KOENIG SOLUTIONS

Data Security and Governance

in the Oil and Gas Industry

Comprehensive 5-Day Training Programme

Duration	Format	Level
5 Days	**Instructor-Led**	**Intermediate–Advanced**

Course Overview

This intensive 5-day programme equips professionals in the Oil and Gas sector with comprehensive knowledge of data governance principles, security frameworks, and industry-specific compliance requirements. Covering everything from foundational governance structures through to advanced IT-OT cybersecurity and digital oilfield data management, participants will leave with practical skills aligned to globally recognised certifications.

Course Overview

Minimum **2–3 years of work experience** in the Oil and Gas, Energy, or related industrial sector. Roles may include IT, OT, engineering, data management, operations, or compliance.

Basic familiarity with **IT and/or OT environments** — understanding of how systems like SCADA, historians, or enterprise applications are used in day-to-day operations.

TABLE OF CONTENTS

1.1.3 Key Drivers for Data Governance in O&G

- 1.1.3.1 Regulatory pressure (OSPAR, EPA, GDPR)
- 1.1.3.2 Operational efficiency and safety
- 1.1.3.3 Digital transformation and Industry 4.0

1.2 Core Components of Data Governance

1.2.1 People Component

- 1.2.1.1 Roles: Data Owners, Stewards, Custodians
- 1.2.1.2 Governance team structure and responsibilities
- 1.2.1.3 Training and cultural adoption

1.2.2 Process Component

- 1.2.2.1 Policies, standards, and business rules
- 1.2.2.2 Data quality metrics and scorecards
- 1.2.2.3 Risk identification and control objectives

1.2.3 Technology Component

- 1.2.3.1 Data modeling tools and system of records (SoRs)
- 1.2.3.2 Data quality and compliance monitoring tools
- 1.2.3.3 Technology evaluation and selection criteria

1.3 Data Governance Organizational Structure

1.3.1 The Governance Pyramid

- 1.3.1.1 Executive Steering Committee (ESC)
- 1.3.1.2 Data Governance Board and Data Governors
- 1.3.1.3 Data Stewardship Council and Business Data Stewards
- 1.3.1.4 IT Support functions

1.3.2 RACI Framework for Data Decisions

- 1.3.2.1 Responsible, Accountable, Consulted, Informed
- 1.3.2.2 Practical RACI matrix for O&G data domains

1.4 Oil & Gas Industry Data Landscape

1.4.1 Data Categories in O&G

- 1.4.1.1 Operational data: topsides, wells, pipelines, sensors
- 1.4.1.2 Process data: units, power/water, facilities
- 1.4.1.3 Enterprise data: safety, drilling, historian, IoT

1.4.2 IT-OT Convergence Challenges

- 1.4.2.1 IT vs. OT systems overview
- 1.4.2.2 Data management in converged environments
- 1.4.2.3 Change management implications

1.4.3 The Digital Oilfield Concept

- 1.4.3.1 Real-time data and integrated production models
- 1.4.3.2 Intelligent alarming and diagnostics
- 1.4.3.3 Enhanced business processes and visualization

DAY 2 — Data Management & Quality

Master data identification, quality frameworks, and lifecycle management

2.1 Identifying Key Enterprise Data & Processes

2.1.1 Key Business Data Identification

- 2.1.1.1 Data inventorying techniques
- 2.1.1.2 Data classification and sensitivity levels
- 2.1.1.3 Critical data elements (CDEs) in O&G

2.1.2 Data Models and System of Records (SoRs)

- 2.1.2.1 Logical and physical data models
- 2.1.2.2 Authoritative data sources and golden records
- 2.1.2.3 Master data management (MDM) principles

2.1.3 Structured vs. Unstructured Data Issues

- 2.1.3.1 Structured data: input, processing, output controls
- 2.1.3.2 Unstructured data: document repositories, email
- 2.1.3.3 Boundary controls and data origination

2.2 Data Quality Management

2.2.1 Data Quality Dimensions

- 2.2.1.1 Accuracy, completeness, consistency, timeliness
- 2.2.1.2 Validity, uniqueness, and integrity
- 2.2.1.3 O&G-specific quality requirements

2.2.2 Data Quality Metrics and Scorecards

- 2.2.2.1 Designing DQ metrics for O&G datasets
- 2.2.2.2 Building and maintaining DQ scorecards
- 2.2.2.3 Threshold setting and escalation procedures

2.2.3 Data Quality Monitoring Tools

- 2.2.3.1 Automated profiling and anomaly detection
- 2.2.3.2 Real-time monitoring for sensor/IoT data
- 2.2.3.3 Reporting and remediation workflows

2.3 Metadata Management

2.3.1 Types of Metadata

- 2.3.1.1 Technical, business, and operational metadata
- 2.3.1.2 Metadata standards (ISO 19115, PPDM, WITSML)

2.3.2 Data Lineage and Cataloging

- 2.3.2.1 Tracing data from origin to consumption
- 2.3.2.2 Enterprise data catalog implementation
- 2.3.2.3 Data dictionary creation and maintenance

2.4 Data Lifecycle Management

2.4.1 Data Retention and Archiving Policies

- 2.4.1.1 Legal and regulatory retention requirements in O&G
- 2.4.1.2 Tiered storage strategies
- 2.4.1.3 Archiving best practices for seismic and well data

2.4.2 Data Cleansing and Synchronization

- 2.4.2.1 Cleansing methodologies and tools
- 2.4.2.2 Data synchronization across SCADA, ERP, and historian
- 2.4.2.3 Conflict resolution and merge strategies

2.4.3 Data Purging and Decommissioning

- 2.4.3.1 Secure data destruction procedures
- 2.4.3.2 Compliance documentation and audit trails

DAY 3

Data Security & Access Control

Apply security frameworks, controls, and privacy principles across the data lifecycle

3.1 Data Security Fundamentals

3.1.1 Information Security Principles (CIA Triad)

- 3.1.1.1 Confidentiality, Integrity, Availability in O&G
- 3.1.1.2 Non-repudiation and authentication
- 3.1.1.3 Security risk assessment frameworks (ISO 27001, NIST)

3.1.2 Threat Landscape in Oil & Gas

- 3.1.2.1 Cyber threats to OT/SCADA environments
- 3.1.2.2 Insider threats and data exfiltration risks
- 3.1.2.3 Notable O&G breach case studies

3.2 Security Controls through the Data Lifecycle

3.2.1 Plan & Collect Phase Controls

- 3.2.1.1 Data origination and authorization controls
- 3.2.1.2 Data input validation and integrity checks
- 3.2.1.3 Secure data collection from IoT and sensors

3.2.2 Process & Analyse Phase Controls

- 3.2.2.1 Data processing controls and transformation security
- 3.2.2.2 Secure analytics environments
- 3.2.2.3 Data masking and tokenization

3.2.3 Preserve, Share & Reuse Phase Controls

- 3.2.3.1 Encryption at rest and in transit
- 3.2.3.2 Secure data sharing and third-party governance
- 3.2.3.3 Data output controls and boundary enforcement

3.3 Data Access & Permission Management

3.3.1 Access Control Models

- 3.3.1.1 Role-Based Access Control (RBAC)
- 3.3.1.2 Attribute-Based Access Control (ABAC)
- 3.3.1.3 Least privilege and need-to-know principles

3.3.2 Identity & Access Management (IAM)

- 3.3.2.1 User provisioning and de-provisioning workflows
- 3.3.2.2 Multi-factor authentication (MFA) for critical systems
- 3.3.2.3 Privileged access management (PAM)

3.3.3 Access Audit and Review

- 3.3.3.1 Periodic access certification and recertification
- 3.3.3.2 Access log monitoring and anomaly detection

3.4 IT-OT Cybersecurity

3.4.1 ICS/SCADA Security Principles

- 3.4.1.1 IEC 62443 standard for industrial cybersecurity
- 3.4.1.2 Network segmentation and DMZ design

- 3.4.1.3 Patch management in OT environments

3.4.2 **Data Privacy & Confidentiality**
- 3.4.2.1 GDPR and data protection regulations
- 3.4.2.2 PII identification and protection in O&G context
- 3.4.2.3 Data classification for confidentiality levels

DAY 4

Governance Implementation & O&G Standards

Design and deploy governance structures aligned to the O&G industry lifecycle

4.1 Steps to Establish Data Governance

4.1.1 **Step 1: Identify Key Enterprise Data & Processes**
- 4.1.1.1 Data discovery workshops and interviews
- 4.1.1.2 Current-state assessment and gap analysis
- 4.1.1.3 Prioritizing critical data domains

4.1.2 **Step 2: Define Governance Structure**
- 4.1.2.1 Designing governance committees and charters
- 4.1.2.2 Assigning accountability for data decisions
- 4.1.2.3 Decision rights and escalation procedures

4.1.3 **Step 3: Monitor Data Quality Performance**
- 4.1.3.1 KPI and OKR selection for data governance
- 4.1.3.2 Developing and publishing DQ scorecards
- 4.1.3.3 Continuous improvement cycles

4.2 O&G Industry Lifecycle & Governance Standards

4.2.1 **The O&G Asset Lifecycle**
- 4.2.1.1 Phase 1: Exploration — seismic and subsurface data
- 4.2.1.2 Phase 2: Appraisal — reservoir data and parameters
- 4.2.1.3 Phase 3: Development — engineering and drilling data
- 4.2.1.4 Phase 4: Production — operational and production data
- 4.2.1.5 Phase 5: Abandonment — decommissioning data governance

4.2.2 **Industry Data Standards**
- 4.2.2.1 PPDM (Professional Petroleum Data Management)
- 4.2.2.2 WITSML for drilling and wellbore data
- 4.2.2.3 OSDU (Open Subsurface Data Universe) overview
- 4.2.2.4 ISO 15926 for process plant lifecycle data

4.3 Change Management & Stakeholder Engagement

4.3.1 **Building a Data-Driven Culture**
- 4.3.1.1 Executive sponsorship and leadership buy-in
- 4.3.1.2 Change communication strategies
- 4.3.1.3 Training and awareness programmes

4.3.2 **Overcoming Governance Challenges**
- 4.3.2.1 Resistance to governance adoption
- 4.3.2.2 Balancing agility with control
- 4.3.2.3 Cross-functional collaboration models

4.4 Application Process Controls & Integration

4.4.1 System Integration Governance

- 4.4.1.1 API governance and data exchange standards
- 4.4.1.2 ETL/ELT pipeline controls
- 4.4.1.3 Data contract management

4.4.2 Digital Oilfield Data Governance

- 4.4.2.1 Governing real-time sensor and historian data
- 4.4.2.2 Production data model governance
- 4.4.2.3 Integrated visualization and dashboard standards

DAY 5 — Advanced Topics, Compliance & Capstone

Integrate advanced governance strategies, compliance requirements, and apply learning through capstone

5.1 Data Governance Maturity Models

5.1.1 Maturity Assessment Frameworks

- 5.1.1.1 DAMA-DMBOK maturity levels
- 5.1.1.2 IBM Data Governance Maturity Model
- 5.1.1.3 Self-assessment tools and scoring

5.1.2 Building a Governance Roadmap

- 5.1.2.1 Gap analysis to roadmap development
- 5.1.2.2 Prioritization and quick wins
- 5.1.2.3 3-year governance improvement plan

5.2 Technology Enablers & Emerging Trends

5.2.1 Enterprise Data Catalog and Governance Platforms

- 5.2.1.1 Collibra, Alation, Microsoft Purview overview
- 5.2.1.2 Selection criteria for O&G use cases
- 5.2.1.3 Implementation considerations

5.2.2 AI/ML in Data Governance

- 5.2.2.1 Automated metadata tagging and classification
- 5.2.2.2 Anomaly detection for data quality
- 5.2.2.3 AI governance and model data management

5.2.3 Cloud Data Governance in O&G

- 5.2.3.1 Cloud-specific governance challenges
- 5.2.3.2 OSDU cloud platform governance
- 5.2.3.3 Hybrid and multi-cloud data strategies

5.3 Compliance, Risk & Incident Management

5.3.1 Regulatory Compliance Management

- 5.3.1.1 Mapping O&G regulations to governance controls
- 5.3.1.2 Compliance monitoring and reporting
- 5.3.1.3 Internal audit and external review preparation

5.3.2 Data Breach and Incident Response

- 5.3.2.1 Incident classification and severity levels
- 5.3.2.2 Response playbook for O&G data incidents

- 5.3.2.3 Post-incident review and remediation
- 5.3.2.4 Regulatory notification obligations

5.3.3 Business Continuity & Disaster Recovery

- 5.3.3.1 Data backup strategies for critical O&G systems
- 5.3.3.2 RTO/RPO definitions and testing

5.4 Capstone Workshop & Assessment

5.4.1 Case Study Reviews

- 5.4.1.1 Major O&G data governance failures and lessons
- 5.4.1.2 Success stories and best-practice benchmarks

5.4.2 Group Capstone Exercise

- 5.4.2.1 Design a governance framework for a given O&G scenario
- 5.4.2.2 Presentation and peer review
- 5.4.2.3 Feedback and scoring by facilitator

5.4.3 Final Assessment & Certification Review

- 5.4.3.1 Written assessment overview
- 5.4.3.2 Certification mapping: CISSP, CISM, CISA, SCADA Security
- 5.4.3.3 Next steps and continued learning resources