellen, dass Sie die regulatorischen Anforderungen in Europa sowie international abdecken. BSI C5 adressiert spezifische europäische Vorschriften, während SOC 2 globale Standards erfüllt. Dies vereinfacht die Compliance und reduziert die Notwendigkeit, separate Systeme für verschiedene regulatorische Anforderungen zu implementieren.

Optimierung von Prozessen und Ressourcennutzung
Da sich viele der Sicherheits- und Datenschutzkontrollen von BSI C5 und SOC 2 überschneiden, können Sie dieselben Kontrollen und Prozesse für beide Zertifizierungen nutzen. Dies ermöglicht eine effiziente Ressourcennutzung, da Sie durch die Integration der Kontrollen nicht nur Zeit und Kosten sparen, sondern auch eine einheitliche Sicherheitsstrategie entwickeln, die beide Standards abdeckt.

Das interne Kontrollsystem

Sicherheit, Compliance und Geschäftserfolg im Fokus

Ein **Internes Kontrollsystem (IKS)** ist für Cloud-Anbieter und IT-Dienstleister unerlässlich, um Sicherheitsanforderungen zu erfüllen, Risiken effektiv zu managen und regulatorische Vorgaben einzuhalten.

Effizientes Risikomanagement und erhöhte Sicherheit

Als Cloud-Anbieter 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 sich nach den Standards **SOC 2** oder **BSI C5** zertifizieren lassen wollen, müssen umfassende Compliance-Anforderungen erfüllen. Beide Zertifizierungen setzen voraus, dass Unternehmen wirksame Sicherheitskontrollen implementiert haben, die regelmäßig überprüft und angepasst werden. Das IKS stellt sicher, dass diese Anforderungen in den täglichen Betriebsprozessen verankert sind. Ob es um die Einhaltung der Datenschutz-Grundverordnung (DSGVO) oder um branchenspezifische Vorgaben geht – ein IKS dokumentiert alle sicherheitsrelevanten Prozesse und bietet bei Audits und Zertifizierungen die notwendige Transparenz und Nachvollziehbarkeit.

Effiziente Steuerung von Prozessen für Cloud-Dienste

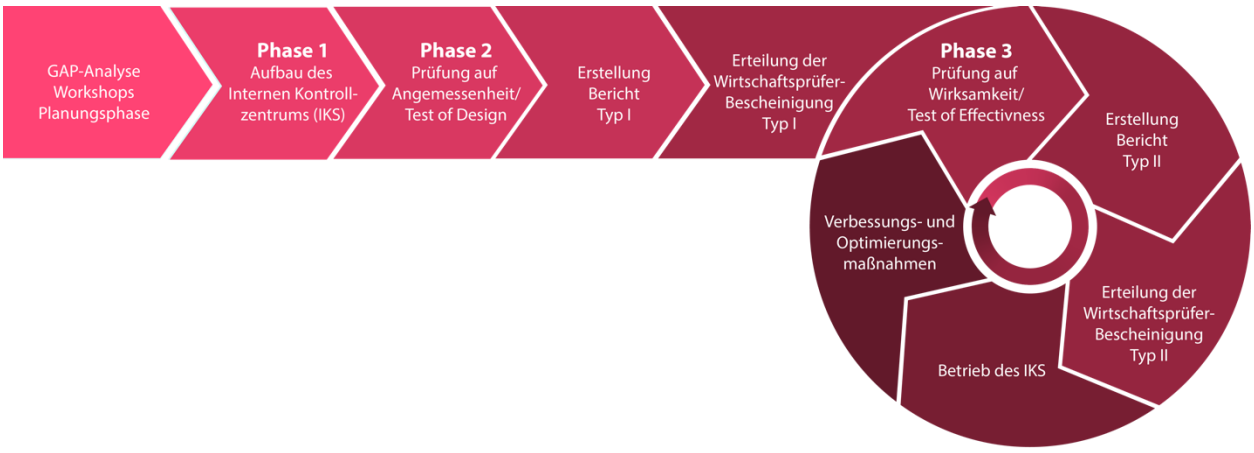
Neben der Einhaltung von Compliance-Vorgaben unterstützt ein IKS die effektive Kontrolle und Steuerung der internen Betriebsprozesse. Es überwacht die Verfügbarkeit von Cloud-Diensten und stellt sicher, dass diese jederzeit funktionsfähig sind. Bei Störungen oder sicherheitsrelevanten Vorfällen ermöglicht 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.

BSI C5 + SOC 2
Prüfung und Testierung

Der iAP-Step-by-step-Ansatz



GAP-Analyse, Workshops & Planung

Zu Beginn stellen wir den Zustand Ihres internen Kontrollsystems fest. In einem gemeinsamen Workshop vergleichen wir den aktuellen Sicherheitsstand Ihres Unternehmens mit den Anforderungen des BSI C5 und identifizieren die Lücken in den vorhandenen Kontrollen.
Für SOC2 ermitteln wir die Anwendbarkeit der Trust Service Criterias, legen den Geltungsbereich fest und entscheiden, welche Kriterien für Ihre Dienstleistungsprodukte relevant sind. Basierend auf den Ergebnissen und dem definierten Implementierungsumfang wird ein detaillierter Plan erstellt, der die verschiedenen Meilensteine identifiziert und Vereinbarungen mit dem Management trifft.

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

Risikobewertung, Prozesse & Kontrollen

Wir führen mit Ihnen Interviews, um Risiken zu identifizieren, die Auswirkungen auf Ihre bestehende Arbeitsweise haben, und erfassen die relevanten Informationen innerhalb Ihrer Organisation. Die Kontrollmaßnahmen werden basierend auf den Interviews gemäß den Anforderungen von BSI C5 und SOC 2 beschrieben und in einer Risikokontrollmatrix erfasst. Durch das Mapping der Kontrollen von BSI C5 und SOC 2 stellen wir sicher, dass gemeinsame und spezifische Anforderungen effizient

integriert werden. Wir beraten proaktiv bei der Implementierung fehlender Kontrollen, einschließlich Prozessbeschreibungen, und sichern die Abdeckung der Anforderungen Ihrer Kunden zu.

Systembeschreibung

Als zentraler Bestandteil des Berichts wird die Systembeschreibung erstellt und der allgemeine Abschnitt des Berichts vorbereitet. Die Systembeschreibung umfasst die Beschreibung der Prozesse, der Organisation und der Dienstleistungsprodukte.

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 BSI C5-Anforderungen und die Anforderungen der Trust Service Criteria (TSC) erfüllen. Wir analysieren die Richtlinien, Verfahren und Sicherheitsmechanismen Ihrer Organisation, die zur Erfüllung der TSC implementiert wurden. Dies umfasst Sicherheitsmaßnahmen, Zugriffskontrollen, Datenverschlüsselung und andere relevante Schutzmaßnahmen. Diese Phase führt zur Berichterstellung.

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 **BSI C5 Bericht zur Wirksamkeit der Kontrollen** sowie der **SOC 2 Typ I-Bericht** erstellt, der die Implementierung der Kontrollen dokumentiert. Der BSI C5-Bericht bewertet, wie gut die implementierten Sicherheitsmaßnahmen die BSI C5-Anforderungen erfüllen. Der SOC 2 Typ I-Bericht umfasst Standard- und gegebenenfalls zusätzliche Abschnitte, darunter die Management-Erklärung, korrespondierende Kontrollen, Kontrollen der Sub-Dienstleister und bei Bedarf zusätzliche Managementkontrollen. Den Entwurf der Berichte besprechen wir detailliert mit Ihnen. Als Ergebnis erhalten Sie die Bescheinigung des Wirtschaftsprüfers über die Angemessenheit der BSI C5-Kontrollen und die Implementierung der SOC 2-Kontrollen.

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 BSI C5 sowie SOC 2-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 sowie Funktionsfähigkeit der Kontrollen sowohl für BSI C5 als auch für SOC 2 bescheinigt. Der Entwurf des Berichts wird detailliert mit Ihnen besprochen, um sicherzustellen, dass alle relevanten Aspekte berücksichtigt sind. Als Ergebnis erhalten Sie die Bescheinigung des Wirtschaftsprüfers zur Wirksamkeit der Kontrollen gemäß BSI C5 und SOC 2 Typ II.

Die Konformität

Der BSI C5 Prüfbericht und der SOC 2 Typ II Bericht sind jeweils 12 Monate gültig.
Um die Konformität aufrechtzuerhalten, muss sich ein Unternehmen regelmäßigen Prüfungen durch eine zugelassene Wirtschaftsprüfungsgesellschaft unterziehen. Dies gilt sowohl für den BSI C5 Prüfbericht als auch für den SOC 2 Typ II Bericht. Diese Audits werden in der Regel jährlich durchgeführt.

Der Bericht

BSI C5- und SOC 2-Audits zur Qualitätssicherung

Ein Prüfbericht bietet eine umfassende Bewertung der Kontrollen und Sicherheitspraktiken einer Organisation anhand des BSI C5-Katalogs und der Trust Service Criteria (TSC). Er beginnt mit der Erklärung der Unternehmensleitung, in der bestätigt wird, dass die Sicherheitskontrollen ordnungsgemäß implementiert und wirksam sind. Der Bericht enthält zudem eine Bewertung des unabhängigen Wirtschaftsprüfers, der den Umfang der Prüfung, die Systeme und Kontrollen sowie sein abschließendes Urteil darlegt. Weiterhin beschreibt der Bericht detailliert die geprüften Systeme und die spezifischen Kontrollen, die zur Erfüllung C5-Anforderungen sowie der Trust Service Criteria implementiert wurden. Zusätzlich werden Informationen bereitgestellt, die über die Prüfungsziele hinausgehen, jedoch für Kunden und Partner von Interesse sein könnten.

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 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 Bericht als Marketinginstrument

Ihr Schlüssel zu höherem Vertrauen und Wettbewerbsvorteilen

BSI C5 und SOC 2-Berichte sind ein wirkungsvolles Marketinginstrument, da sie Organisationen als vertrauenswürdige Partner positionieren. Durch die detaillierte Dokumentation spezifischer Sicherheits- und Datenschutzkontrollen gemäß den Trust Service Criteria vermittelt der Prüfbericht ein klares Bild der Sicherheitsmaßnahmen eines Unternehmens. Dies ermöglicht es dem Unternehmen, sich deutlich von Wettbewerbern abzugrenzen und gezielt auf die spezifischen Anforderungen seiner Kunden einzugehen. Da die Berichte in vielen Branchen als wichtige Norm anerkannt sind, können Organisationen, die keinen solchen Bericht vorlegen, bedeutende Geschäftsmöglichkeiten verpassen und ihre Marktchancen schmälern.

RISIKO-EXCELLENZ

Erzielt einen positiven Effekt auf die Qualität des Risikomanagements und das interne Kontrollrahmenwerk.

PROFESSIONALITÄT

Unterstützt die Organisation bei der Professionalisierung interner Prozesse und Verfahren.

MÖGLICHKEITEN

Schafft Möglichkeiten, neue Kunden zu gewinnen und bestehende Kunden zu binden, indem Sicherheit und Transparenz geboten werden.

ANERKANNT

BSI C5 und SOC 2 sind weithin anerkannt, da sie eine gründliche Prüfung der Kontrollaktivitäten einer Dienstleistungsorganisation darstellen.

VERTRAUEN SCHAFFEN

Erfüllt das Kriterium der Bestätigung durch einen unabhängigen Dritten.

SPART ZEIT

Spart Zeit, indem Partnern und Kunden Fragen effizient beantwortet werden und verringert die Notwendigkeit, IT-Fragebögen zu beantworten.

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!"

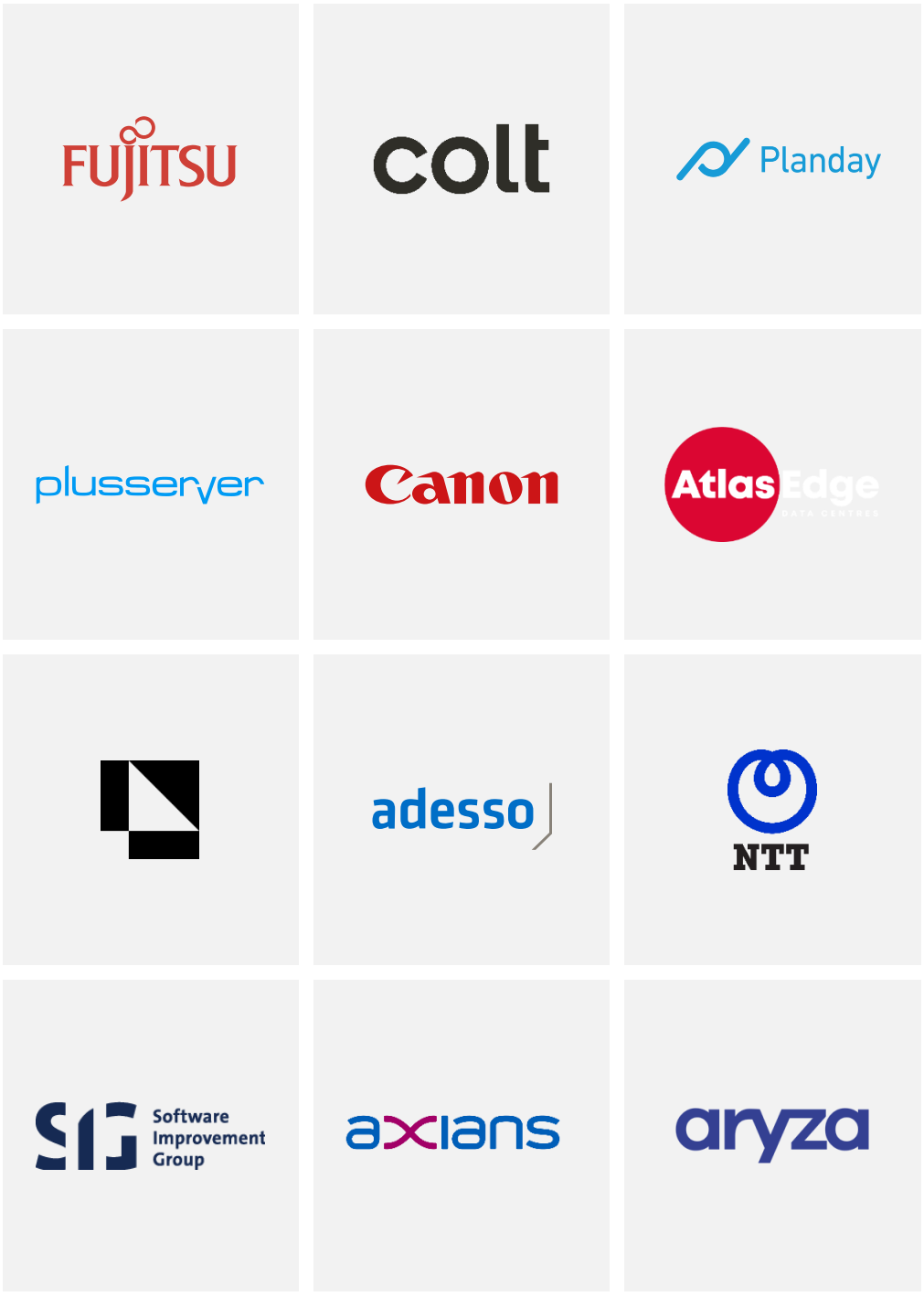
Investieren Sie in Effizienz, Wertschöpfung und Partnerschaft

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

Die Implementierung von SOC 2 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