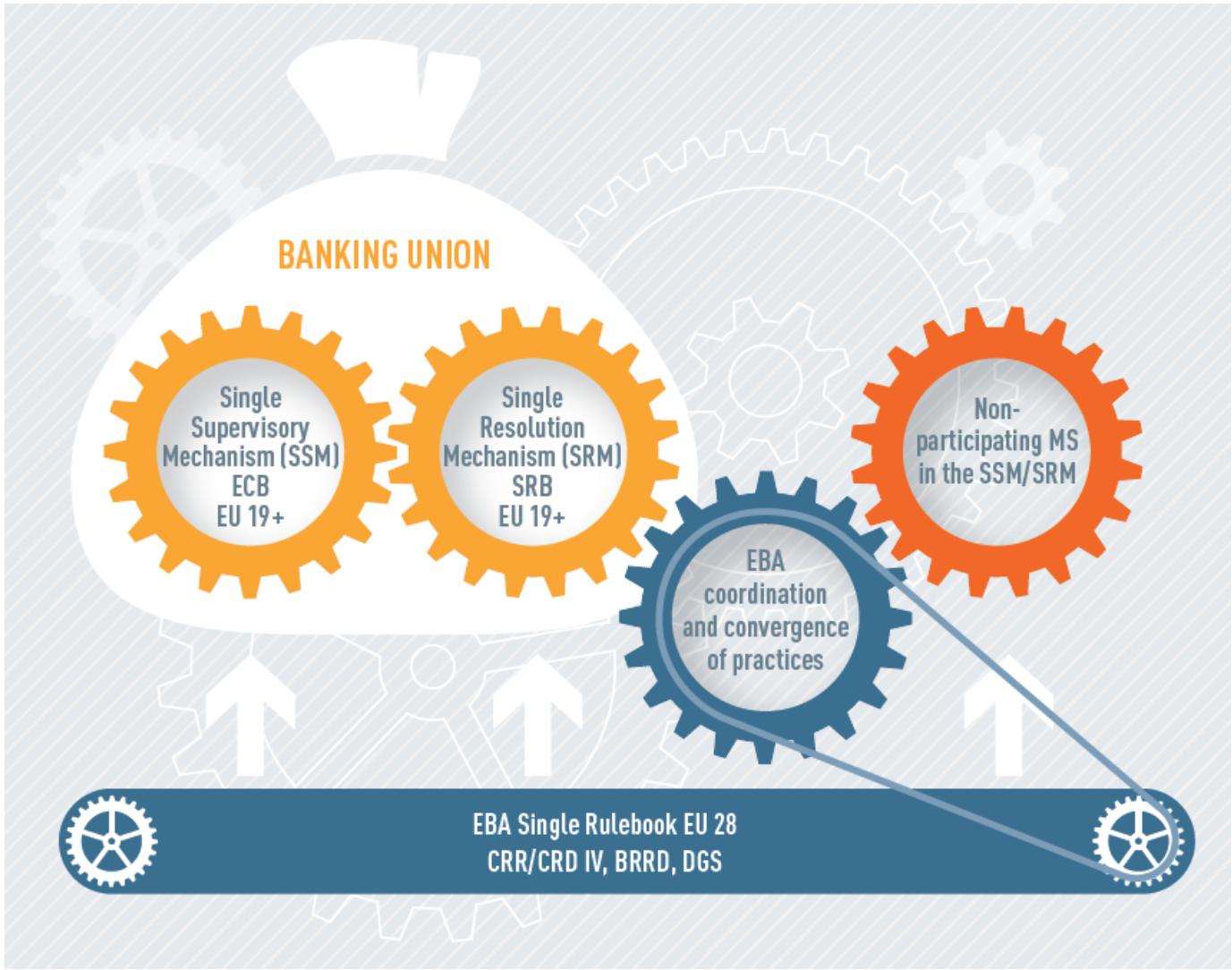
Latest Developments on Governance and Outsourcing

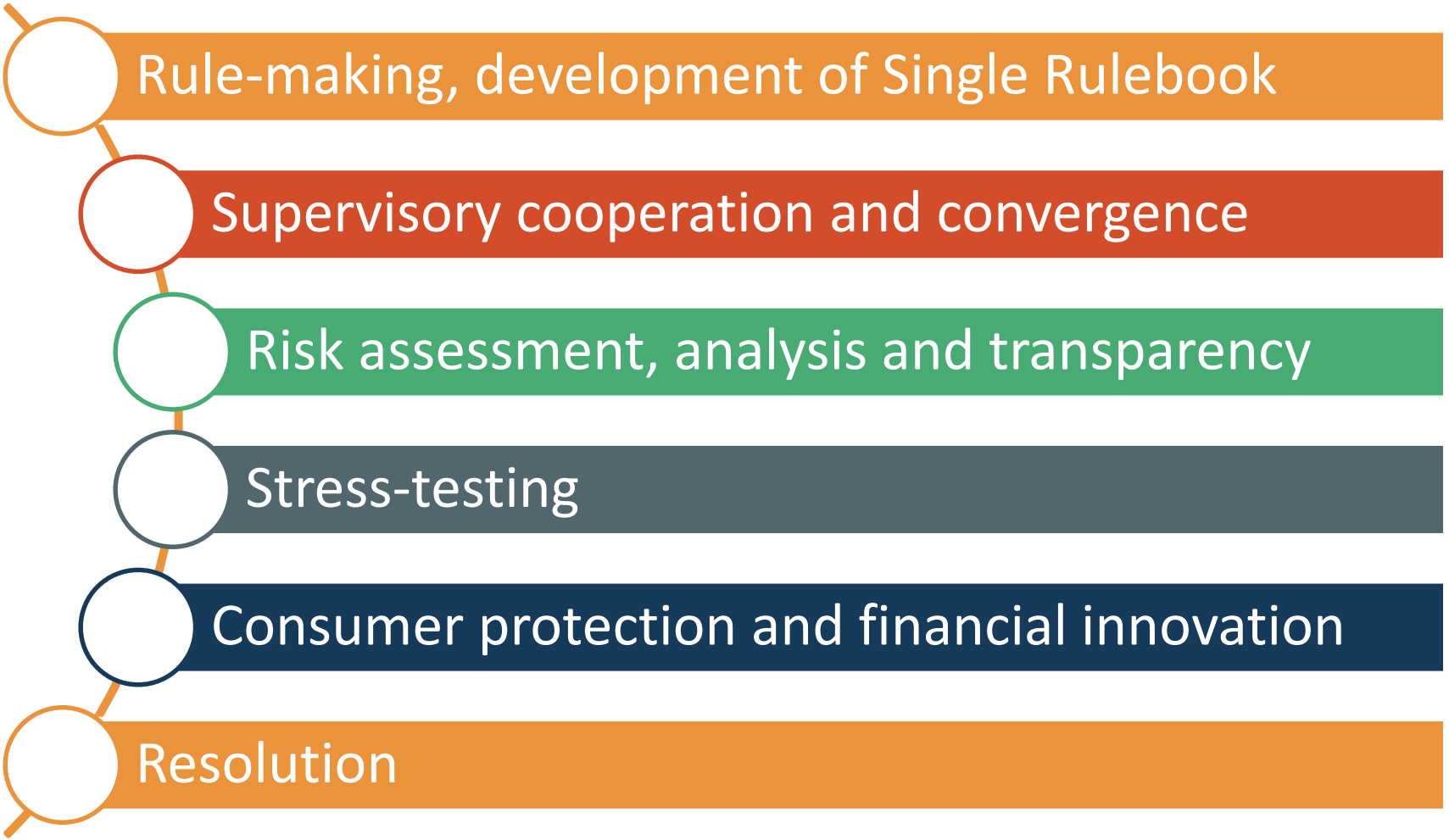
Bernd Rummel

ECIIA, 18 September 2019

EBA in the context of the Banking Union



EBA main areas of work



EBA's Organisation

Chairperson
José Manuel Campa

Executive Director
Adam Farkas

Banking Markets, Innovation and Consumers
Piers Haben

Economic Analysis and Statistics
Mario Quagliariello

Prudential Regulation and Supervisory Policy
Isabelle Vaillant

Liquidity, Leverage, Loss Absorbency and Capital
Delphine Reymondon

Risk-based Metrics
Lars Overby

Supervisory Review, Recovery and Resolution
Francesco Mauro

Team Governance and Remuneration
Bernd Rummel (Senior Policy Expert)
Djamel Bouzemarene (Policy Expert)
Margarita Steinbach-Shmeljov (Policy Expert)

The Single Rulebook uses a variety of tools

Binding	• Level 1 Regulation and Directives • Level 2 regulations (BTS: RTS – ITS)
Comply and Explain	• Guidelines mandated • Guidelines own initiative • Recommendations
Market discipline	• Opinions • Q&As • Peer reviews and Monitoring Reports

Overview - Latest Developments

CRD V/CRR2 - update of the regulatory framework

- Governance and remuneration
  - Review RTS identified staff, update of fit and proper requirements re independence and AML aspects, inclusion of holding companies
  - Waivers for the application of deferral and pay out in instruments

Fintech Roadmap (Cyperrisks, ICT risks, Innovation hubs, Sandboxes)

IFD/IFR - Separate rulebook for investment firms

Sustainable finance (ESG factors)

- Challenges ahead due to change of the whole economy
- Financial inclusion, diversity, human rights

EBA Guidelines on outsourcing

EBA Guidelines on Outsourcing

- Guidelines **update 2006 CEBS Guidelines on Outsourcing** and integrate the cloud recommendation
- Published on 25 February 2019, **enter into force 30 September 2019**
- Transitional arrangements: for the register and review of the contracts **31 December 2021**
- **Guidelines specify the outsourcing process on a risk based approach** from the initial risk assessment, due diligence process, contractual phase and exit from outsourcing arrangements for **Institutions under CRD, Payment institutions and EMI**

Legal Basis (Art. 74 CRD and Art 16 EBA Regulation)

All institutions must have robust governance arrangements and manage their risks with all third parties. In particular:

- Under the overall internal control framework, institutions and payment institutions should identify and **manage all their risks**, including risks caused by arrangements with third parties.
- Institutions and payment institutions should establish whether an arrangement with a third party falls under the **definition of outsourcing**.
- Where **critical or important functions** are outsourced (including in the case of intragroup outsourcing or outsourcing within institutional protection schemes), the institution should **exercise appropriate oversight** and be able to manage the risks that are created by such outsourcing and **not unduly rely on controls performed by the service providers**.

Critical or important outsourcing (replaces term material OS)

In line with Regulation (EU) 2017/565, institutions should always consider an operational function as critical or important where a defect or failure in its performance would materially impair:

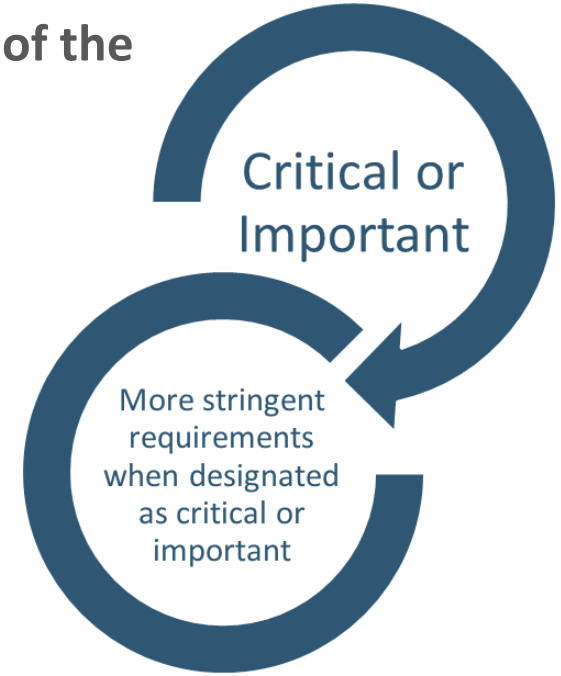
- their continuing **compliance with the conditions of their authorisation** or regulatory obligations under CRD/CRR and/or PSD ;
- their **financial performance**; or
- **soundness or continuity of** their banking, investment and payments **services and activities**.

Critical or important outsourcing

Outsourcing arrangements should always be considered critical or important, if they:

- concerns an operational tasks of internal control functions are outsourced, unless the assessment establishes that a failure to provide the outsourced function or the inappropriate provision of the outsourced function would not have an adverse impact on the **effectiveness of the internal control function;**

- when institutions intend to outsource functions of banking activities or payment services to an extent that would require **authorisation.**



Risk assessment

Institutions to assess all risks before outsourcing and as part of their monitoring, the guidelines have a focus on operational and reputational risks

- Institutions should assess the **potential impact of the outsourcing** on their outsourcing arrangement (where appropriate, **scenarios of possible risk events, including high-severity operational risk events**).
- **Assess concentration risks** (multiple outsourcings in one area or to one provider)
- Institutions to consider the **risk that may result from sub-outsourcing**
- **Measures implemented** by the institution or payment institution and by the service provider **to manage and mitigate the risks**

Contracts and Register

- **Written outsourcing arrangements – minimum content defined**
- **The institution should maintain a register of all outsourcing arrangements.**
- Register should distinguish between outsourcing of critical or important operational functions and other outsourcing arrangements; extent of documentation differs, but all outsourcings are to be documented
- Register or part of it should be made available to the competent authority on request and in a process able electronic form
- Institutions and payment institutions should adequately inform competent authorities in a timely manner or engage in a supervisory dialogue with the competent authorities about the planned outsourcing of critical or important functions

Access information and audit rights

For all outsourcing:

The agreement should refer to information gathering and investigatory powers of competent authorities and resolution authorities (Art 65(3) CRD)

- Applies automatically within EEA
- To be contractual agreed with service providers in third countries

For critical and important outsourcing (and for non critical and important on a risk based approach):

The service provider grants institutions and their competent authorities, including resolution authorities, and any other person appointed by them or the competent authorities:

a. full access to all relevant business premises

b. unrestricted rights of inspection and auditing related to the outsourcing arrangement

Audit process

- Outsourced functions to be considered in **audit plan**
- Qualification of auditors (e.g. high level of technical complexity, cloud etc.)
- Provide **reasonable notice** to the service provider, unless this is not possible due to an emergency or crisis situation or would lead to a situation where the audit would no longer be effective.
- audits in **multi-client environments** to be planned carefully
  - Consider burden for service provider
  - Ensure that there are no material risks to another client's environment (e.g. impact on service levels, availability of data, confidentiality aspects)

Audit methods

a. **pooled audits** organised jointly with other clients of the same service provider, and performed by them and these clients or by a third party appointed by them

b. third-party certifications and third-party or internal audit **reports, made available by the service provider.**

- quality of certification
- should not rely solely on these reports over time (i.e. own audit to be performed or own external auditor mandated)

Sub-outsourcing

- Agree if sub outsourcing is permitted
- Record in the register of the part being sub outsourced is critical or important.
- Service providers should execute appropriate oversight over the sub-service providers. (still the institution needs to maintain also its own control)
- Sub- contractor must agree to comply with applicable laws, and grant the institution and competent authority the same access and audit rights as those granted by the provider (effective supervision must be ensured).
- Institution may object or terminate the contract if the sub outsourcing could have material adverse effects on the outsourcing.

Sub-outsourcing and Cloud

- Cloud outsourcing involves frequent sub-outsourcing, but does not have a different treatment as other outsourcing in the Guidelines

- Para 78 (f) requires that 'where appropriate the institution has the right to object to intended sub-outsourcing, or material changes thereof, or that explicit approval is required'

- 'where appropriate' means that where relevant for the institution meaning that this implies a case by case analysis considering:

  - Impact on business resilience and continuity
  - Impact on risk
  - Impact on data security
  - Impact on effective oversight and supervision

- Practical solution: pre-assessment and pre-approval (where possible) of certain types and providers of sub- outsourcing

Security of data and systems

- Service providers should comply with appropriate IT security standards.
- Institutions should define data and system security requirements in their outsourcing agreements.
- For personal or confidential data, institutions should adopt a risk-based approach to data storage and data processing locations.
- Information and data should be protected in line with all legal requirements that apply to the institution (taking into account differences in national provisions).

Exit strategies

Institutions should have an exit strategy when outsourcing critical or important functions taking into account the possibility of:

a. termination of outsourcing arrangements;

b. the failure of the service provider;

c. the deterioration of the quality of the function provided and/or actual potential business disruptions caused by the inappropriate or failed provision of the function;

d. material risks arising for the appropriate and continuous application of the function

Exit strategies should

- not cause undue disruption to business activities.
- Be documented and tested
- Identify solutions for date transfer to alternative providers or back to the institution

Summary of the outsourcing process

Pre outsourcing phase

- Economical need
- Risk analysis
- Critical or important?
- Due Diligence
- Compliance with legal requirements
- Decision

Contractual phase

- Regulatory contractual standards
- Clear contract
- Audit and access rights
- Implementation
- BCP

Monitoring

- Documentation (register)
- Service Level met?
- Compliance?
- Monitoring and controlling of risks
- Concentration risks
- Change of scale -> becomes critical?
- Internal audit

Exit

- Reintegration
- Transfer to other provider
- Other arrangements to ensure continuity of business activities

EUROPEAN BANKING AUTHORITY

Floors 24-27, 20 Av André Prothin, 92927 Paris La Défense

Tel: +33 1 86 52 7000

E-mail: info@eba.europa.eu

http://www.eba.europa.eu