info@isae3402.de
www.isae3402.de

ISAE 3402 IMPLEMENTIERUNG

WHITEPAPER ZUR OUTSOURCING PRÜFUNG

WHITEPAPER

INHALT

ISAE 3402 5

VORTEILE 6

UMSETZUNG 10

RISIKO EXCELLENZ 11

PROJEKTPLANUNG 12

WEITERE INFORMATIONEN 14

WETTBEWERBS-VORTEIL

ISAE 3402 verschafft einen Wettbewerbsvorteil, indem es Dienstleistungsorganisationen von der Konkurrenz abhebt. Die Vorteile reichen von der Stärkung des Risikomanagements bis zur Schaffung von Vertrauen durch Transparenz in den Kontrollrahmen. ISAE 3402 erhöht die Effizienz von Audits und reduziert Auswirkungen auf Geschäftsabläufe.

Organisationen suchen kontinuierlich nach Möglichkeiten, Wettbewerbsvorteile zu nutzen, um Märkte zu erweitern und Gewinne zu steigern. Immer häufiger werden nicht-essenzielle Geschäftsbereiche ausgelagert. Dennoch bleibt das Management verantwortlich für das Risikomanagement und die Implementierung eines effektiven Kontrollrahmens. Dies hat zu einer steigenden Nachfrage nach Prüfungen von Kontrollmechanismen für Tätigkeiten geführt, die von Dritten ausgeführt werden.

Geschichte

Im 20. Jahrhundert war das Modell des großen, integrierten Unternehmens, das Vermögenswerte besitzt, verwaltet und kontrolliert, weit verbreitet. Diversifikation diente der Erweiterung der Unternehmensbasis und der Nutzung von Skaleneffekten. Später entwickelten viele Unternehmen eine Strategie, sich auf ihr Kerngeschäft zu konzentrieren, um Flexibilität und Innovationskraft zu steigern. Dies machte es notwendig, kritische Prozesse zu identifizieren und zu entscheiden, welche ausgelagert werden könnten.

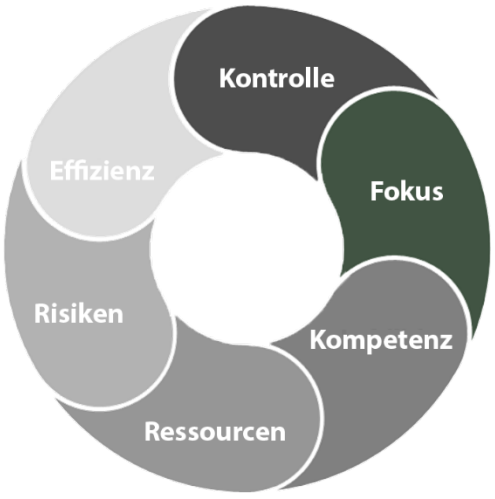
Outsourcing

Globalisierung, steigender Wettbewerb und Kostendruck führen dazu, dass Unternehmen zunehmend wichtige Geschäftsbereiche an Dienstleister auslagern. Die Auslagerung von Kernprozessen wirkt sich direkt auf die Finanzberichte und Schlüsselprozesse eines Unternehmens aus. Outsourcing beschränkt sich längst nicht mehr auf einfache Back-Office-Aufgaben. Wie kann man Vertrauen in ausgelagerte Geschäftsprozesse gewinnen? Wie können Unternehmen Kontrolle und Sicherheit über ausgelagerte Prozesse erlangen?

Mit der Zunahme des Outsourcings von geschäftskritischen Informationen steigen auch die Risiken und Sicherheitsbedenken. Sicherheitsmängel bei externen Dienstleistern können zu operativen, finanziellen oder reputationsbezogenen Schäden führen. Eine unabhängige Prüfung kritischer Geschäftsprozesse oder unterstützender IT-Systeme hilft, Risiken zu identifizieren, zu kontrollieren und Sicherheit über ausgelagerte Prozesse wiederherzustellen.

Die wichtigsten Gründe für ein Outsourcing:

- Kontrolle und Senkung der Betriebskosten
- Verbesserung des Unternehmensfokus auf die Kernprozesse
- Zugang zu erstklassigen Kompetenzen
- Freisetzung interner Ressourcen für andere Zwecke
- Steigerung der Effizienz in spezifischen Funktionen
- Ausgleich unzureichender interner Ressourcen
- Teilen von Risiken mit anderen Organisationen



Die heutige Entwicklung des Outsourcings ist geprägt von strategischen Partnerschaften. Früher war es undenkbar, Kernkompetenzen auszulagern, doch mit ISAE 3402/SOC 1 und ISAE 3000/SOC 2 hat sich dies zur gängigen Praxis entwickelt.

ISAE 3402

Der ISAE 3402-Standard, herausgegeben vom International Auditing and Assurance Standards Board (IAASB), ist ein international anerkannter Prüfungs-standard. Die Prüfung durch den Auditor einer Dienstleistungsorganisation genießt hohe Akzeptanz, da sie eine gründliche Bewertung der Kontrollziele und -maßnahmen umfasst. Das Kontrollrahmenwerk und die zugehörigen Kontrollen werden detailliert im Systems and Organization Report (SOC) beschrieben. Ein ISAE 3402/SOC-Bericht deckt Kontrollen über Informationstechnologie und operative Prozesse ab, die die Finanzlage eines Unternehmens beeinflussen.

SOC 1 ODER SOC 2

SOC-Berichte unterteilen sich in SOC 1- und SOC 2-Berichte. Ein ISAE 3402/SOC 1-Bericht fokussiert sich auf die Finanzberichterstattung und alle relevanten Prozesse. Ein ISAE 3000 (SOC 2)-Bericht adressiert eine breitere Palette an Nutzeranforderungen, wie Datenschutz, Vertraulichkeit und Systemverfügbarkeit. SOC 2-Berichte basieren modular auf den Trust Services Principles und Kriterien.

ABSTIMMUNG EXTERNER ANFORDERUNGEN AUF INTERNES RISIKO-MANAGEMENT

Im Kontext des Outsourcings stellen sich viele Fragen: Werden Dienstleistungen kontrolliert ausgeführt? Wie wird die Sicherheit gewährleistet, und wer hat Zugriff auf Informationen? Sind Maßnahmen gegen Betrug implementiert?
ISAE 3402 bietet hierfür eine umfassende Lösung. Der Standard unterstützt Organisationen bei der Bewertung von Risiken und der Abstimmung des Kontrollrahmenwerks auf strategische Ziele. Eine einmalige Investition in dieses Rahmenwerk stärkt das Marktvertrauen und fördert die organisatorische Exzellenz.

Ein ISAE 3402 Type I-Bericht enthält die Beurteilung eines externen Auditors über die zu einem bestimmten Zeitpunkt bestehenden Kontrollen. Der Auditor prüft, ob die Kontrollen so konzipiert sind, dass sie eine angemessene Sicherheit bieten, die finanziellen Berichtsziele zu erreichen, und ob diese Kontrollen tatsächlich vorhanden sind. Ein ISAE 3402 Type II-Bericht bewertet darüber hinaus die operative Wirksamkeit dieser Kontrollen über einen festgelegten Zeitraum. ISAE 3402-Berichte decken in der Regel die Angemessenheit und Wirksamkeit der Kontrollen über einen Zeitraum von 12 Monaten ab. Ein Bericht kann jedoch auch einen Mindestzeitraum von sechs Monaten umfassen.

VORTEILE

VERBESSERUNG DER RISIKOKONTROLLE UND TRANSPARENZ

Sowohl Nutzer als auch Dienstleistungs-organisationen profitieren von SOC 1- oder SOC 2-Berichten.

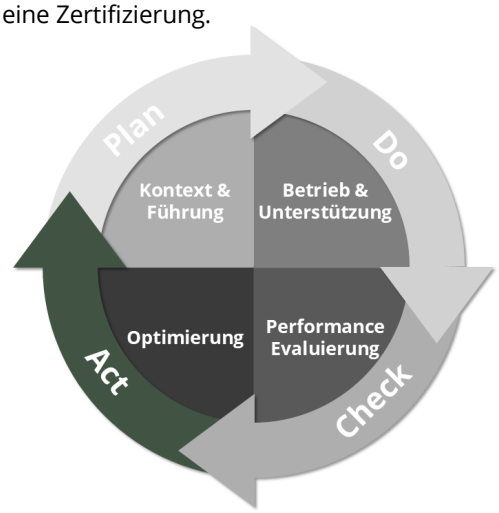
Organisationen werden von (potenziellen) Kunden häufig zu Sicherheitsstandards befragt: Worin unterscheiden sich ISAE 3402/SOC 1-, ISAE 3000/SOC 2- und ISO 27001-Prüfungen? Welcher Standard ist geeigneter – ISAE oder ISO 27001? Was sind die Vor- und Nachteile? Tatsächlich unterscheiden sich ISAE 3402 und ISO 27001 erheblich in Art und Anwendung. Die Hauptunterschiede liegen in der Berichterstattung und der Durchführung der Prüfungen.

ISAE und Sicherheit

ISAE 3402 ist eine Bescheinigung eines unabhängigen Wirtschaftsprüfers oder einer WP-Gesellschaft, die System- und Organisationskontrollen (SOC) anhand der Prüfziele bewertet. Ein ISAE 3402 (SOC 1)-Bericht umfasst IT-Kontrollen, fokussiert sich aber auf finanzielle Prozesse. Ein ISAE 3000 (SOC 2)-Bericht orientiert sich an den Trust Service Criteria für Sicherheit, Verfügbarkeit und Datenschutz und ähnelt ISO 27001. Der wesentliche Unterschied: ISAE 3402 und ISAE 3000 (SOC 2) sind Berichte, ISO 27001 ist eine Zertifizierung.

ISO 27001

ISO 27001 ist ein risikobasierter Standard zur Etablierung, Implementierung und Verbesserung eines Informationssicherheits-Managementsystems (ISMS) in einer Organisation. Der Standard wird von der ISO und der IEC verwaltet und durch unabhängige Zertifizierungsstellen geprüft. Organisationen müssen die in Anhang A beschriebenen Verfahren und Kontrollen umsetzen, um Risiken zu minimieren. ISO 27001 bietet ein umfassendes System zur Gewährleistung der Informationssicherheit, und alle Organisationen sollten mindestens ein System zur Verwaltung der Informationssicherheit haben.



ISO 27001 oder ISAE 3402?

Die Anforderungen an Informationssicherheit haben sich gewandelt. ISO 27001 bleibt der Standard für Informationssicherheit, aber mit der wachsenden Bedrohungslage benötigen viele Organisationen eine höhere Sicherheitsebene. Während ISO 27001 starre Kontrollen bietet, basieren ISAE 3402 und ISAE 3000 auf flexiblen Prinzipien, die dennoch wirksame Kontrollen erfordern. Funktionieren diese nicht, wird der Auditor die Bescheinigung einschränken. Eine ISAE 3402/3000-Prüfung bewertet umfassend die Effektivität des Risikorahmens und deckt Mängel im Risikomanagement auf – ein Maß an Transparenz, das heute unverzichtbar ist.

ABSTIMMUNG VON TRANSPARENZ AUF SPEZIFISCHE KUNDEN-ANFORDERUNGEN

ISAE 3402/SOC 1 ist darauf ausgerichtet, Kunden von Dienstleistungsorganisationen bei einer Finanzprüfung zu unterstützen. ISAE 3000/SOC hingegen adressiert ein breiteres Spektrum an Nutzer-bedürfnissen. Unterschiedliche Branchen erfordern jeweils einen spezifischen Umfang und eine angepasste SOC-Berichterstattung. Im Folgenden finden Sie eine Übersicht der gängigen Berichtsarten pro Branche, einschließlich der relevanten Anwendungsbereiche.

MANAGED SERVICES

Managed Service Provider managen die Infrastruktur, Server und Anwendungen für unterschiedliche Kunden. ISAE 3402-Berichte werden mit einem ITGC-Umfang genutzt.

RECHENZENTREN

Betriebs- und Finanzsysteme, die finanzielle Prozesse beeinflussen, sind hier untergebracht. ISAE 3402/SOC 1 (in Kombination mit ISAE 3000/SOC 2) konzentriert sich auf die physische Sicherheit.

FINANZ-DIENSTLEISTER

Bereitgestellt für SOx404 (ICOFR)-Zwecke oder Anforderungen von Aufsichtsbehörden. Betriebliche und finanzielle Prozesse sind im Umfang enthalten.

SOFTWARE AS A SERVICE

Anwendungen, die mit betrieblichen oder finanziellen Prozessen verbunden sind und (in)direkten Einfluss auf den Jahresabschluss haben. ITGCs fallen in den Umfang der ISAE 3402/ SOC 1-Berichte.

HR UND GEHALT

Personal- und Gehaltsprozesse, die den Jahresabschluss oder finanzielle Abläufe betreffen, sind im ISAE 3402/SOC 1-Bericht von HR-Dienstleistern enthalten.

ABWICKLUNG

Abwicklung, Versand oder Druck werden an spezialisierte Unternehmen ausgelagert. Logistische und finanzielle Prozesse sind im Umfang des ISAE 3402/SOC 1-Berichts enthalten.

SOC steht für „System and Organization Controls“ und wurde früher als „Service Organization Control Reports“ bezeichnet. Diese Berichte stammen aus den USA. ISAE 3402 ist an den US-Standard „Statement on Standards for Attestation Engagements“ (SSAE) 18 angelehnt. Ein ISAE 3402-Bericht liefert durch den Service-Auditor eine Bestätigung über die Systembeschreibung einer Dienstleistungsorganisation sowie die Eignung und Wirksamkeit der implementierten Kontrollen.

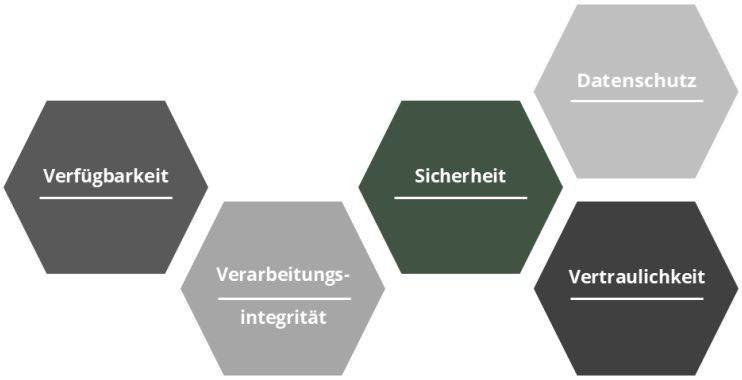
ISAE 3402 SOC 1

Ein ISAE 3402 SOC 1-Bericht ermöglicht es Organisationen, ihre eigenen Kontrollziele und -maßnahmen festzulegen und diese an die Anforderungen ihrer Kunden anzupassen. Der Bericht umfasst in der Regel alle operativen und finanziellen Kontrollen, die die Finanzberichterstattung beeinflussen, sowie IT General Controls wie Sicherheitsmanagement, physische und logische Sicherheit, Änderungsmanagement, Vorfallmanagement und Systemüberwachung. Wenn Ihre Organisation finanzielle Daten hostet, die die Berichterstattung Ihrer Kunden betreffen könnten, ist ein ISAE 3402 SOC 1-Auditbericht sinnvoll und wird häufig gefordert. Der Prüfungsumfang umfasst ITGCs (IT General Controls), operative und finanzielle Kontrollen. Bei SOC 1-Prüfungen sind Kontrollziele, die die interne Kontrolle über die Finanzberichterstattung (ICOFR) darstellen, erforderlich, wenn die Organisation SEC-Meldungen in den USA einreichen muss.

ISAE 3000 SOC 2

ISAE 3000 SOC 2-Berichte wenden die Trust Services Principles and Criteria (TSPs) an, die von der AICPA und dem Canadian Institute of Chartered Accountants (CICA) entwickelt wurden, um Sicherheit, Verfügbarkeit, Vertraulichkeit, Integrität der Verarbeitung und Datenschutz zu gewährleisten. Organisationen können die Prinzipien auswählen, die den Anforderungen ihrer Kunden entsprechen, und ein SOC 2-Bericht kann einen oder mehrere dieser Aspekte abdecken. Wenn Ihre Organisation Informationen hostet oder verarbeitet, die nicht die Finanberichterstattung Ihrer Kunden betreffen, ist ein ISAE 3000 SOC 2-Bericht geeigneter. Kunden sind dann vor allem an der sicheren und vertraglich vereinbarten Verfügbarkeit ihrer Daten interessiert. Ein SOC 2-Bericht bewertet, wie ein SOC 1-Bericht, interne Kontrollen, Richtlinien und Verfahren.

SOC 1 oder SOC 2?



Organisationen, die Systeme oder Informationen verarbeiten, hosten oder verwalten, die sich auf die Finanzberichterstattung auswirken, sollten stets einen ISAE 3402 SOC 1-Bericht vorlegen. ISAE SOC 2 ist dagegen für Systeme und Prozesse geeignet, die keine Verbindung zur Finanzberichterstattung haben. Rechenzentren sowie IaaS- und PaaS-Anbieter erstellen häufig hybride Berichte: ISAE 3402 SOC 1 für finanzrelevante Prozesse und ISAE 3000 SOC 2 für nicht finanzbezogene Systeme. Der Inhalt beider Berichte bleibt dabei identisch.

UMSETZUNG

INVESTIEREN SIE IN STRATEGIE UND RAHMENWERK

RISIKEN ANALYSIEREN, PROJEKT PLANEN, SYSTEMBESCHREIBUNG ERSTELLEN UND READINESS ASSESMENT DURCHFÜHREN

Die Umsetzung von ISAE 3402 erfordert eine effektive Planung, die Einbindung der Führungsebene, eine gründliche Analyse der Prozesse sowie zuverlässige Ressourcen und ein effizientes Projektmanagement.

Ein ISAE 3402-Projekt startet in der Regel mit einer Implementierungsphase, in der der SOC-Bericht vorbereitet wird. Der Erfolg des Projekts hängt entscheidend davon ab, wie effektiv die Kontrollziele und das Rahmenwerk der Dienstleistungs-organisation auf die Anforderungen und Erwartungen aller Stakeholder abgestimmt werden.

RISIKO-EXCELLENCE

DIENSTLEISTUNGSORGANISATIONEN // NUTZER

Ein ISAE 3402-Audit bietet Vorteile für Dienstleistungsorganisationen und Nutzer, indem es die Prüfungseffizienz steigert, das Risikomanagement auf ausgelagerte Prozesse abstimmt und die Einhaltung regulatorischer Vorgaben gewährleistet.

DIENSTLEISTUNGS-ORGANISATIONEN

Dienstleistungsorganisationen profitieren von deutlich verbessertem Risikomanagement, gestärkten Kontrollen, die optimal auf Risiken abgestimmt sind, und einer erhöhten Prüfungseffizienz. Das gestiegene Marktvertrauen resultiert aus größerer Transparenz und besseren Einblicken in die Risiken und deren Management. ISAE 3402 reduziert die Anzahl der Audits und minimiert

NUTZER

Unterbrechungen im Geschäftsbetrieb, während Sicherheits- und Risikobedenken verringert werden. Externe Bestätigungen durch professionelle Auditoren liefern wertvolle Einblicke, fördern das Verständnis und harmonisieren Ihre Prozesse mit denen Ihrer Lieferanten. So wird eine transparente und effektive Absicherung ausgelagerter Geschäftsbereiche gewährleistet.

ISAE 3402 VORTEILE

ABSTIMMUNG RISIKO-MANAGEMENT
STRUKTURIERTER ANSATZ

COMPLIANCE
INTEGRIERTES REGELWERK

PRÜFUNGSEFFIZIENZ
WENIGER AUDITS

MARKTVERTRAUEN
DURCH TRANSPARENZ

PROJEKTPLANUNG

TIMELINE

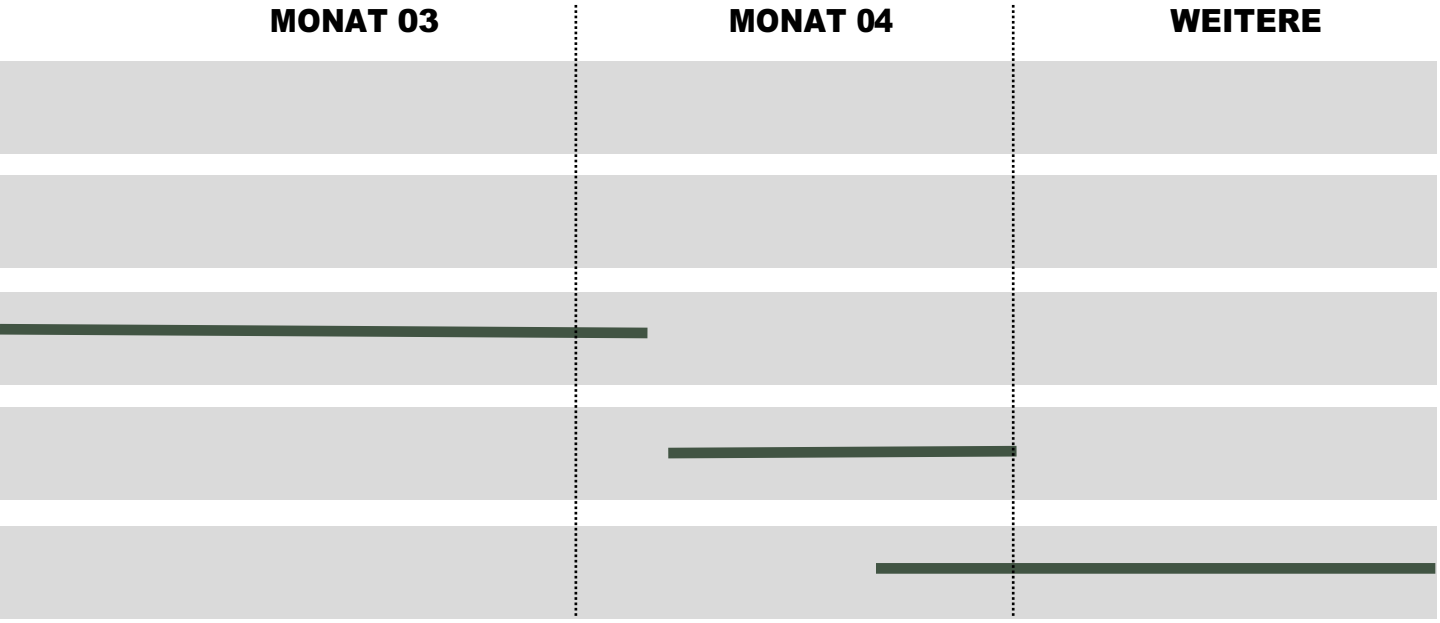
PLANUNG, RISIKO- & PROZESSANALYSE

Aktivitäten und Zeitplan festlegen, Managementerwartungen steuern. Eine vollständige und genaue Risiko-bewertung durchführen, die ver-schiedene Ebenen und Funktionen einbezieht.

UMFANG & ZIELE, FESTLE-GUNG DER BERICHTS-STRUKTUR

Umfang an die Anforderungen aller Stakeholder (Nutzerorganisation, Auditoren) anpassen. Kontrollziele basierend auf der Jahres-berichter-stattung der typischen Nutzerorga-nisation festlegen.

Die Implementierung eines ISAE 3402-Rahmenwerks dauert bei einer durchschnittlichen Organisation (<100 Mitarbeiter) typischerweise 2 bis 4 Monate, abhängig von der Komplexität der Prozesse, der Unternehmensgröße und den verfügbaren Ressourcen.



DETERMINE KEY CONTROLS & PREPARE REPORT

SCHLÜSSELKONTROLLEN FESTLEGEN & SOC-BERICHT ERSTELLEN

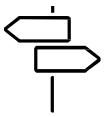
Schlüsselkontrollen basierend auf den definierten Kontrollzielen bestimmen und den SOC-Bericht erstellen, der das Kontrollrahmenwerk, eine Kontrollmatrix (Ziele und Kontrollen) und weitere Abschnitte enthält.

READINESS ASSESSMENT & BERATUNG

Kontrollen mittels Walkthroughs auf Wirksamkeit prüfen und Funktionen zur Verfahrensoptimierung bewerten. Bericht mit führenden Praktiken für SOC-Berichte abgleichen.

PRÜFUNGS- & OPTIMIERUNGS-MANAGEMENT

Das interne Projekt in Bezug auf Zeitplanung, Prozesse und Erwartungen mit externen Auditoren abstimmen. Das ISAE 3402-Projekt und die Prozesse umfassend bewerten und interne sowie externe Entwicklungen einbeziehen



WEITERE INFORMATION

IHRE NÄCHSTEN SCHRITTE

BESUCHEN SIE ISAE3402.DE

Kontaktieren Sie unsere ISAE 3402 SOC-Experten, um Ihre spezifischen Anforderungen und Wünsche für die Implementierung von ISAE 3402 in Ihrem Unternehmen zu besprechen. Senden Sie Ihre Anfrage gerne per E-Mail an **info@isae3402.de**.

HAFTUNGSAUSSCHLUSS

ISAE3402.DE

KONTAKT

E-MAIL:
info@isae3402.de