CHECKLIST

Compliance and sustainability risk reporting

General compliance questions

- [ ] Is there an up-to-date list of all relevant legal requirements (national/international)?
- [ ] Is a compliance officer appointed and trained within the company?
- [ ] Does management have a comprehensible and binding regulation regarding the responsibilities and areas of responsibility of the compliance organization?
- [ ] To what extent is the responsibility for compliance management perceived by company management as an integral part of its legal supervisory duty?
- [ ] Is there organizational independence of the compliance function within the company – particularly in relation to operational management?
- [ ] Is the compliance function equipped with sufficient human, technical and financial resources and appropriate authority?
- [ ] In your opinion, is an active and credible commitment to compliance by the company management reflected in its leadership culture ("tone from the top")?
- [ ] Is there a written compliance plan or program?
- [ ] Have the basic framework conditions of the compliance management system been documented and defined?
- [ ] Does the documentation include key aspects such as the objectives, scope and structure of the CMS, the risk analysis methodology, staffing, responsibilities and integration into existing business processes?

CHECKLIST

Compliance and sustainability risk reporting

Training & Communication

- [ ] Are training courses on compliance and sustainability topics offered regularly?
- [ ] Is there documented evidence of participation by all relevant employees?
- [ ] Are new employees introduced to the compliance strategy?
- [ ] Is it ensured that employees are informed about and understand the rules that apply to them?
- [ ] Is there a communication concept for communicating compliance content to specific target groups?

Risk analysis

- [ ] Are structured surveys of potential compliance risks carried out regularly within the company?
- [ ] Are risk-relevant topics defined in a relevance analysis – e.g., based on criteria such as business model, market environment, or international structure?

CHECKLIST

Compliance and sustainability risk reporting

ESG (Environment, Social, Governance)

- [ ] Are there defined ESG goals and KPIs?
- [ ] Are environmental and social risks regularly assessed and reported?
- [ ] Is there a sustainability strategy that is linked to the corporate strategy?
- [ ] Are there sustainability indicators (e.g. CO2 emissions, energy consumption, diversity)

Prevention

- [ ] Is there a company-wide code of conduct that defines binding principles for legal and ethical behavior?
- [ ] Is this supplemented by specific compliance guidelines on relevant topics?
- [ ] Is there a structured advisory service for questions relating to compliance-related issues?
- [ ] Is the compliance function regularly involved in decision-making processes with regulatory relevance?
- [ ] Is there a whistleblower system and can it be used anonymously?

CHECKLIST

Compliance and sustainability risk reporting

Reporting & Documentation

- [ ] Is a regular compliance and/or sustainability report prepared?
- [ ] Is this report part of the internal risk reporting?
- [ ] Has the report been reviewed or validated by an independent audit?
- [ ] Are significant compliance processes reported outside of the regular cycle (ad hoc) if necessary?
- [ ] Are significant compliance processes reported outside of the regular cycle (ad hoc) if necessary?
- [ ] Are violations systematically documented and analyzed?

Response to violations or risks

- [ ] Are there established escalation processes for compliance violations?
- [ ] Are indications of potential misconduct responded to promptly and consistently?
- [ ] Are root cause analyses carried out after violations?
- [ ] Are improvement measures systematically documented and tracked?
- [ ] Are any weaknesses in the control system or structural causes that contributed to a breach of rules systematically analyzed and remedied?