SECURANCE
BE SURE

INDEPENDENT
CONSULTING
+ AUDIT
PROFESSIONALS

Step-by-step Guide

SOC 2 Compliance.

SOC 2 Compliance

Outsourcing von IT-Dienstleistungen | Trust Service Criteria

SOC 2 (System and Organization Controls 2) ist ein Prüfungsstandard, der vom American Institute of Certified Public Accountants (AICPA) initiiert wurde, um sicherzustellen, dass Dienstleistungsanbieter robuste und effektive Kontrollen zum Schutz der Kundendaten implementieren.
Dieser Standard ist besonders entscheidend für Unternehmen, die IT-Dienstleistungen an externe Anbieter auslagern, da er spezifisch auf die Sicherheits- und Compliance-Kontrollen fokussiert ist, die über die Anforderungen der Finanzberichtserstattung hinausgehen. Er konzentriert sich auf die Kontrollen einer Organisation, die für die Finanzberichtserstattung nicht relevant sind.

Eine Prüfung nach SOC 2 ist weithin anerkannt, da sie eine eingehende Prüfung der Kontrolltätigkeiten einer Dienstleistungsorganisation darstellt, die Kontrollen der internen Kontrolle, der Sicherheit, des Risikomanagements und der damit verbundenen Prozesse umfasst. SOC 2 prüft anhand der sogenannten Trust Service Criteria (TSC) fünf wesentliche Bereiche: Sicherheit, Verfügbarkeit, Vertraulichkeit, Integrität der Verarbeitung und Datenschutz. Diese Kriterien bieten eine strukturierte Methode zur Bewertung und Minderung der Risiken, die mit dem Outsourcing von IT-Dienstleistungen verbunden sind.

Modularität

Ein wichtiges Merkmal von SOC 2 ist seine Modularität. Die Unternehmen können je nach ihren spezifischen Geschäftsanforderungen und den Bedürfnissen ihrer Kunden flexibel entscheiden, welche der TSC-Kriterien in die Prüfung einbezogen werden sollen. Diese Flexibilität ermöglicht eine maßgeschneiderte Prüfung, die den spezifischen Compliance-Anforderungen des Unternehmens entspricht.

Das interne Kontrollsystem

Ein Internes Kontrollsystem (IKS) ist ein strukturiertes Set an Richtlinien und Verfahren, das Unternehmensprozesse schützt, Risiken mindert und gesetzliche Anforderungen erfüllt. Es schafft einen klaren und transparenten Rahmen für die Verwaltung, Dokumentation und kontinuierliche Überwachung der SOC 2-Kontrollen, was die Vorbereitung und Durchführung des SOC 2-Audits erleichtert und das Risikomanagement optimiert. Ein IKS stellt sicher, dass Verantwortlichkeiten klar definiert sind und Compliance-Vorgaben eingehalten werden.
Das IKS wird kontinuierlich an Veränderungen in der Unternehmensstruktur, den Geschäftsprozessen und den regulatorischen Anforderungen angepasst. Es enthält Mechanismen zur kontinuierlichen Verbesserung, um Schwächen frühzeitig zu identifizieren und das System anzupassen. Regelmäßige Prüfungen gewährleisten, dass das System effektiv und wirksam bleibt.

Trust Services Criteria

Erläuterung der Kriterien

SOC 2-Berichte konzentrieren sich auf fünf Hauptkriterien, den "Trust Service Criterias" (TSC). Diese Kriterien werden vom AICPA (American Institute of Certified Public Accountants) festgelegt und sind entscheidend für die Bewertung der internen Kontrollen eines Serviceanbieters in Bezug auf Datenschutz, Sicherheit und Verfügbarkeit. Wenn eine Organisation beschließt, zusätzliche Kriterien zu berücksichtigen, müssen die damit verbundenen Anforderungen und Points of Focus berücksichtigt und gegebenenfalls implementiert werden. Die wichtigsten Merkmale jedes Kriteriums sind nachfolgend aufgeführt.

SICHERHEIT

Sicherheit bezieht sich auf den Schutz von Daten während ihres gesamten Lebenszyklus. Sicherheitskontrollen werden implementiert, um unbefugten Zugriff oder Schäden an Systemen zu verhindern, die andere Kriterien beeinträchtigen könnten.

VERFÜGBARKEIT

Verfügbarkeit bezieht sich auf Kontrollen, die nachweisen, dass Systeme betriebsbereit bleiben und so funktionieren, dass die festgelegten Geschäftsziele und Service-Level-Agreements erfüllt werden.

VERTRAULICHKEIT

Vertraulichkeit erfordert von Unternehmen den Nachweis ihrer Fähigkeit, vertrauliche Informationen während ihres gesamten Lebenszyklus zu schützen, einschließlich der Erfassung, Verarbeitung und Entsorgung.

VERARBEITUNGSINTEGRITÄT

Integrität der Nutzung muss sicherstellen, dass Daten auf vorhersehbare Weise verarbeitet werden, ohne unerklärliche oder zufällige Fehler.

DATENSCHUTZ

Datenschutz ist ähnlich wie Vertraulichkeit, hat jedoch eine besondere Anwendung auf personenbezogene Daten (PII), insbesondere auf Informationen, die Ihre Organisation von ihren Kunden erhält.

Die Anwendbarkeit der Trust Service Kriterien

So definieren Sie den Geltungsbereich eines SOC 2-Berichts

Der Geltungsbereich eines SOC 2-Berichts bezieht sich auf die Kontrollen innerhalb einer Dienstleistungsorganisation, die in den Trust Services Kriterien für Sicherheit, Verfügbarkeit, Verarbeitungsintegrität, Vertraulichkeit und/oder Datenschutz definiert sind. Der SOC 2-Bericht sollte einen Abschnitt über den Geltungsbereich enthalten, der die Hauptkomponenten beschreibt. Dazu gehören Angaben über die Art der erbrachten Dienstleistung sowie über die relevante Infrastruktur, Software, Mitarbeiter, Richtlinien und Verfahren.

Beispiel für die Definition des Geltungsbereichs für einen Cloud-Anbieter

"Der Geltungsbereich dieses SOC 2-Berichts umfasst die Cloud-Dienstleistungen des Anbieters CloudGuard Data Center, die als Infrastructure as a Service (IaaS) bereitgestellt werden. Die Prüfung deckt die Rechenzentren in Hamburg und Berlin ab, in denen die physischen Server, Netzwerkinfrastrukturen und Speichersysteme untergebracht sind. Die Trust Service Criteria „Sicherheit" und „Verfügbarkeit" wurden aufgrund der Anforderungen unserer Kunden ausgewählt. Der Zeitraum der Prüfung erstreckt sich vom 1. Januar 20XX bis zum 31. Dezember 20XX."

Der Geltungsbereich eines SOC 2-Berichts wird von der Geschäftsleitung festgelegt. Er soll klar und präzise definiert sein, um sicherzustellen, dass alle relevanten Aspekte der Cloud-Dienste in der SOC 2 Prüfung berücksichtigt werden.

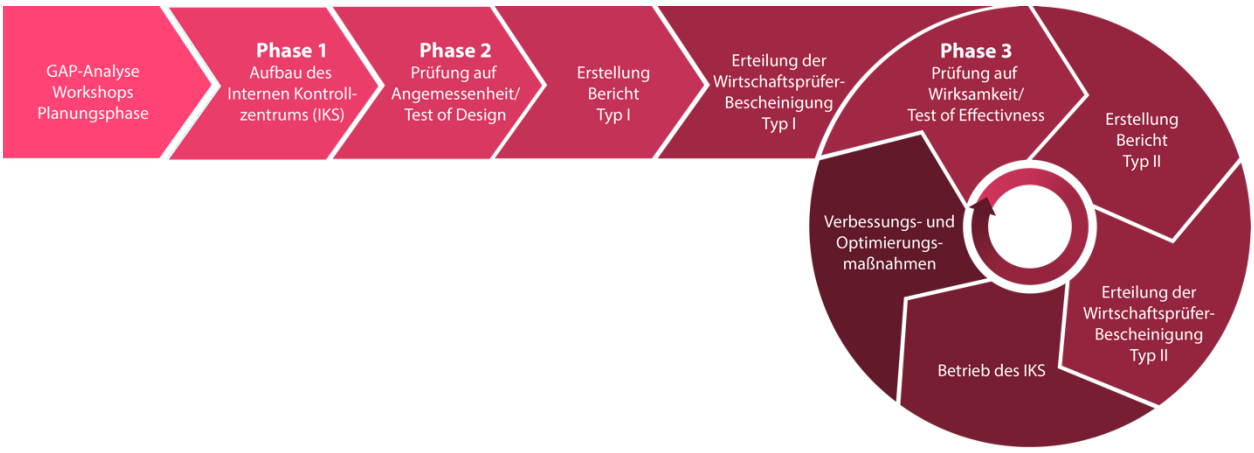
5 gute Gründe für SOC 2

Wesentliche Vorteile der SOC 2-Zertifizierung für Ihr Unternehmen

- **Robustes Sicherheitskonzept:** SOC 2 hilft Ihnen, Ihre Systeme gegen moderne Bedrohungen abzusichern, indem es eine umfassende Bewertung der Sicherheitsrichtlinien und -verfahren bietet.
- **Reputation und Vertrauenswürdigkeit:** Die SOC 2-Zertifizierung zeigt das Engagement Ihrer Organisation für hohe Sicherheits- und Datenschutzstandards und stärkt das Vertrauen von Kunden und Geschäftspartnern.
- **Risikomanagement:** SOC 2 umfasst eine Risikobewertung und unterstützt Sie dabei, ihre Risikomanagementpraktiken zu verbessern und proaktive Sicherheitsmaßnahmen zu implementieren.
- **Kostenreduzierung:** SOC 2-Audits helfen, Kosten durch Datenschutzverletzungen zu vermeiden, indem sie Schwachstellen aufdecken und Maßnahmen zur Vermeidung von Vorfällen empfehlen und schützt somit Ihren Unternehmensruf.
- **Komplementäre Compliance:** SOC 2 bietet eine solide Grundlage für die Einhaltung weiterer Compliance-Standards wie HIPAA oder ISO 27001 und erleichtert die Integration zusätzlicher Vorschriften.

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 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 SOC 2-Anforderungen beschrieben und in einer Kontrollmatrix erfasst. Wir beraten proaktiv bei der Implementierung fehlender Kontrollen, einschließlich Prozessbeschreibungen, und sichern die Abdeckung der Anforderungen Ihrer Kunden zu.

Systembeschreibung

Als zentraler Bestandteil des SOC 2-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 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 zum endgültigen SOC 2 Typ I-Bericht.

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 2 Typ I-Bericht, bestehend aus den Standard- und gegebenenfalls zusätzlichen Abschnitten, erstellt. Unter anderem finden sich hier die Management-Erklärung, korrespondierende Kontrollen, Kontrollen der Sub-Dienstleister und bei Bedarf auch zusätzliche Managementkontrollen. Den Entwurf des Berichts besprechen wir mit Ihnen im Detail.
Als Ergebnis erhalten Sie die Bescheinigung des Wirtschaftsprüfers auf Angemessenheit des SOC 2-Kontrollsets.

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 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 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 auf Wirksamkeit des SOC 2-Kontrollsets.

Die SOC 2 -Konformität

Die SOC-2-Konformität ist für einen Zeitraum von einem Jahr ab dem Ausstellungsdatum gültig. Um die SOC 2-Konformität aufrechtzuerhalten, muss sich ein Unternehmen regelmäßigen Prüfungen durch eine zugelassene Wirtschaftsprüfungsgesellschaft unterziehen, um sicherzustellen, dass seine Kontrollen und Prozesse weiterhin die Trust Services Criteria (TSCs) für Sicherheit, Verfügbarkeit, Verarbeitungsintegrität, Vertraulichkeit und Datenschutz erfüllen. Diese Audits werden in der Regel jährlich durchgeführt

Der Bericht

SOC 2-Audits zur Qualitätssicherung

Ein SOC 2-Bericht bietet eine umfassende Bewertung der Kontrollen und Sicherheitspraktiken einer Organisation anhand 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 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 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 2-Bericht als Marketinginstrument

Ihr Schlüssel zu höherem Vertrauen und Wettbewerbsvorteilen

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 SOC 2-Bericht 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 SOC 2-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

SOC 2 ist weithin anerkannt, da es eine gründliche Prüfung der Kontrollaktivitäten einer Dienstleistungsorganisation darstellt.

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