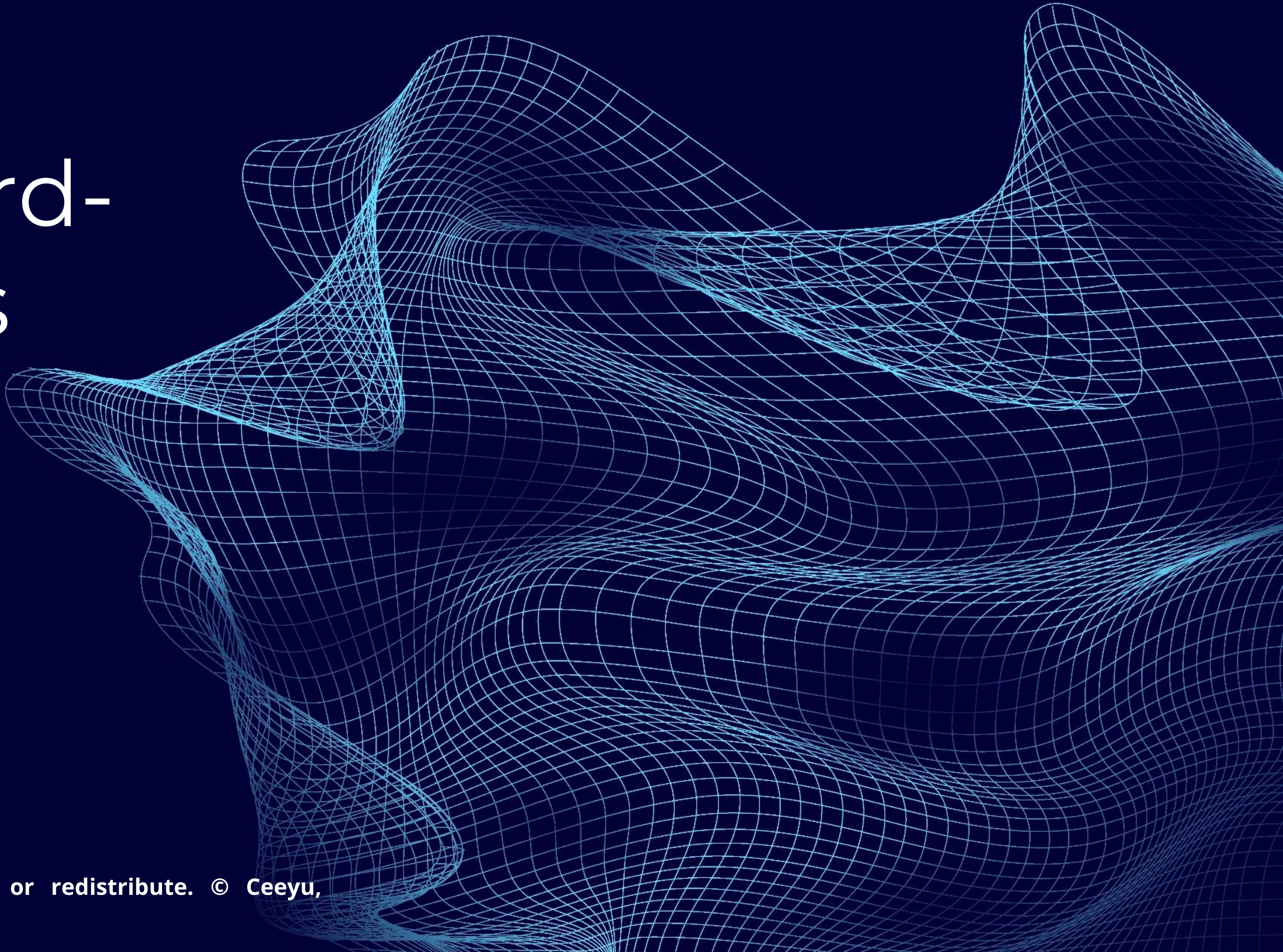
Ceeyu

How to reduce third-party security risks



Jimmy Pommerenke, CEO

14 september 2023

Who am I?

- **+20 years of experience in Cyber Security**
- **Degree in computer science, started as a security engineer. Duties included installing firewalls, vulnerability scanning and pen testing**
- **Responsible for cyber security programmes at major financial institutions and consulting firm EY**
- **Founded Ceeyu in 2020 after years of careful preparation**

Can you answer these questions?

- ❓ Do you know who are your **critical** suppliers?
- ❓ What is the **risk** they pose to your organization?
- ❓ Are you able to **quantify** that risk?
- ❓ Do you have a **TPRM** programme?
- ❓ On a scale of 1-10, how **satisfied** are you with the output of the programme?

Knowing third-party risks is important ...

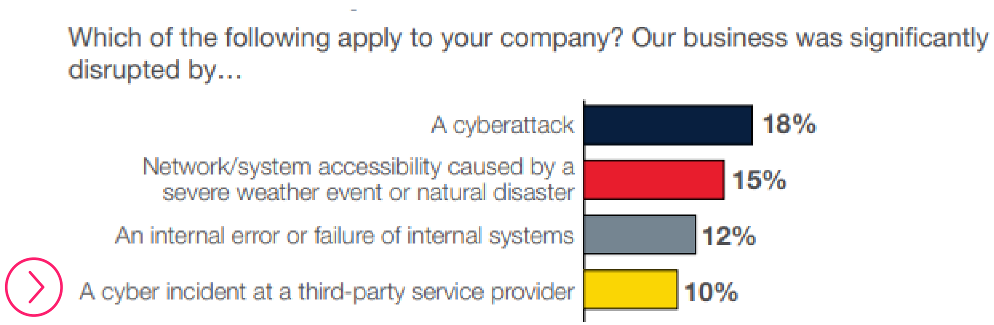
These companies have recently been breached because of a third party breach

- The metropolitan police
- The UK Electoral Commission
- Linkedin 2023 (and 2012, 2015, 2021, ...)
- Twitter (X)
- ChatGPT
- Atlassian
- MailChimp
- T-Mobile

The IBM MOVEit Cyber Attack: BBC, British Airways, Aer Lingus, ...

Some older ones: Equifax (2016), Tesco (2106), Dixons Carphone (2018), EasyJet (2020), NHS (2012), Virgin Media (2020)

It's not only about the security risks, it's about business continuity (average downtime after an attack = 20 days)



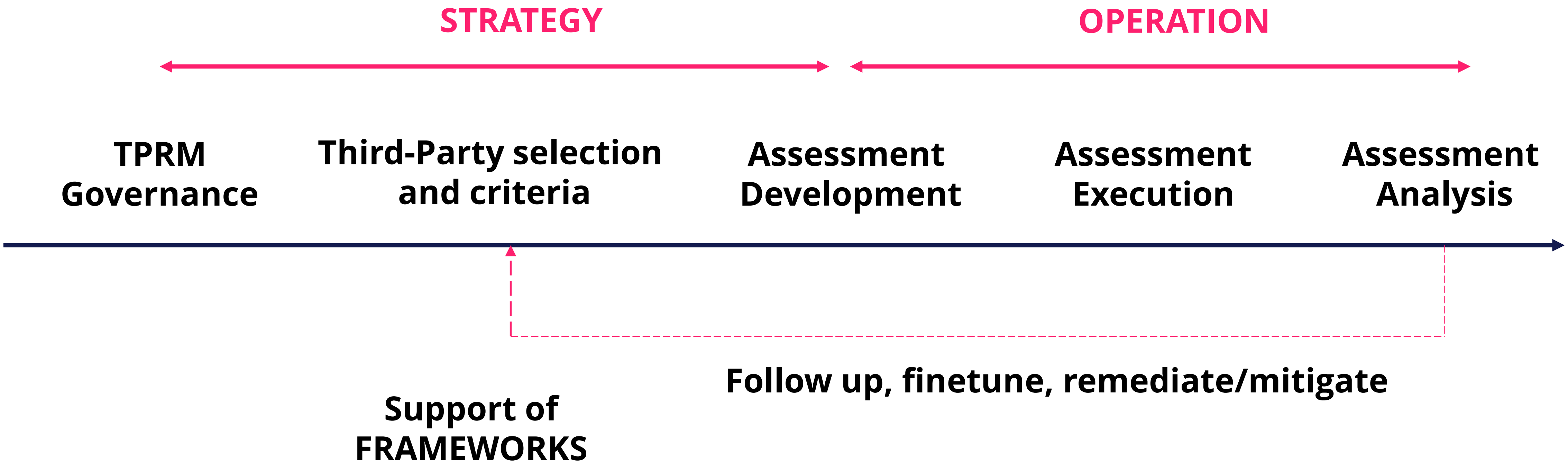
Which of the following apply to your company? Our business was significantly disrupted by…

Source:

INFORMATIONWEEK

06/2023, n=180 IT managers

Let’s start by having a look at the phases of a Third-Party Risk Management Program



STRATEGY

OPERATION

TPRM Governance

Third-Party selection and criteria

Assessment Development

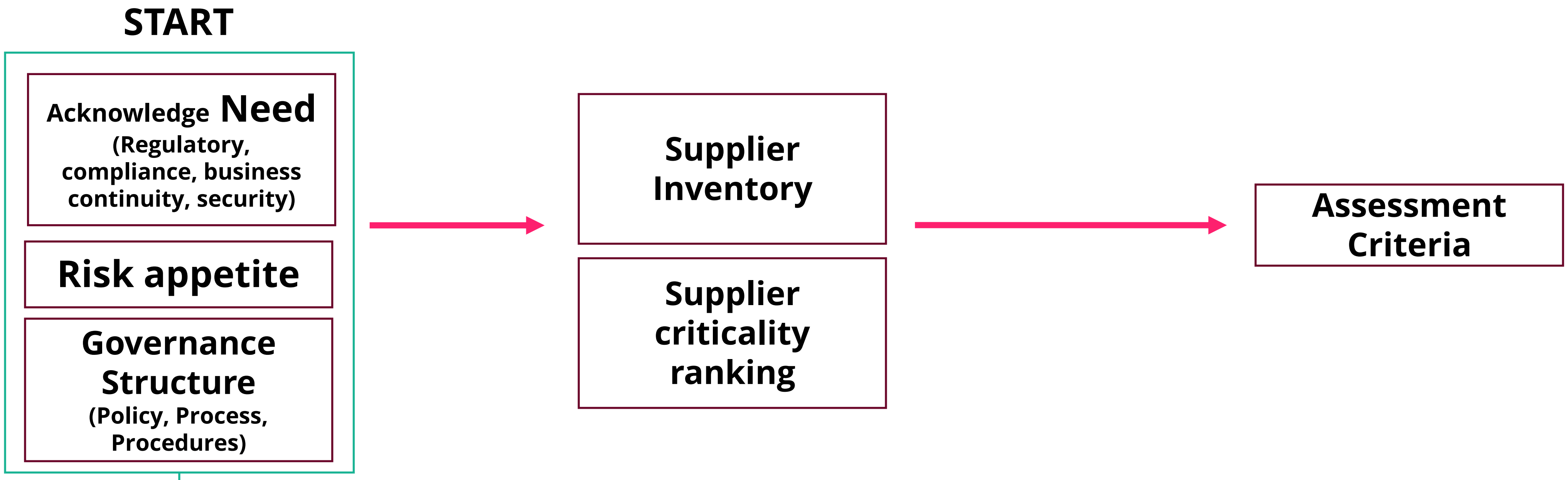
Assessment Execution

Assessment Analysis

Follow up, finetune, remediate/mitigate

Support of FRAMEWORKS

STRATEGY - TPRM governance



START

Acknowledge **Need** (Regulatory, compliance, business continuity, security)

Risk appetite

Governance Structure (Policy, Process, Procedures)

Supplier Inventory

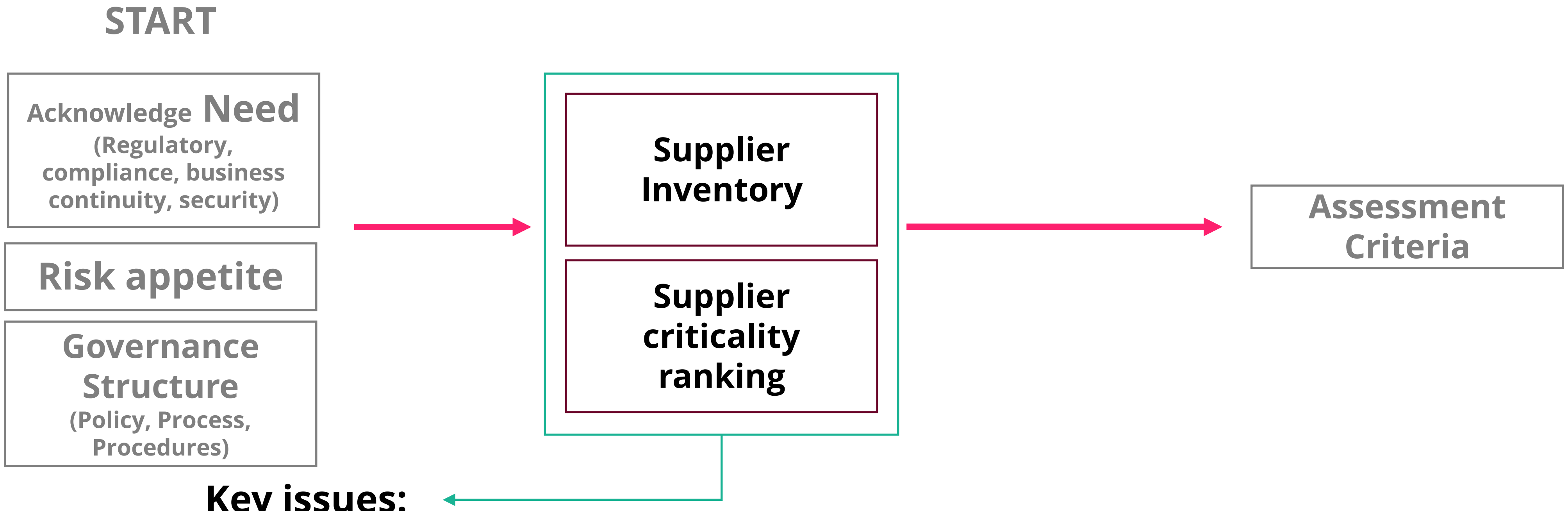
Supplier criticality ranking

Assessment Criteria

Key issues:

- Not having a TPRM Governance
- The need wasn't properly captured, difficult to get people on board
- Risk appetite is not clearly defined

STRATEGY - Third Party inventory and selection criteria



START

Acknowledge **Need** (Regulatory, compliance, business continuity, security)

Risk appetite

Governance Structure (Policy, Process, Procedures)

Supplier Inventory

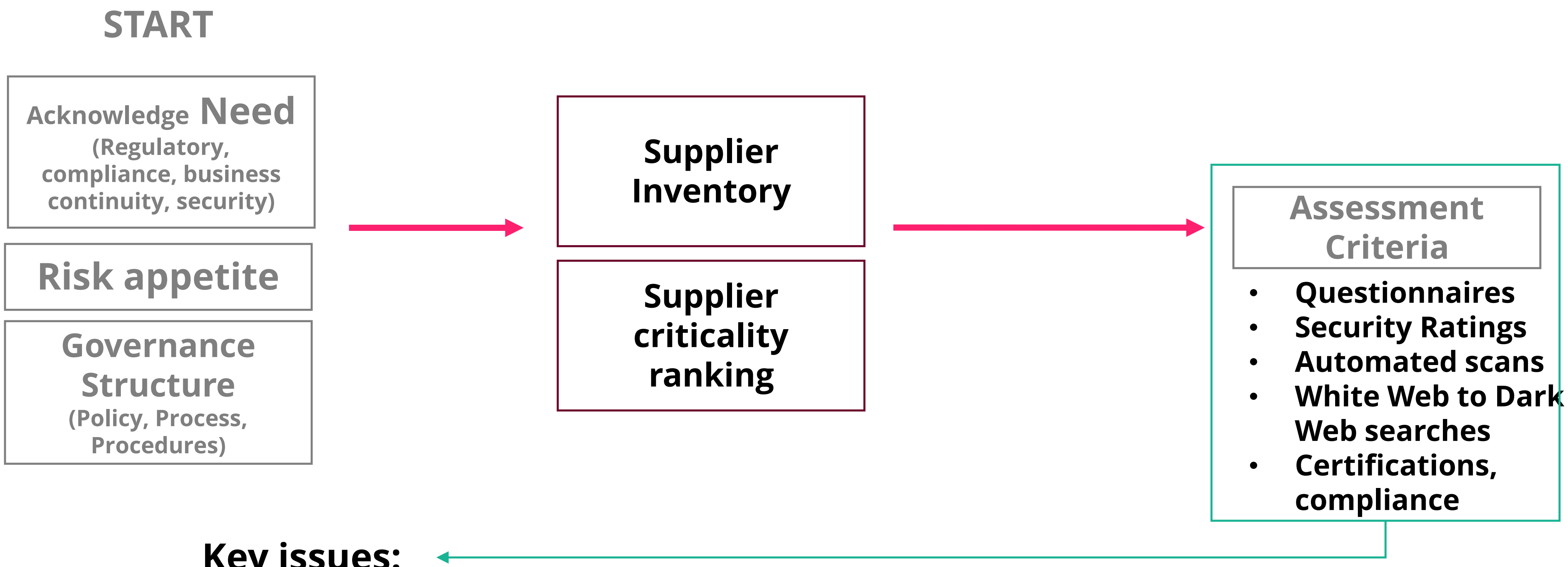
Supplier criticality ranking

Assessment Criteria

Key issues:

- **Some suppliers (of specific departments) are missing (=> Importance of Senior Management buy in)**
- **Over- or underestimating the criticality (=> High workload may affect supplier relationship)**
- **Overquantifying the impact of a vendor (=> KISS, in most cases, this is common sense)**
- **Underestimating the resources you need to operate the process**

STRATEGY - Assessment criteria definition



START

Acknowledge **Need** (Regulatory, compliance, business continuity, security)

Risk appetite

Governance Structure (Policy, Process, Procedures)

Supplier Inventory

Supplier criticality ranking

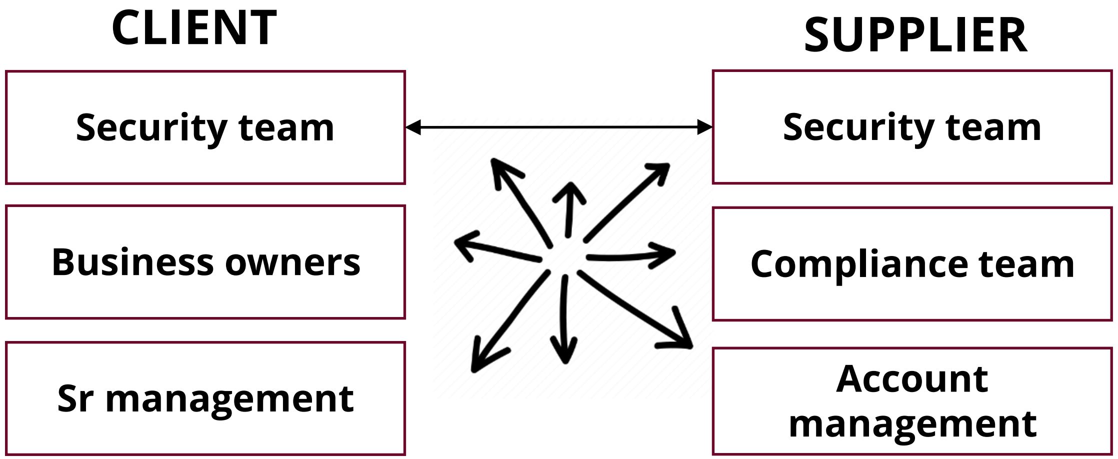
Assessment Criteria

- **Questionnaires**
- **Security Ratings**
- **Automated scans**
- **White Web to Dark Web searches**
- **Certifications, compliance**

<u>Key issues:</u>

- **Questionnaires can be too long (or short), too many, too generic (or specific), irrelevant => MAJOR impact on participation rate**
- **Other types of assessment are useful and can provide insight, but dangerous to solely rely on them as they are not specific to your relationship, however acceptable depending of risk appetite and supplier severity**

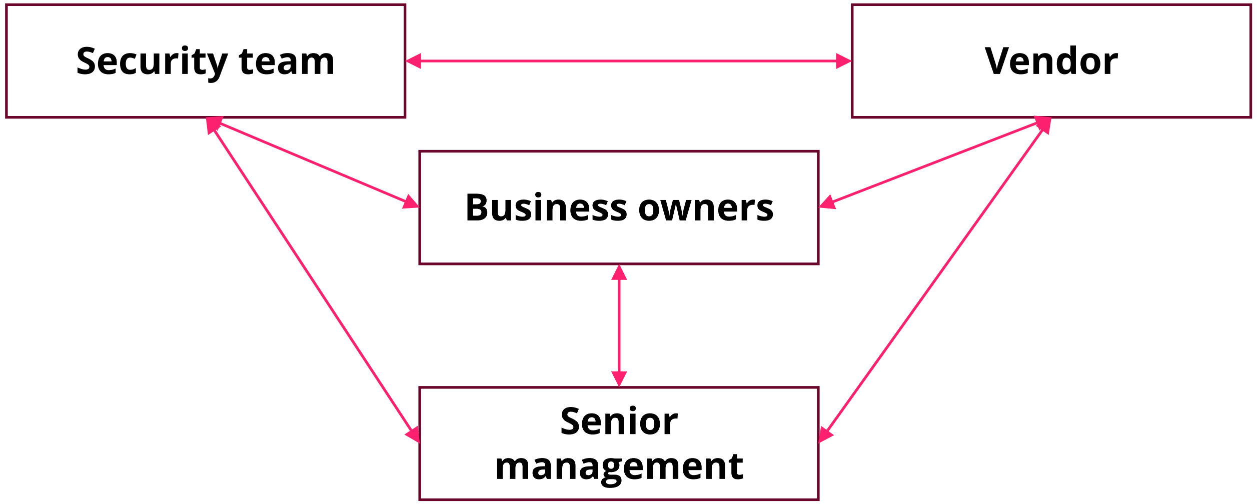
OPERATIONS - Assessment execution



Key issues:

- It takes time! => Time consuming; please align the risk appetite with the resources available
- Limit the assessment to what's necessary given the type and criticality of the vendor
- No support from business owners at the client side => Business and and senior management support are key to success
- Unresponsive vendors/low quality answers => take this into account in the buying process (security is key), alternative assessments (ratings, certifications) are an acceptable fall back depending on vendor criticality, be able to escalate
- Malicious compliance
- Suppliers referring to self-assessments and certifications => restrict your assessment to what's key and insist

OPERATIONS - Assessment conclusions



Key issues:

- **Too much data to go through**
- **Back and forth between teams and vendors**
- **Low quality of information received prevents good interpretation**
- **Subjective analysis**
- **No consequences in case of a poor conclusion**

Key Takeaways

1. **TPRM Governance: Have a realistic plan, backed by Senior Management**

2. **Third-Party Selection and Criteria: Know your key suppliers and their impact on your organization, have business owners backing**

3. **Assessment Definition: Use compact but relevant questionnaires for key suppliers**

4. **Assessment Execution: Be very clear on what you expect by when from suppliers, have an escalation path defined prior to the start**

5. **Assessment Analysis: Use pre-defined objective criteria for analysis, involve business owners**

Who’s Ceeyu?

Ceeyu **identifies** IT and network **security risks**

for **your company and your supply chain**

by combining **automated scans** with online **questionnaire-based risk assessments**

Trusted by

GlobalSign by GMO

De Watergroep

ORDINA

casa

KONINKRIJK BELGIË
Federale Overheidsdienst
Buitenlandse Zaken,
Buitenlandse Handel en
Ontwikkelingssamenwerking

LRQA NETTITUDE

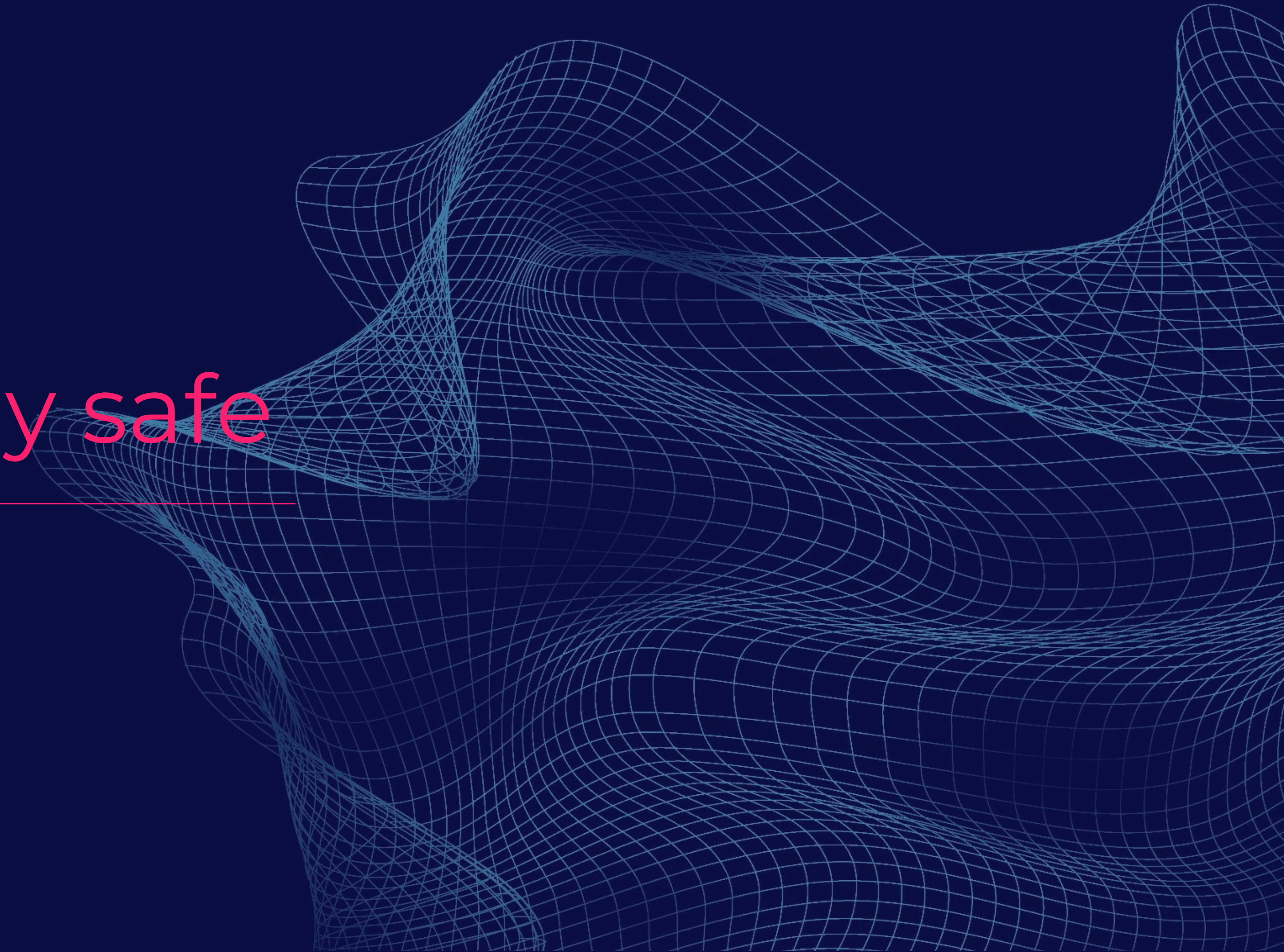
modero

VERELST
BEDRIJFSBOUW & RENOVATIE

Ceeyu

Ceeyu

External risk identification and management



Thank you and... stay safe

CEEYU

hello@ceeyu.io
+32(0)15 48 14 14

www.ceeyu.io