A regulator's point of view with regard to the application of cloud

Vincent Morren
Prudential IT Supervision

National Bank of Belgium
Eurosystem

Agenda

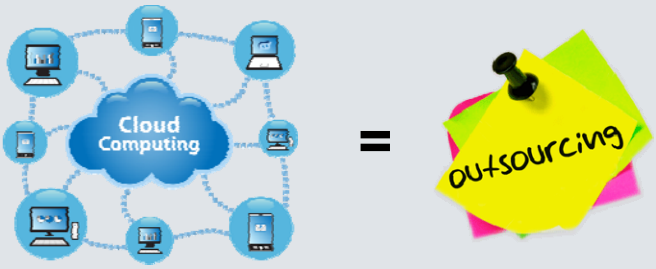
- Introduction
- Outsourcing Circular
- Risk assessment
- Examples of Compliance Issues
- Conclusion
- Q&A

Introduction

- 2012: first cloud projects submitted to NBB
- NBB approach

  Communication of October 9th, 2012:

  Usage of cloud computing with a third party service provider is considered as a form of outsourcing



- Application of NBB outsourcing circular (2004)

Outsourcing Circular

- What do we consider as an outsourcing ?
- No direct and no permanent control performed by the FI

- Concerns important activities
- Measure of the importance = What is the impact if the outsourced activity is not operating ?

- First risk = loss of control

Outsourcing Circular - Principles

- 1. Outsourcing policy

- 2. FI remains accountable
  - Internal and external control
  - Reporting adapted to outsourced activities and underlying risks
  - Communication of important incidents

- 3. Decision to outsource is based on a thorough analysis
  - Risk assessment

Outsourcing Circular - Principles

- 4. Provider selection, ensuring continuity
  - Due diligence
  - Documentation
  - Dependency
  - Disaster recovery

- 5. Service Level Agreement
  - Reflects the outsourcing circular

- 6. Protection
  - Confidentiality
  - Integrity

Outsourcing Circular - Principles

- 7. Cascading outsourcing
  - Described in the agreement
  - Internal and external control

- 8. Internal audit & compliance
  - Right to audit for FI

- 9. Prudential & external audit control
  - Right to audit for regulators

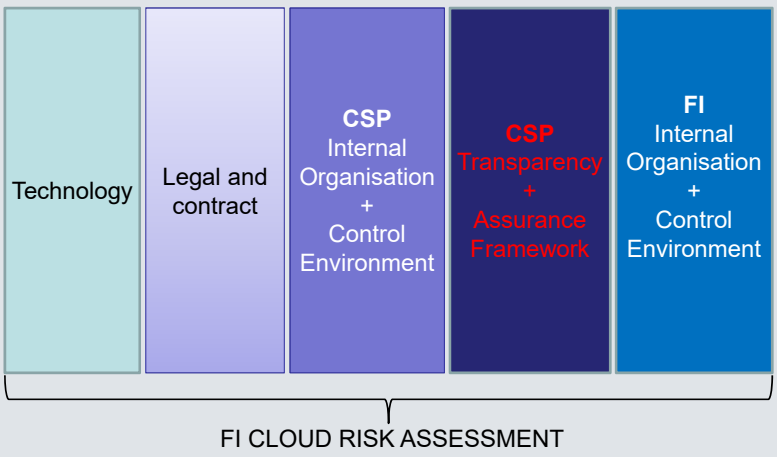
Outsourcing Circular - Principles

- 10. Applicability of Belgian laws and regulations

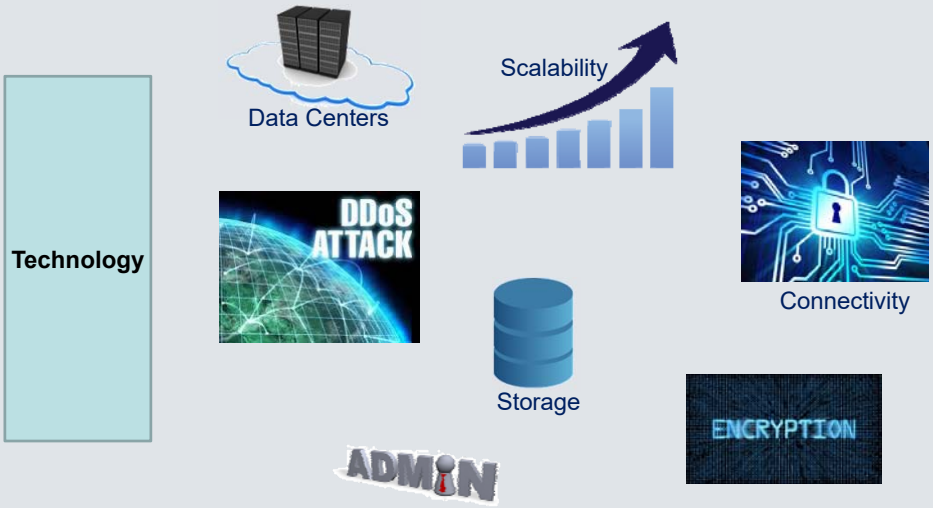
Risk Assessment General Information

- Overview of outsource activities
- Criticality / sensitivity
- Alternative solutions
- Roadmap
- Integration with current IT environment
- New or increased weaknesses
- Exit strategy

Risk Assessment Layers



Risk Assessment Layers



Risk Assessment Layers

Risk Assessment Layers

Quality Assurance

CSP Internal Organisation + Control Environment

Operational Teams

Controls

Internal Audit

R	Responsible
A	Accountable
C	Consulted
I	Informed

Risk Management

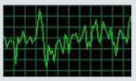
Compliance

Risk Assessment Layers

To FI 1st LoD

Logging data

Administrators Activities



Performance Monitoring

To FI 2nd LoD

New threats follow-up

Policy to access customer data

CSP Transparency + Assurance Framework

To FI 3rd LoD

Internal + External Audit Coverage

Risk Assessment Layers

1st LoD

Operational Teams

Using the provided control environment

2nd LoD

Risk Management

Internal policies
- Applicable?
- Challenge the provider

3rd LoD

Internal Audit

Opinion about Internal/external audit coverage

FI Internal Organisation + Control Environment

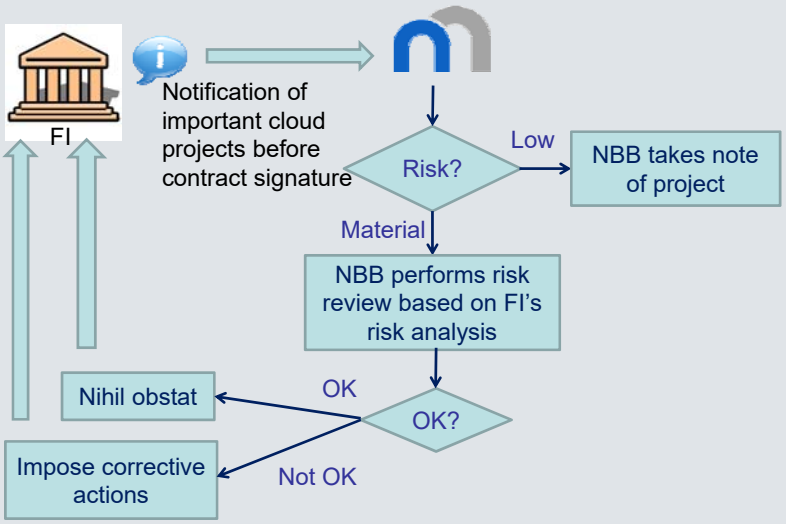
Risk Assessment Layers

Technology	Legal and contract	CSP Internal Organisation + Control Environment	CSP Transparency + Assurance Framework	FI Internal Organisation + Control Environment	Concentration risk and/or systemic risk

FI CLOUD RISK ASSESSMENT

FINANCIAL STABILITY IMPACT ASSESSMENT

Process



Examples of Compliance Issues

- Black boxes/insufficient information
- Non compliant cloud contracts
  - No right to audit for FI
  - No right to audit for the regulator
  - Termination clauses
- Inadequate audit assurance for FIs
  - External certifications not complete enough

→ Objections from regulators

Conclusion

- Compliance with NBB outsourcing circular
- FI performs a risk assessment

- Progress made by some CSPs regarding:
  - Compliance
  - Transparency

References

- Mededeling NBB_2012_11 / Prudentiële verwachtingen ten aanzien van Cloud Computing
https://www.nbb.be/doc/cp/nl/ki/circ/pdf/nbb_2012_11nl.pdf

- Circulaire PPB 2004/5/ Gezonde beheerspraktijken bij uitbesteding door kredietinstellingen en beleggingsondernemingen
https://www.nbb.be/nl/artikels/circulaire-ppb-20045-gezonde-beheerspraktijken-bij-uitbesteding-door-kredietinstellingen-en