E&P CONSULTING

Evidence Driven Compliance

"Compliance at your fingertips"

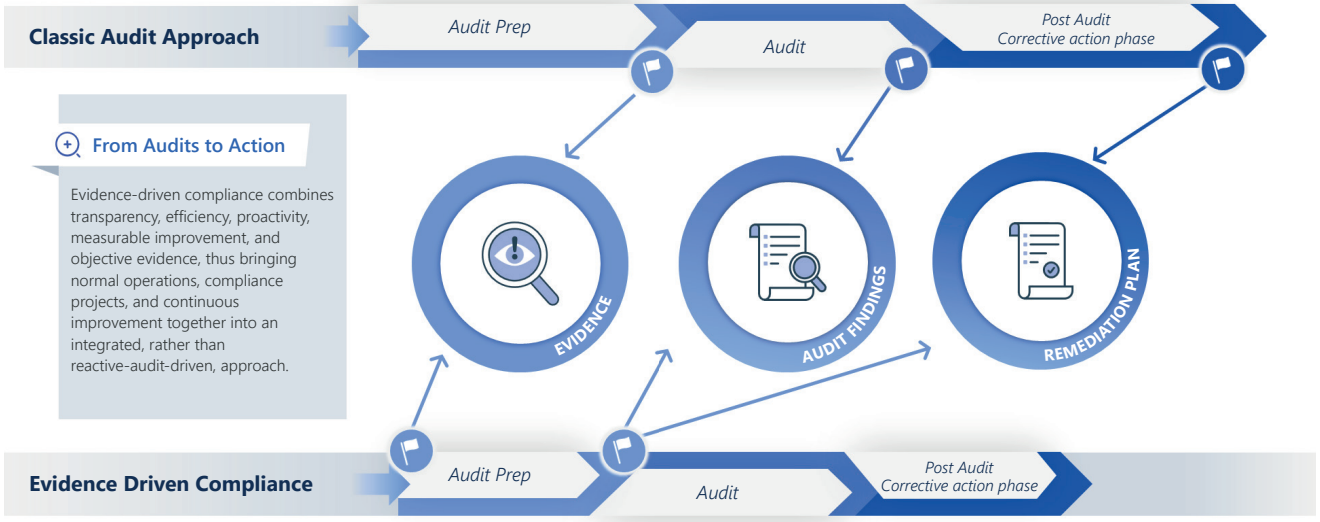
What is Evidence Driven Compliance?

- ***Continuous*** *compliance verification trough evidence based on data*
- ***Consistent*** *objective reporting through standardization*
- ***Automated*** *reporting through connected Data Sources*

- **"Centralized"** tool-supported evidence including history and trending
- **Near "Real time"** compliance verification
- **On Demand** always available
- **Transparency** regarding non-compliance
- **Low manual effort** required to provide evidence

Holistic ICT *risk management through unequivocal data collection*

Classical Audit Approach vs. EDC Audit Approach



The 6 Pillars of the Evidence Driven Compliance Methodology

1 REGULATORY / COMPLIANCE REQUIREMENTS

Comprehensive Requirements Mapping:
Recording of regulatory, compliance-related, as well as internal and group-wide requirements.
New requirements can be seamlessly matched and integrated into the requirements catalog if necessary.

2 INTERNAL GOVERNANCE (POLICIES / GUIDELINES / STANDARDS)

Definition of requirements within the framework of internal governance:
Translation of the requirements into concrete control measures, documentation in guidelines, policies, work instructions, and standards.

3 INTERNAL CAPABILITIES

Definition of IT Capabilities:
Identification and description of central IT capabilities.

Mapping to Control Requirements:
Assignment of the IT capabilities to the internal control requirements to ensure compliance and efficiency.

4 CONTROL ITEMS

Definition of internal control items:
Development of technical measures for the implementation of internal capabilities and ensuring the achievement of objectives.

5 EVIDENCES

Identification of Evidence:
Identification of evidence that demonstrates the fulfillment of the control items. Where possible, data-based evidence is used.

6 RISK

Identification of risk:
Failure to meet or only partial fulfillment of control items automatically results in risks. Other sources, such as internal audits or vulnerability management, can identify additional risks as a result of their execution.

Continuous Compliance Improvement Cycle

On-Demand Identification and Qualification:
Rapid detection, assessment, and quantification of compliance gaps at the asset level – timely and precise.

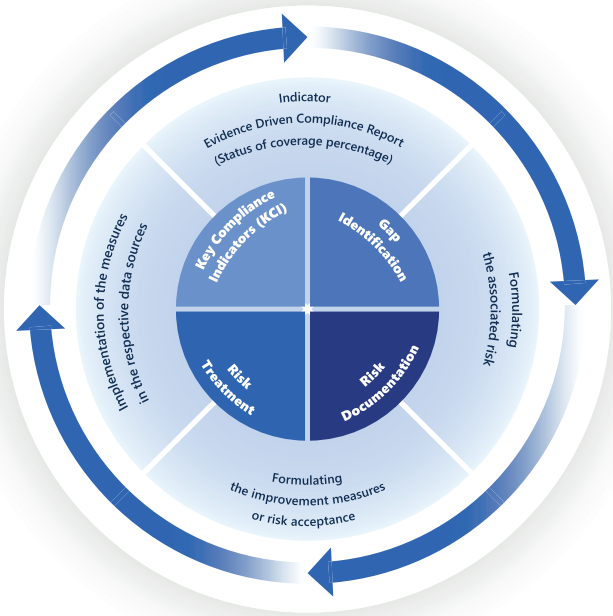
Targeted Risk Analysis:
Clear documentation of associated risks enables an informed assessment and transparent communication.

Prioritization of Measures:
Easily understandable decision-making foundation for the implementation of improvement measures as well as well-founded considerations of risk acceptance.

Near "Real-Time" Overview:
Direct visibility of implementation progress of measures through connected data sources – for proactive management.

Efficient Risk Reduction:
Simplified closure of identified risks through a clear evidence-based approach using the Key Compliance Indicator (KCI) reporting.

Key Compliance Indicators (KCI):
Transparency and efficiency through standardization.



Future Growth Potential

Compliance documentation management as a DB-native solution in EDC
Policies are documented centrally in a database instead of in multiple documents. This simplifies and automates the required annual review processes; in the audit context, targeted deployment of audit-relevant paragraphs including evidence-based proofs can therefore take place.

Flexible scalability for new regulatory requirements
Both internal and external guidelines (e.g., AI Act) can be seamlessly integrated – reporting is automatically expanded accordingly and documented with evidence.

Usage in addressing regulatory findings
The handling of findings and the closing of regulatory gaps primarily differ in their temporal priority. The existing organization and the established process can be used unchanged for the formal processing of findings, setting up "task forces" can be avoided.

Gap analysis for new or expanded requirements
System-supported analysis to identify gaps between current implementation statuses and newly introduced or expanded requirements (e.g., DORA, internal policies) at an early stage.

After the MVP – Roadmap Planning
The MVP serves to familiarize with the EDC concept, after which the remaining elements of the compliance framework need to be integrated. Based on the respective business priorities, a clear roadmap is developed with all the resources needed for implementation, as well as the relevant projects for evidence provision being prioritized.

Contacts

Nikolaus Musil
Head of Cyber & Regulatory
+49 173 4730345
nm@eberhardt-partner.com

Verena Diehl
Managing Director
+49 152 310 38427
vd@eberhardt-partner.com