Nordea

International TPRM Rollout

Challenges and Triumphs

Ken Wolckenhauer, VP Vendor Management

6.6.2018

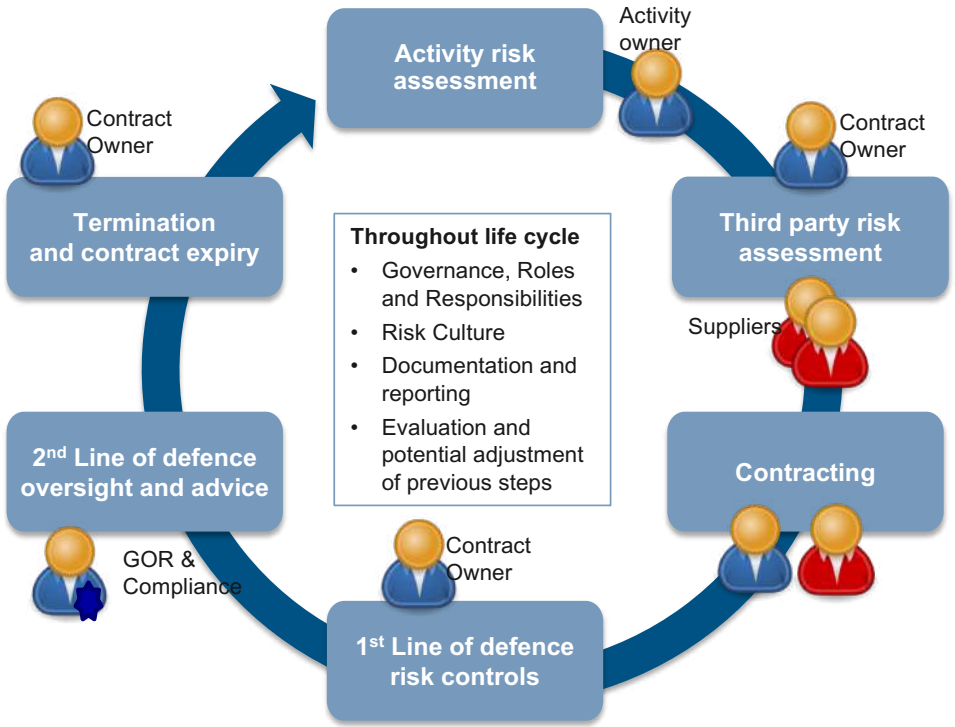
Background

- 2013 – Local NY audit finding led to compliance with SR-1319 at the branch
- 2014 – NY Program reviews all its vendors in accordance with Fed and NY guidelines
- 2015 – Nordea Group creates operational risk team to develop TPRM program
  - OCC model recommended by consultants and NY branch as comprehensive
- 2016 – Framework is launched in Nordics
- 2017 – Operation is handed over to a project team of risk specialists to create permanent operations.
  - Critical suppliers are reviewed
  - New suppliers and new contracts are reviewed
- 2018 - Operations begins merger with 1st line Business Risk organization

Third Party Status Report (TPS Report)

Framework

- The risk assessment of a selected process/activity **includes all relevant risk from an activity angle**
- Flag which risk control frameworks should be applied later on in the process



- Establish transition plan with the third party **ensuring a secure transition** when contract is terminated

- 2nd Line of defence **monitors and performs independent review** of the banks' third party risks

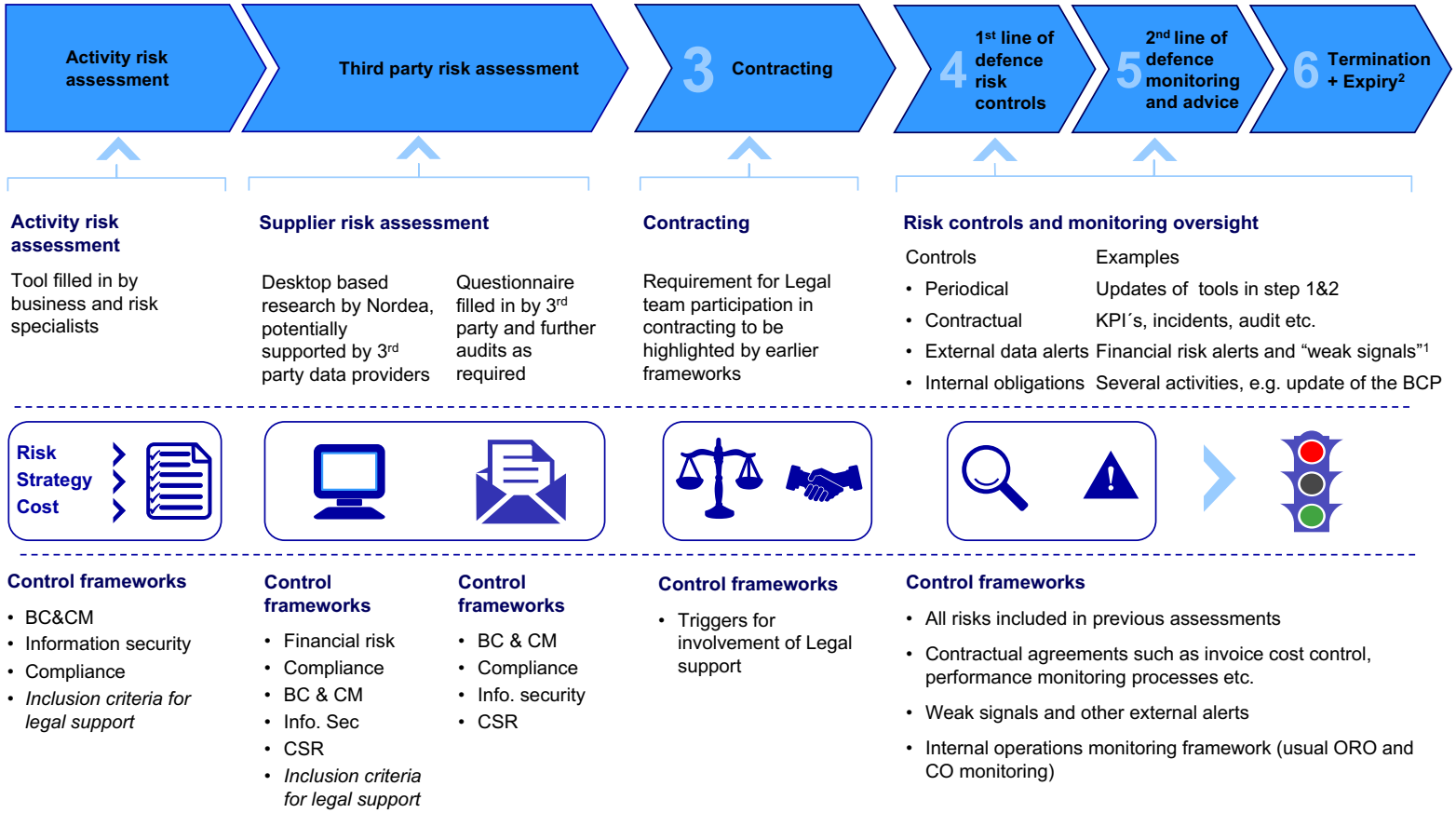
- The 3rd party risk assessment **includes all relevant risks from a 3rd party angle**
- This results in a 3rd party specific dashboard guiding next steps in the TPRM process

- After assessing 3rd party risk, **the responsible unit for the contract decides to contract with the 3rd party**
- The legal team engages in contracts where legal risk is flagged in preceding activity and 3rd party risk assessments

- Based on steps 1, 2 and 3 and in light of the general requirements in the framework, **the responsible unit for the contract performs controls regarding third party risks**

Nordea

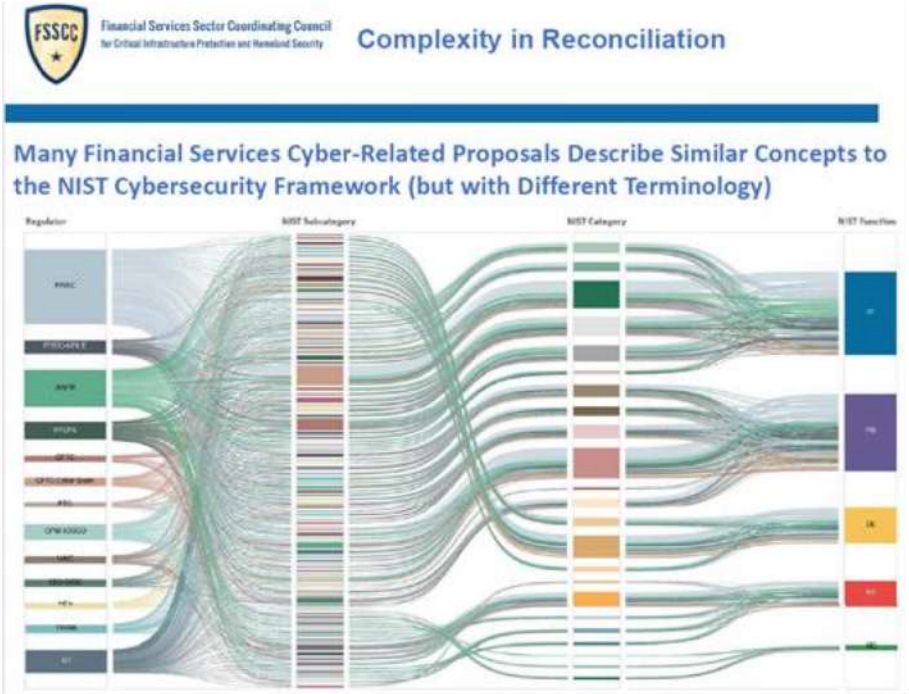
Who Developed the Framework


Activity risk assessment
Third party risk assessment
3 Contracting
4 1st line of defence risk controls
5 2nd line of defence monitoring and advice
6 Termination + Expiry2
Activity risk assessment
Tool filled in by business and risk specialists
Supplier risk assessment
Desktop based research by Nordea, potentially supported by 3rd party data providers
Questionnaire filled in by 3rd party and further audits as required
Contracting
Requirement for Legal team participation in contracting to be highlighted by earlier frameworks
Risk controls and monitoring oversight
Controls
Examples
• Periodical
Updates of tools in step 1&2
• Contractual
KPI´s, incidents, audit etc.
• External data alerts
Financial risk alerts and "weak signals"1
• Internal obligations
Several activities, e.g. update of the BCP
Risk
Strategy
Cost
Control frameworks
• BC&CM
• Information security
• Compliance
• Inclusion criteria for legal support
Control frameworks
• Financial risk
• Compliance
• BC & CM
• Info. Sec
• CSR
• Inclusion criteria for legal support
Control frameworks
• BC & CM
• Compliance
• Info. security
• CSR
Control frameworks
• Triggers for involvement of Legal support
Control frameworks
• All risks included in previous assessments
• Contractual agreements such as invoice cost control, performance monitoring processes etc.
• Weak signals and other external alerts
• Internal operations monitoring framework (usual ORO and CO monitoring)

Nordea

International Regulations

- US
  - DFS 500
  - FFIEC SR 04-20, 13-19, 00-17
  - OCC 2013-29
- Singapore
  - MAS Guidelines on Outsourcing Risk Management
- EAB
  - Basel Committee – Outsourcing of Financial Services
- China
  - Article 25 of the Guidelines on Internal Control of Commercial Banks issued by the CBRC.



Nordea

Risk Categories

- Financial
  - High financial risk exposure and vendor credit checks
- Information Security
  - Includes Cybersecurity and confidentiality
  - Cloud Review Board
- Business Continuity & Crisis Management
  - Tiers for criticality
- Compliance
  - Investment
  - Conflict of Interest
  - Sanctions and AML
- Corporate Social Responsibility and Sustainability
  - Labor
  - Environment
  - Human Rights

Nordea

Information Security

- SISQ –
  - ISO Framework
  - Nordic regulations and guidelines
  - GDPR (added 2018)
  - DFS 500 (added later 2018)
- Information Security Guidelines documents for suppliers
  - Follows the framework and provides details
  - Supplier has to agree to the guidelines
- Internal Controls
  - Cloud Review Board
  - Early architecture assessment
- Contractual Controls
  - Right to Audit
  - KPIs
  - Assure 4th party due diligence
  - MFA (if necessary)

Challenge: With so many local regulations and guidelines, how do we create a questionnaire that is comprehensive and yet compliant?

Challenge: How to we move to a shared assessments model when local requirements vary.

Business Continuity & Crisis Management

- Tier structuring
- Exit Strategy
  - Contractual concerns
  - SLA
  - Alternate suppliers
- Contingency Plan
  - Timeline
  - Alternate suppliers

Challenges:
- Suppliers with sub-contractors
- Time zones
- SLA/ priorities of head office and branches

Compliance

- Laws/regs involving investment services
- AML/Sanctions
- Conflict of Interest
- Anti-bribery and corruption
- Compliance with internal policies

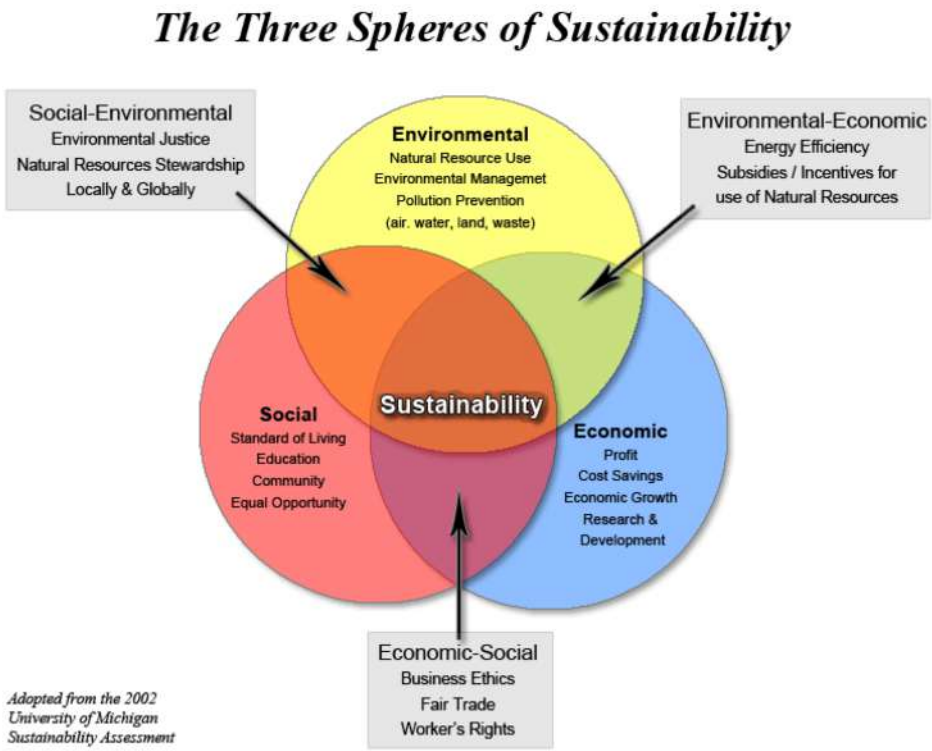
Challenges:
- Local laws, regs, customs
- Use of subcontractors and international offices
- Dealing in high risk countries
- Group compliance vs. local legal & compliance

Nordea

Corporate Social Responsibility & Sustainability

- UN Global Compact
- The Paris Agreement

- Challenges:
  - Local rules and customs in non-Euro countries, including US, Russia, China
  - Attitude towards UN
- The Paris Agreement
  - Commitments and measurement



Nordea

Who is Doing the Assessment

What‘s in Scope

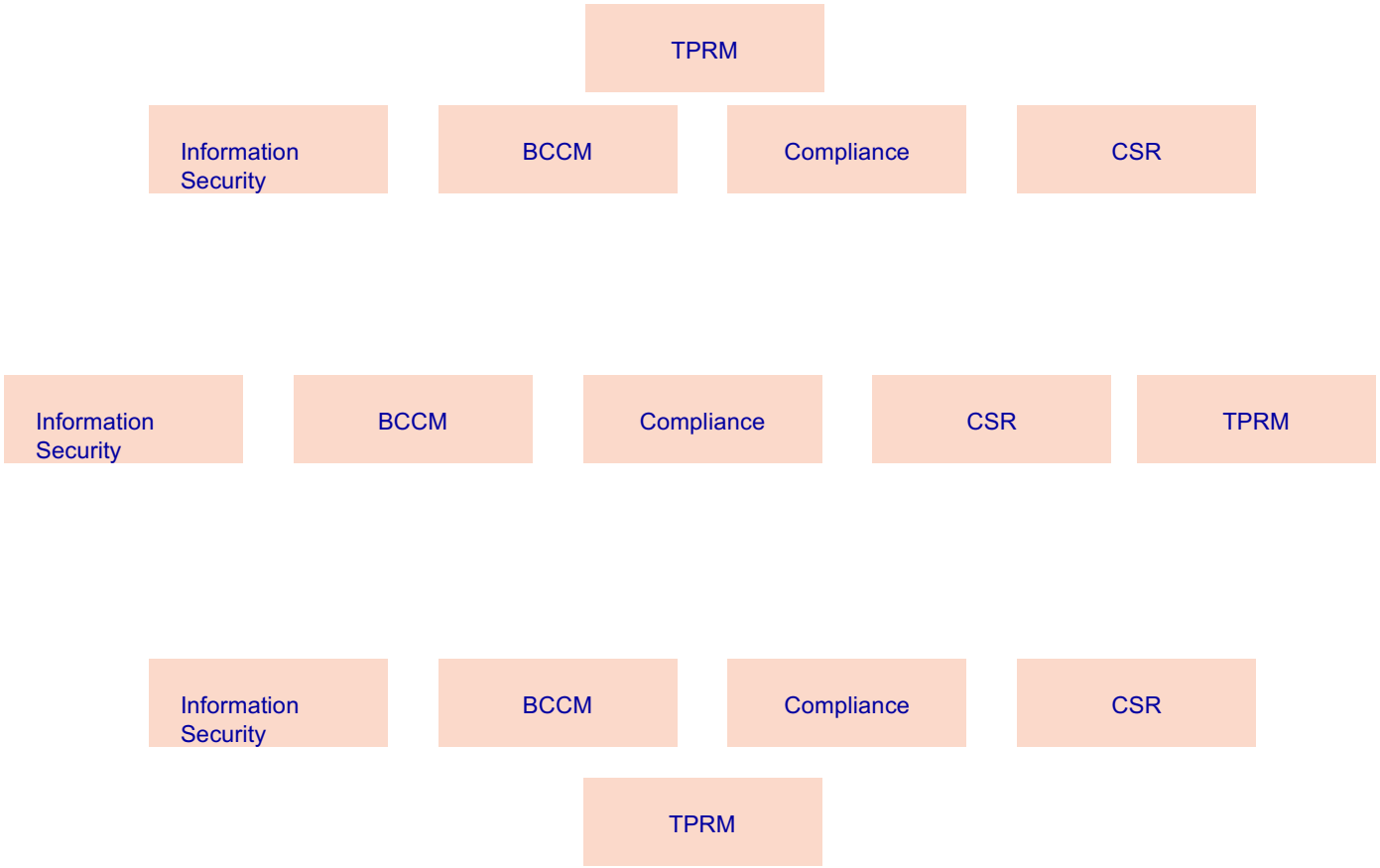
- Tier 1 & 2
- Change Management
- Access
- Large contracts
- Outsourcing
- Regulated Activites
- Charities
- Intra-Group contracts

How to Structure the TPRM Organization

- Governance Ranking
  - Policies, Guidance, CEOs
- Authority of TPRM vs Control Groups
- 1st LOD / 2nd LOD
- Competencies and role of TPRM organization
  - Help Desk
  - Managing the tool
  - Procedural Guidance
  - Risk Guidance
  - Enforcement
  - Reporting
- What organization should run 1st line?
  - Sourcing/Procurement
  - Vendor Management
  - Risk Specialists

Nordea

1st LOD Organizational Models



Nordea

How to Identify New Activities and Contracts

- Reconciling with Accounts Payable
- Contract management system
- Vendor management system
- Business line inventory reporting

- Pain points
  - A/P
  - 2nd Line
  - Audit

Identifying Phase 1 and 2

- Identifying and ranking third parties
- Estimating time to review
- Priorities – new activities and contracts vs backfill

Nordea

Thank you!

Ken Wolckenhauer, VP Vendor Management
kenneth.wolckenhauer@nordea.com