MAYER|BROWN

BRIEFING SERIES

INTERNAL INVESTIGATIONS

PART II: COMPLIANCE MANAGEMENT SYSTEMS: SET-UP, REPORTING AND DECISION-MAKING

By Pauline Stadler and Dr. Hagen Köckeritz

A series of client briefings led by our Employment & Benefits Group

This **Part II** of our Series sets out how to design and operate an effective **compliance management system** (*CMS*) that is both credible across jurisdictions and tailored to German corporate practice. The core message is clear: compliance should be organized on a riskbased, independent, and welldocumented footing, aligned with recognized frameworks, and supported by structured reporting lines and clearly defined decisionmaking rights visàvis management and the supervisory board.

In Germany, the baseline is formed by boardlevel duties to properly organize and monitor the enterprise, including the obligation to ensure early risk detection. These expectations are heightened for listed companies and complemented by the German Corporate Governance Code (*Deutscher Corporate Governance Kodex – DCGK*), which requires a transparent description of the internal control and risk management system, including the *CMS*, and an assessment of its adequacy and effectiveness.

In addition, **specialized statutory regimes**, most notably the Whistleblower Protection Act (*Hinweisgeberschutzgesetz – HinSchG*) and the Supply Chain Due Diligence Act (*Lieferkettensorgfaltspflichtengesetz – LkSG*), impose concrete architectural, procedural, and timing requirements, particularly with respect to reporting channels and complaints handling mechanisms.

WHAT'S INSIDE

Compliance mandate and its practical anchor points 3

Governance design: roles, independence, and reporting lines 5

Building blocks of an effective CMS 6

Reporting architecture and decision-making 8

Implementation roadmap and operating discipline 10

Special topics and current developments 11

Conclusion 12

COMPLIANCE MANDATE AND ITS PRACTICAL ANCHOR POINTS

BOARD ORGANIZATION DUTIES AND EARLY RISK DETECTION

The obligation to establish and operate an effective compliance organization derives from the duty to ensure lawful conduct and an appropriate organizational framework, including an earlywarning system for risks that could jeopardize the company's continued existence.

For **listed companies**, the legislator has further clarified that an appropriate and effective internal control system and risk management system must be in place; in practice, the *CMS* is treated as an integral component of this overall framework. Even where statutory provisions are formally limited to listed entities, comparable expectations may arise for other companies under the general duty of care and principles of prudent organization where size, complexity, or risk exposure so require.

In **limited liability companies**, the managing directors' duty of care is interpreted along similar lines. Although operational responsibilities may be delegated within the organization, ultimate accountability remains with management, in particular with respect to the mandate, resourcing, independence, and ongoing oversight of the compliance function.

SPECIALIZED REGIMES THAT SHAPE CMS ARCHITECTURE

Regardless of industry, **specialized statutory regimes** give rise to specific design requirements for compliance management system.

The *HinSchG* requires organizations with 50 or more employees to establish internal reporting channels, appoint an impartial reporting unit, ensure strict confidentiality, and comply with defined service levels, acknowledgment of receipt within seven days and outcomeoriented feedback within three months. The *LkSG* mandates riskbased due diligence with respect to humanrights and certain environmental risks, including the designation of responsible functions, regular and eventdriven risk analyses, the implementation of preventive and remedial measures, and the operation of an accessible complaints mechanism. While the Federal Office for Economic Affairs and Export Control (*BAFA*) announced in late 2025 that it would discontinue routine reviews of company reports and that enforcement would temporarily focus on serious violations as legislative amendments are prepared, the core due diligence and complaintshandling obligations remain in force and are subject to riskbased *ex officio* audits.

Beyond German law, many corporate groups are also subject to supervisory expectations in **regulated industries** and to issuerrelated obligations in **capital markets**. Taken together, these requirements underscore the need for a structured, adequately resourced, and welldocumented *CMS*, with clearly defined decision rights, reporting lines, and escalation pathways.

INTERNATIONAL FRAMEWORKS AND THE THREE-LINES OPERATING MODEL

ISO 37301:2021 is an international, certifiable standard issued by the International Organization for Standardization that defines requirements and guidance for an effective *CMS*. It follows the do-check-act-cycle and emphasizes leadership commitment, compliance culture, risk assessment, controls, and continuous improvement.

In German practice, *IDW PS 980* is also widely recognized as the relevant **auditing standard** for providing assurance on the design and effectiveness of a *CMS*.

From an organizational perspective, companies should operate a **threelines model**:

- the first line (the business) owns compliance within daytoday processes;
- the second line (compliance and other control functions) establishes frameworks, provides advice, monitors, and challenges; and
- the third line (internal audit) delivers independent assurance and reports to the audit committee.

This internationally established model aligns well with German corporate governance structures and supervisory expectations.

GOVERNANCE DESIGN: ROLES, INDEPENDENCE, AND REPORTING LINES

MANAGEMENT MANDATE, INDEPENDENCE SAFEGUARDS, AND RESOURCES

A clear compliance charter should define the scope and objectives of the *CMS*, the authorities of the compliance function, and safeguards to ensure its independence. It should expressly provide for unrestricted access to relevant information, set out conflictofinterest rules for matters involving senior leadership, and secure direct reporting rights to the CEO or General Counsel and, where appropriate, to the chair of the audit committee. Management should approve an **annual compliance plan** aligned with the company's risk profile and ensure that the *CMS* is adequately resourced. While centralizing compliance at group level is often efficient, this presupposes impartial case handling, effective local accessibility, sufficient language coverage, and robust service arrangements that comply with local codetermination and dataprotection requirements.

SUPERVISORY BOARD OVERSIGHT AND THE AUDIT COMMITTEE INTERFACE

The supervisory board, typically acting through the **audit committee**, is responsible for overseeing the *CMS*. Regular reporting to the audit committee should address material compliance risks, significant investigations and their outcomes, the status of remediation measures, material policy updates, training coverage, results of monitoring and testing activities, and key performance indicators (*KPIs*). Matters of a material nature, particularly cases involving senior leadership or indicating systemic control deficiencies, should be escalated to the full supervisory board without undue delay.

THE THREE LINES IN PRACTICE AND COORDINATION PROTOCOLS

Effective **coordination mechanisms** are essential to avoid gaps and duplication between compliance, risk management, internal control, and internal audit. Shared risk and control taxonomies, a centralized issuesandactions register with clear singlepoint accountability, and a quarterly executive compliance or risk committee help ensure that second and thirdline activities translate into timely management action and coherent, highquality reporting to the board. In **crossborder groups**, it is also critical to ensure that **central compliance teams** have appropriate access to local data and personnel to enable impartial case handling and effective monitoring.

SPECIALIZED OFFICERS AND INTERFACES

A practical *CMS* integrates **specialized officers** and their statutory programs, including, for example, the data protection officer (*DPO*), the antimoneylaundering officer (*AMLO*), and the humanrights officer or other designated responsible person under the *LkSG*. The internal reporting unit established under the *HinSchG* serves as a central hub for case intake and followup. Clear and welldefined interfaces between these roles and the central compliance function, supported by consistent casemanagement standards and harmonized escalation criteria, are essential to ensure coherence, accountability, and effective oversight.

BUILDING BLOCKS OF AN EFFECTIVE CMS

FRAMEWORK ALIGNMENT, PROPORTIONALITY, AND AUDITABILITY

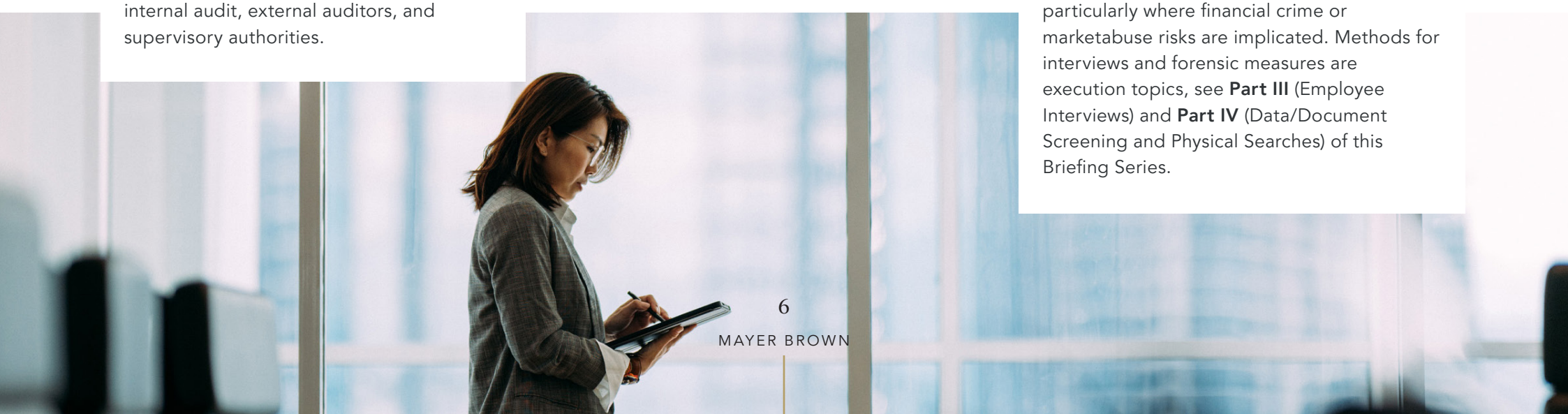
Alignment with *ISO 37301* provides a **common language** for global stakeholders and facilitates certification where this adds value. In the German context, *IDW PS 980* assurance, whether focused on design, implementation, or operating effectiveness, can deliver credible external comfort. Proportionality remains critical: the sophistication of controls, the depth of monitoring, and the rigor of documentation should scale with the company's risk exposure and potential impact. Designing the *CMS* with auditability in mind from the outset helps minimize friction with internal audit, external auditors, and supervisory authorities.

POLICY ARCHITECTURE AND RISK ASSESSMENT

A **coherent policy framework** should cascade from a core code of conduct to targeted, riskspecific policies and procedures. The compliance risk assessment should be systematic, well documented, and integrated with enterprise risk management, drawing on factors such as geographic footprint, business model, distribution channels, counterparty profiles, and incident history. Its outputs should directly inform policy updates, control design, training priorities, and secondline monitoring activities.

SPEAK-UP, CASE INTAKE, AND PROTECTED HANDLING

The **speak-up system** must accommodate **multiple intake channels**, including anonymous options where feasible, and integrate the *HinSchG* unit's impartial handling. Receipt should be acknowledged within a few days, and outcomeoriented feedback should be provided within a few months, unless legal constraints require otherwise. A standardized intake, triage, and escalation protocol should include conflictofinterest checks, consideration of legal privilege, early preservation of evidence, and safeguards against prohibited tippingoff, particularly where financial crime or marketabuse risks are implicated. Methods for interviews and forensic measures are execution topics, see **Part III** (Employee Interviews) and **Part IV** (Data/Document Screening and Physical Searches) of this Briefing Series.



CONTROLS, MONITORING, METRICS, AND ASSURANCE

Preventive and detective controls should be embedded directly into business processes, supported by secondline monitoring and periodic testing. A defined suite of *KPIs* should track, among other things:

- speakup activity and reporting channels usage,
- timeliness of intake and triage,
- investigation cycle times,
- recurring rootcause patterns,
- timeliness and effectiveness of remediation,
- policy attestations,
- training completion and coverage, and
- the performance of key controls.

Where appropriate, obtaining voluntary **external assurance** over the *CMS* under *IDW PS 980* can further strengthen board oversight and provide additional external credibility.

DOCUMENTATION BACKBONE

Maintain a **documentation spine** that supports contemporaneous management awareness and later scrutiny: risk assessment workpapers, policy versions and attestations, training evidence, monitoring and testing results, investigation files, remediation trackers, and minutes of management reviews and board briefings.

REPORTING ARCHITECTURE AND DECISION-MAKING

DECISION RIGHTS AND ESCALATION MATRICES

A clear **decisionrights matrix** should be defined for highstakes compliance actions, including:

- case scoping and prioritization,
- approval of forensic measures and dawnraid preparedness,
- authorization of interviews and interview sequencing,
- engagement and mandate of external counsel or forensic experts,
- determination and preservation of legalprivilege protocols,
- decisions on external reporting to authorities,
- suspension or offboarding of counterparties,
- disciplinary actions,
- approval of control remediation measures, and
- notifications to the supervisory board.

Decision criteria should be riskbased and consider, in particular, the severity and credibility of the allegations, potential legal, financial, and reputational exposure, involvement of senior leadership, and crossborder implications. For applicable thresholds and timing requirements relating to ad hoc disclosures and insiderlist management, reference is made to **Part I** of this series.

STRUCTURED REPORTING TO MANAGEMENT

Management should receive regular and ad hoc **reporting** that consolidates material compliance risks, incidents and outcomes, remediation progress and control enhancements, policy and training developments, results of monitoring and testing activities, and relevant assurance findings. The audit committee should be provided with a consolidated, systemlevel view focusing on overall *CMS* effectiveness, emerging trends, and systemic issues, and should actively track remediation measures through to closure. Matters involving senior leadership or indicating material or systemic control deficiencies should be escalated immediately.

CLOSURE DISCIPLINE

Each significant case should conclude with a **documented analysis**, and a **remediation package** addressing control redesign, process enhancements, targeted training refreshers, and, where applicable, counterparty measures. **Lessons learned** should be systematically fed back into the compliance risk assessment, relevant policies, and training curricula to strengthen prevention. Considerations relating to disciplinary actions and potential amnesty are addressed in **Part VII** of this series.

Governance blueprint: roles, mandates, and reporting lines

Function	Core mandate	Primary management reporting	Supervisory board interface
First line (business/functions)	Process ownership and control operation; issue remediation	Operational reporting to business leadership; issue logs to compliance	Aggregated view via compliance and internal audit
Compliance (second line)	CMS framework, risk assessment, policies, advice, monitoring, case intake/triage, escalation	Quarterly to CEO/GC and executive risk/ compliance committee	Periodic to audit committee; ad hoc on material matters
Internal Audit (third line)	Independent assurance over ICS/ RMS/CMS and remediation	Management response tracking and follow-up	Plan approval and results oversight by audit committee
Specialized officers (e.g., AML, DPO, LkSG)	Regime-specific duties and regulator interfaces	To designated executive sponsor and compliance	Where material, periodic briefings to audit committee

Notes: The table is illustrative and should be tailored to company size, sector, and listing status. Dual reporting lines should preserve second- and third-line independence and direct access to the audit committee chair.

IMPLEMENTATION ROADMAP AND OPERATING DISCIPLINE

DIAGNOSTIC, CHARTERING, AND ROADMAP

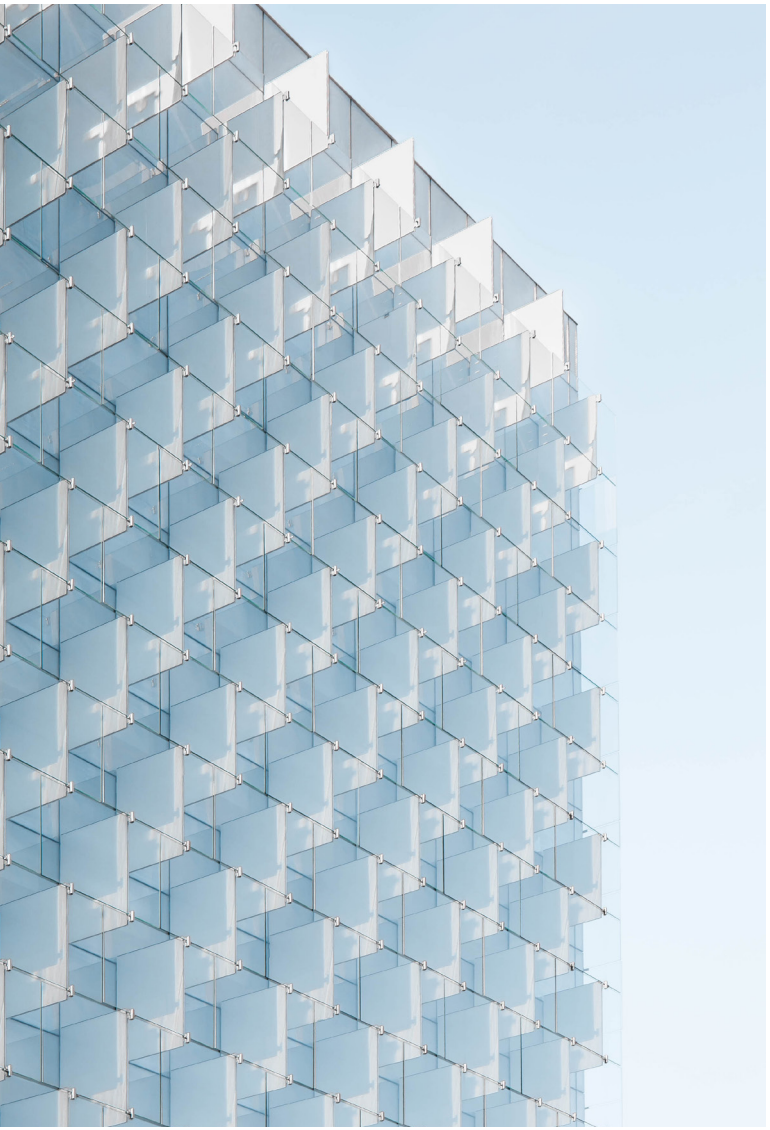
Start with a structured **gap assessment** benchmarked against ISO 37301 and the elements expected under German practice, calibrated to the company's specific risk profile. Based on the findings, develop a compliance charter that clearly defines the *CMS* scope, mandates, decision and escalation rights, and safeguards for independence. Management should then approve **a two to threeyear CMS maturity roadmap**, sequenced by risk and complexity, and align oversight milestones with audit committee agendas.

CASE MANAGEMENT WORKFLOW AND SERVICE LEVELS

Establish a standardized **casemanagement framework** covering intake channels, triage categories, decisionrights thresholds, evidence preservation, conflictofinterest checks, and closure documentation. Statutory servicelevel requirements under the *HinSchG* (acknowledgment and feedback timelines) and the complaintshandling obligations under the *LkSG* should be embedded by design. Clearly delineate interfaces with Legal, Human Resources, Data Protection, and IT Forensics to ensure seamless coordination. For detailed guidance on interviewing standards and data screening protocols, reference **Part III** and **Part IV** of this series.

SYSTEMS, METRICS, AND OVERSIGHT

Support the CMS with appropriate systems, including a **casemanagement tool** with rolebased access controls, a **policymanagement platform** offering version control and attestations, and a **training solution** with completion and coverage analytics. Define a robust set of KPIs that management and the audit committee can consistently rely on. A quarterly compliance or risk committee, typically chaired by the CEO or General Counsel, should review performance insights, prioritize remediation actions, and determine the content and focus of boardlevel reporting.



SPECIAL TOPICS AND CURRENT DEVELOPMENTS

LKSG PRACTICE AND ENFORCEMENT

The core duediligence architecture of the ***LkSG*** remains fully operative, including risk management, periodic and eventdriven risk analyses, preventive and remedial measures, and an accessible complaints mechanism. While BAFA's announcements in 2025 scaled back routine reviews of company reports and signaled a narrower enforcement focus as legislative amendments are prepared, and comprehensive reviews of report submissions were deferred, riskbased *ex officio* audits continue. The substantive duediligence obligations therefore remain intact. Companies should maintain robust documentation, conduct stakeholderfocused and riskbased analyses, and operate accessible and barrierfree complaints channels. At EU level, upon implementation into national laws of the EU Member States, the **Corporate Sustainability Due Diligence Directive** *(CSDDD)* will reshape scope and obligations over the coming years. Designing scalable and adaptable processes now can help avoid costly rework later.

MULTINATIONAL ALIGNMENT AND LOCAL NUANCE

For **multinational groups**, a centrally designed *CMS* aligned with *ISO 37301* can provide a coherent global backbone. At the same time, **local addenda** are essential to reflect jurisdictionspecific requirements, including labor codetermination, dataprotection rules, whistleblowing frameworks, and sectorspecific regulation, particularly in Germany. Groupwide servicelevel agreements should clearly define impartial handling standards, access rights, language coverage, and escalation pathways. The role and rights of employee representatives under German law are addressed in **Part VI** of this series.

CONCLUSION

An effective compliance organization starts with a clear mandate, proportionate design, and demonstrable independence. In Germany, the board's duties to properly organize and monitor the enterprise, heightened for listed companies, form the legal baseline, while the *DCGK* has evolved into a practical standard for describing the CMS and assessing its adequacy and effectiveness.

Specialized statutory regimes translate general principles into concrete organizational requirements, defined service levels, and disciplined documentation practices. To achieve **international credibility**, implementation typically aligns with *ISO 37301*, is structured along a **threelines model**, and is supported by systematic internal monitoring and, where appropriate, external assurance to reinforce both board oversight and external communications.

Key operating imperatives include clearly defined decision rights, disciplined escalation and reporting, robust documentation and metrics, and continuous improvement grounded in incident analysis and integrated assurance. Where compliance execution intersects with interviewing, data screening, data processing, or codetermination requirements, organizations should align their approach with the guidance set out in **Parts III** through **VI** of this Briefing Series.

TALK TO US

ASSOCIATE
PAULINE STADLER
EMPLOYMENT & BENEFITS
FRANKFURT +49 69 7941 0
PSTADLER@MAYERBROWN.COM

PARTNER
HAGEN KÖCKERITZ
EMPLOYMENT & BENEFITS
FRANKFURT +49 69 7941 2323
HKOECKERITZ@MAYERBROWN.COM

MAYER | BROWN