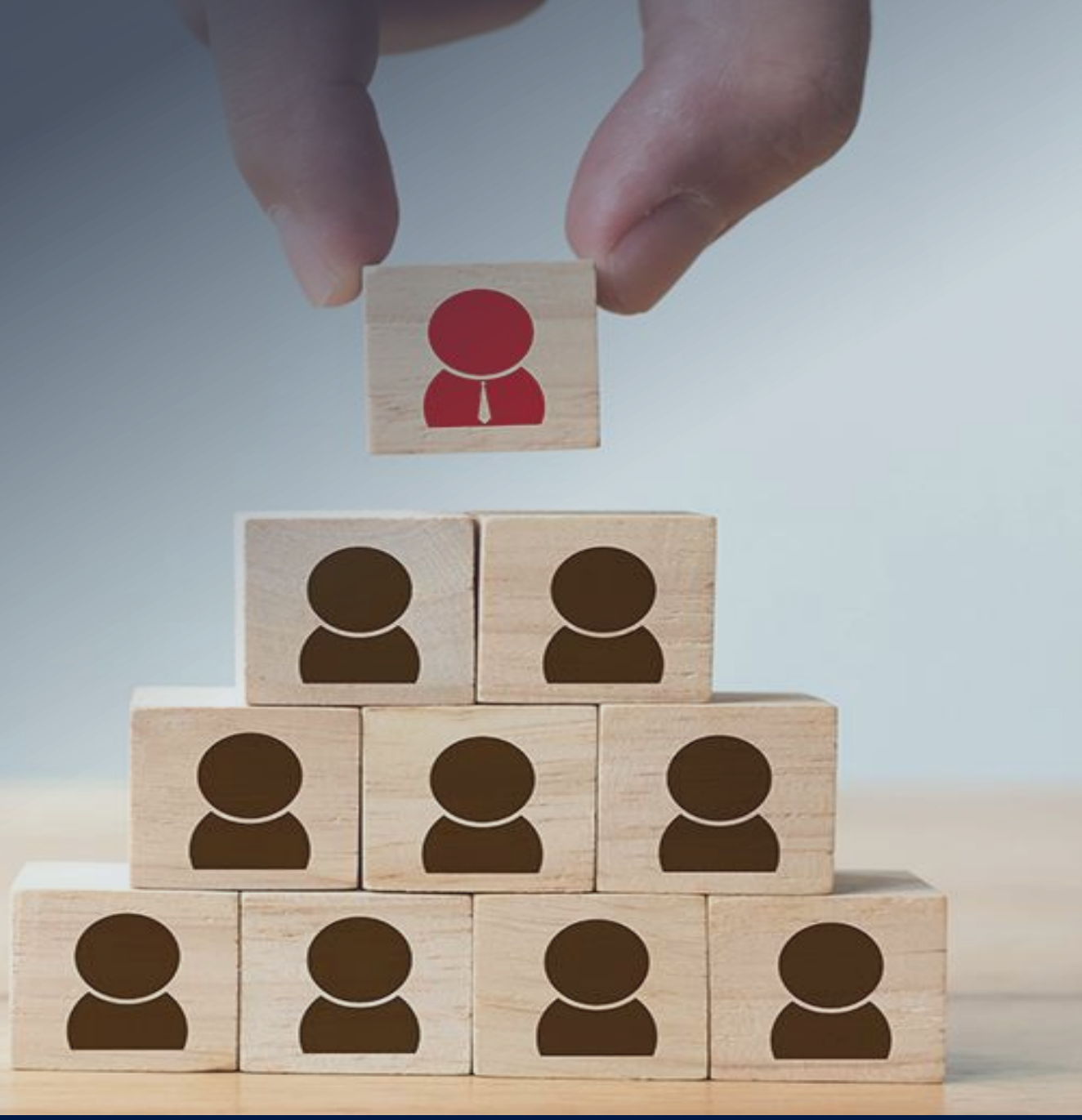
Management Solutions
Making things happen

Technical note on

Guidelines on internal governance

EBA´s consultation highlights



1. General overview
2. Proportionality
3. Role and composition of the management body and committees
4. Governance framework
5. Risk culture and business conduct
6. Internal control framework and mechanisms
7. Business continuity management
8. Transparency
9. Why Management Solutions?

1 General overview

Executive summary

The EBA revised Guidelines on internal governance under CRD VI will update the 2021 framework, reinforcing management bodies with role statements and mapping of responsibilities, strengthening independence and diversity requirements, integrating ESG and ICT risks, aligning business continuity with DORA, and tightening conflicts of interest and whistleblowing rules

Context

- **Article 74(3)** of the Capital Requirements Directive (**CRD**) mandates the EBA to develop **guidelines** on **governance arrangements** applicable to **credit institutions**, and Article 48g(9) extends this mandate to third-country branches.
- In **2021**, the EBA issued its **Guidelines on internal governance**, which reinforced the responsibilities of management bodies, the role of internal control functions and the need to establish a sound risk culture. These Guidelines were later complemented by the **ECB Guide on governance and risk culture**, published in 2024, which further detailed supervisory expectations in this area.
- As part of the roadmap for implementing the **banking package** (**CRR III and CRD VI**), which entered into force on 1 January 2025, the EBA published, the 6th of august, a **Consultation Paper** on the **draft revised Guidelines on internal governance** under the CRD. The aim of the revised Guidelines is to align **governance arrangements** with **legislative changes**, strengthen **supervisory expectations,** and harmonise **practices** across the EU.

Next steps

- The consultation period is open until **7 November 2025**.

Highlights

Proportionality	• Clearer articulation of how **proportionality** should be **applied**, with additional guidance on **expanding considerations to third-party service providers, ICT systems and third-country branches.**
Role and composition of the management body and committees	• Introduction of **individual role statements** and mapping of **responsibilities**; reinforced **independence** and **composition** of **committees**; **remuneration committee** to assess alignment of incentives with **ESG risks**.
Governance framework	• New obligations to maintain **transparent organisational structures**, to avoid **empty shells** or **letter-box entities**, and to ensure **consistent governance** across groups and third-country branches.
Risk culture and business conduct	• Stronger **focus** on **equality**, **diversity** and **inclusion**; monitoring of gender and pay **indicators**; broader **conflict of interest** rules; enhanced **whistleblowing** aligned with GDPR.
Internal control framework and mechanisms	• Clarified mandates and **independence** of **internal control functions**; explicit integration of **AML/CFT responsibilities** at board level; **risk management frameworks** extended to **ESG** and **ICT risks**.
Business continuity management	• **Alignment** with **DORA**, ensuring **ICT continuity**, documented and audited **contingency** and **recovery plans**, regular testing, staff training and reporting to the management body.
Transparency	• **Enhance** transparency by requiring **clear documentation** of governance arrangements and responsibilities, alongside **timely communication** of policies and material changes.

Access to Document

2 Proportionality
Principle tailored to size, complexity and risk profile of institutions

The proportionality principle ensures that governance requirements are tailored to each institution's size, complexity and risk profile, with revised Guidelines expanding considerations to third-party service providers, ICT systems and third-country branches

Proportionality:
aspects to consider

- When applying proportionality, institutions and competent authorities should take into account:
  - **Size and consolidation scope** of the institution and subsidiaries.
  - **Geographical presence** and **scale of operations** in each jurisdiction.
  - **Legal form**, including group membership and proportionality assessment.
  - **Listed status** of the institution.
  - **Use of internal models** for capital requirements (e.g. IRB approach).
  - **Authorised activities and services** performed.
  - **Business model and strategy**; **nature and complexity** of activities and organisational structure.
  - **Risk strategy, appetite and profile**, considering SREP capital and liquidity assessments.
  - **Ownership and funding structure**.
  - **Type of clients** (retail, corporate, SMEs, public entities) and contract complexity.
  - NEW **Involvement of third-party service providers and distribution channels**, beyond outsourcing only.
  - NEW **ICT systems explicitly include third-party service providers**, broadening scope from previous wording.
  - **Classification under CRR** as SME's or large institution.
  - NEW **New reference to third-country branches**, specifying whether they are:
    - **Qualifying third-country branches** as defined in CRD: those third-country branches that meet specific conditions on size, activities or importance, and are subject to enhanced supervisory requirements.
    - **Class 1 or 2 branches** under CRD: categories distinguishing branches by their risk profile and significance, with Class 1 branches subject to the most stringent requirements.

NEW New or updated compared to the EBA 2021 Guidelines.

3 Role and composition of the management body and committees

Clearer roles, stronger oversight and reinforced committees

Revised Guidelines reinforce the accountability of the management body, strengthen supervisory independence and require clearer responsibilities, robust committees and stronger risk culture

Role and responsibilities of the management body

- The **management body** has the **ultimate responsibility** for the **sound governance** of the institution. It shall define, oversee and be accountable for the implementation of governance arrangements, risk management processes and internal control mechanisms: these responsibilities cannot be delegated.
- NEW The revised Guidelines introduce **individual statements of roles and duties** and a comprehensive **mapping of responsibilities** for all members of the management body. They also require the management body to integrate **ESG risks** into the institution's strategy and risk appetite, and to ensure digital operational resilience in line with the **DORA**.

Management function of the management body

- The **management body** in its management function should actively engage in the **institution's business**, be responsible for implementing the strategies set by the supervisory function, **constructively challenge** and critically review information, and report comprehensively and without undue delay on material risks, decisions and developments.
- NEW A **member** of the **management body** in its **management function** may be **responsible** for an **internal control function**, provided that the member does not have other mandates that would compromise the member's internal control activities and the independence of the internal control functions. In addition, one member should be identified as responsible for the implementation of the AML/CFT framework under AMLD.

Supervisory function of the management body

- The **supervisory function** should **monitor** and constructively **challenge the institution's strategy** and include independent members in line with the ESMA and EBA **joint suitability guidelines**.
- It should oversee **management decision-making** and performance, **review governance**, **risk appetite**, **risk culture** and **remuneration policies**, ensure **independence** of control functions, and monitor **financial reporting** and the **internal audit plan**.

Role of chair of the management body

- The chair should **lead the management body, ensure effective overall functioning, contribute to an efficient flow of information, and promote open and critical discussion where dissenting views can be expressed**.
- NEW The chair should **be a non-executive member**; where executive duties are permitted, mitigating measures must be in place, and in line with the CRD, the chair must not simultaneously be CEO. The chair should also **set meeting agendas, prioritise strategic issues, and ensure decisions are well-informed with timely documentation**.

Committees of management body in supervisory function

- **Significant institutions** are required to **establish** a **risk committee**, a **nomination committee** and a **remuneration committee**. The revised Guidelines clarify that institutions may also set up **additional committees**, for example on ethics or AML/CFT, and allow smaller institutions to **combine committees** where justified. The **composition of committees** must ensure sufficient **expertise** and **independence**.
- NEW The revised Guidelines require that **committees** are **composed** mainly of **non-executive members**, include **independent** members, and consider the **rotation of chairs and members**. They also reinforce the cooperation between the remuneration and risk committees on ESG risks, and require committees to document agendas, deliberations and outcomes, including dissenting opinions.

NEW New or updated compared to the EBA 2021 Guidelines.

4 Governance framework

Transparency in frameworks, group and branch arrangements, and outsourcing oversight

Revised Guidelines strengthen organisational frameworks, promote transparency of structures, and reinforce governance across groups, third-country branches and third-party arrangements

Organisational framework and structure

- The management body must ensure a transparent organisational structure with independent control functions, clear reporting lines and adequate resources.
- NEW The revised Guidelines add a detailed **mapping of duties** and **individual statements of roles and duties**, to be updated, approved and shared with supervisors, ensuring accountability and avoiding empty shells or letter-box entities.
- NEW **Institutions** must also **know their structure**, which means having a comprehensive and up-to-date understanding of their legal, ownership and operational arrangements. Institutions are required to **keep documentation describing** their **structure**, **subsidiaries** and **interconnections**, and make this information available to competent authorities upon request.
- **Institutions** should **avoid opaque** or **complex structures** without **clear economic purpose**, as they may enable financial crime. The management body must assess and approve such structures only if risks are identified, managed and reported, ensure proper documentation, and apply the same governance standards to non-standard or non-transparent client activities.

Organisational framework and third-country branches

- NEW In a **group context**, **parent institutions** are **responsible** for ensuring that **governance arrangements** are consistent and effectively applied throughout the **group**. The revised Guidelines stress the **importance of integration**, requiring that internal control functions such as risk management, compliance and internal audit operate with sufficient authority, independence and resources at both parent and subsidiary level.
- NEW For **third-country branches**, the Guidelines provide more **detailed expectations** regarding their **internal governance arrangements**. Branches must demonstrate sufficient local substance, including a local management committee with clear roles and responsibilities, and independent risk management, compliance and internal audit functions.
- NEW **The competent authority** must be able to **assess** whether a **branch's governance framework** ensures **sound and prudent management of activities** within the **EU**. Institutions are therefore required to document the governance set-up of their branches and ensure that internal controls are effective and aligned with the wider group framework.

Third-party risk management body

- NEW Institutions are required to establish a comprehensive **third-party risk management policy** covering all **outsourcing** and **other material third-party arrangements**. The policy must identify, assess, monitor and manage risks associated with third parties, ensuring that these do not compromise governance and control frameworks.
- NEW The revised Guidelines **emphasise** that **outsourcing arrangements** must **not lead** to an **undue increase in operational** risk or **undermine the quality of internal governance**. Institutions are expected to retain sufficient skills and resources in-house to effectively monitor outsourced functions.
- NEW Finally, the policy must include **exit strategies**, **contingency plans** and **regular performance reviews** of **third parties**. This ensures that institutions can manage disruptions, safeguard continuity of critical functions and remain compliant with supervisory expectations and the EBA Guidelines on outsourcing.

NEW New or updated compared to the EBA 2021 Guidelines.

5 Risk culture and business conduct
Reinforcing risk culture, values, conflicts of interest and whistleblowing

Guidelines strengthen risk culture and conduct by embedding equality, diversity, and ethical values, reinforcing conflict-of-interest safeguards, and ensuring robust whistleblowing protections

Risk culture

- NEW Stronger emphasis on **equality, diversity, and inclusion** within the risk culture, including explicit reference to preventing discrimination and harassment.
- Clarification that **business units** (not only risk/control functions) are primarily responsible for day-to-day risk management, under the oversight of the management body.
- Reinforcement of **tone from the top**: management body should set and communicate the institution's core values, and staff behaviour should reflect them.
- Introducing detailed **indicators** to monitor staff representation and equal treatment (e.g. gender representation across levels/committees, succession planning, training days by gender, complaints regarding discrimination or equal pay).

Corporate values and code of conduct

- Obligation for the management body to **develop, adopt, adhere to, and promote high ethical standards**, ensuring implementation through codes of conduct or similar instruments. Policies must be **gender neutral**, covering recruitment, career development, succession, training, and mobility.
- NEW Institutions should use **additional indicators** to monitor the development of the representation and **equal treatment** of staff of different genders and take the results of their monitoring into account within their approach to **manage staff**.

Conflict of interest at institutional level

- Scope clarified: policy must cover **all institutions within a group** (consolidated or sub-consolidated basis).
- NEW New rules for **simultaneous exercise of functions** (e.g. CEO and Chair, or cross-appointments within a group) to avoid conflicts of interest.
- NEW Requirement to **document and assess** actual or potential conflicts at management body level, ensuring independence of decision-making.
- NEW Strengthened expectations for **segregation of duties** and **information barriers** to mitigate conflicts of interest.

Conflict of interest for staff

- Expanded coverage to include not only **present interests** but also **past personal/professional relationships** that may still influence staff behaviour.
- Explicit list of conflict situations: **economic interests, family relationships, external stakeholders, employment history, political influence**.
- Obligation to ensure proper **reporting and disclosure processes**, with responsibilities clearly defined.
- Policies must ensure that conflicts disclosed are **assessed, managed, documented, and reported** to the management body.

Internal alert procedures

- Institutions must implement **specific, independent, and autonomous whistleblowing channels**.
- Enhanced **confidentiality and data protection** requirements (alignment with GDPR).
- Stronger **protection against retaliation** for staff reporting breaches.
- New detailed requirements: documentation in staff handbooks, confirmation of receipt, record-keeping, tracking of investigations, escalation to competent authorities when needed.

Reporting breaches to competent authorities

- Competent authorities should establish **effective and reliable mechanisms** for staff to report actual or potential regulatory breaches.
- Introduction of **dedicated whistleblowing departments/units** for handling reports.
- Reinforced requirements on **data protection** for both the reporting person and the person allegedly responsible (GDPR alignment).
- Authorities may encourage staff to **first use internal alert procedures**, while preserving the right to external reporting..

NEW New or updated compared to the EBA 2021 Guidelines.

6 Internal control framework and mechanisms

Strengthening risk frameworks, compliance, and independence of control functions

The updated Guidelines strengthen the independence and proportionality of internal control functions, broaden risk frameworks with ESG and AML/CFT, and enhance compliance and audit oversight

Internal control framework

- NEW The revised Guidelines move away from **prescriptive references** and instead require institutions to embed a **risk-control and compliance culture**. The framework should be **tailored** to the institution's complexity, risk profile and group context, ensuring **effective information exchange** across management, business lines and control functions.
- Emphasis is placed on **AML/CFT,** requiring institutions to implement processes to **identify, assess and mitigate ML/TF risks**, raise staff awareness; safeguard operational; and reputational integrity and ensure **effective operations, prudent conduct, reliable reporting and compliance** with regulatory requirements.

Implementing framework

- Institutions are required to establish and maintain **written internal control policies**, formally approved by the management body, with a **clear allocation of responsibilities** and **adequate segregation of duties**. Internal control functions should verify implementation through **regular reporting**, propose corrective measures and ensure **timely follow-up**.

Risk management framework

- NEW The Guidelines now require a **holistic risk management framework** covering all business lines and internal units, with explicit integration of ESG risks. Institutions must **assess ESG risks** not only in the short and medium term but also over a **long-term horizon of at least 10 years**, considering channels through which environmental, physical and transition risks may impact prudential soundness. The framework must be **aligned with the EBA Guidelines on ESG risk management**.
- The framework continues to ensure **comprehensive coverage** of risks across entities, with **clear policies**, **risk appetite limits**, **escalation procedures**, independent reviews and **effective communication** throughout the institution.

New products & changes

- NEW The Guidelines refine the scope of the **NPAP**, explicitly covering **third-party arrangements** and **ICT change processes**, and requiring alignment with the institution's **risk strategy and appetite**.
- The NPAP should cover **material transactions** such as mergers and restructurings, with **clear procedures for risk assessment, compliance checks and resource adequacy**, ensuring that **risk management and compliance functions** have a central role.

Internal control functions

- NEW In accordance with the CRD, the scope is clarified to include **risk management**, **compliance and internal audit**, with **AML/CFT responsibilities reinforced** and new wording allowing operational tasks to be performed by **third-party providers under proportionality**, while keeping accountability with the management body and function heads. AML/CFT compliance must now follow **AMLR**, replacing older references to AMLD.
- NEW The new text highlights **safeguards against conflicts of interest**, including objective KPIs and independent appraisal. The ability to escalate concerns directly to the supervisory function is maintained, with added emphasis on **mapping of duties and individual statements**.
- NEW Internal control functions must now be independent not only from **business lines** but also from the **management body in its management role** and from senior management. They should have sufficient authority and standing to escalate issues directly to the supervisory function whenever necessary.
- NEW The **combination of risk management and compliance** is permitted only under strict proportionality, while the **internal audit function must remain separate**.
- NEW Resources requirements are expanded, underlining the need for **qualified staff, ongoing training and adequate ICT systems**.

NEW New or updated compared to the EBA 2021 Guidelines.

7 Business continuity management

Stronger business continuity planning, alignment with DORA, and regular resilience testing

Revised Guidelines reinforce BCM with stronger integration of ICT risks, alignment with DORA, and systematic testing to ensure resilience against severe disruptions

Business continuity management

- NEW Institutions should establish a **sound and comprehensive BCM** framework that encompasses business continuity policies, contingency arrangements, and response and recovery plans. The objective is to ensure the institution's ability to continue operating on an ongoing basis and to limit financial, operational, legal and reputational losses in the event of severe business disruption. This represents a stronger and more prescriptive approach compared to the 2021 Guidelines.
- NEW BCM must be **fully consistent with the DORA** on ICT business continuity policies. The revised Guidelines allow institutions to establish a **specific independent business continuity function**, which may also include the **ICT crisis management function** established under DORA.
- NEW Institutions should perform a **business impact analysis** to identify and measure, both **qualitatively and quantitatively**, the potential **impact** of severe business disruptions. The **analysis should cover all business lines and internal units**, including the RMF, take into account key interdependencies, and rely on internal and external data as well as scenario analysis. Its results should contribute to defining the institution's recovery priorities and objectives.
- NEW Based on the impact analysis, **institutions should establish business continuity and contingency plans** to ensure the ability to react to disruptions and maintain **important functions**. They should also **adopt response and recovery plans** for critical resources to enable a return to ordinary operations within an appropriate timeframe. Any residual risk from disruptions should be consistent with the **institution's risk appetite**.
- NEW Plans must be **formally documented, communicated and made accessible** to relevant staff, including through systems that are physically separated and available in case of emergency. They should also be **regularly tested, reviewed and updated**. Testing results, including any failures or deficiencies, must be documented and reported to the management body, which is responsible for overseeing improvements. The revised Guidelines place greater emphasis on **staff awareness, training and internal audit reviews** of business continuity arrangements, strengthening accountability at both management and operational levels.

NEW New or updated compared to the EBA 2021 Guidelines.

8 Transparency
Clear communication, consistent disclosure

Transparency requires institutions to clearly communicate strategies and policies to staff and to disclose governance and organisational structures, ensuring accountability, consistency and trust

Transparency

- **Relevant staff** must be informed of strategies, policies and procedures, and should clearly understand and follow them as part of their duties.
- The **management body** must **inform and regularly update staff about strategies and policies** in a clear and consistent manner, using written guidelines, manuals, or equivalent means.
- Institutions must **publish annually** a description of their legal structure, governance, and organisational framework, including all entities within the group as defined in Directive 2013/34/EU. The publication should include at least:
  - Overview of the **internal organisation** and group structure, with main **reporting lines**.
  - **Material changes** since the previous publication.
  - New **legal**, **governance** or **organisational** structures.
  - **Structure** and **members** of the **management body**, including independence, gender, mandate **duration**, and **number** of members.
  - Key **responsibilities** of the management body.
  - List and composition of **supervisory committees**.
  - Overview of the **conflict-of-interest policy**. **internal control framework and business continuity management framework**.

NEW New or updated compared to the EBA 2021 Guidelines.

9 Why Management Solutions?
Key aspects and differential value

MS has the necessary capabilities and proven experience to develop projects related to internal governance and control frameworks, which aim to ensure comprehensive risk management practices

1. MS has participated in the **definition, development and evolution of internal governance and control frameworks,** including **GRC** (Governance, Risk and Control) approaches in leading financial institutions, ensuring **comprehensive governance, risk and compliance management practices.**

2. Extensive experience in **supporting projects related to the EBA Guidelines related to risk management**, including: development of diagnostics, adaptation plans, deployment and execution of initiatives in *both G-SIBs* and *D-SIBs*, **with *benchmarking* capabilities and knowledge of best practices in the market.**

3. Extensive experience in **defining, reviewing and developing governance models, risk management models, risk appetite frameworks, control models**, **as well as updating institutional policies, procedures and methodologíes across key functions**.

4. Experience in defining and implementing **governance processes and GRC data models that link risk management with process management (including GRC Solutions, like our propietary solution SIRO®)**, collaborating with leading Spanish and European financial institutions (*G-SIB* and *D-SIB*).

5. Cutting-edge **R&D department** that provides ongoing support for developments, with extensive regulatory knowledge, *analytics* expertise and proven experience.

6. **Multidisciplinary teams** that combine profiles with **functional** knowledge**, data processing** and ***data scientists*,** with in-depth methodological knowledge and **high analytical skills and a unique *partnership* model.**

7. Recognised ***delivery* capacity and commitment to our clients**, as well as proven experience in complex projects of various kinds (regulatory, transformation projects, etc.).

1: MIR (risk integrated management tool), Gamma (model governance system) and SIRO (Enterprise Governance, Risk Management and Compliance –GRC- software).

Annex I
Abbreviations

Abbreviation	Meaning
AML	Anti-Money Laundering
AMLD	Anti-Money Laundering Directive
AMLR	Anti-Money Laundering Regulation
AML/CFT	Anti-Money Laundering / Countering the Financing of Terrorism
BCBS	Basel Committee on Banking Supervision
BCM	Business Continuity Management
CEO	Chief Executive Officer
CRA	Climate-Related Assessment
CRD	Capital Requirements Directive
CRR	Capital Requirements Regulation
CST	Climate Stress Test
DORA	Digital Operational Resilience Act
D-SIB	Domestic Systemically Important Bank
EBA	European Banking Authority
EC	European Commission
ESG	Environmental, Social and Governance
ESMA	European Securities and Markets Authority

Abbreviation	Meaning
EU	European Union
GAMMA	Model Governance tool
GDPR	General Data Protection Regulation
G-SIB	Global Systemically Important Bank
ICT	Information and Communication Technology
IRB	Internal Ratings-Based
KFH	Key Function Holder
KPI's	Key Performance Indicators
LoD	Line of Defence
MIR	Risk Information Model
NGFS	Network for Greening the Financial System
NPAP	New Product Approval Policy
PMO	Project Management Office
RMF	Risk Management Function
RTS	Regulatory Technical Standards
SIRO	Operational Risk Information System
SMEs	Small and medium enterprises
SREP	Supervisory Review and Evaluation Process

Management Solutions
Making things happen

International *One Firm*

Multiscope Team

Best practice *know-how*

Proven Experience

Maximum Commitment

Antonio García Perez
Partner at Management Solutions
Antonio.Garcia.Perez@msspain.com

Marta Hierro
Partner at Management Solutions
marta.hierro@msspain.com

For more information please visit

www.managementsolutions.com

Or follow us at: