GRC-Fähigkeiten von Insight: Governance, Risikomanagement und Compliance neu definiert

Insight

Einleitung

Kurz gesagt geht es bei GRC darum, Vertrauen aufzubauen: Vertrauen bei Ihren Kunden, Vertrauen bei Aufsichtsbehörden und Vertrauen in Ihr eigenes Unternehmen, dass Sie verantwortungsbewusst und belastbar handeln.

Die GRC-Grundpfeiler:

1 Governance

Von der Unternehmensspitze den Ton angeben und dies in klare Richtlinien umsetzen. Das ist die Verpflichtung der Führungsebene, die Dinge richtig zu machen – von der Datenethik bis zur Unternehmensverantwortung. Eine starke Governance sorgt dafür, dass Ihre Teams bei der Entscheidungsfindung einen Kompass haben, der auf die Ziele und Werte Ihres Unternehmens ausgerichtet ist.

2 Risikomanagement

Identifizieren Sie potenzielle Risiken (von versehentlichem Datenverlust bis hin zu Ransomware-Angriffen) und mindern Sie diese proaktiv. Die Aufgabe besteht darin, zukünftige Ereignisse vorherzusagen und sich entsprechend darauf vorzubereiten. Unternehmen, die Risiken gut bewältigen können, erleben weniger Krisen. Treten dennoch Vorfälle auf, gehen sie schnell und effektiv damit um. Sie können sich darauf verlassen, dass Ihre strategischen Wetten sicher sind, weil Sie sich gegen Verluste abgesichert haben.

3 Compliance

Spielen Sie nach den Regeln – seien es Gesetze wie die DSGVO, Industriestandards wie ISO oder interne Verhaltenskodizes. Damit stellen wir nicht “nur die Aufsichtsbehörden zufrieden”, sondern signalisieren auch Ihren Kunden und Partnern, dass Ihnen Sicherheit und Datenschutz wichtig sind. Compliance schafft Vertrauen und öffnet Türen. Eine Zertifizierung (z. B. nach ISO 27001) kann für Unternehmen, die mit Top-Kunden zusammenarbeiten und Best Practices nachweisen wollen, ein Türöffner sein.

Der geschäftliche Nutzen von GRC

Die Vernachlässigung von Governance, Risikomanagement oder Compliance kann für ein Unternehmen schwerwiegende Folgen haben:

- **Finanzieller Schaden:** Datenschutzverletzungen, Betrug oder behördliche Sanktionen können zu direkten finanziellen Kosten in Form von Bußgeldern, Rechtskosten und Kosten für die Behebung von Verstößen führen. Darüber hinaus können sie zu entgangenen Einnahmen durch Unterbrechungen des Unternehmens führen. Studien zeigen, dass Unternehmen, die sich nicht an die Regeln halten, deutlich höhere Kosten haben als solche, die sich an die Regeln halten.
- **Betriebsunterbrechung:** Ungemanagte Risiken, wie beispielsweise Cyberangriffe oder Prozessausfälle, können den Betrieb zum Erliegen bringen und zu Ausfallzeiten führen. Diese beeinträchtigen wiederum die Produktivität und die Servicebereitstellung. Beispiele: Durch Ransomware-Angriffe könnten kritische Systeme für mehrere Tage gesperrt werden. Solche Risiken können mithilfe von GRC-Praktiken identifiziert und gesenkt werden, bevor sie eintreten. So wird die Kontinuität des Unternehmens gewahrt.
- **Reputationsschaden:** Vertrauen ist schwer zu gewinnen, aber leicht zu verlieren. Compliance-Verstöße oder ethische Mängel untergraben das Vertrauen von Kunden und Stakeholdern. Eine veröffentlichte Datenschutzverletzung oder ein Compliance-Skandal kann einer Marke nachhaltig schaden und Kunden vertreiben. Eine starke Governance und Compliance zeigen der Öffentlichkeit, den Partnern und den Aufsichtsbehörden, dass das Unternehmen verantwortungsbewusst und vertrauenswürdig ist.
- **Regulatorische Sanktionen:** Die Aufsichtsbehörden setzen zunehmend Gesetze mit hohen Geldbußen und sogar strafrechtlichen Sanktionen für den Fall der Nichteinhaltung durch. So können nach der EU-DSGVO bei schwerwiegenden Verstößen Bußgelder bis zu 20 Mio. € oder 4 % des weltweiten Jahresumsatzes verhängt werden.

Tatsächlich haben die europäischen Regulierungsbehörden seit 2018 DSGVO-Bußgelder in Höhe von insgesamt 5,88 Milliarden Euro verhängt, darunter eine Rekordbuße von 1,2 Milliarden Euro gegen ein einzelnes Unternehmen. GRC unterstützt Sie dabei, sicherzustellen, dass alle erforderlichen Kontrollen und Berichterstattungen vorhanden sind, um diese Strafen zu vermeiden.

Zusammenfassend lässt sich sagen, dass eine Investition in GRC deutlich günstiger und sicherer ist als die Bewältigung der Folgen von Compliance-Verstößen oder schwerwiegenden Vorfällen. Ein kohärentes GRC-Programm schützt die **finanzielle Gesundheit, die betriebliche Kontinuität sowie den öffentlichen Ruf** eines Unternehmens. Gleichzeitig ermöglicht es eine bessere Entscheidungsfindung und strategische Ausrichtung. Eine Studie fasst zusammen: *"Nichtkonformität kostet fast dreimal so viel wie Compliance"*.

Unternehmen geben im Durchschnitt jährlich 5,47 Mio. $ für Compliance aus, bei Nichteinhaltung sind es jedoch 14,82 Mio. $. Die Kosten für Nichteinhaltung sind somit etwa 2,7 Mal höher. Zu diesen Verlusten zählen Ausfallzeiten des Unternehmens, die Reaktion auf Vorfälle sowie Kundenabwanderung.

Wichtige Rahmenbedingungen und Vorschriften

In der GRC-Landschaft gibt es zahlreiche Standards, Rahmenbedingungen und Vorschriften, die Unternehmen beachten müssen. Nachfolgend finden Sie eine Übersicht über die wichtigsten Begriffe und ihre Anwendung in verschiedenen Organisationen:

Regelwerk / Regulation	Zweck	Anwendungsbereiche	Wichtigste GRC-Implikationen
ISO/IEC 27001	Etablieren Sie ein Information Security Management System (ISMS), um Ihre Informationen systematisch zu sichern.	Alle Branchen weltweit (Finanzen, Technologie, Fertigung usw.).	Die Baseline für Cybersicherheits-Governance überschneidet sich oft mit NIS2 und anderen Rahmenbedingungen. Eine starke Sicherheitsposition wird durch die Zertifizierung angezeigt.
Cyber Essentials Plus	Ein von der britischen Regierung unterstütztes Programm für grundlegende Cyberhygiene, das auf fünf Schlüsselkontrollen basiert.	Unternehmen mit Sitz im Vereinigten Königreich, darunter insbesondere KMU und Zulieferer für die Regierung.	Bietet die Gewähr für wesentlichen Schutz. Unabhängiges Audit für „Plus"-Level erforderlich. Oftmals ein Einstieg in strukturierte Sicherheit.
CAF (Cyber Assessment Framework)	CAF wurde vom britischen National Cyber Security Centre (NCSC) entwickelt und bietet einen strukturierten Ansatz zur Bewertung der Cyberresilienz von Unternehmen, die kritische Funktionen betreiben.	Dies betrifft Organisationen des Vereinigten Königreichs in kritischen nationalen Infrastruktursektoren (CNI) sowie Betreiber wesentlicher Dienstleistungen, insbesondere im Rahmen der britischen NIS-Vorschriften.	Stimmt technische Kontrollen mit den Governance-Ergebnissen ab. Hilft, Reife gegenüber den NIS-konformen Prinzipien nachzuweisen. Support für risikobasierte Entscheidungen und regulatorischen Dialog. Wird häufig zusammen mit ISO 27001 oder der internen Qualitätssicherung verwendet.
EU AI Act	Die EU hat Rechtsvorschriften erlassen, die die Regelung von KI-Systemen nach Risikokategorien vorsehen. Hochrisikokategorien sind beispielsweise Systeme zur Bonitätsbewertung.	Jede Organisation, die KI auf dem EU-Markt anbietet.	Hochrisiko-KI erfordert Dokumentation, Risikomanagement und kontinuierliche Überwachung. Eine starke KI-Governance trägt dazu bei, Compliance und Marktzugang zu gewährleisten.
NIS2-Richtlinie	Es gibt EU-weite Cybersicherheitsvorschriften für kritische und digitale Infrastrukturen.	Mittelgroße Unternehmen aus Schlüsselsektoren (Energie, Telekommunikation, Cloud, Fertigung, Gesundheitswesen usw.), darunter auch Nicht-EU-Anbieter, die den EU-Markt bedienen.	Erfordert risikobasierte Sicherheit, Vorfallberichterstattung, Lieferkettensicherheit. Die Sanktionen entsprechen den Bußgeldern auf DSGVO-Ebene. Wesentliche Überschneidungen mit ISO 27001.

Regelwerk / Regulation	Zweck	Anwendungsbereiche	Wichtigste GRC-Implikationen
DSGVO	EU-Verordnung zum Umgang mit personenbezogenen Daten – Einwilligung, Datenschutzrechte, Meldung von Verstößen usw.	Jede Organisation, die personenbezogene Daten von EU-Bürgern verarbeitet.	Datenschutz wird zum Vorstandsthema. Dies erfordert eine starke Governance, Datenbestände, einen Datenschutzbeauftragten und eine schnelle Meldung von Verstößen. Erhebliche Geldbußen bei Nichteinhaltung.
SOC 2	Es handelt sich um einen in den USA entwickelten Rahmen zur Bewertung interner Kontrollen für den Datenschutz, insbesondere in der Cloud/SaaS.	Technologie- und Service Provider, insbesondere im B2B- oder SaaS-Bereich.	Freiwillig, aber häufig vertraglich vorgeschrieben. Zeigt starke betriebliche Sicherheit und baut Vertrauen auf.
PCI-DSS	Globale Standardversion zum Schutz von Karteninhaberdaten und zur Reduzierung von Betrug.	Jede Einrichtung, die Kreditkartendaten speichert, verarbeitet oder übermittelt.	Pflicht für Händler und Zahlungsabwickler. Erfordert strenge Kontrollen und regelmäßige Audits durch zertifizierte Gutachter.
DORA (Digital Operational Resilience Act)	Die EU-Verordnung soll sicherstellen, dass Unternehmen des Finanzsektors IKT-bezogenen Störungen standhalten und sich davon erholen können.	Dies betrifft Finanzunternehmen, die in der EU tätig sind, darunter Banken, Versicherer, Wertpapierfirmen sowie kritische Drittanbieter.	Erfordert ein robustes ICT-Risikomanagement, Vorfallberichterstattung, Tests der digitalen operativen Resilienz und die Überwachung des Risikos Dritter. Ergänzt NIS2 und DSGVO.

Die Einhaltung mehrerer Vorschriften und Rahmenbedingungen ist erforderlich.

Unternehmen stehen heute vor der Herausforderung, mit einer Vielzahl von Compliance-Anforderungen umzugehen. Sie sind häufiger mit einem Flickenteppich aus sich überschneidenden Rechtsvorschriften, regulatorischen Verpflichtungen und Branchenrahmen konfrontiert. Die Compliance-Landschaft kann schnell komplex und mühsam werden. Sie besteht aus vielen verschiedenen Standards wie der DSGVO, NIS2, ISO 27001, DORA oder branchenspezifischen Standards wie PCI-DSS.

Viele Unternehmen erkennen jedoch nicht, wie stark sich diese unterschiedlichen Anforderungen überschneiden. Kernprinzipien wie Risikobewertung, Zugriffskontrolle, Reaktion auf Vorfälle und Governance ziehen sich wie ein roter Faden durch die meisten Vorschriften zur Cybersicherheit und zum Datenschutz. Ein intelligenter, integrierter Compliance-Ansatz kann Doppelarbeit daher erheblich reduzieren.

Führende Unternehmen verfolgen einen einheitlichen Ansatz, anstatt jede Vorschrift isoliert zu behandeln. Sie bilden Kontrollen und Prozesse über mehrere Normen hinweg ab und entwickeln ein Sicherheitskonzept, das diesen Normen insgesamt gerecht wird. Eine nach ISO 27001 zertifizierte Organisation ist beispielsweise bereits auf dem besten Weg, die Sicherheitsanforderungen der NIS2 zu erfüllen – wenn auch nur zu 80 %.

Durch den Aufbau eines zentralisierten, kontrollbasierten Compliance-Rahmens können Unternehmen Audits optimieren, Kosten senken und die Sicherheit gewährleisten. eine nachhaltige, geschäftsorientierte Praxis statt ständigen Feuerwehrübungen.

Tools zur automatischen Einhaltung von Vorschriften

Die Verfolgung von Anforderungen über verschiedene Rahmenbedingungen wie ISO 27001, NIS2, DSGVO, PCI-DSS und andere hinweg kann schnell überwältigend werden – insbesondere, wenn jede dieser Rahmenbedingungen ihre eigenen Kontrollen, Nachweisanforderungen und Auditanforderungen mit sich bringt.

In diesem Zusammenhang kommen die Automatisierungswerkzeuge „Compliance" und „GRC" (Governance, Risk and Compliance) zum Einsatz.

Mit Hilfe dieser Plattformen können Unternehmen Kontrollen über mehrere Rahmenbedingungen hinweg abbilden, verwalten und überwachen. Darüber hinaus lassen sich Überschneidungen identifizieren und Compliance-Bemühungen optimieren. Anstatt die Arbeit für jede Standardversion zu duplizieren, können Sie mithilfe von Automatisierungstools eine Kontrolle einmal implementieren - beispielsweise für die Zutrittskontrolle oder die Reaktion auf Vorfälle - und sie dann den relevanten Anforderungen über mehrere Vorschriften hinweg zuordnen.

Damit verbundene Vorteile:

- **Reduzierte Doppel- und Nacharbeit:** Kontrollen einmalig implementieren und rahmenübergreifend wiederverwenden.
- **Kontinuierliche Einhaltung der Vorschriften:** Die automatisierte Beweiserfassung, die Kontrollüberwachung sowie das Workflow-Management tragen dazu bei, dass Sie stets auditbereit sind.
- **Transparenz:** Mit Hilfe von Dashboards und Berichten erhalten Stakeholder in Echtzeit einen Überblick über den Compliance-Status und die Risikoexposition des gesamten Unternehmens.
- **Auditeffizienz:** Zentralisierte Dokumentationen und automatisierte Kontrollmappings machen interne und externe Audits schneller und weniger störend, was die Effizienz und Effektivität solcher Audits deutlich erhöht.
- **Skalierbarkeit:** Automatisierungstools können an sich ändernde Vorschriften oder neue Standardversionen angepasst werden. Dadurch müssen Sie Ihr Compliance-Programm nicht ständig neu erfinden.

Mit Compliance-Tools können Sie die jährliche Hektik bei der Rezertifizierung in einen robusten Prozess verwandeln, der das ganze Jahr über läuft, sodass Sie immer über Ihren Compliance-Status informiert sind und genügend Zeit haben, um etwaige Lücken zu schließen.

Zahlen, Daten, Fakten

Kosten der Nichteinhaltung im Vergleich zu den Kosten der Einhaltung der Vorschriften: Es ist gut dokumentiert, dass die Nichteinhaltung von Vorschriften weitaus teurer ist als die erforderlichen Investitionen zur Einhaltung der Vorschriften. Eine Benchmark-Studie ergab, dass die durchschnittlichen Kosten für Einhaltung von Vorschriften (Umsetzung von Richtlinien, Schulungen, Audits usw.) bei großen Unternehmen bei ~5,5 Millionen US-Dollar pro Jahr lagen. Während die durchschnittlichen Kosten für die Nichteinhaltung der Vorschriften (in Form von Geldbußen, Geschäftsunterbrechungen, Produktivitätsverlusten und Sanierungen) bei ~14,8 Millionen US-Dollar lagen – fast dreimal so hoch.
Reference: **corporatecomplianceinsights.com**

Trends bei Geldbußen: Aufsichtsbehörden setzen die Einhaltung der Vorschriften aktiv durch. So beliefen sich die DSGVO-Bußgelder im Bereich Datenschutz beispielsweise von 2018 bis 2024 europaweit auf insgesamt **5,88 Mrd. €**
Reference: **dlapiper.com**

Positiv anzumerken ist, dass Unternehmen mit strengen Compliance-Programmen häufig niedrigere Bußgelder aushandeln oder Verstöße ganz vermeiden können. Da Vorschriften wie das EU-KI-Gesetz und NIS2 in Kraft treten, erwarten wir, dass eine erste Welle hochkarätiger Durchsetzungsmaßnahmen – ähnlich wie in den Anfangsjahren der DSGVO – den Bedarf an ausgereiften GRC-Funktionen weiter verstärken wird.

Einführung von GRC- und Compliance-Programmen: Die meisten Unternehmen erkennen die Notwendigkeit von GRC. Laut einer globalen Umfrage von Accenture **haben 95 % der Unternehmen eine „Compliance-Kultur" etabliert oder sind dabei**, dies zu tun. Dies deutet darauf hin, dass auf den Führungsebenen ein nahezu universelles Bewusstsein dafür vorhanden ist, dass Compliance und Ethik Teil der Unternehmenskultur sein müssen. Der Reifegrad variiert jedoch: Lediglich **36 % der Unternehmen verfügen über ein formelles Enterprise Risk Management (ERM)-Programm**. Dies deutet darauf hin, dass die meisten Unternehmen zwar die Absicht haben, Konformität zu erreichen, aber immer noch an der Entwicklung der Infrastruktur und Prozesse für umfassende GRC arbeiten. Da die Branche neuen Risiken ausgesetzt ist - darunter Cyberbedrohungen, Unterbrechungen der Lieferkette und Pandemien -, fordern die Vorstände zunehmend eine bessere Risikoüberwachung. Tatsächlich **planen 36 % der Unternehmen, ihre Investitionen in die Bereiche Risikomanagement und Compliance in den nächsten zwei Jahren zu erhöhen**.

Reference: **procurementtactics.com**

Umfang der regulatorischen Änderungen: Eine der größten Herausforderungen im Bereich der Compliance ist es, mit neuen Gesetzen und Updates Schritt zu halten. Weltweit gibt es Hunderte von Regulierungsbehörden, die täglich Updates veröffentlichen. Mit den Datenschutz- und Finanzvorschriften hat sich dieses Tempo in den letzten Jahren noch einmal erhöht. Dieser „Tsunami" an Vorschriften bedeutet, dass Unternehmen Mechanismen benötigen, um relevante Änderungen zu verfolgen. Diese sind oft technologiegesteuert, wie regulatorische Einspeisungen in GRC-Systeme oder das Abonnement von Compliance-Update-Services.

Marktwachstum und Zukunft von GRC: Der Markt für GRC-Technologie wächst rasant, da Unternehmen nach Software suchen, mit der sich diese Komplexitäten verwalten lassen. Schätzungen zufolge betrug der **globale GRC-Softwaremarkt** im Jahr 2023 etwa 5 Mrd. $. Bis 2029 soll er sich **fast verdoppeln** (auf 9–10 Mrd. $), da die Nachfrage nach integrierten Risikomanagement-Tools steigt.
Reference: **verdantix.com**

Cybersicherheitsversicherung und GRC: Versicherer, die Cyberversicherungen anbieten, untersuchen nun die GRC-Maßnahmen ihrer Kunden, beispielsweise ob diese Rahmenbedingungen wie ISO27001 befolgen oder über bestimmte Compliance-Zertifizierungen verfügen, bevor sie Polizzen abschließen. Ein starkes GRC-Programm kann somit die Versicherungsprämien senken und Unternehmen einen weiteren finanziellen Anreiz bieten, in Compliance und Risikomanagement zu investieren.

Sind Sie bereit für Governance, Risikomanagement und Compliance?

1. Governance – Führung & Rechenschaftspflicht

- [ ] Verfügen Sie über einen formellen Governance-Rahmen, der Richtlinien, Rollen und Verantwortlichkeiten für Risikomanagement und Compliance festlegt?
- [ ] Ist Ihr Vorstand bzw. Ihr C-Level in die Entscheidungsfindung bezüglich Risikomanagement und Compliance involviert?
- [ ] Stellen Sie durch regelmäßige Berichte sicher, dass die Governance-Richtlinien mit den Unternehmenszielen und regulatorischen Änderungen übereinstimmen?
- [ ] Verfügen Sie über einen dokumentierten Ethik- und Verhaltenskodex für Ihre Mitarbeiter und Führungskräfte?
- [ ] Unterliegen Drittanbieter und Partner einer Governance- und Risikoaufsicht?

Wenn Sie eine dieser Fragen mit „Nein“ beantwortet haben, könnten in Ihrer Governance-Überwachung Lücken bestehen.

2. Risikomanagement – Bedrohungen identifizieren und mindern

- [ ] Führen Sie ein Risikoregister, in dem Sie die Unternehmens-, Cybersicherheits-, Finanz- und Betriebsrisiken Ihres Unternehmens dokumentieren?
- [ ] Werden Risiken auf Basis ihrer Auswirkungen und Wahrscheinlichkeit bewertet und priorisiert?
- [ ] Führen Sie regelmäßige Risiko-Assessments durch (Cybersicherheit, Betrieb, Finanzen, Reputation, Lieferkette usw.)?
- [ ] Haben Sie eine formelle Risikominderungsstrategie, in der Verantwortliche und Zeitpläne für Korrekturmaßnahmen festlegt sind?
- [ ] Existiert für wichtige Systeme und Abläufe des Unternehmens ein Geschäftskontinuitäts- und Notfallwiederherstellungsplan?

Wenn Sie eine dieser Fragen mit „Nein“ beantwortet haben, können Sie unangesprochenen Risiken ausgesetzt sein.

3. Compliance – Einhaltung gesetzlicher Vorschriften und Branchenstandards

- [ ] Kennen Sie die wichtigsten Vorschriften und Rahmenbedingungen Ihrer Branche (z. B. DSGVO, ISO 27001, NIS2, PCI DSS, SOC 2, KI-Governance usw.)? Verfügen Sie über formelle Compliance-Richtlinien und -Kontrollen für diese Vorschriften?
- [ ] Wird die Compliance regelmäßig intern oder extern überwacht und auditiert?
- [ ] Verfügen Sie über automatisierte Compliance-Tracking- oder Reporting-Tools?
- [ ] Können Sie im Falle einer regulatorischen Überprüfung eine auditfähige Dokumentation schnell bereitstellen?

Haben Sie eine dieser Fragen mit „Nein“ beantwortet, können Sie regulatorischen oder finanziellen Risiko ausgesetzt sein.

4. Cybersicherheit & Datenschutz – Sicherer Betrieb

- [ ] Verfügen Sie über eine dokumentierte Cybersicherheitsrichtlinie, die den Compliance-Anforderungen genügt?
- [ ] Haben Sie in den letzten zwölf Monaten ein Cyberrisiko-Assessment durchgeführt?
- [ ] Sind die Mitarbeiter in Bezug auf Sicherheitsbewusstsein und Compliance-Verpflichtungen geschult?
- [ ] Verfügen Sie über Protokolle zur Reaktion auf Vorfälle und zur Meldung von Verstößen?
- [ ] Werden sensible Daten durch Verschlüsselung, Zugriffskontrollen und Datenklassifizierung geschützt?

Wenn Sie eine dieser Fragen mit „Nein“ beantwortet haben, entspricht Ihre Sicherheitsposition möglicherweise nicht den GRC-Best Practices.

5. Kontinuierliche Überwachung & Verbesserung

- [ ] Ist GRC in die Kultur Ihres Unternehmens integriert und wird nicht als einmaliges Projekt betrachtet?
- [ ] Verwalten Sie Governance, Risikomanagement und Compliance mit einer GRC-Technologieplattform an einem Ort?
- [ ] Werden Compliance- und Risikomanagementaktivitäten regelmäßig überprüft, getestet und auf der Grundlage neuer Bedrohungen oder regulatorischer Änderungen aktualisiert?
- [ ] Führen Sie laufend Bewertungen oder Prüfungen durch Dritte durch, um die Einhaltung der Vorschriften sicherzustellen?
- [ ] Ist die Berichterstattung über die Einhaltung der Vorschriften automatisiert und in Ihre Geschäftsabläufe integriert?

Wenn Sie auf eine dieser Fragen mit „Nein“ geantwortet haben, fehlen Ihnen möglicherweise Nachhaltigkeit und Effizienz bei Ihren GRC-Bemühungen.

Wie wir Ihnen als vertrauenswürdiger GRC-Partner helfen

Bei Insight wissen wir, dass es bei Governance, Risikomanagement und Compliance (GRC) nicht nur darum geht, Kontrollkästchen anzukreuzen. Es geht darum, Ihren Ruf zu schützen, eine sichere Entscheidungsfindung zu ermöglichen und dafür zu sorgen, dass Sie wachsen können, ohne Angst vor regulatorischen oder betrieblichen blinden Flecken haben zu müssen.

Wir unterstützen Sie dabei, diese Komplexität mit einem ganzheitlichen, praktischen und technologiegestützten GRC-Ansatz zu bewältigen, der sowohl Resilienz als auch Agilität bietet.

Advisory & Audit Services:

Unsere erfahrenen Berater helfen Ihnen dabei, Ihre Verpflichtungen zu verstehen, Benchmarks mit führenden Standardversionen zu erstellen und einen klaren Weg nach vorne zu planen.

Gap-Assessments und Readiness-Berichte - für ISO 27001, Cyber Essentials+, NIS2 und CAF und noch mehr

Policy & Framework Design - Aufbau skalierbarer Governance-, Risikomanagement-und Compliance-Programme, die auf Ihr Unternehmen zugeschnitten sind.

Vorstands- und Geschäftsleitungsberichterstattung - Umsetzung der GRC-Position in aussagekräftige Erkenntnisse über Geschäftsrisiken.

Interner Audit-Support - einschließlich Nachweiserstellung, Sanierungsplanung und kontinuierlicher Sicherstellung.

Managed GRC-Services

Wenn Sie nicht über die interne Bandbreite oder Expertise verfügen, sorgt unser Managed GRC-Angebot für einen reibungslosen Ablauf Ihres Compliance-Programms.

Kontinuierliches Risiko- und Compliance-Management - wir verwalten Ihre Kontrolltests, Problemverfolgung und Berichterstattung.

Virtueller CISO oder Virtueller Informationssicherheitsbeauftragter - Zugang zu fachkundigem Support ohne den Aufwand für den Aufbau eines vollständigen internen Teams.

Warum sich Kunden für Insight entscheiden

Branchenübergreifend vertrauenswürdig - von Finanzdienstleistungen über das Gesundheitswesen bis hin zur Fertigung und Technologie.

Zertifiziert nach den Standards, bei deren Einhaltung wir Sie unterstützen - einschließlich ISO 27001 und Cyber Essentials+.

Anbieterunabhängig - wir arbeiten mit führenden GRC-Plattformen, aber unsere Beratung beginnt mit Ihren Zielen und nicht mit einem Produktargument.

Geschäftsorientiert - wir sprechen sowohl die Sprache der Vorstandsetage als auch die des Back Office.