

SQUARE TABLE

**Operational Resilience.
The new normal for keeping
services running**

Speaker: Mirna Bognar

**October 21, 2020 - Online Webinar
19:00 - 20:00
CPE: 1 point**



ISACA®
Netherlands Chapter

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS



Talking about resilience...



Why Operational Resilience

Slide from Feb 2020

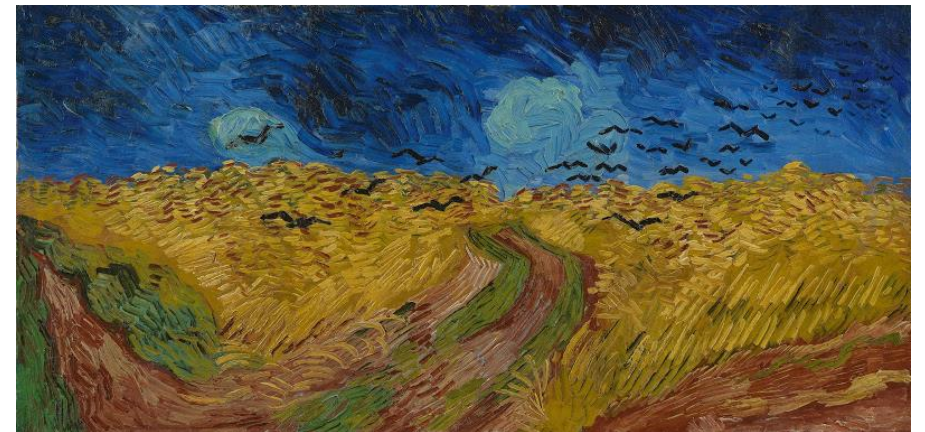
- Digitalisation of services and products
- Dependency on digitalisation is high:
 - E.g. WEF: critical infrastructure failure listed as sixth global risk in terms of impact
- Operational resilience is key
 - For organisations to stay in business
 - For consumers to safeguard their trust in digitalised economy and society



Credits: Van Gogh Museum, Amsterdam
(Vincent van Gogh Stichting)

Improving IT operations and strengthening Business continuity. Are we done?

- From an organisation's perspective:
 - E.g. IT changes that result in triggering a crisis or media attention due to unavailability
 - E.g. Can we handle data corruption incidents?
 - What should the target state be?



Credits: Van Gogh Museum, Amsterdam
(Vincent van Gogh Stichting)

Expectations regarding availability of digitalised services are high...

- Dutch National Bank requires availability of time-critical payment orders in peak demand periods



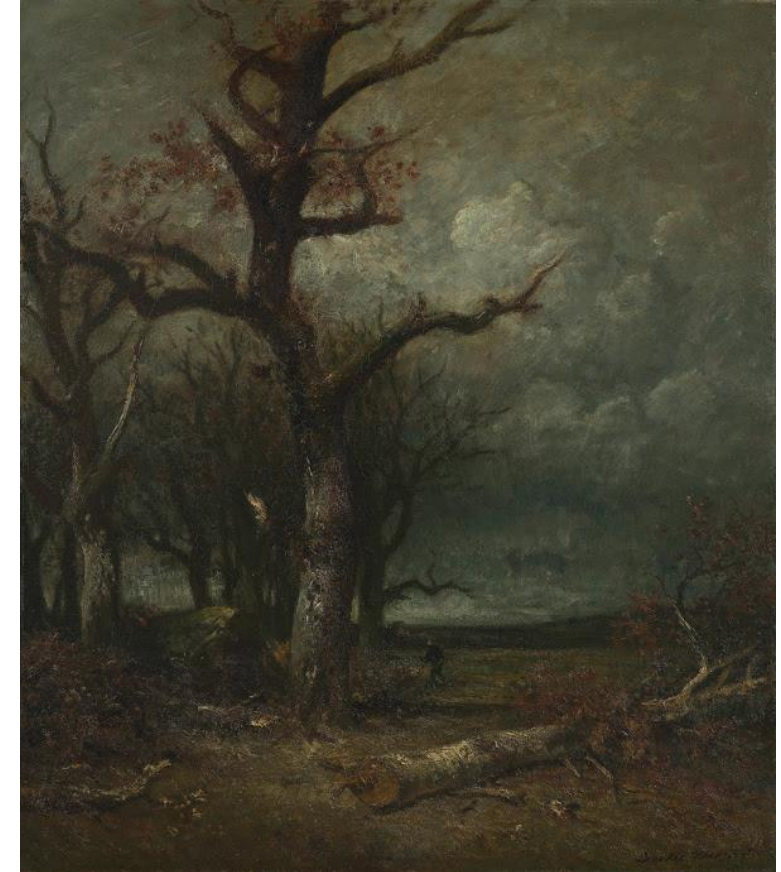
Availability of payment chains				
Availability	2016 (%)	2017 (%)	2018 (%)	2019 (%)
Chip-and-pin and contactless	99,88 (>99,64)	99,88 (>99,76)	99,89 (>99,88)	99,89 (>99,88)
Mobile banking	99,77	99,83	99,75	99,81
Internet banking	99,79	99,83	99,72	99,78

Source: Dutch Payment Association

- Internationally:
 - National critical infrastructures
 - Resilience against “severe but plausible events”

... While threats to digitalised services and processes are increasing

- Cybercrime
- Complexity of IT systems/unintended impact of innovation and IoT
- Interconnectedness in supply chain
- WEF: *"The lack of a global governance framework for technology risks fragmenting cyberspace, which could deter economic growth, aggravate geopolitical rivalries and widen divisions within societies."*



Credits: Van Gogh Museum, Amsterdam
(Vincent van Gogh Stichting)

Some regulatory trends (in FI) regarding operational resilience...

- In finance (all draft)
 - UK: Bank of England/FCA/PRA Building Operational resilience
 - EC Digital operational resilience act (DORA)
 - BCBS Operational resilience
- Objectives:
 - Stability – of “system” (economic, financial...)
 - Protection of consumers’ interest
 - Own strategies
- Drivers:
 - Dependency on availability of banking services
 - Cyber crime
 - Pandemic lessons learned: WFH, supply chain resilience



... Where Operational resilience is defined as...

- [illegible]

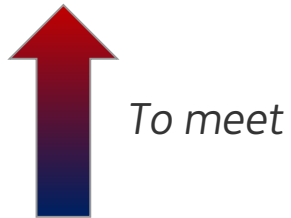


... And requires the following measures:



Approach at ING: Operational resilience of products/business services...

- Operational resilience target:
(e.g. 99,88% for customer-facing services during peak hours)



Objective:
E.g. Availability of
products/ business services

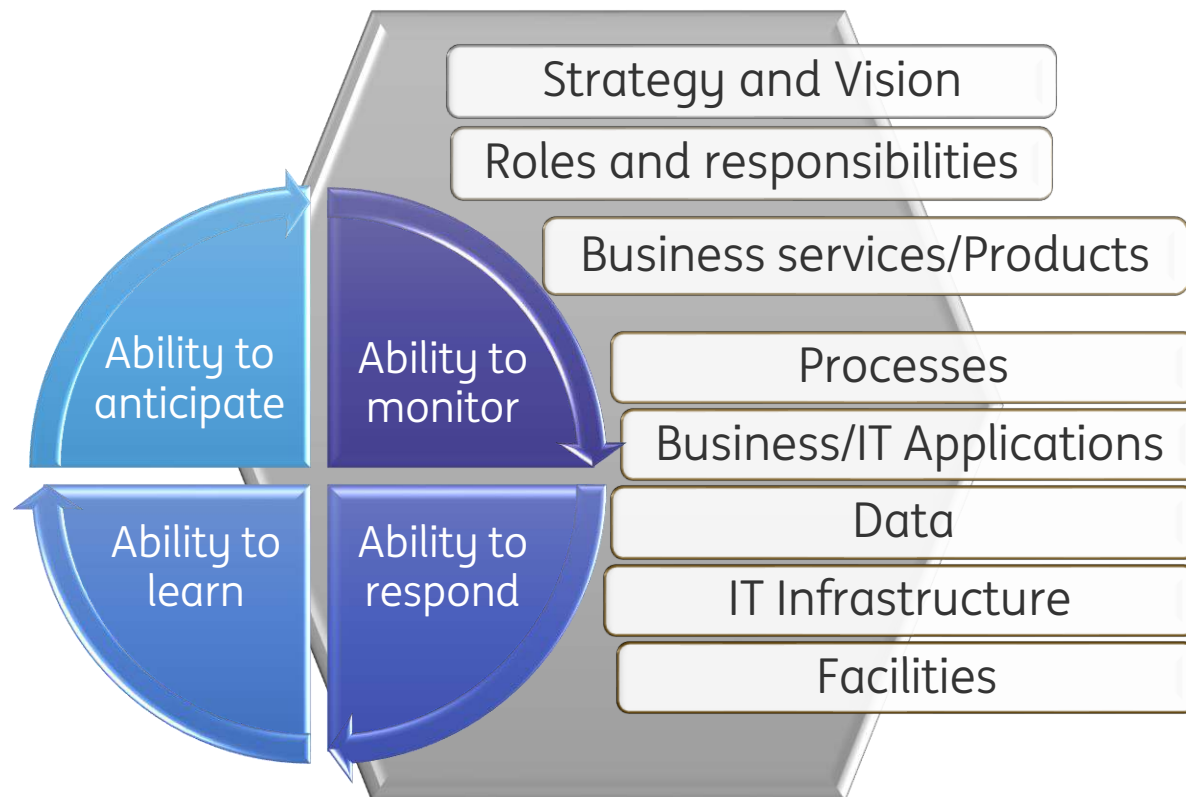
Achieved by

Measures:
Operational resilience

- *Operational resilience*
is the adaptability of an organisation to maintain its business functions in the face of
(turbulent) internal or external changes/events which do not exceed organisation's operational
limit

... by building the abilities to monitor, respond, learn and anticipate

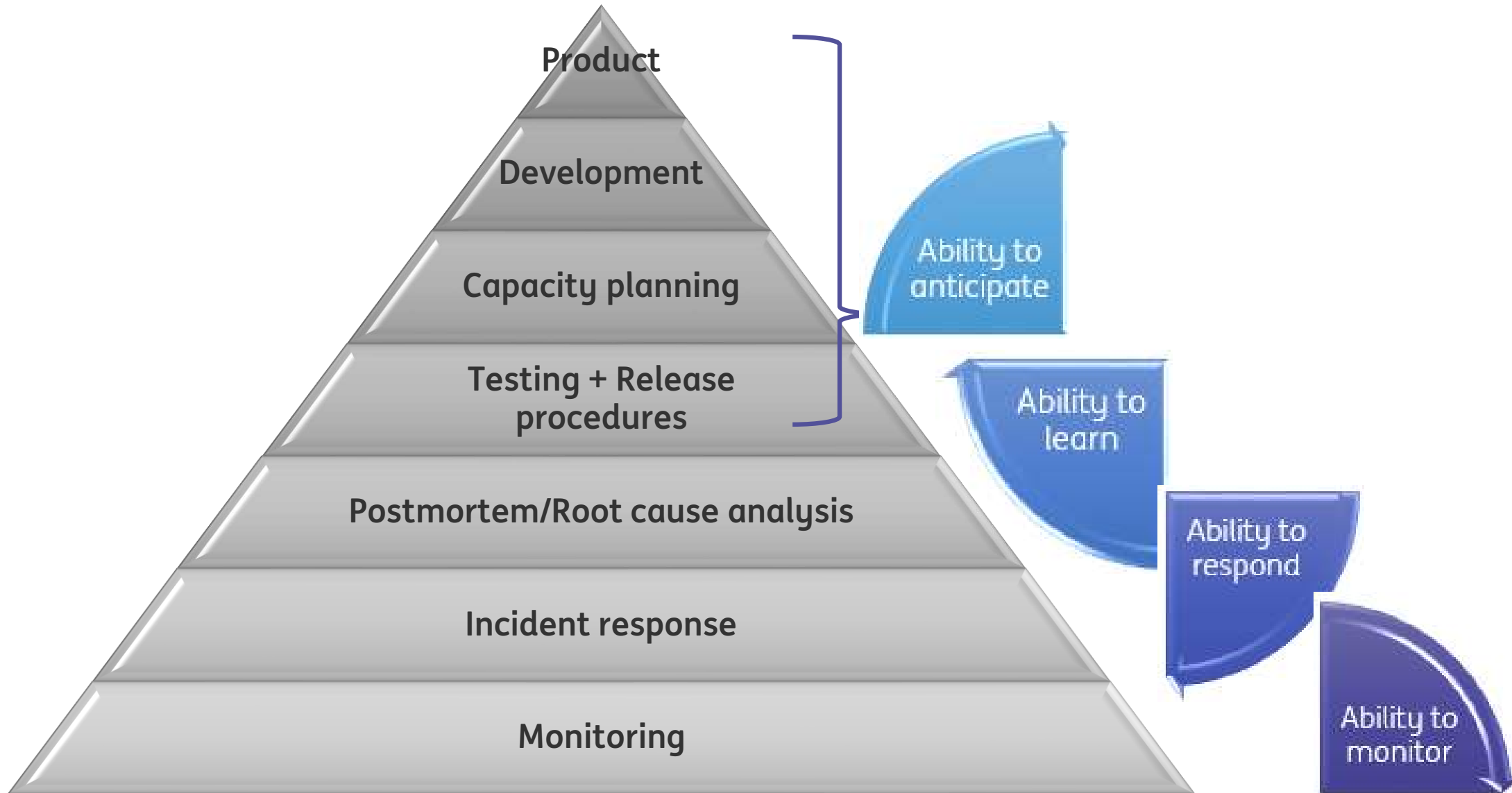
Expectations and requirements regarding operational resilience within Customer Experience

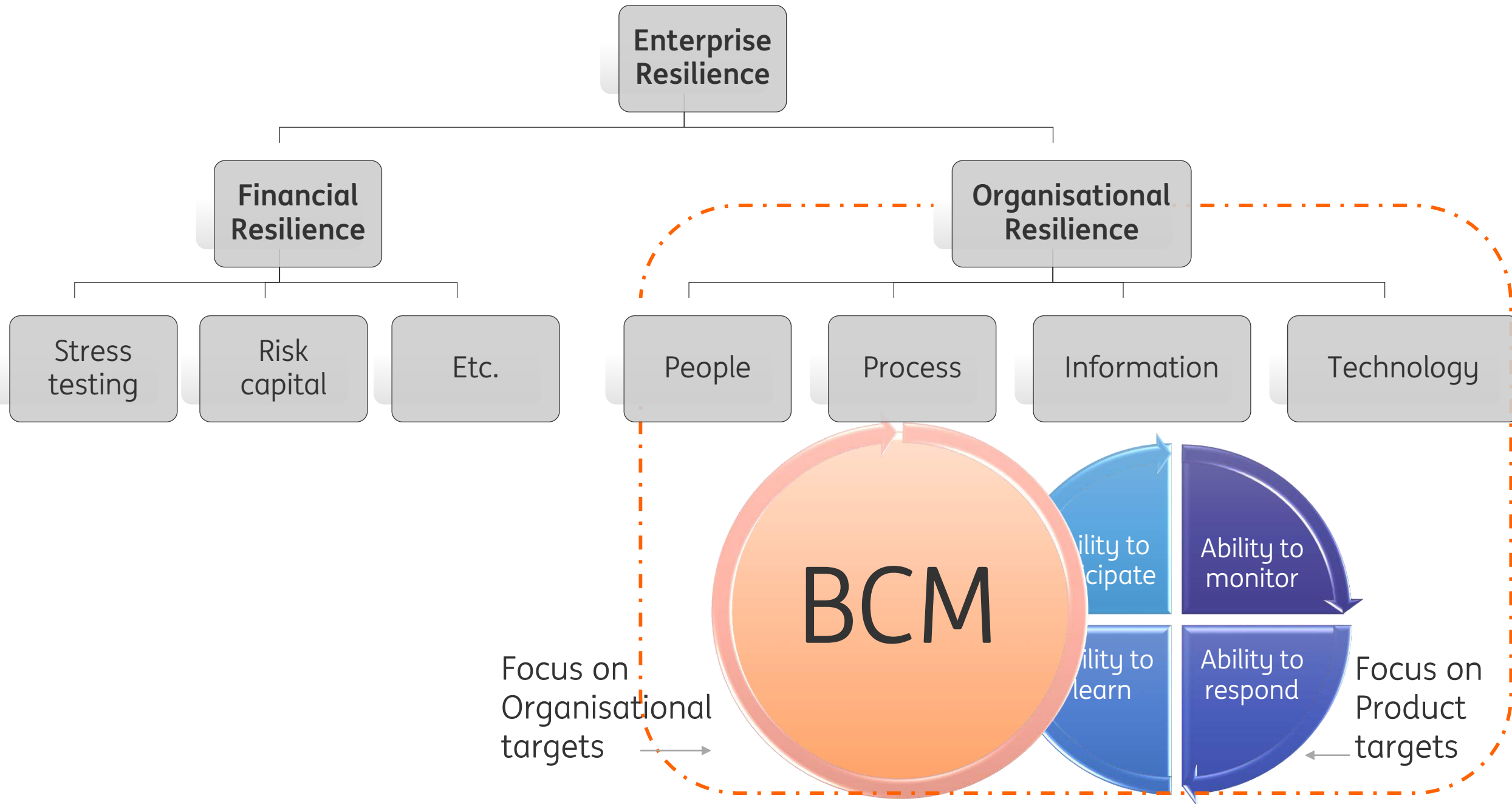


Objectives:

- Adopt a consistent end-to-end view on Business- and IT services' operational resilience, taking into account the targets to comply with
- Design resilient Business and IT services, and pro-actively monitor, respond to, and learn from any (turbulent) internal or external changes/events in order to meet the current or future operational resilience targets

Framework: Google* meets Resilience Analysis Grid model**



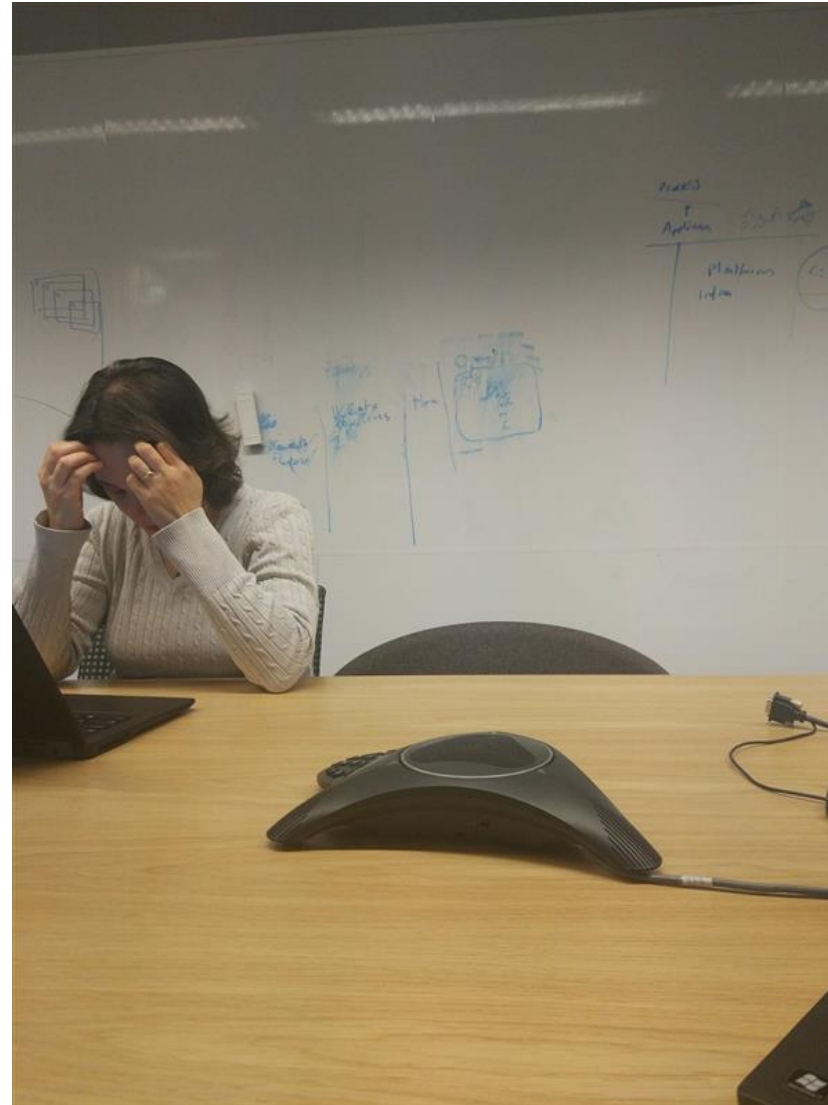


Implementation: Adopting a consistent end-to-end view, defining targets

- In scope:
 - Resilience-critical business services (with outside-in monitoring)
 - E.g. Business services with availability targets like critical payments 99,88%
 - Scoping is responsibility of Business
 - IT assets* with high-availability requirements (with internal monitoring)
 - As derived from resilience-critical business services
 - Scoping is responsibility of IT, based on business requirements
- Not all IT assets in scope:
 - Outside-in monitoring of business services will detect unavailable service; the IT asset(s) that caused it will be exposed



Implementation: Adopting a consistent end-to-end view, defining targets (ctd)



Implementation: Monitoring – responding – learning – anticipating in small entity

Triggers from Trends/Threats, Risk strategies, changes to targets

Resilience-by-design:

- IT Architecture
- Testing
- Capacity planning
- Monitoring relevant third parties

Monitoring and alerting

- (Real-time) Monitoring
- Thresholds vs targets
- Monitoring consumer complaints

Ability to
anticipate

Ability to
monitor

Ability to
learn

Ability to
respond

IT Problem management

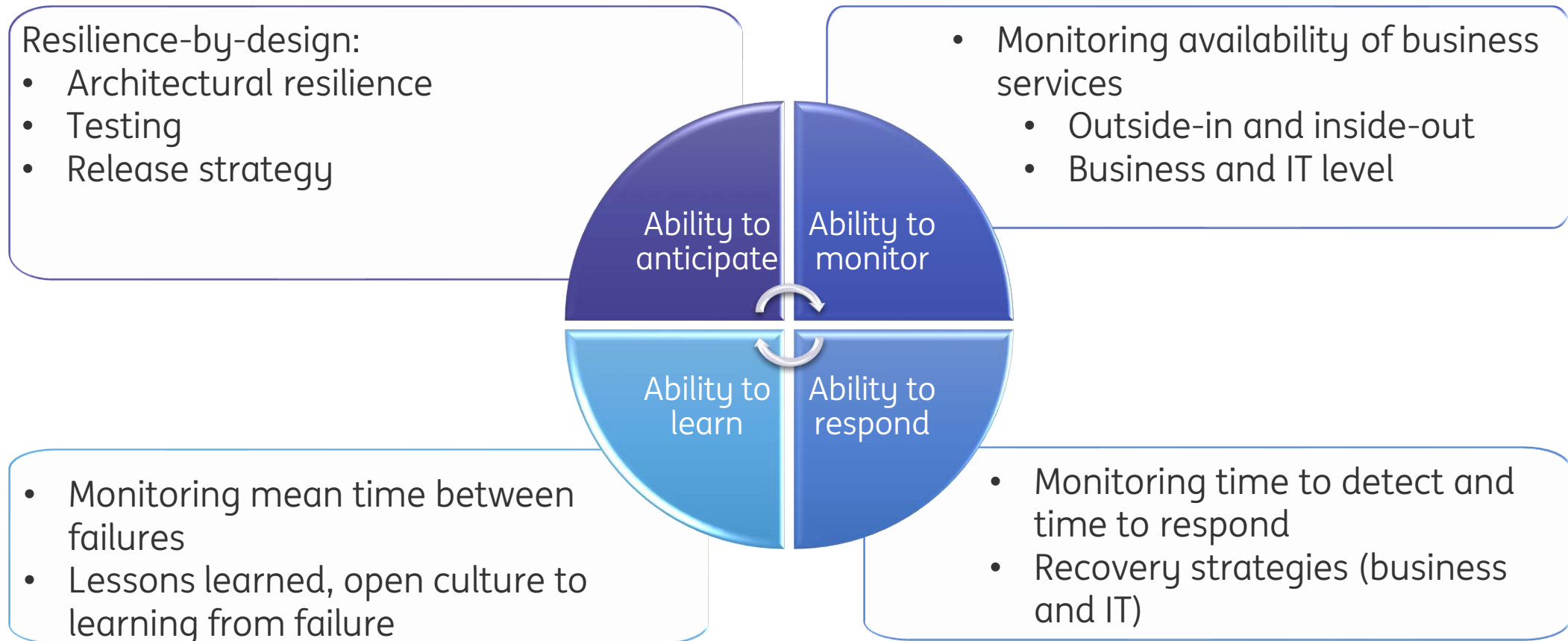
- Input for Process improvement
- Root cause analysis

IT Incident management

- Incident priorities vs consumer impact
- Backup and restore

Is it 'good enough': Measuring according to measurement model against defined targets

Implementation: Monitoring – responding – learning – anticipating in mature entity



Is it 'good enough': Measuring according to measurement model against defined targets

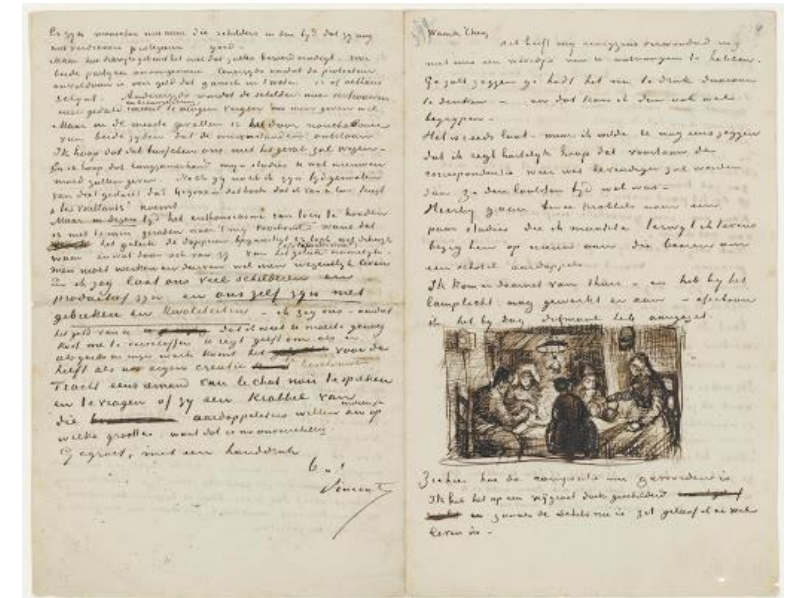
Implementation: Ability to anticipate – steering on priorities in DevOps by the Business

For example:

- Error budget
 - Business service must establish availability target
 - Error budget is $1 - \text{availability target}$, i.e. permitted unavailability of the service
 - Engineers can spend the budget on anything as long as it is not overspent
- Error budget becomes common incentive of developers and operations
 - Room for failure when innovating
 - A way to decide on the rate of releases and innovation (vs service availability)
 - A way to connect to the business

Implementation: Ability to anticipate – managing third parties

- Scope: third parties that materially support critical business services
- Two categories of risks: the risks of the use of third party and the risks caused by third parties
- Requirements for contracting, contract lifecycle, exit
 - Risk assessment, due diligence before contracting
 - Access to information, Right to audit
 - Exit strategies
 - Etc
- But also
 - Monitoring and testing security, including operational resilience



Credits: Van Gogh Museum, Amsterdam
(Vincent van Gogh Stichting)

EC DORA Article 28-39: OVERSIGHT FRAMEWORK
OF CRITICAL ICT THIRD-PARTY SERVICE PROVIDERS

Implementation: Guild

Organisation-wide

- Bi-weekly call to monthly call
- Members: anybody, started with IT and IT Risk, extended to business
- Objective: Interpretation of controls, sharing good practices, demos, questions
- Feedback loop on implementation
- In practice:
 - Open market for tooling, templates, transparency, consistency
 - Early warning to management regarding impediments
 - “Owned” by participants



Credits: Van Gogh Museum, Amsterdam
(Vincent van Gogh Stichting)

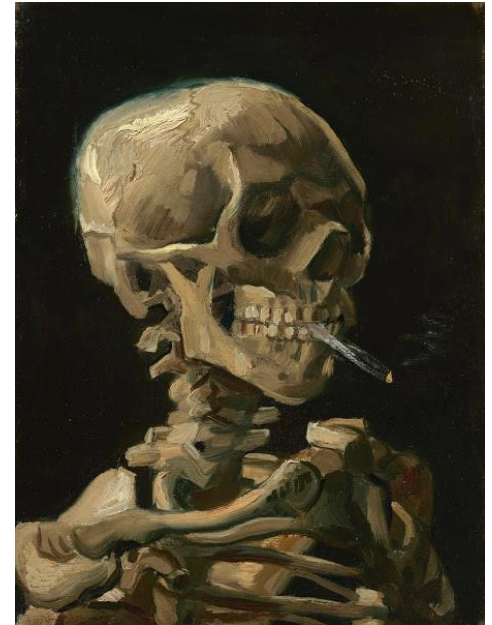
Implementation: Roles and responsibilities

- Executive committee responsible for
 - Defining operational resilience targets in line with expectations and requirements from the Customer Experiences and regulators; and
 - Designing, implementing and executing the controls
- Chief Operations Officer (COO) responsible for
 - Defining and maintaining the measurement models
 - Monitoring performance
- Chief Information Officer responsible for
 - Supporting COO in defining and maintaining the measurement models for IT;
 - Managing the abilities to anticipate, monitor, respond (including recovery) and learn for the resilience-critical IT services to meet the operational resilience target
- Business service owners responsible for his/her Business services
- Asset owners responsible for his/her IT Assets



Implementation: What went well

- Strong buy-in by the Bank CIO for
 - Move from IT asset-based approach to service-based approach
 - Collaboration between CIO and COO lines in implementation
- Outcome-based:
 - Whether a service is resilient or not, can be measured by whether the defined targets are met
- Measures in line with targets defined
- Teams helping each other
- Challenges in implementation have direct feedback to management and “policy makers”



Credits: Van Gogh Museum, Amsterdam
(Vincent van Gogh Stichting)

Implementation: What is improving

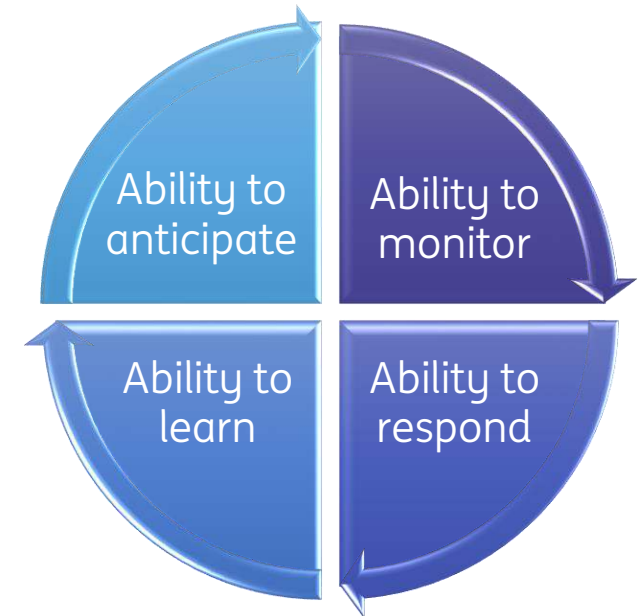
- Reaching out to the business at operational level: from IT resilience to operational resilience
- Maturing approach and implementation
 - No one-size-fits all approach between entities
 - Maturing in measurement methods
 - Maturing in steering



Credits: Van Gogh Museum, Amsterdam
(Vincent van Gogh Stichting)

Take aways

- Invest in alignment between business services and IT
- Operational resilience targets and measurement will enable outcome-based steering and will improve (business and IT) operations
- There are many ways to implement operational resilience
- Invest in the full cycle to optimise the outcome



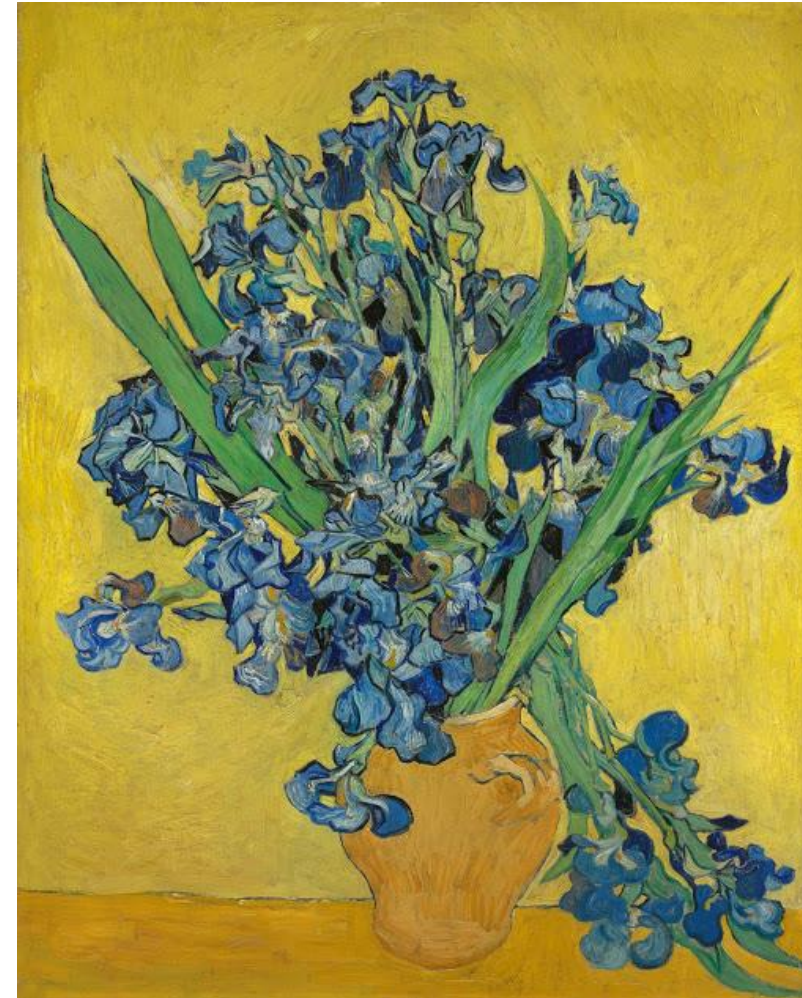
Questions?



Thank you for your attention

Mirna Bognar

ING Bank
Corporate Information Risk Management
M +31 622490260
E mirna.bognar@ing.com



All pictures of paintings are courtesy of Van Gogh Museum Amsterdam (Vincent van Gogh Stichting)

References

- [EC Digital Operational Resilience Framework for financial services \(in consultation till 17 Dec 2020\)](#)
- [BCBS Principles for operational resilience](#)
- UK: Bank of England [Operational resilience](#)
- [Oliver Wyman Striving For Operational Resilience](#)