E&P CONSULTING

Evidence Driven Compliance

"Compliance at your fingertips"

Was ist Evidence Driven Compliance?

- ***Kontinuierliche*** *Compliance Überprüfung durch datenbasierte Evidenzen*
- ***Konsistentes*** *objektives Reporting durch Standardisierung*
- ***Automatisiertes*** *Reporting durch angebundene Datenquellen*

- **Zentralisierte** - toolgestützte Evidenzen mit Historie und Trends
- **Real time** - Überprüfung der Compliance
- **On Demand** - stets verfügbar
- **Transparenz** - hinsichtlich Noncompliance
- **Geringer manueller Aufwand** - für die Evidenzerbringung

Abgrenzung zu Date Driven Compliance

Identifikation der relevanten Daten mit Fokus auf ausgewählte, qualitätsgesicherte Quellen, um nachzuweisen, dass Kontrollen effektiv umgesetzt sind – Top-Down statt Bottom-Up. Evidence Driven Compliance destilliert den Data Driven Ansatz zu effektiven, evidenzbestätigenden Datensätzen. Das führt zu einem verbesserten Kosten-Nutzen-Verhältnis durch gezielten Ressourceneinsatz und eine zuverlässigere Datenqualität.

DATA DRIVEN COMPLIANCE

- **Hoher Implementierungsaufwand** und Kosten durch komplexe Prozesse
- **Erforderliches Fachwissen** in Data Science und zusätzlicher **Aufwand** durch Abstimmung hinsichtlich z.B. **Aggregation von Daten**
- **Datenschutzrisiken** bei sensiblen Daten, die sorgfältig gemanagt werden müssen

EVIDENCE DRIVEN COMPLIANCE

- **Flexibel erweiterbar,** um neue Anforderungen nahtlos zu integrieren
- **Gezielter Implementierungsaufwand** mit geringem Risiko unvorhergesehener Kosten – kein Gießkannenprinzip
- **Einfache Integration** in eine auditierbare und compliance-orientierte Prozesslandschaf

5-Säulen der Evidence Driven Compliance Methodik

1 REGULATORISCHE/ COMPLIANCE ANFORDERUNG

Umfassendes Anforderungs-Mapping: Erfassung regulatorischer, Compliance-bezogener sowie interner und gruppenweiter Anforderungen. Neue Anforderungen können nahtlos abgeglichen und bei Bedarf in den Anforderungskatalog integriert werden.

2 INTERNE GOVERNANCE

Definition der Anforderungen im Rahmen der internen Governance: Übersetzung der Anforderungen in konkrete Kontrollmaßnahmen, Dokumentation in Richtlinien, Policies, Arbeitsanweisungen und Standards.

3 INTERNE CAPABILITIES

Definition der IT-Capabilities: Identifikation und Beschreibung der zentralen IT-Fähigkeiten. **Mapping zu Kontrollanforderungen:** Zuordnung der IT-Capabilities zu den internen Kontrollanforderungen zur Sicherstellung von Compliance und Effizienz.

4 CONTROL ITEMS

Definition interner Control Items: Entwicklung technischer Maßnahmen zur Umsetzung der internen Capabilities und Sicherstellung der Zielerreichung.

5 EVIDENCES

Identifikation von Evidenzen: Ermittlung von Belegen, die die Erfüllung der Control Items belegen. Wo möglich, werden datenbasierte Evidenzen genutzt.

Continious Compliance Improvement Cycle

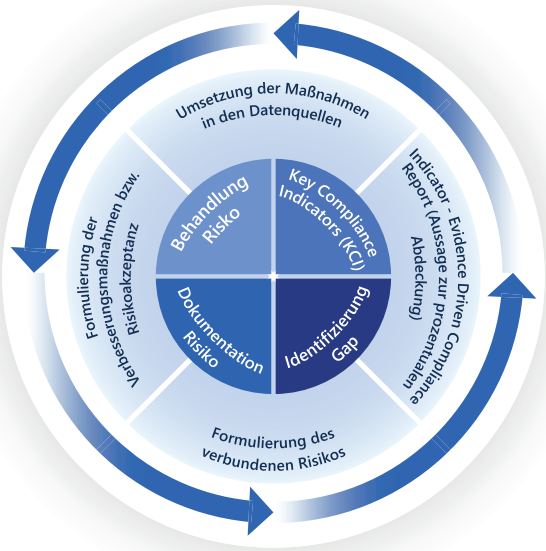
On-Demand-Identifikation und -Qualifizierung:
Schnelle Erkennung, Bewertung und Quantifizierung von Compliance-Gaps auf Asset-Ebene – zeitnah und präzise.

Gezielte Risikoanalyse:
Klare Dokumentation der damit verbundenen Risiken ermöglicht eine fundierte Einschätzung und transparente Kommunikation.

Priorisierung von Maßnahmen:
Leicht verständliche Entscheidungsgrundlagen zur Umsetzung von Verbesserungsmaßnahmen sowie fundierte Abwägung von Risikoakzeptanzen.

Echtzeit-Überblick:
Direkte Sichtbarkeit des Fortschritts bei der Umsetzung der Maßnahmen durch angebundene Datenquellen – für eine proaktive Steuerung.

Effiziente Risikominderung:
Vereinfachte Schließung identifizierter Risiken durch klare Evidenzbasierung auf Basis des KCI-Reportings.



Future Growth Potential

Schriftlich fixierte Ordnung-Management als DB-native Lösung in Evidence Based Compliance
Policies werden zentral in einer Datenbank dokumentiert und jährliche Review Prozesse automatisiert angestoßen, im Audit-Kontext erfolgt eine gezielte Ausspielung auditrelevanter Paragraphen inkl. evidenzbasierter Nachweise.

Flexible Erweiterbarkeit für neue regulatorische Anforderungen
Sowohl interne als auch externe Vorgaben (z. B. AI Act) lassen sich nahtlos integrieren – das Reporting wird automatisch entsprechend erweitert und evidenzgestützt abgebildet.

Anwendung bei der Behebung von regulatorischen Findings
Die Bearbeitung von Findings und die Schließung von regulatorischen Gaps unterscheiden sich primär in ihrer zeitlichen Priorität. Die bestehende Organisation kann einen Factory-Ansatz für die formale Bearbeitung von Findings nutzen und so die Notwendigkeit zur Einrichtung von „Task Forces" vermeiden.

Gap Analyse zu neuen oder erweiterten Anforderungen
Systemgestützte Analyse, um Lücken zwischen aktuellen Umsetzungsständen und neu eingeführten oder erweiterten Anforderungen (z. B. DORA, interne Policies) frühzeitig zu erkennen.

Ihre Ansprechpartner

Nikolaus Musil
Head of Cyber & Regulatory
+49 173 57 11 084
nm@eberhardt-partner.com

Verena Diehl
Lead of Cyber & Regulatory
+49 152 310 38427
vd@eberhardt-partner.com

E&P CONSULTING
www.eberhardt-partner.com