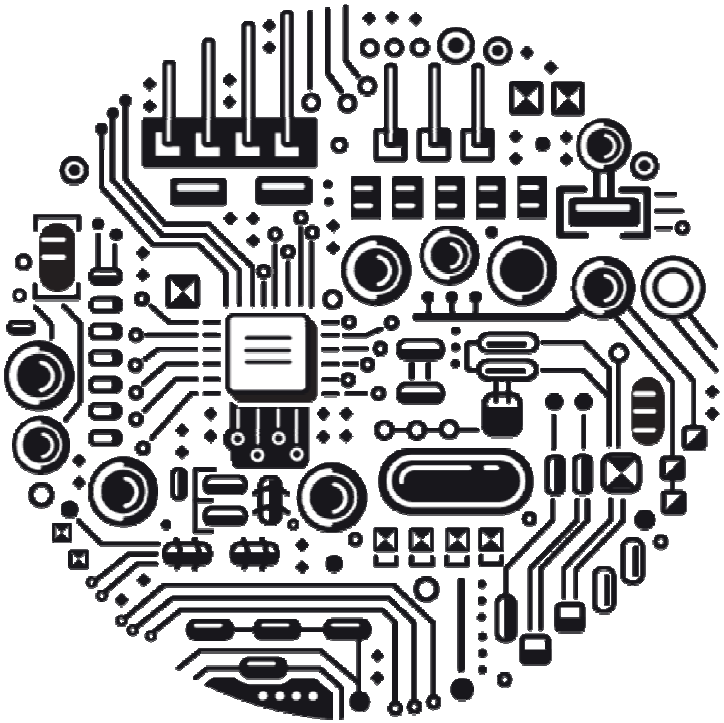
Deloitte.

CISQ
Consortium for IT Software Quality



Cyber risk and prudential requirements

Consortium for IT Software Quality

Nicolas Fleuret, Partner, Deloitte Risk Advisory France

Brussels, June 6th, 2017

contact

Deloitte, Paris

Nicolas FLEURET

Partner
Deloitte FSI Risk Advisory

nfleuret@deloitte.fr
+33 1 55 61 61 89

Foreword

In an era of rapid change, characterized by digital transformation and the use of ever increasing amounts of data, cybersecurity is becoming a priority for organizations of all sizes and across all industries.

Deloitte experience demonstrates that clients implementing a proactive cybersecurity model do more than deal successfully with threats. They also achieve better business results, reflected in growth in their bottom line.

Our practitioners provide capabilities across the four main domains of cybersecurity – Cyber Strategy, Security, Vigilance and Resilience.

Thanks to Deloitte's alliances with many vendors on the EMEA cybersecurity market, we are not restricted by technology.

These strengths enable us collectively to deliver a large number of projects every year in advisory, implementation and managed services, all with solutions tailored to the precise needs of each individual client.

Regardless of geography, Deloitte's Cyber practices in EMEA provide the same exceptional quality of service across all the 14 capability areas showcased in this document.

Chris Verdonck
EMEA Cyber Risk Leader

Deloitte global network of Cyber Intelligence Centers (CICs)

CYBER INTELLIGENCE CENTER

Our solutions are supported by Deloitte network of Cyber Intelligence Centers (CICs)

As cyber threats evolve and become more complex, many business leaders recognize they can't manage the challenge alone. Our CICs provide fully customizable managed security solutions including advanced security event monitoring, threat analytics, cyber threat management and incident response for businesses in the region to meet the increasing market demand in cybersecurity services.

Deloitte Cyber Risk awards and recognitions

Deloitte ranked #1 globally in security consulting by Gartner (fourth consecutive year)

Gartner, a technology research company, has once again ranked Deloitte #1 globally in Security Consulting, based on revenue, in its market share analysis entitled Market Share: Security Consulting Services, Worldwide, 2015. This is the fourth consecutive year that Deloitte has been awarded the #1 ranking.

Deloitte named a global leader in cybersecurity consulting by ALM Intelligence

ALM Intelligence (a research firm, formerly known as Kennedy) named Deloitte a leader in Cybersecurity Consulting in its report entitled Cybersecurity Consulting 2015. The report notes: "The firm's notable depth across the breadth of the cybersecurity consulting portfolio coupled with its ability to effectively communicate and work with the span of a client organization (boardroom down to IT operations) solidifies its position in the vanguard."

Deloitte named global leader in security operations consulting by ALM Intelligence (2016)

ALM Intelligence notes, "The firm's emphasis on aligning SOC initiatives to what matters to the business – including legal and regulatory requirements and education on threat actors – makes Deloitte an elite firm among its peers when it comes to building a case for investment that resonates with business-side stakeholders."

Deloitte Cyber Risk portfolio

End-to-end cybersecurity
More than 1400 Cyber Risk professionals across EMEA

Cyber Strategy

Deloitte helps organizations develop a business-driven and threat-based cyber risk program which is in line with the strategic objectives and risk appetite of the organization.

- Cyber Risk Management and Compliance
- Cyber Training, Education and Awareness
- Cyber Strategy, Transformation and Assessments

More than 350 professionals

Cyber Security

We focus on establishing effective controls around the organization's most sensitive assets and balancing the need to reduce risk, while enabling productivity, business growth and cost optimization objectives

- Infrastructure Protection
- Vulnerability Management
- Application Protection
- Identity and Access Management
- Information Privacy and Protection

More than 600 professionals

Cyber Vigilance

We integrate threat data, IT data and business data to equip security teams with context-rich intelligence to proactively detect and manage cyber threats and respond more effectively to cyber incidents.

- Advanced Threat Readiness and Preparation
- Cyber Risk Analytics
- Security Operations Centre
- Threat Intelligence and Analysis

More than 200 professionals

Cyber Resilience

We combine proven proactive and reactive incident management processes and technologies to rapidly adapt and respond to cyber disruptions whether from internal or external forces.

- Cyber Incident Response
- Cyber Wargaming

More than 250 professionals

Delivery models

Advise

Implement

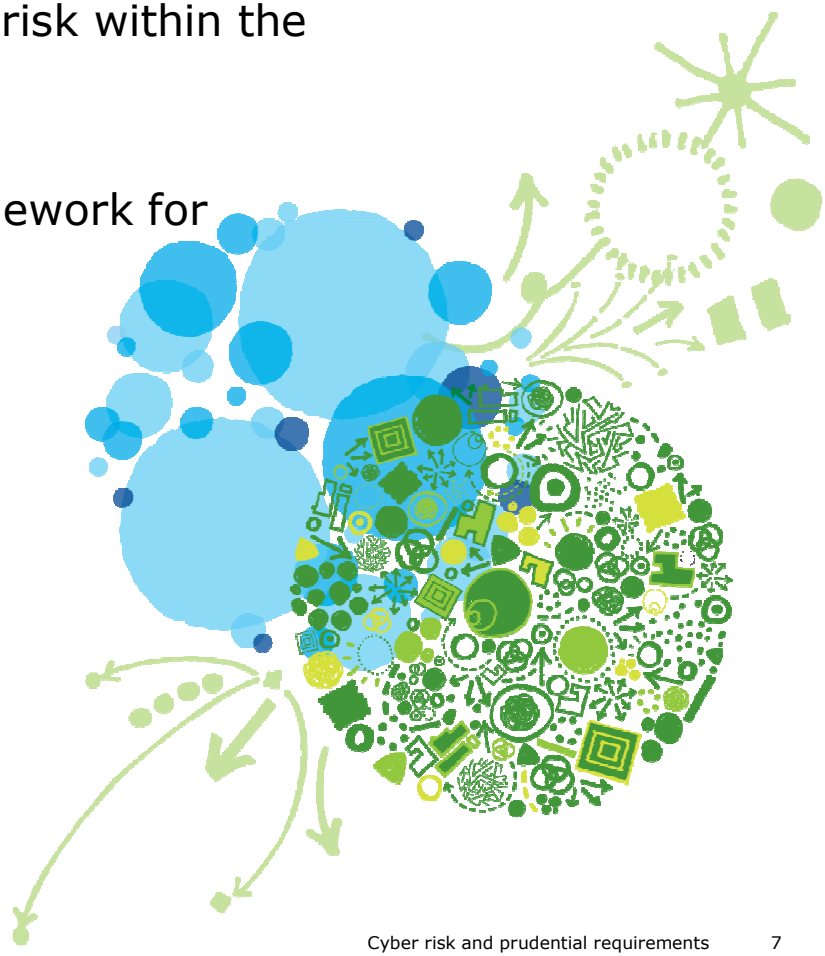
Manage

1. Cyber risk within Basel III pillar 1

2. An evolution towards pillar 2 - Cyber risk within the supervisory scope of supervisors

3. The importance of a structured framework for Cyber and IT Risks monitoring

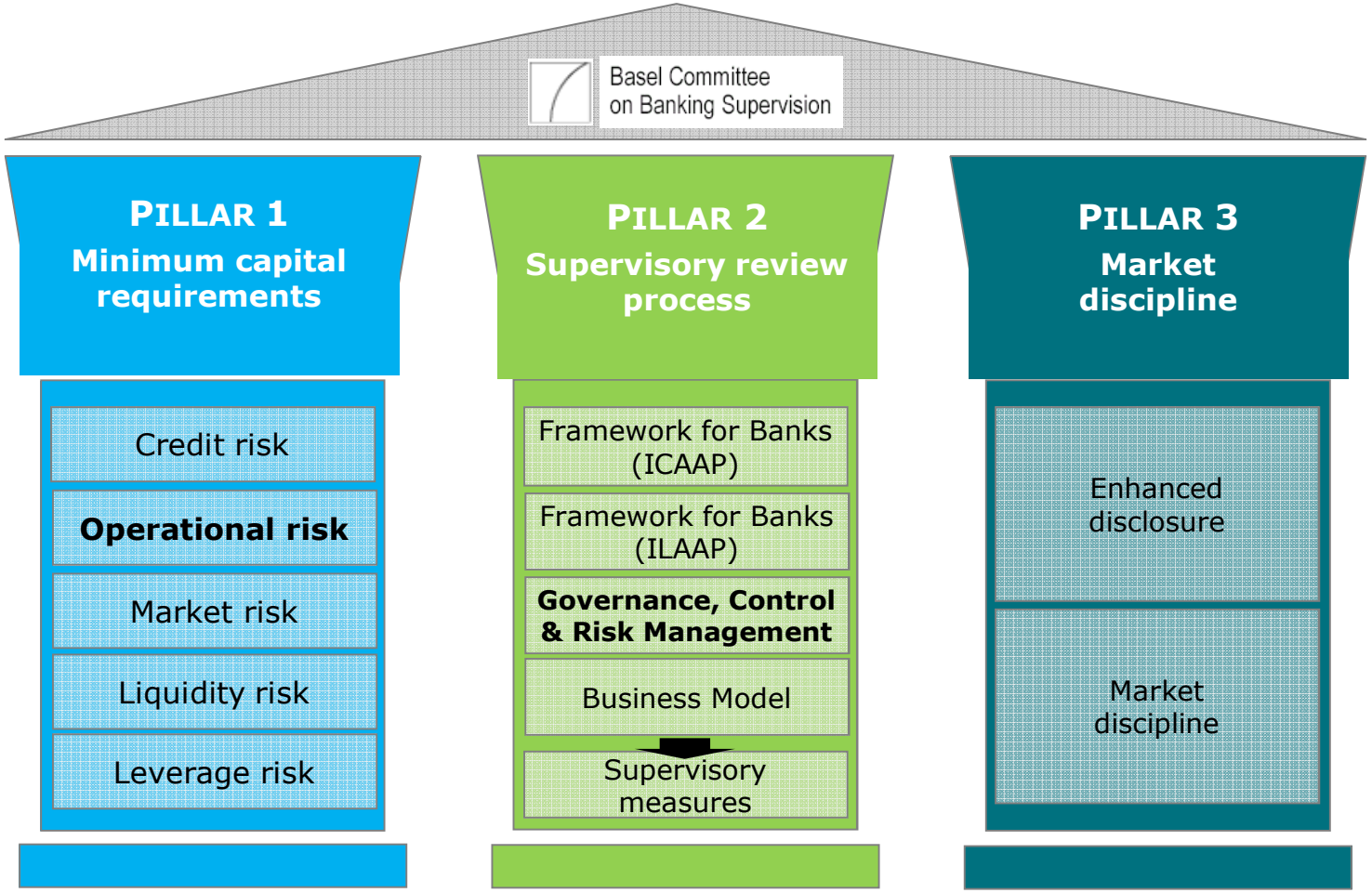
4. Conclusion



Cyber risk within Basel II or III pillar 1

Cyber risk within Basel II & III pillar 1

Basel principle reminder



Cyber risk within Basel II & III pillar 1

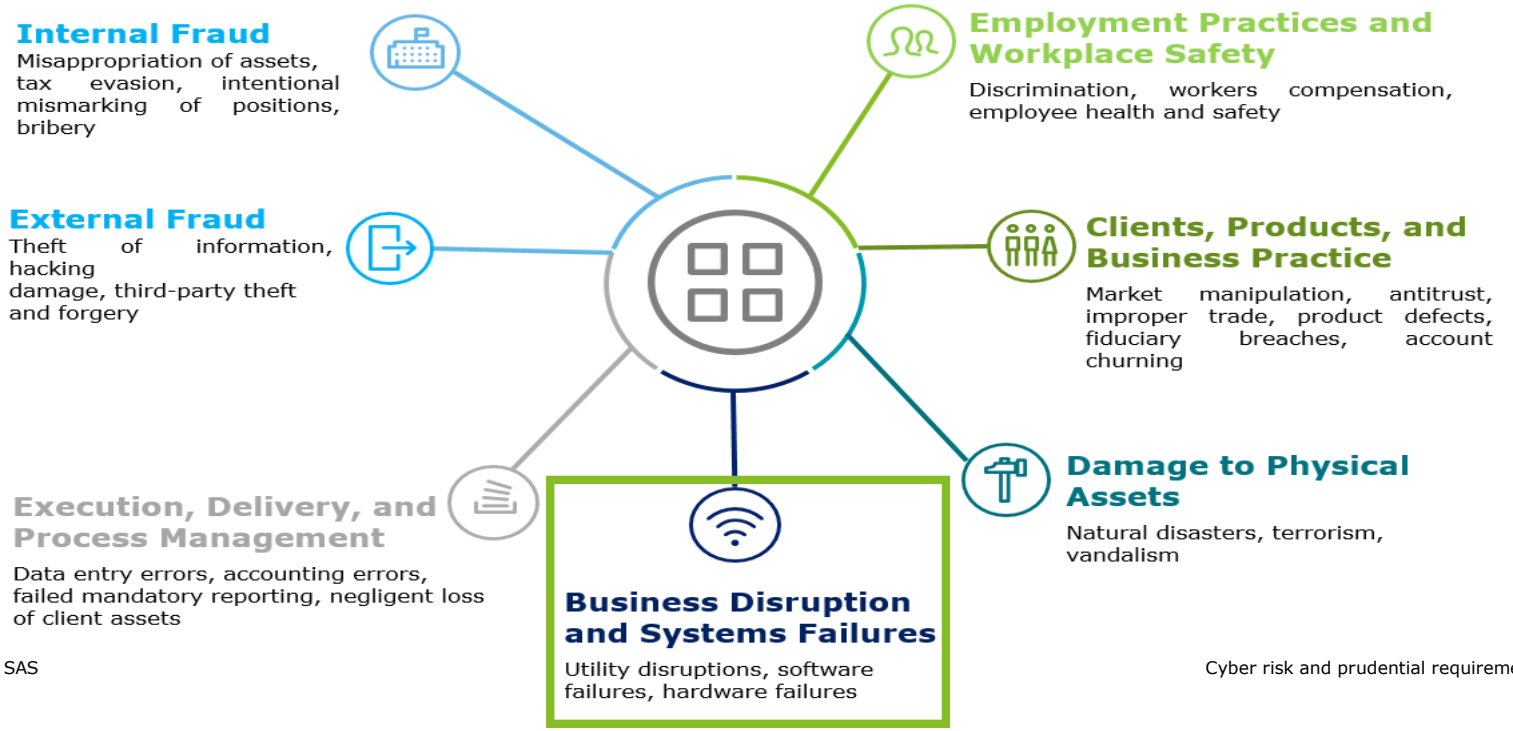
Focus on operational risk 1/2

Definition

The Basel Committee defines operational risk as the risk of loss resulting from inadequate or failed internal processes, **people and systems or from external events**. This definition includes, among many notions:

- ✓ **Human errors,**
- ✓ **Fraud,**
- ✓ **IT failure,**
- ✓ **Legal risk**

It does not, however, include reputational risk (risk of loss arising from damage to the bank's reputation) and strategic risk (risk of loss arising from poor strategic decisions).



Cyber risk within Basel III pillar 1

Focus on operational risk 1/2

As of today, banks have been authorised (by Basel Committee and CRR) to use 3 alternative calculation methodologies, with increasing complexity

Advanced measurement approaches (AMA)

Use of an internal model developed by the bank, based on qualitative and quantitative requirements and constraints, which should be approved by the regulator

Little guidance is provided on calculation methodologies to be used for modelling.

Standardised Approach (TSA)

Idem with a view by business lines and the value of a depending to each type of activity

Basic Indicator Approach (BIA)

EI = exposure indicator reflecting the overall bank's business activity. The relevant indicator (GI) equals the average over the 3 previous years of positive annual gross income, defined as the sum of net interest income and net non-interest income

$FP_{BIA} = \sum(\alpha \times EI_i)$, **with α = 15 %**

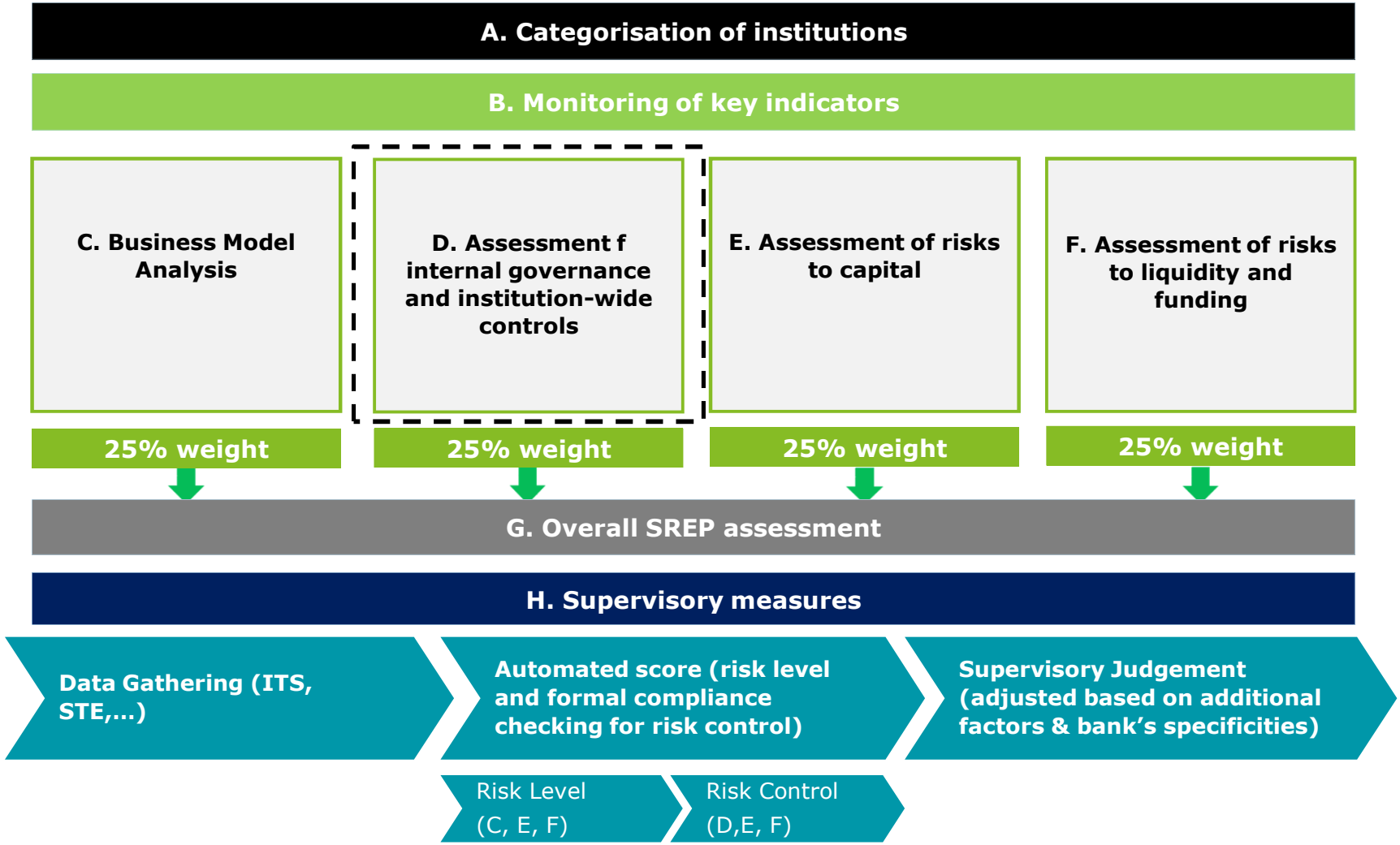
The Advanced Measurement Approach (AMA)

- The AMA is an **operational risk method** that can be used under Basel II or III
- Under AMA, the banks are allowed, subject to approval, to develop their own empirical model to quantify required capital for operational risk.
- **In terms of IT risk, AMA lacked precision and was not very inclusive. In general, it was seldom used by banking institutions and is now being left out by the supervisory authorities, therefore likely to disappear.**

An evolution towards pillar 2

Pillar 2 - Overarching SREP framework

Stricter SREP requirements and inclusion of Business Model Analysis



IT & Cyber - An evolution towards pillar 2

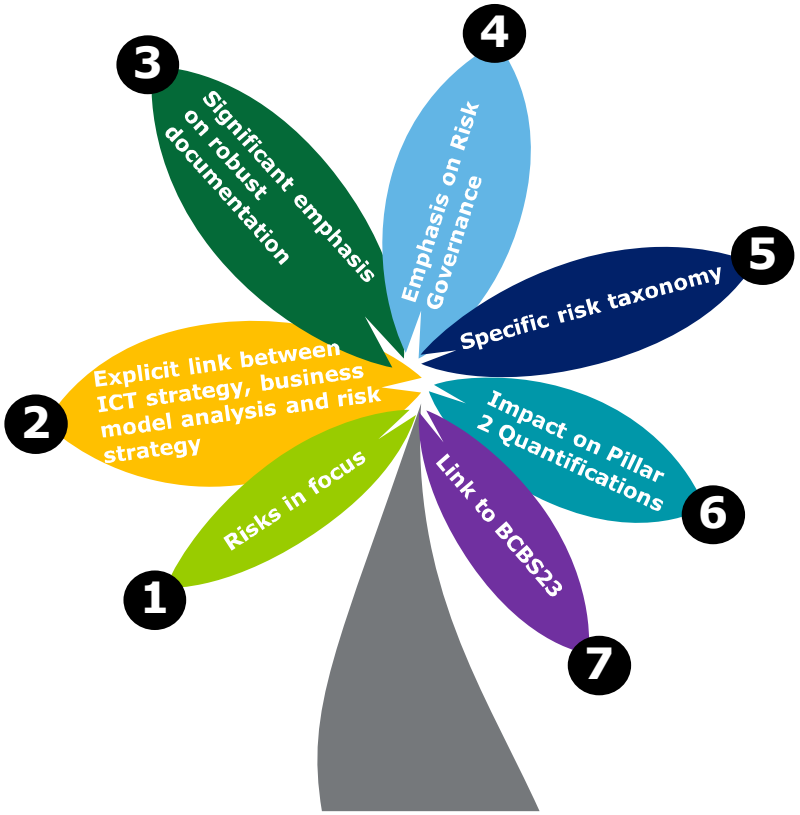
Focus on the Information and Communication Technology (ICT) Risk Assessment 1/3

Context

EBA consultation on ICT Risk assessment in 2016 to promote common procedures and methodologies for the assessment of the ICT risk under the supervisory review and evaluation process.

- enhance existing SREP Guidelines
- establish common practice and application by National Competent Authorities (NCAs) in ICT risk assessment
- strengthen prudential supervision.

The Guidelines flesh out key expectations regarding ICT risk assessment which have been hinted at in previous publications (the EBA SREP Guidelines, Guidelines on ICAAP-ILAAP information requirements and the EBA report on convergence).



IT & Cyber - An evolution towards pillar 2

Focus on the Information and Communication Technology (ICT) Risk Assessment 2/3

Key Themes

Theme 1: Risks in focus: EBA has articulated key ICT risks requiring increased supervisory attention:

FIs will need to demonstrate that they have established appropriate risk assessment processes and controls to manage these risks.

Theme 2: Explicit link between ICT strategy, business model analysis and risk strategy:

FIs will need to demonstrate that their ICT strategies are adequate for the nature and complexity of their business, consistent with their business strategy and support their business model.

Theme 3: Significant emphasis on robust documentation:

More diligence will be required in maintaining robust internal ICT documentation

Theme 4: Emphasis on Risk Governance:

FIs will need to demonstrate that senior management are familiar with, have oversight of, and assess the ICT strategy and risks.

Theme 5: Specific risk taxonomy:

FIs will have to overhaul their risk taxonomies and update their operational risk registers

(ICT availability and continuity risks ; ICT security risks ; ICT change risks ; ICT data integrity risks ; ICT outsourcing)

IT & Cyber - An evolution towards pillar 2

Focus on the Information and Communication Technology (ICT) Risk Assessment 3/3

Theme 6: Impact on Pillar 2 Quantifications:

Supervisors may expect FIs to develop specific Pillar 2 stress tests and scenarios for capital quantification, with a robust analysis of direct and indirect financial and non-financial (e.g. reputational) impacts.

Theme 7: Link to BCBS239:

FIs will need to leverage their BCBS239 programs and capabilities to support the assessment and management of ICT risks. NCAs should pay increasing attention to data integrity issues.

In a nutshell

- The Guidelines are expected to impact FIs' supervisory scoring and assessment, leading to potential impacts on SREP engagement and capital requirements.
- FIs should therefore undertake a detailed review of these Guidelines, identify key areas of impact and initiate appropriate program and actions to address the key issues.
- The proposed Guidelines will have a significant organizational impact on how FIs plan, assess and Manage ICT risks. Particularly, there is greater emphasis on the relationship between :
  - **ICT strategy and business model strategy,**
  - **ICT risk appetite with the overall risk strategy,**
  - **Comprehensive assessment of ICT risk,**
  - **Greater diligence in ICT related documentation**.

Cyber risk within the supervisory scope of the European Central Bank

2017 supervisory priorities

General ECB 2017 risk drivers

1. Ultra-low/negative interest rate environment
2. High levels of non-performing loans (NPLs)
3. Lackluster economic growth across euro area countries
4. EU geopolitical uncertainties
5. Reactions of banks and markets to new regulation
6. Non-bank competition
7. Potential reversal of risk premia in financial markets
8. Situation in emerging market economies
9. EU fiscal imbalances, cases of misconduct by banks
10. Developments in real estate lending markets
11. **Cybercrime and IT disruptions**

- ECB questionnaire on cybercrime in 2015. Analysis followed by on-site visits in 2015 & 2016.

In 2016 Deloitte has launched a survey on IT Risk Management for Financial Institution in order to gather feed-back from CIO and IT officer and trends observed in terms of IT Risk Management

Top IT risks identified

1. Cyber risk and cyber resilience
2. IT continuity and operational resilience
3. Vendor management ad outsourcing risk
4. Identity and access management
5. Patch and vulnerability management
6. IT complexity
7. Transformation program risk
8. Data architecture, quality and governance
9. IT skills

Leading supervisory practices identified

1. Central coordination and governance of IT risk supervision
2. IT risk assessment leading to priorities
3. Self- assessments and questionnaires
4. Issuing more detailed guidance
5. Red-teaming assessments
6. Promotion of information sharing
7. Thematic/horizontal supervisory approach
8. Performing in-depth on-sire inspections
9. Training for non-IT supervisors

Cyber Risk Governance

Aspects to consider in order to respond to supervisory expectations

Reporting consideration

- Cyber related committees, functions and necessary information
- Cyber risk indicators and

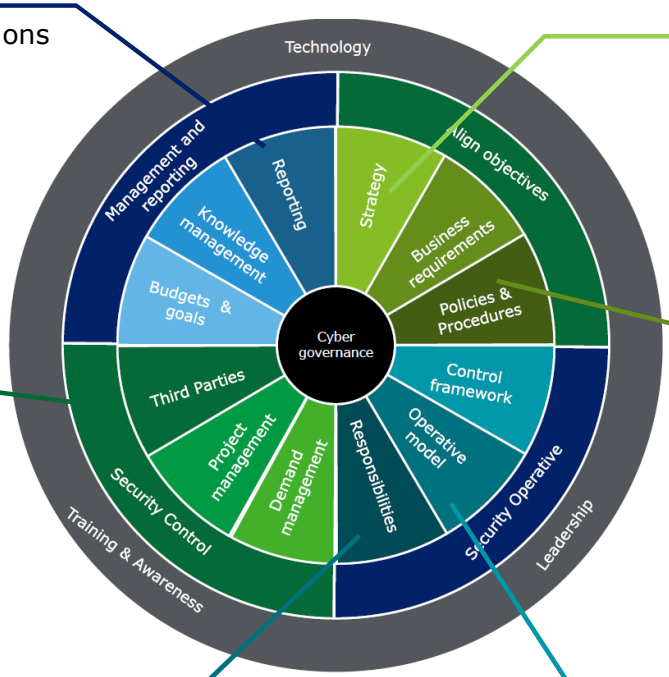
reporting process

- Reporting s a toll for

decisions-making

Third party considerations

- ECB IT outsourcing questionnaire
- Legal and security clauses in contra
- Specific cloud risk analyses and fra
- Cyber security checks included ir lifecycle and workflows t



Strategy considerations

- Existence of a specific cyber strategy
- Alignment with business strategy
- Adequate level of approval
- Strategy advance monitoring

Business requirements considerations

- Identification of business-sensitive information
- Inclusions of business units in Business Continuity Planning
- Business input for risk mitigation prioritisation

Responsibilities considerations

- Assignation, acceptance and approval of roles and responsibilities
- Regulation implications (i.e. Data Privacy Officer)
- Definition and revision of objectives

Operative model considerations

- Incorporation of a comprehensive cyber strategy framework based on identifications, protection, detection, response and recovery
- Periodic assessment of state and progress
- Integration with cyber risk models

The importance of a structured framework for Cyber and IT Risks monitoring

The importance of a structured framework for Cyber and IT Risks monitoring

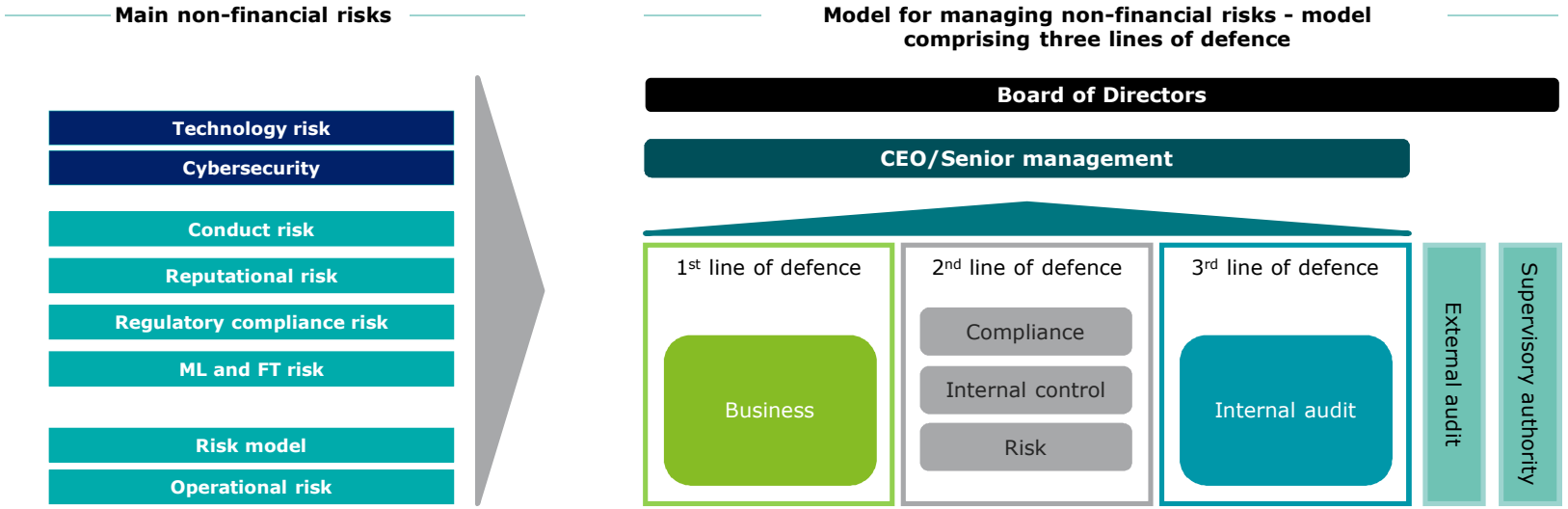
Definition and control of non-financial risks (including Cyber Risk)

Risks that might **entail an economic impact or deterioration of the image or processes** of a bank through its normal operations, and do not include the risks it traditionally manages itself (financial risks).

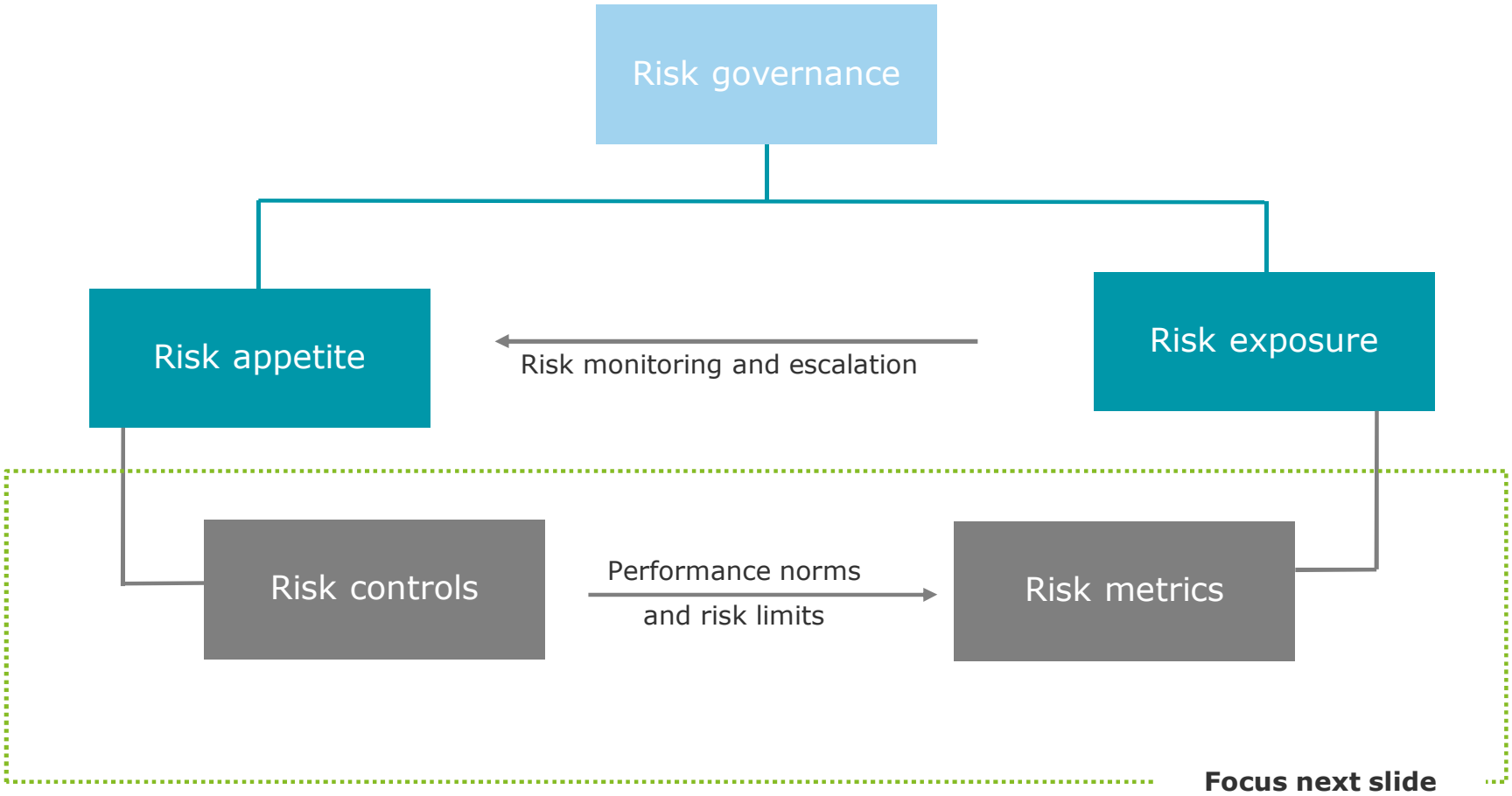
Among them,

- ✓ **Technology risk**
- ✓ **Cybersecurity**

A model built around three lines of defence



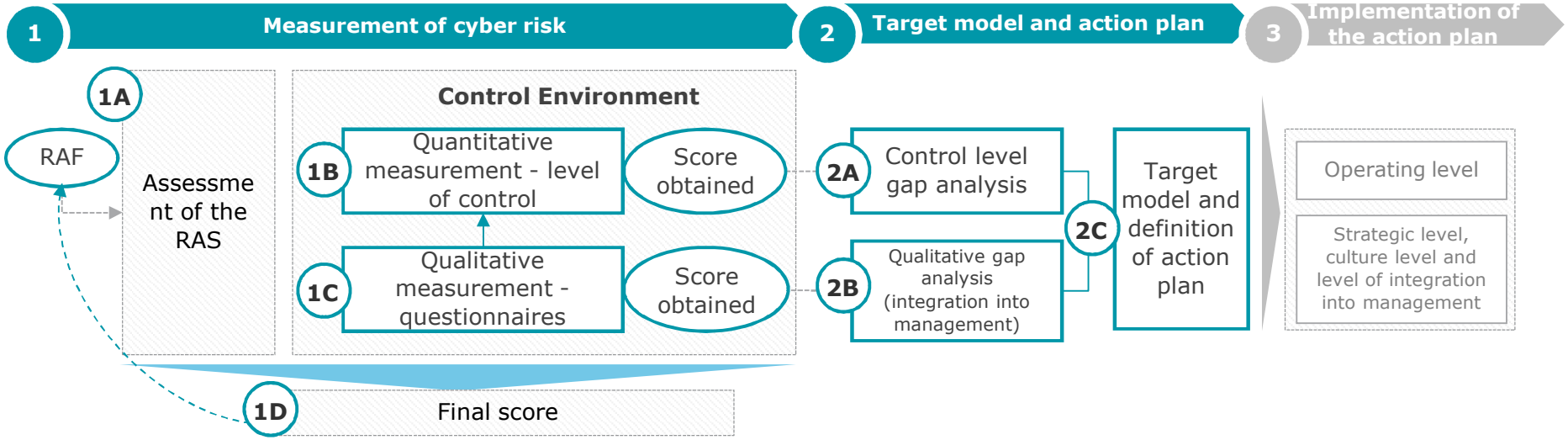
Typical risk governance, risk appetite and risk control cascade



Example of cyber risk

Institutions will have to face the challenges of managing cyber risk

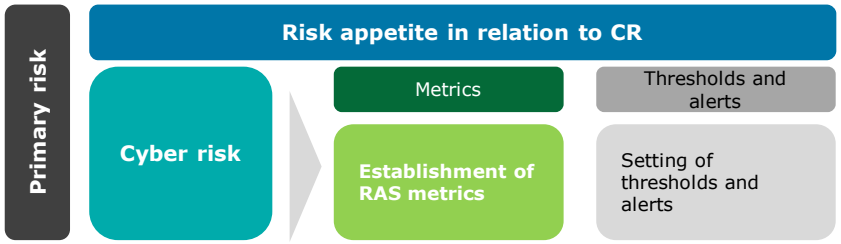
The approach proposed by Deloitte for identifying, measuring and managing cyber risk is structured in **two phases**:



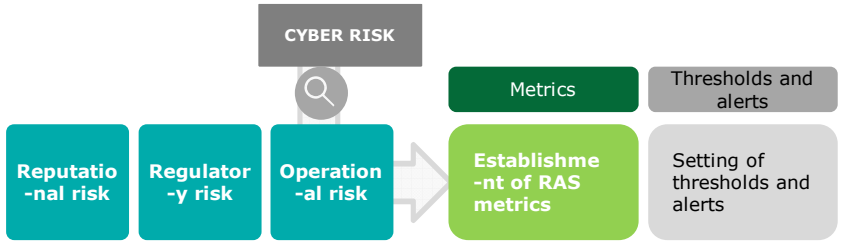
Assessment of the RAS 1A

Two possible approaches are proposed:

1 Establishment of cyber risk as a primary risk in the RAF and establishment of RAS metrics, thresholds and alerts



2 Identification of cyber risk among the risks already established in the RAF



Conclusion

Conclusion

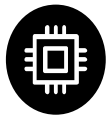
Top priorities for the banking industry

Common and simple actions can be considered to increase efficiency while responding to new supervisory requests

Build a strong governance system covering all dimensions of Cyber Risk with involvement and commitment from the general management

Ensure greater articulation of cyber risk monitoring framework within the existing operational processes, decision making process, management reporting,…

Enhance oversight of Cyber & IT risk under all dimensions of products, markets, competition, risks, P & L, ... in a prospective logic



Implement effective tools, systems and methodology to facilitate Cyber Risk monitoring

Deloitte.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms. In France, Deloitte SAS is the member firm of Deloitte Touche Tohmatsu Limited, and professional services are provided by its subsidiaries and affiliates.

Deloitte provides audit, tax, consulting, and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 150 countries, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges. Deloitte's approximately 244 400 professionals are committed to becoming the standard of excellence.

In France, Deloitte calls on diversified expertise to meet the challenges of its clients of all sizes from all industries - major multinationals, local micro-companies and medium-sized enterprises. With the expertise of its 10 300 professionals and partners, Deloitte is a leading player in audit, risk advisory, consulting, financial advisory, tax & legal and accounting, based on a multidisciplinary offering and a set of action principles attuned to the requirements of our environment.

OFFICIAL PARTNER FRANCE 2025