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 with history and trends

☑ **Real time** - compliance verification

☑ **On Demand** - always available

☑ **Transparency** - regarding non-compliance

☑ **Low manual effort** - for providing evidence

Distinction from Data Driven Compliance

Evidence Driven Compliance focuses on identifying relevant data from selected, quality-assured sources to clearly demonstrate that controls are effectively implemented – applying a top-down rather than bottom-up approach. It refines the Data Driven model into meaningful, evidence-based datasets, resulting in a stronger cost-benefit ratio, smarter resource allocation, and more reliable data quality.

DATA DRIVEN COMPLIANCE

- **High implementation effort and costs** due to complex processes.
- **Required expertise in Data Science** and additional effort for coordination, e.g. Data Aggregation.
- **Data protection risks** when dealing with sensitive information which must be carefully managed.

EVIDENCE DRIVEN COMPLIANCE

- **Flexible expandability** to seamlessly integrate new requirements.
- **Targeted implementation effort** with low risk of unforeseen costs – no "watering can principle".
- **Easy integration** into an auditable, compliance-oriented process landscape.

The 5 Pillars of the Evidence Driven Compliance Methodology

1
REGULATORY / COMPLIANCE REQUIREMENTS

Comprehensive requirements mapping:
Capturing regulatory, compliance-related as well as internal and group-wide requirements.
New requirements can be seamlessly matched and integrated into the requirements if needed.

2
INTERNAL GOVERNANCE

Definition of requirements within internal Governance:
Translating requirements into concrete control measures, documentation in guidelines, policies, work instructions, and standards.

3
INTERNE CAPABILITIES

Definition of IT capabilities:
Identification and description of central IT functions.
Mapping to control requirements:
Assigning IT capabilities to internal control requirements to ensure compliance and efficiency.

4
CONTROL ITEMS

Definition of internal control items:
Development of technical measures for implementing internal capabilities and ensuring objectives are achieved.

5
EVIDENCES

Identification of evidence:
Identification of evidence that confirm fulfillment of Control Items. Where possible, evidence based on data is used.

Continious Compliance Improvement Cycle

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

Targeted Risk Analysis:
Clear documentation of related risks enables well-founded assessment and transparent communication.
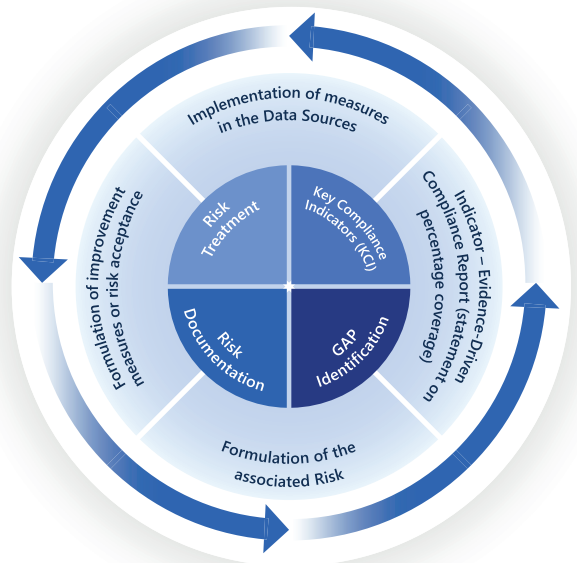
Prioritization of Measures:
Easily understandable decision-making foundations for implementing improvement measures, along with well-founded evaluations of risk acceptances.

Real-time Overview:
Direct visibility of progress in implementing measures through connected data sources – enabling proactive management.

Efficient Risk Mitigation:
Simplified closure of identified risks through clear evidence-based documentation using KCI reporting.

Implementation of measures in the Data Sources

Indicator – Evidence-Driven Compliance Report (statement on percentage coverage)

Formulation of improvement measures or risk acceptance

Risk Treatment

Key Compliance Indicators (KCI)

Risk Documentation

GAP Identification

Formulation of the associated Risk

Future Growth Potential

Set of written rules management as a DB-native solution in Evidence Based Compliance
Policies are centrally documented in a database and annual review processes are automatically initiated. In the audit context, audit-relevant paragraphs are specifically displayed including evidence-based evidence.

Flexible expandability for new regulatory requirements
Both internal and external requirements (e.g., EU AI Act) can be seamlessly integrated – reporting is automatically expanded and evidence-based.

Application in addressing regulatory findings
The handling of findings and the closure of regulatory gaps mainly differ in their timing priority. The existing organization and can utilize a factory approach for formal processing of findings, avoiding the need to set up "Task Forces".

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

Contacts

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