E&P CONSULTING

Evidence Driven Compliance

"Compliance at your fingertips"

Was ist Evidence Driven Compliance?

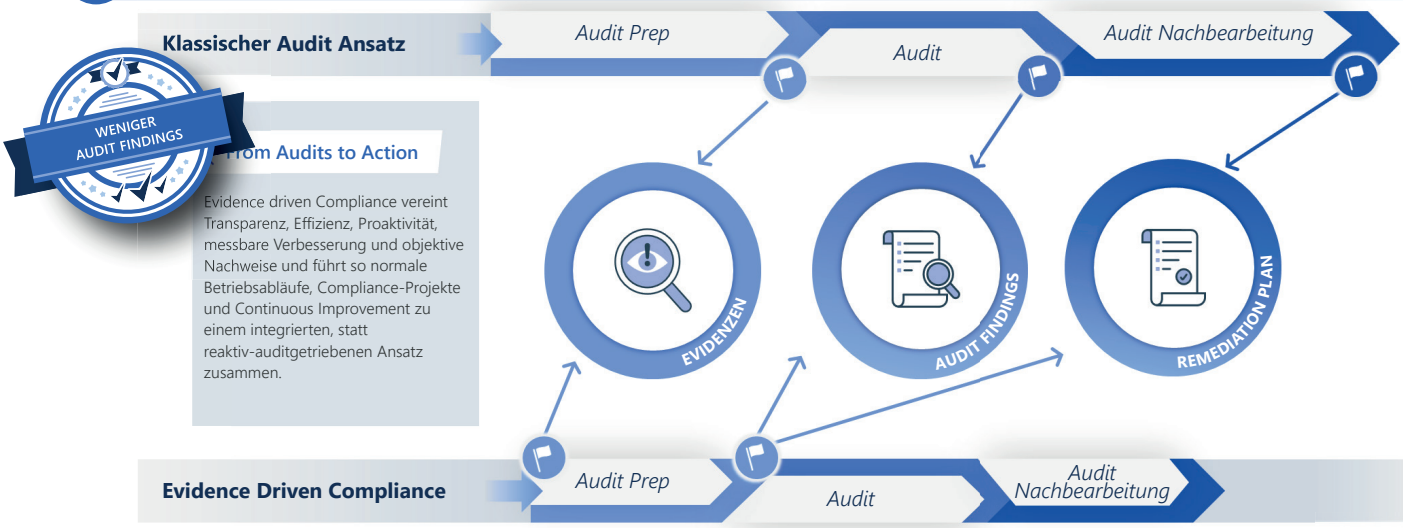
- ***Kontinuierliche*** *Compliance Überprüfung durch datenbasierte Evidenzen*
- ***Konsistentes*** *objektives Reporting durch Standardisierung*
- ***Automatisiertes*** *Reporting durch angebundene Datenquellen*

- **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

ZENTRALISIERTE GOVERNANCE DOKUMENTATION

Holistisches IKT*-Risikomanagement durch eindeutige Erhebungen*

Klassischer Audit Ansatz vs. EDC Audit Ansatz



6-Säulen der Evidence Driven Compliance Methodik

REDUZIERTE AUDIT NACHBEARBEITUNGSKOSTEN

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.

6 RISIKO

Identifikation von Risiko: Fehlende Erfüllung oder nur Teilerfüllung von Control Items ergibt automatisch Risiken. Weiter Quellen, wie interne Audits oder Vulnerability Management, können als Resultate ihrer Durchführung weitere Risiken identifizieren.

Continuous Compliance Improvement Cycle

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

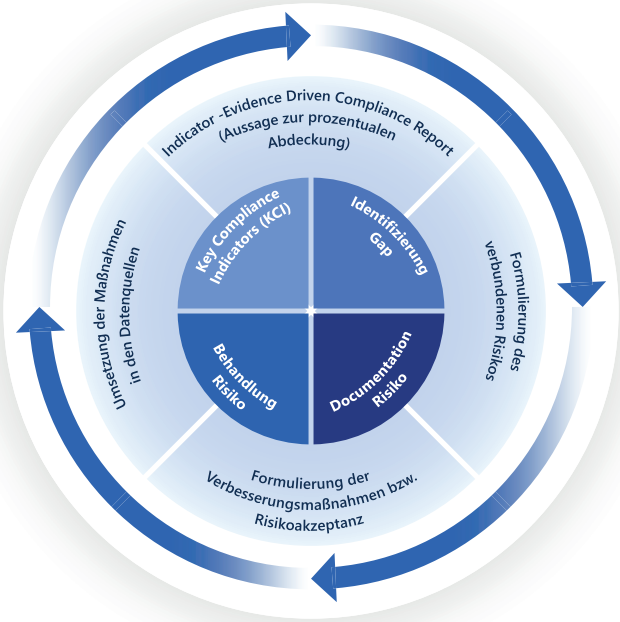
Gezielte Risikoanalyse:
Klare Dokumentation der damit verbundenen Risiken ermöglicht eine fundierte Einschätzung und transparente Kommunikation.

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.

Key Compliance Indicators (KCI):
Transparenz und Effizienz durch Standardisierung



Future Growth Potential

SfO-Management als DB-native Lösung in EDC
Policies werden, anstatt in multiplen Dokumenten, zentral in einer Datenbank dokumentiert. Das vereinfacht und automatisiert die benötigten jährliche Review Prozesse, im Audit-Kontext können daher gezielte Ausspielung auditrelevanter Paragraphen inkl. evidenzbasierter Nachweise erfolgen.

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 und der etablierte Prozess können für die formale Abarbeitung von Findings unverändert genutzt werden, das Aufsetzen von „Task Forces" kann vermieden werden.

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.

Nach dem MVP – Roadmap Planung
Der MVP dient zur Familiarisierung mit dem EDC Konzept, danach müssen die restlichen Elemente des Compliance Frameworks integriert werden. Basierend auf den jeweiligen Business Prioritäten wird eine klare Roadmap mit allen benötigen Resourcen für die Implementierung entwickelt, sowie die relevanten Projekte für die Eveidenzerbringung priorisiert.

Ihre Ansprechpartnerin

Verena Diehl
Managing Director

+49 152 310 38427
vd@eberhardt-partner.com