Comments on Basel Committee documents open for consultation - June 2026

Dr. Rania Azmi

My key comments are organized by selected modules from the thirteen listed on the consultation website, in their presented sequence, reflecting relevance to the Committee's requests (Q1: whether the framework effectively removes outdated and duplicative materials; Q2: whether the redrafting achieves clarity and readability without introducing new expectations; Q3: whether particular topics merit more substantive review or further guidance), as follows:

SCA – Supervision and corrective actions

- Outdated: Conventional stress testing scenarios.
- Needs emphasis: Forward-looking stress tests for cyber, climate, and geopolitical shocks.
- Supervisory Review (Pillar 2) Stress testing, ICAAP: Stress testing and ICAAP practices are well-established, but the scenarios remain too general. They do not consistently capture geopolitical shocks or systemic cyber events, and the scope and depth are not clearly defined. Enhancing these elements would strengthen resilience.

CGO – Corporate governance

- Potential outdated content: Earlier versions place strong emphasis on board oversight and risk culture, but give limited attention to digital governance—including AI, cyber risk, and fintech oversight.
- Needs more emphasis: The integration of ESG governance and sustainability risk has become central in recent years. Elevating these elements would align the framework with current supervisory priorities and strengthen long-term resilience.

RMA – Risk management

- Needs more emphasis: While the framework covers traditional risk categories, it would benefit from an explicit treatment of climate-related financial risks and systemic risk from interconnected digital platforms. These are now recognized by BIS and other international authorities as critical to financial stability.
- Risk Data Aggregation & Reporting: The principles are sound and clearly articulated, but the supporting examples and implementation guidance remain limited. Providing more practical illustrations and supervisory benchmarks would reduce ambiguity and help institutions align more confidently with expectations.

CAD – Capital adequacy

- Needs more emphasis: Forward-looking buffers for cyber resilience and pandemic risks remain underdeveloped. Despite BIS/BCBS (2023–2026) recognizing climate, cyber, and geopolitical risks as systemic, these are not yet integrated into CAD stress testing or buffer design.
- Stress testing scope: Still focused mainly on economic and market risks, with limited treatment of geopolitical scenarios such as wars, sanctions, or regional fragmentation.

LQY – Liquidity

- Needs emphasis: Liquidity stress from crypto assets, digital payment platforms, and cross-border capital flows.
- Current gap: Recent BIS publications highlight these vulnerabilities, yet the LQY module remains focused on traditional LCR/NSFR metrics without embedding such systemic risks.

MIR – Market risk and interest rate risk

- Emphasis needed: Stronger focus on cyber resilience, sustainability governance, climate risk, and geopolitical stress testing (e.g., tail risks from geopolitical shocks, climate-related asset repricing, and crypto volatility).
- Potential outdated content: The module continues to reference Value at Risk (VaR), even though BIS has formally adopted Expected Shortfall (ES) under the FRTB. Any residual VaR guidance should be clarified or removed to avoid confusion and ensure alignment with current standards.

ORR – Operational risk and resilience

- The definitions: Clear and well-structured, but resilience expectations (e.g., cyber and third-party risk) are described broadly, leaving room for interpretation.
- Potential outdated content: Continued reliance on loss event databases and older standardized approaches such as the Basic Indicator Approach (BIA), which Basel has already phased out.
- Forward-looking emphasis: Outdated references can be phased out, with the module instead highlighting scenario-based, forward-looking resilience methods, aligned with BIS's 2026 operational resilience principles.

FRD – Financial reporting and public disclosure

- Emphasis needed: Greater focus on ESG transparency, cyber resilience disclosures, and fintech exposures.
- Potential outdated content: While disclosure templates remain comprehensive for traditional risks, they are outdated in not embedding ESG, cyber, and fintech dimensions, which BIS publications (2023–2026) recognize as systemic disclosure priorities.

General Additional Comments:

- **AI and Digital Risk**: The framework has only recently begun to acknowledge AI model risk and digital oversight. Yet most modules, including operational risk, credit risk, and Pillar 2 stress testing, remain anchored in traditional approaches. As a result, they do not fully address systemic vulnerabilities from algorithmic decision-making, bias, and rapid AI adoption. This gap leaves boards and supervisors without clear guidance on the governance of digital transformation, at a time when resilience and trust in AI systems are becoming increasingly vital.
- **Crypto and Digital Assets**: While targeted guidance has been issued on the prudential treatment of crypto exposures (2021–2023), the consolidated modules have not embedded crypto asset risks into liquidity, leverage, or market risk standards. This gap leaves institutions uncertain about how to manage volatility, custody challenges, and systemic spillovers from digital asset markets.
- **Fintech Platforms**: Concentration risk from large technology providers, cloud services, payment systems, and digital lending platforms, is acknowledged but not systematically integrated. Modules on large exposures, operational risk, and governance do not yet reflect the scale of dependency on these infrastructures, leaving systemic risk under-addressed.
- **Climate Risk**: Climate considerations remain peripheral. Risk management, capital adequacy, and stress testing modules reference climate only tangentially, even as supervisors worldwide press for explicit integration. The framework has yet to fully embed sustainability as a core risk dimension.
- **Geopolitical and Systemic Shocks**: Capital adequacy, liquidity, and market risk modules do not fully capture the impact of sanctions, supply chain disruptions, wars, or cyber warfare. Stress testing remains primarily economic and market-focused, without systematically embedding geopolitical fragmentation or systemic contagion.
- **Systemic Risks**: Risks such as cyber warfare, contagion from digital platforms, and sovereign defaults are insufficiently addressed across operational, liquidity, and market risk modules. This may weaken the framework's ability to anticipate and mitigate shocks that are now central to global financial stability, leaving it reactive rather than resilient.