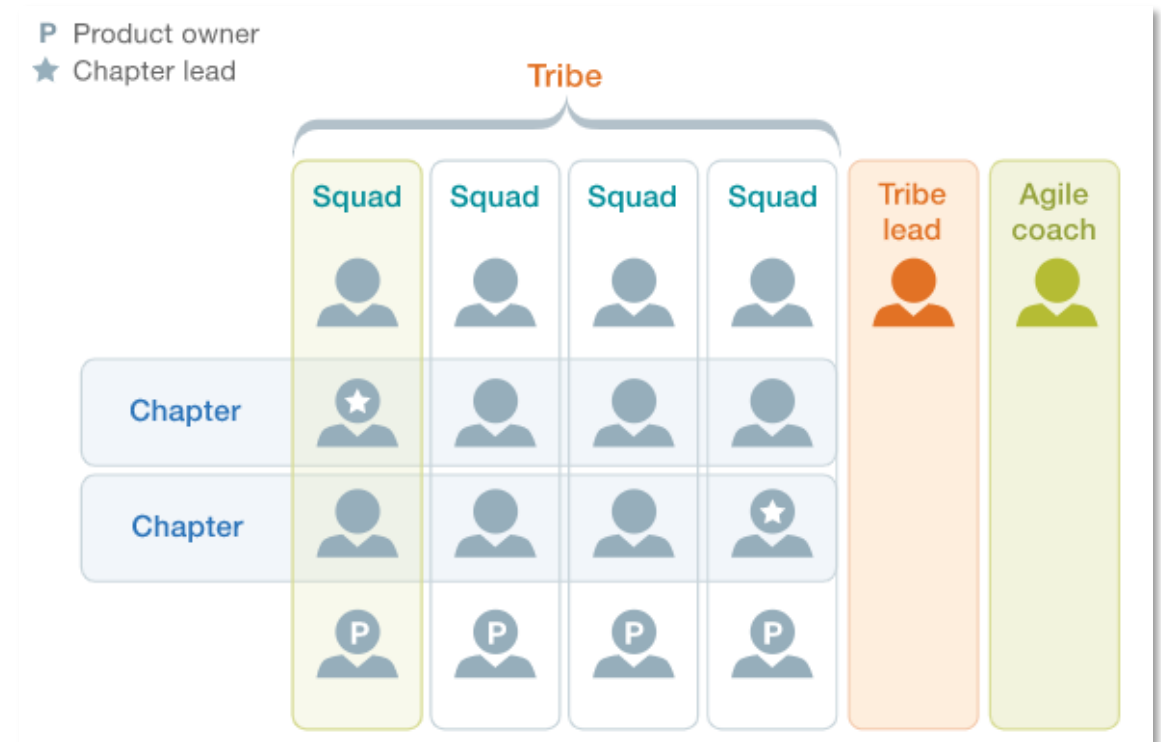










Journey to Agile Way of Working at ING

- Started with Agile in 2015
 - Tribes and squads
 - Site Reliability Engineering (SRE) teams
- Challenge to organise managing dependencies between the teams:
 - E.g. ownership of platforms
- Today: profiling of teams with designated services such as Infra-as-a-Service
- Tribe Leads, IT Leads, Product owners (POs), Engineers



Journey to Agile Way of Working at ING (ctd)

- Characteristics: Autonomy of teams, multidisciplinary with POs, short-cyclic delivery
- Business requirements on Product backlog, in Themes – Epics – Features – User stories
- Update in controls: e.g.
 - Autonomy of teams/PO -> delegation from Asset Owner
 - Delivery is short-cyclic -> low(er) impact
 - No segregation of duties between devs/testers/ops
 - Short-cyclic WoW vs. classic tollgates&connection to risk
- Also: divergence in WoW/tooling, challenge to connect as risk officer, challenge to test operating effectiveness

-  We work in **high performing teams**
-  We **empower** teams
-  We care about **talent** and craftsmanship
-  We continuously **learn** from customers and apply learnings to **improve**
-  We set **priorities** with the **big picture** in mind
-  We are **consistent** in our organisational design and way of working
-  We organise for **simplicity**
-  We **re-use** instead of reinvent

Risk journey with regulators and best practices makers

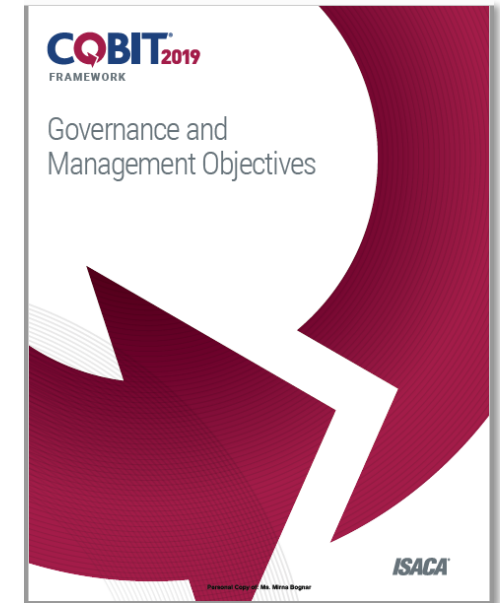
- Regulators recognize the scale of dependency on digitalised services and on resilience thereof
- Many IT related regulations for FI
- Requirements matured e.g. SoD within IT with respect to change management

Classic view	More outcome-based	Stating the objective
<i>[...] g) the duties of individuals responsible for development, testing and implementation are segregated.</i>	<i>[...] to ensure adequate segregation of duties and to mitigate the impact of unverified changes to production systems. Specifically, [...] ensure the segregation of production environments from development, testing and other non-production environments. [...]</i>	<i>Segregation/separation of duties—[...]. Commonly used in large IT organisations so that no single person is in a position to introduce fraudulent or malicious code without detection.</i>






- Examples of mandating delegation and approach to controls regarding test of IT Changes

Control objectives and implementation

- References:
 - Cobit 2019
 - Regulations like EBA Guidelines, EC NIS etc.
 - Best practices like ISF Standard of Good Practice
- Back to the drawing table:
 - What is the risk?
 - What is the objective?
 - Then (re)formulate the control
- In principle, risks and control objectives remained the same
 - Alignment between Business requirements and IT change delivery
 - Outcome of IT change is compliant
 - IT change is deployed with managed impact on production



Control objectives and implementation (ctd)

Cobit control objective	ING Control objective
EDM02 Ensured Benefits Delivery (Agile specific)	1. Roles and responsibilities Roles and responsibilities defined and mandated to ensure business ownership for IT changes. 
BAI07 Managed IT Change Acceptance and Transitioning (Agile specific)	2. Well-established systems development methodologies to a) prevent introducing fraudulent or malicious code without detection by e.g. peer review b) [...] 
BAI02 Managed Requirements Definition	3. Requirements management IT solutions meet business requirements (both functional and non-functional) and address the identified risks 
BAI07 Managed IT Change Acceptance and Transitioning (tweaked to Agile WoW)	4. Testing Before deployment to production, IT changes are tested, and the test results are accepted and risks mitigated to ensure IT changes are in line with the agreed expectations and outcomes. Shortcomings of the test strategies (or compliance thereof) are monitored for sustainable improvements 
BAI06 Managed IT Changes	5. IT Change deployment IT changes are authorised and applied in a structured and controlled manner, according to a defined and approved process 

In practice, how IT Lead sees management of IT changes

- Goal: improving our ability to deliver software
 - **Deployment Frequency** - How often an organization successfully releases to production
 - **Lead Time for Changes** - The amount of time it takes a commit to get into production
 - **Change Failure Rate** - The percentage of deployments causing a failure in production
 - **Time to Restore Service** - How long it takes an organization to recover from a failure in production
 - Additional: **Availability** – How well are availability targets met

- Based on DORA Agile metrics



In practice, how IT Risk Officer reflects on managing IT changes

Secure, compliant

- Goal: improving our ability to deliver software
 - **Deployment Frequency** - How often an organization successfully releases to production
 - **Lead Time for Changes** - The amount of time it takes a commit to get into production
 - **Change Failure Rate** - The percentage of deployments causing a failure in production
 - **Time to Restore Service** - How long it takes an organization to recover from a failure in production
 - Additional: **Availability** – How well are availability targets met
- **Non-functionals**
- **PO approvals for releases**

EC

- Based on DORA Agile metrics

Digital Operational Resilience Act

TESTING!!!!



ING Continuous Integration/Continuous Delivery (CI/CD) pipeline

- 2016
 - Built in-house
 - Everything-as-a-code, cattle vs pets
 - Immutable containers
- 2021
 - Moved to standard CI/CD environment
 - Integration, automation
 - Collaboration with other processes



Job Blom (ING Group) - The CI/CD journey: ING Bank study case



Controls related to change management in the CI/CD pipeline

Roles and responsibilities:

- PO mandated role by Asset owner to define and accept requirements, set priorities, accept rest risk of testing, approve a release
- Stakeholders group – mandated depending on impact of IT change

1

- Integration with ITSM change mgt (IT change records)

4

5

- Integration with access mgt and role/team mgt

1

- Capabilities for testing

4

Pipeline Tollgate enforces that releases to production meet the following:

1. Related **code is peer reviewed**
2. Related **code is linked to a user story(ies)**
3. Release is linked to a **IT change record with proper status** (IT change record approved, time window ok etc.)

2

3

5



- Traceability between releases and its code (commits) out of the box

2

- Audit logs available
- Audit reports

4

CI/CD pipeline: Provider vs consumer


- CI/CD pipeline is a service – consumers responsible for proper use thereof
- Consumers are responsible for compliance
- CI/CD pipeline should enforce WoW/controls where possible (standardised WoW, tooling)
 - Enforcement of steps/controls (blocking)
 - Facilitating capability and evidencing the use of these capabilities
 - Providing audit logs



CI/CD pipeline: Provider vs consumer (ctd) – example controls

Control objective	Responsibility of CI/CD Pipeline	Responsibility of Consumer
Systems development methodology 2	<ul style="list-style-type: none"> – Tollgate enforced for releases to production <ol style="list-style-type: none"> 1. Peer review check 2. Link to user stories check 3. Link to and check on IT change record status 	<ul style="list-style-type: none"> – Adhere to WoW
Testing 4	<ul style="list-style-type: none"> – Facilitate capabilities for testing – Facilitate audit reporting 	<ul style="list-style-type: none"> – Creative work responsibility of Consumer – Responsible for overseeing and follow up, in particular for (security) testing
Change deployment 5	<ul style="list-style-type: none"> – Ensure tollgate enforces related IT change record status check before deployment to production (tollgate, blocking) 	<ul style="list-style-type: none"> – Adhere to WoW

Automation in CI/CD pipeline: example of automated controls

- 
- Identify releases to production and assess whether
 1. Related code is peer reviewed -> one engineer cannot bring her code to production singlehandedly
 2. Related code is linked to a user story(ies) -> PO approved change requirement
 3. Release is linked to a IT change record with proper status -> PO approved change deployment

Add to the agile metrics?

- Goal: improving our ability to deliver software
 - **Deployment Frequency** - How often an organization successfully releases to production
 - **Lead Time for Changes** - The amount of time it takes a commit to get into production
 - **Change Failure Rate** - The percentage of deployments causing a failure in production
 - **Time to Restore Service** - How long it takes an organization to recover from a failure in production
 - Additional: Availability
- **Release compliance***: The percentage of compliant releases with evidence (should be 100% in the pipeline)

¹² (*) compliance here addresses only the controls as highlighted above

Creative work in CI/CD pipeline: e.g. testing

- Requirements regarding IT change testing, e.g.

Classic view	Stating the objective
<i>Plan acceptance tests. Establish a test plan based on enterprisewide standards that define roles, responsibilities, and entry and exit criteria. Ensure that the plan is approved by relevant parties.</i>	<i>Financial institutions should establish and implement an ICT change management process to ensure that all changes to ICT systems are recorded, tested, assessed, approved, implemented and verified in a controlled manner.</i>

- Consumers are responsible for testing and evidencing thereof

- Testing in CI/CD pipeline
 - Capabilities for testing
 - Audit logs
 - Needs test strategies per release and per product
 - Part of the tollgate



In general, when going for automation

- Preconditions:
 - Convergence of WoW, including shift left
 - Standardisation of tooling (role&team mgt, ITSM/change mgt, source code review etc.)
- Some principles for CI/CD pipeline
 - Creative work cannot be automated
 - Automation of risk and controls, make use of traceability in the CI/CD pipeline
 - Enable fast feedback to engineers for continuous improvement
 - Facilitate capabilities and audit logging



A dialogue between IT and Risk remains necessary...

We have no
major changes

No downtime after
change
deployments, means
no security gaps

Automated
testing of
changes

IT change
approvals by Asset
Owners are “soooo
2014”

Evidence discovery
instead of evidence
generation after the
fact

Thank you for your attention!

Mirna Bognar PhD CISSP CISA EMITA CDPO

ING Bank

Corporate Information Risk Management

M +31 622490260

E mirna.bognar@ing.com



do your thing

Questions



References

[The CI/CD journey: ING Bank study case by Job Blom \(Product Owner at ING Group\)](#)

[DORA Agile metrics: Using the four keys to measure your DevOps performance](#)

[2019 Accelerate State of DevOps Report](#)

Team topologies, M. Skelton and M. Pais

[EC Digital Operational Resilience Act - proposal](#)