Deloitte.
Legal



Key Functions and Governance Mapping under BRUBEG

Regulatory requirements, structuring options, and initial practical experience

October 7, 2026 | Deloitte Legal Webcast

MAKING AN IMPACT THAT MATTERS since 1845

Today’s Speakers

Dr. Lars Hinrichs

Deloitte Legal Rechtsanwaltsgesellschaft mbH

Employment & Pensions

Attorney at Law, Certified Specialist in Labor Law

Partner

Phone: +49 40 3785 3828
Email: lhinrichs@deloitte.de





Dr. Mathias Hanten

Deloitte Legal Rechtsanwaltsgesellschaft mbH

Banking & Finance

Attorney

Partner

Phone: +49 69 7191 88424
Email: mhanten@deloitte.de

Leonie Scharwächter

Deloitte Legal Rechtsanwaltsgesellschaft mbH

Employment & Pensions

Attorney

Counsel

Phone: +49 40 3785 3815
Email: lscharwaechter@deloitte.de





Franz Schlothofer

Deloitte GmbH, an audit firm

Strategy, Risk & Transactions

Senior Consultant

Phone: +49 341 99270 599
Email: fschlothofer@deloitte.de

Our Agenda for Today

01 Overview: BRUBEG Updates

02 Identification of key function holders

03 Assessment of the suitability of key function holders

04 Governance Mapping

05 Q&A



Prologue: Legal Rules and Principles

Prologue: Legal Regulations and Foundations

People, Tasks, and Responsibility in the European Governance Concept

Legal and supervisory framework

CRD VI | BRUBEG / KWG | EBA Guidelines | MaRisk

Person-Centered Approach

Key Functions

Identify significant influence,
determine function and responsibilities,
and assess suitability and ensure it is maintained on an ongoing basis.

Suitability requires Task-based approach – Governance requires accountable individuals.

Organizational perspective

Governance Mapping

Map tasks and responsibilities
Visualize reporting and escalation paths
identify interfaces and gaps

Key Question

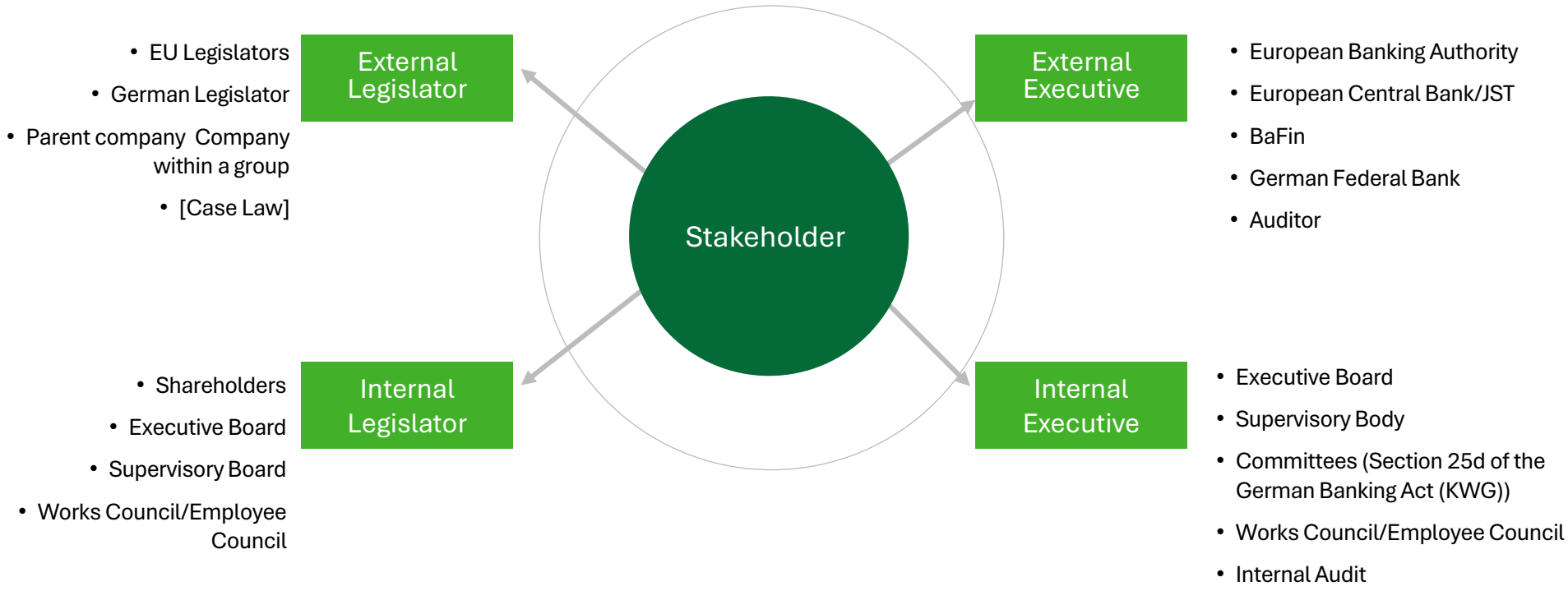
Are tasks, authorities, and reporting lines assigned in such a way that responsibility is transparent and verifiable?

People and the architecture of responsibility must be considered together.

** A Material Risk Taker is not automatically a key function.*

Prologue: Legal Rules and Foundations

Stakeholders



Overview: New Provisions in BRUBEG

BRUBEG Updates

Key Functions: Overview of the New Regulations (1/2)

- Section 1(2b) and (2d) of the German Banking Act (*Kreditwesengesetz, KWG*): Definition of “holders of key functions” and “holders of special key functions”

- Section 6(3) KWG: BaFin’s authority to issue orders (now also) to holders of key functions that are appropriate and necessary to prevent or stop violations of supervisory regulations or enforceable orders issued by the supervisory authority, or to prevent or eliminate irregularities within an institution that could jeopardize the security of the assets entrusted to the institution or impair the proper conduct of banking business or financial services;

- *Section 24(1)(15b) and (16), as well as (2a) and (3a), sentence 1, nos. 6 and 7 KWG: Reporting obligations upon the appointment and removal of holders of specific key functions at large companies, and upon becoming aware of new facts that significantly affect the initial assessment of the reliability, suitability, expertise, or sufficient availability of holders of specific key functions*

- Section 25e KWG: Requirements for holders of key functions, institutional obligations to ensure the proper performance of key functions, and BaFin’s powers to intervene in the event of non-compliance with the requirements

Changes to the BRUBEG

Key Functions: Overview of the New Regulations (2/2)

- Section 25c(4a) (7) /(4b) sentence 2 No. 7 KWG: Responsibility of senior management regarding appropriate policies and procedures to ensure compliance with the requirements of Section 25e(1) of the KWG

- Section 25d (11) sentence 1 No. 5 KWG: Expansion of the nomination committee's supporting role in reviewing management's principles for the selection and appointment of key function holders

- Section 50(1) sentence 1 KWG: Authority of BaFin to impose a periodic penalty payment on holders of key functions in the event of a persistent violation of the KWG or the associated regulations, Regulation (EU) No. 575/2013 (CRR), or enforceable orders issued by BaFin

Identification of persons in key functions

Identification of key function holders

Definition of key function holders

Section 1(2b) KWG:

Persons who exert significant influence on the management of the institution but who are neither executives nor members of the administrative or supervisory body.

Determination based, among other things, on the following parameters:

- duties and responsibilities
- the individual's influence on corporate management
- Hierarchical level/reporting line to senior management
- Decision-making authority and influence on the risk profile
- Criticality of the function for business operations and for compliance with regulatory requirements regarding proper business organization
- (Regulatory) legal obligation to establish the function (e.g., anti-money laundering officer pursuant to Section 7(1), sentence 1 of the Anti-Money Laundering Act (GwG))

In any case, this includes:

No uniform definition:
Classification is always the result of an institution-specific assessment, taking into account the business and risk strategy, the associated risk profile, and the institution's organizational structure, in accordance with the prudential principle of proportionality.

Holders of specific key functions
(Section 1(2d) KWG):

- Head of Risk Control
- Head of Compliance
- Head of Internal Audit
- Head of Finance (CFO)

(unless they are members of management)

Identification of key function holders

Starting point: An appropriate framework for conducting the identification



Recommended approach for analyzing the holders of key functions within the institution:

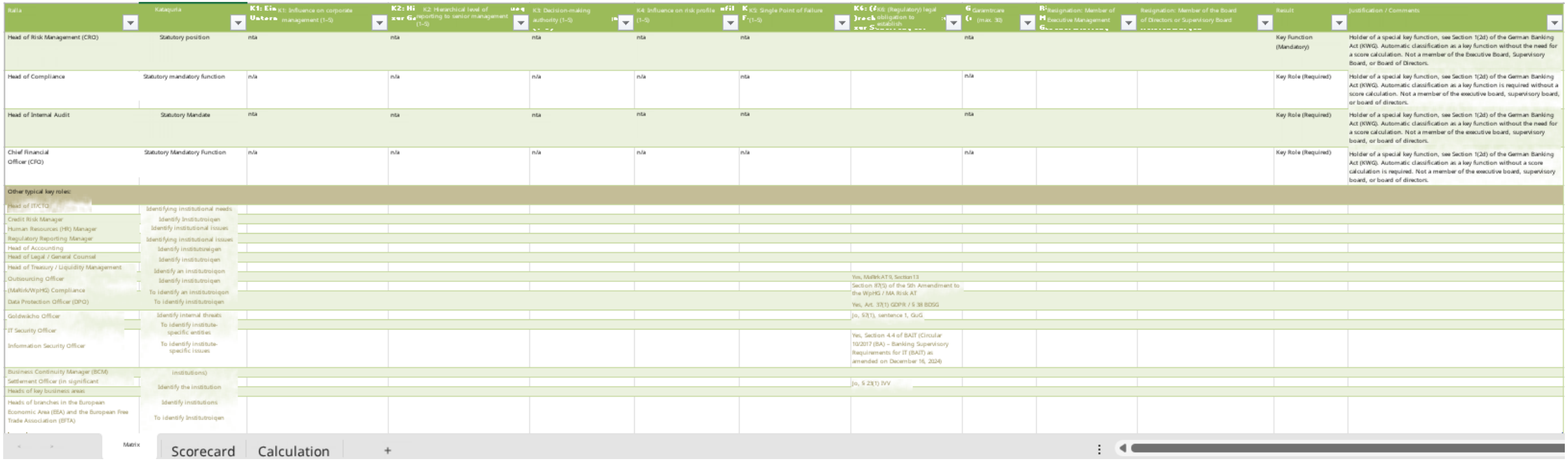
1. Mapping of all management, control, and governance functions
2. Evaluation based on defined criteria
3. Documented overall assessment and final decision
4. Regular review in the event of organizational changes

Distinction from Material Risk Takers (MRT):

MRT = Impact on the institution's risk profile
Key function = Impact on the institution's management

Identification of key function holders

Possible approach for appropriate assessment: Assessment matrix



Rolle	Kategorie	K1: Einfluss auf Unternehmensführung (1–5)	K2: Hierarchische Ebene der Berichterstattung an Geschäftsleitung (1–5)	K3: Entscheidungsbefugnis (1–5)	K4: Einfluss auf Risikoprofil (1–5)	K5: Single Point of Failure (1–5)	K6: (Gesetzliche) Pflicht zur Bestellung	Garantiecare (max. 30)	Rücktritt: Mitglied der Geschäftsleitung	Rücktritt: Mitglied des Vorstands oder Aufsichtsrats	Ergebnis	Begründung / Anmerkungen
Head of Risk Management (CRO)	Statutory position	n/a	n/a	n/a	n/a	n/a		n/a			Key Function (Mandatory)	Holder of a special key function, see Section 1(2d) of the German Banking Act (KWG). Automatic classification as a key function without the need for a score calculation. Not a member of the Executive Board, Supervisory Board, or Board of Directors.
Head of Compliance	Statutory mandatory function	n/a	n/a	n/a	n/a	n/a		n/a			Key Role (Required)	Holder of a special key function, see Section 1(2d) of the German Banking Act (KWG). Automatic classification as a key function is required without a score calculation. Not a member of the executive board, supervisory board, or board of directors.
Head of Internal Audit	Statutory Mandate	n/a	n/a	n/a	n/a	n/a		n/a			Key Role (Required)	Holder of a special key function, see Section 1(2d) of the German Banking Act (KWG). Automatic classification as a key function without the need for a score calculation. Not a member of the executive board, supervisory board, or board of directors.
Chief Financial Officer (CFO)	Statutory Mandatory Function	n/a	n/a	n/a	n/a	n/a		n/a			Key Role (Required)	Holder of a special key function, see Section 1(2d) of the German Banking Act (KWG). Automatic classification as a key function without a score calculation is required. Not a member of the executive board, supervisory board, or board of directors.
Other typical key roles:												
Head of IT/CTO	Identifying institutional needs											
Credit Risk Manager	Identify institutional issues											
Human Resources (HR) Manager	Identifying institutional issues											
Regulatory Reporting Manager	Identify institutional issues											
Head of Accounting	Identify institutional issues											
Head of Legal / General Counsel	Identify institutional issues											
Head of Treasury / Liquidity Management	Identify an institutional issue											
Outsourcing Officer	Identify institutional issues						Yes, MaRisk AT 9, Section 13					
(MaRisk/WpHG) Compliance	To identify an institutional issue						Section 87(5) of the 5th Amendment to the WpHG / MA Risk AT					
Data Protection Officer (DPO)	To identify institutional issues						Yes, Art. 37(1) GDPR / § 38 BDSG					
Goldwäsche Officer	Identify internal threats						Jo, 5/7(1), sentence 1, GuG					
IT Security Officer	To identify institute-specific entities											
Information Security Officer	To identify institute-specific issues						Yes, Section 4.4 of BAIT (Circular 10/2017 (BA) – Banking Supervisory Requirements for IT (BAIT) as amended on December 16, 2024)					
Business Continuity Manager (BCM)	institutions)											
Settlement Officer (in significant	Identify the institution						Jo, § 23(1) IVV					
Heads of key business areas												
Heads of branches in the European Economic Area (EEA) and the European Free Trade Association (EFTA)	Identify institutions To identify institutional issues											

Matrix | Scorecard | Calculation | +

Identification of key function holders

Current Issues in Regulatory Practice Regarding the Identification of

Parameters	Specific question(s)
Head of Finance and CFO as a member of management (Section 1(2d) KWG))	• Identification of the holder of the key position of Head of Finance in a centralized organizational structure (CFO also serving as Head of Finance)
Deputies to the Heads of Internal Control Functions (Section 1(2d) KWG)	• (Also) Identification of the deputies to the heads of internal control functions as holders of key positions within the meaning of Section 1 (2d) KWG
Heads of internal control functions whose obligation to perform their duties has been suspended (Section 1(2d) KWG)	• Continued identification of the holder of the internal control function as a holder of a special key function even during maternity leave/parental leave, sabbatical, or caregiving leave
External third parties as holders of the respective key functions (Section 1(2b) of the German Banking Act (KWG))	• Required inclusion of third parties in the identification process, particularly when externally appointing the legally required officers (e.g., anti-money laundering officer, compensation officer)
Changes to the business and risk strategy during the fiscal year (Sections 1(2b), 25e KWG)	• Review of the identified holders of key positions in the event of a material change to the business and risk strategy during the fiscal year • Permissibility of changes to the valuation matrix
Process: Event-Driven Review	• Definition of the relevant case categories for event-driven reviews (as illustrative examples, e.g., material changes to the business strategy and/or risk profile, changes to authority or signing regulations, consolidation or separation of key functions, new material outsourcing arrangements)

Assessment of suitability (Fit&Proper) of key function holders

Assessment of the suitability of key function holders

Overview

BRUBEG establishes new requirements for holders of key functions in Section 25e KWG.

These include:

- **Professional competence and reliability** (Section 25e(1) KWG)
- The institution's **duty to ensure compliance** : The proper performance of key functions must be ensured; unsuitable persons must be replaced by the institution (Section 25e(2) KWG)
- **BaFin's powers of intervention** with respect to holders of specific key functions (Sections 25e(3), 6(3) KWG)

Professional competence and integrity include ongoing regulatory obligations:
The criteria must be met upon initial appointment and thereafter on an ongoing basis throughout the entire duration of the performance of the relevant key function.

Assessment of the suitability of key function holders

Overview: Professional Qualifications and Reliability

	Suitability	Integrity
01 Characteristic	The criterion of professional competence for individual holders of key functions is not legally defined in the KWG. The EBA and ESMA, in EBA/GL/2021/06, as well as BaFin in its circular, have stated that the substantive requirements can be determined by referring to the guiding principles for the professional competence of management bodies. Accordingly, holders of key functions must possess sufficient knowledge, skills, and experience with respect to the professional and management-related activities associated with the specific key function, whereby the role and responsibilities of the specific position must be taken into account when assessing knowledge, skills, and experience.	Unlike professional suitability, integrity does not require positive proof. From a supervisory perspective, integrity is presumed unless there are specific facts that give cause to doubt it. Relevant indicators of potential unreliability include, in particular, criminal investigations or convictions, financial crimes, tax offenses, and previous supervisory measures.
02 Sub-aspects	• Sufficient theoretical knowledge: Demonstrated through education, academic studies, courses, or training programs covering banking, business administration, law, taxation, or information technology; Option: Training programs • Sufficient practical knowledge: Relevance of the experience, the number of years of experience, and the level of management positions held in the respective field of activity of the key function; Option: Appropriate justification	Examples of lack of integrity: • Regulatory measures by BaFin that are or were directed against the individual or a company in which the individual served or serves as a member of management or a member of an administrative or supervisory body, • criminal offenses involving property or tax matters, money laundering offenses, • violations of regulatory provisions To be reviewed: Conflicts of interest

Assessment of the suitability of key function holders

Assessment Process

Step	Key Step	Content
1	Function-Specific Requirements Profile	• Definition of the role-specific target profile (with classification of individual requirements as essential/substantial/supplementary)
2	Information about the individual	• Collection of documents and supporting evidence
3	Professional Qualifications	• Conducting the target-actual assessment • using an appropriate assessment methodology (4/5-point scale; 4-point scale, e.g., with ratings (i) fully met, (ii) essentially met, (iii) room for improvement, (iv) requirement not met)
4	Integrity	• Conducting the qualitative review • Using an appropriate evaluation methodology (proven in practice: 3-level scale with gradations (i) No evidence of unreliability, (ii) Further review required, (iii) Unreliable)
5	Gap Analysis	• Assessment of the results of the review according to (3) and (4)
6	Decision	• Overall assessment of professional competence and reliability (including any action plan to be developed)
7	Documentation	• Registration and Follow-up

Assessment of the suitability of key function holders

Current Issues in Regulatory Practice Regarding the Methodology and Process of Suitability Assessments

Parameters	Specific Question(s)
Assessment Governance	• Definition of relevant responsibilities and appropriate involvement of key stakeholders in conducting the suitability assessment • Stakeholders who must be involved at a minimum: (i) Executive Management (overall responsibility), (ii) line managers with subject-matter expertise (confirmation of individual requirement profiles and technical assessment), (iii) HR/Committee Support (administrative support), (iv) Compliance
Assessment Process	• (Exclusive) collection of information via questionnaires ⇔ additional interviews with individual holders of the respective key functions
Process: Event-Triggered Re-Assessments	• Definition of the relevant case groups for event-driven reassessments (as illustrative examples, e.g., significant changes in duties and responsibilities/significant expansion of the specific key function, transition to another key function, significant changes in the institution's business strategy and/or risk profile, new material conflicts of interest)

Governance Mapping

Governance Mapping

From a Focus on Individuals to a Responsibility Architecture

Suitability requires a reference to duties—governance requires accountable individuals.

The suitability assessment alone does not answer the governance question.

It presupposes that the institution's tasks, authorities, reporting lines, and interfaces are truly understood.

WHO?

Individuals and Roles

Which roles shape management, oversight, and risk management?

WHAT?

Responsibilities and Authorities

What responsibilities, decision-making authority, and competencies actually exist?

HOW?

Reporting and Escalation Channels

How are information, decisions, and conflicts managed within the institution?

The following section focuses on making the actual accountability structure verifiable:

Opportunities for Influence | Decision-Making Authority | Reporting Lines | Escalation Channels | Independence | Documentation

Governance mapping is not just another organizational chart—it makes accountability visible.

Key Functions and Governance Mapping

Assessment of key functional relevance, opportunities for influence, and independence requirements

Assessment of actual scope for influence

- Analysis of the actual influence on senior management and on the institution’s strategic direction
- Assessment of material influence on the risk profile and key business decisions
- Review of direct and indirect decision-making authority regarding budget, personnel, product, and risk approvals
- Analysis of the actual position within the governance structure, regardless of the formal hierarchical level

Assessment of governance relevance

- Identification of essential functions for the proper organization of business operations
- Assessment of the criticality of the tasks performed for the management and oversight of the institution
- Assessment of institution-specific characteristics, taking into account size, complexity, and risk profile
- Analysis of the impact on regulatory compliance, risk management, and internal control systems

Analysis of reporting lines and escalation paths

- Review of direct reporting lines to the Executive Board and supervisory bodies
- Assessment of the effectiveness of existing escalation processes
- Analysis of involvement in governance, risk, and control committees
- Assessment of existing information and decision-making channels with regard to transparency and traceability

Review of organizational independence

- Analysis of potential conflicts of interest arising from multiple roles or overlapping responsibilities
- Review of authority to issue instructions and potential dependencies on supervised entities
- Assessment of the organizational separation of business and control functions

Regulatory Classification and Documentation

- Validation of the classification as a key function or special key function
- derivation of a robust regulatory rationale for classification and demarcation decisions
- Establishment of an audit-proof basis for special and annual financial statement audits

Key Functions and Governance Mapping

Key Implementation Measures

- Systematically map the existing governance structure—including all management, control, and support functions—and document it in accordance with the actual organizational and reporting lines.
- Present responsibilities, decision-making authorities, and escalation mechanisms transparently across the entire institution to ensure a clear assignment of governance tasks.
- Identify and evaluate functions that have a significant impact on business management, the risk profile, or the control environment.
- Review the governance structure for consistency with organizational charts, business allocation plans, guidelines, and the actual operational setup.
- Define key functions based on specific tasks, competencies, and scope of influence, and document them in a manner that is traceable under regulatory requirements.
- Integrate regulatory follow-up obligations—in particular, fit-and-proper requirements, suitability assessments, and documentation requirements—into the governance architecture at an early stage.
- Establish a regular review of the governance structure to promptly reflect changes in responsibilities, functions, and reporting lines.
- Create a robust documentation framework that enables a transparent presentation of the governance structure to regulators, auditors, and internal stakeholders.

Q&A

Thank you very much

for your attention

Your contact

Dr. Lars Hinrichs

Deloitte Legal Rechtsanwaltsgesellschaft mbH

Employment & Pensions

Attorney at Law, Certified Specialist in Labor Law

Partner

Phone: +49 40 3785 3828
Email: lhinrichs@deloitte.de





Dr. Mathias Hanten

Deloitte Legal Rechtsanwaltsgesellschaft mbH

Banking & Finance

Attorney

Partner

Phone: +49 69 7191 88424
Email: mhanten@deloitte.de

Leonie Scharwächter

Deloitte Legal Rechtsanwaltsgesellschaft mbH

Employment & Pensions

Attorney

Counsel

Phone: +49 40 3785 3815
Email: lscharwaechter@deloitte.de





Franz Schlothofer

Deloitte GmbH, an audit firm

Strategy, Risk & Transactions

Senior Consultant

Phone: +49 341 99270 599
Email: fschlothofer@deloitte.de

A part of Deloitte

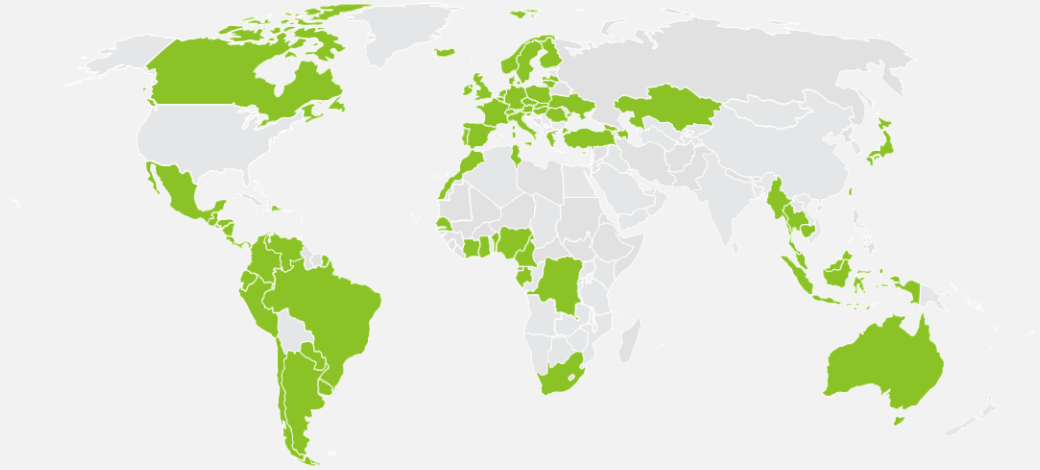
Renowned for our global reach and business expertise, one relationship opens the door to endless opportunities

We bring the scale and consistency of Deloitte Legal...

The Deloitte Legal practices share the same DNA and track record of getting things done.

70+ countries

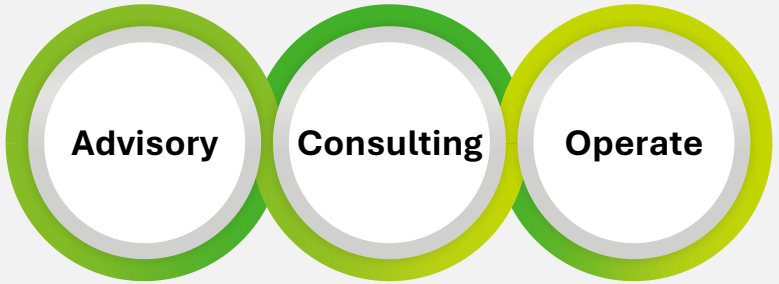
3,100+ legal-s professionals



collaborating seamlessly
across borders and with other Deloitte service lines

... with a different legal perspective

Traditional legal services provide event-based specialist advice. Deloitte seeks out solutions aimed at delivering lasting business value. Deloitte Legal offers an integrated legal service focused on delivering a solution to a business challenge or opportunity by leveraging our expertise in each of these key areas.



Jurisdictional advisory, legal function strategy, process, and technology, and outsourced legal managed services.

As part of Deloitte, our legal services are inherently ***broader***, ***global***, ***cross-functional***, ***industry-informed***, and ***technology-enabled***, with a focus on action and advice through our business-solution-centered approach.

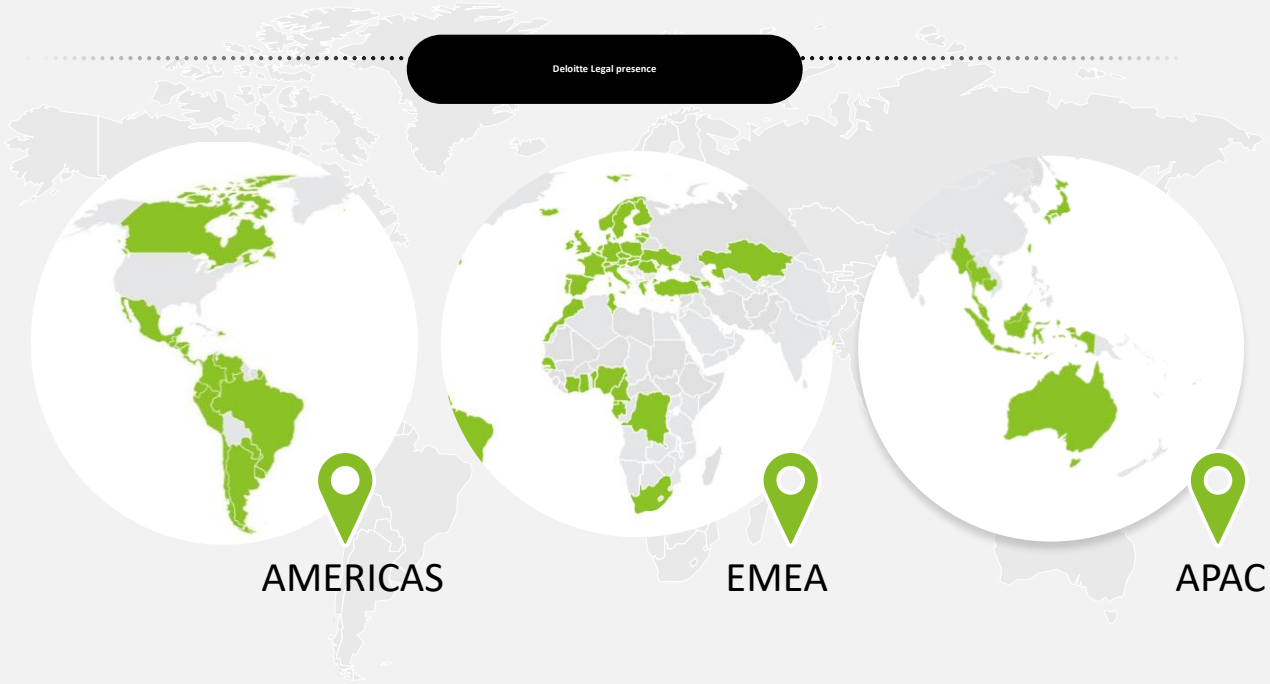
Deloitte Touche Tohmatsu Limited (DTTL) is the largest private professional services network in the world, with revenues of $70.5 billion in fiscal year 2025.
With more than 470,000 people worldwide, DTTL member firms provide services in audit, risk and financial advisory, tax, legal, and consulting through offices in more than 150 countries and territories.

A part of Deloitte

Renowned for our global reach and business expertise, one relationship opens the door to endless connections

We bring the scale and consistency of Deloitte...

...where Deloitte Legal practices share the same DNA and track record of getting things done.



collaborating seamlessly
across borders and with other Deloitte service lines

Deloitte Legal Practices

1. Argentina
2. Australia
3. Austria
4. Azerbaijan
5. Belgium
6. Benin
7. Brazil
8. Cameroon
9. Canada
10. Chile
11. Colombia
12. Costa Rica
13. Cyprus
14. Czech Republic
15. Democratic Republic of the Congo
16. Denmark
17. Dominican Republic
18. Ecuador
19. El Salvador
20. Equatorial Guinea
21. Finland
22. France
23. Gabon
24. Georgia
25. Germany
26. Ghana
27. Greece
28. Guatemala
29. Honduras
30. Hong Kong SAR, China
31. Hungary
32. Iceland
33. Indonesia
34. Ireland
35. Italy
36. Ivory Coast
37. Japan
38. Kazakhstan
39. Latvia
40. Lithuania
41. Luxembourg
42. Malaysia
43. Malta
44. Mexico
45. Morocco
46. Myanmar
47. Netherlands
48. Nicaragua
49. Nigeria
50. Norway
51. Panama
52. Paraguay
53. Peru
54. Poland
55. Portugal
56. Romania
57. Senegal
58. Singapore
59. Slovakia
60. South Africa
61. Spain
62. Sweden
63. Switzerland
64. Taiwan
65. Thailand
66. Tunisia
67. Turkey
68. Ukraine
69. Uruguay
70. United Kingdom
71. Venezuela

Deloitte Touche Tohmatsu Limited (DTTL) is the world's largest private professional services network, with revenues of $70.5 billion in fiscal year 2025.
With more than 470,000 people worldwide, DTTL member firms provide services in audit, risk and financial advisory, tax, legal, and consulting through offices in more than 150 countries and territories.

Deloitte.
Legal

Deloitte Legal refers to the legal advisory practices of the member firms of Deloitte Touche Tohmatsu Limited, their affiliates, or partner firms that provide legal services.

Deloitte refers to Deloitte Touche Tohmatsu Limited (DTTL), its global network of member firms, and their affiliates (collectively, the "Deloitte Organization"). DTTL (also referred to as "Deloitte Global") and each of its member firms, as well as their affiliates, are legally separate and independent entities that cannot assume obligations or make commitments on behalf of one another vis-à-vis third parties. DTTL, each DTTL member firm, and their affiliates are liable only for their own acts and omissions and not for those of the others. DTTL itself does not provide services to clients. For more information, visit www.deloitte.com/de/UeberUns.

Deloitte provides leading audit and advisory services to nearly 90% of the Fortune Global 500® companies and thousands of private companies. Legal services in Germany are provided by Deloitte Legal. Our people deliver measurable, long-term results that help strengthen public confidence in the capital markets and support our clients through change and growth. Deloitte builds on 180 years of history and operates in more than 150 countries. Learn more about how Deloitte's approximately 460,000 employees live out the mission statement "making an impact that matters" every day: www.deloitte.com/de.

This publication contains only general information, and neither Deloitte Legal Rechtsanwaltsgesellschaft mbH nor Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, nor their affiliates (collectively, the "Deloitte Organization") are providing a professional service through this publication. This publication is not intended to serve as a basis for making business or financial decisions or taking any action. For such matters, you should seek advice from a qualified advisor regarding your specific circumstances.

No statements, guarantees, or representations (whether express or implied) are made regarding the accuracy or completeness of the information in this publication, and neither DTTL nor its member firms, affiliates, employees, or agents shall be liable or responsible for any loss or damage of any kind arising directly or indirectly in connection with persons relying on this publication. DTTL and each of its member firms, as well as their affiliates, are legally separate and independent entities.

Key Functions and Governance Mapping

People, Roles, and Responsibilities in the European Governance Framework

Regulatory Levels: **CRD VI → BRUBEG / KWG → MaRisk → EBA Guidelines**

Two Perspectives

Person-Centered Approach

Key Functions*
- significant influence,
- identification,
- Determining suitability
- Continuously ensure suitability



** A risk-taker is not automatically a key function.*

Suitability requires a reference to duties—governance requires accountable individuals.

Organizational Perspective

Governance Mapping
- Tasks & Responsibilities
- Lines of Authority
- Reporting and Escalation Channels
- Interaction Between Functions



Considering People and Responsibility Structures Together

Practical Implementation Issues

Utilizing existing governance | Determining an appropriate level of detail | Delegation, representation, and interfaces | Timeliness

