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

<table>
<thead>
<tr>
<th>Classic view</th>
<th>More outcome-based</th>
<th>Stating the objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>[...] g) the duties of individuals responsible for development, testing and implementation are segregated.</td>
<td>[...] 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. [...]</td>
<td>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.</td>
</tr>
</tbody>
</table>

- 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)

<table>
<thead>
<tr>
<th>Cobit control objective</th>
<th>ING Control objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>EDM02 Ensured Benefits Delivery</td>
<td>1. <strong>Roles and responsibilities</strong>&lt;br&gt;Roles and responsibilities defined and mandated to ensure business ownership for IT changes.</td>
</tr>
<tr>
<td>(Agile specific)</td>
<td></td>
</tr>
<tr>
<td>BAI07 Managed IT Change Acceptance and Transitioning</td>
<td>2. <strong>Well-established systems development methodologies</strong> to&lt;br&gt;a) prevent introducing fraudulent or malicious code without detection by e.g. peer review&lt;br&gt;b) […]</td>
</tr>
<tr>
<td>(Agile specific)</td>
<td></td>
</tr>
<tr>
<td>BAI02 Managed Requirements Definition</td>
<td>3. <strong>Requirements management</strong>&lt;br&gt;IT solutions meet business requirements (both functional and non-functional) and address the identified risks</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>BAI07 Managed IT Change Acceptance and Transitioning</td>
<td>4. <strong>Testing</strong>&lt;br&gt;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</td>
</tr>
<tr>
<td>(tweaked to Agile WoW)</td>
<td></td>
</tr>
<tr>
<td>BAI06 Managed IT Changes</td>
<td>5. <strong>IT Change deployment</strong>&lt;br&gt;IT changes are authorised and applied in a structured and controlled manner, according to a defined and approved process</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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

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**

Secure, compliant

- 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
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 an IT change record with proper status (IT change record approved, time window ok etc.)

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

- Integration with access mgt and role/team mgt
- Integration with ITSM change mgt (IT change records)

Capabilities for testing
- Audit logs available
- Audit reports

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

Controls related to change management in the CI/CD pipeline
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

<table>
<thead>
<tr>
<th>Control objective</th>
<th>Responsibility of CI/CD Pipeline</th>
<th>Responsibility of Consumer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Systems development methodology</td>
<td>- <strong>Tollgate</strong> enforced for releases to production&lt;br&gt;1. Peer review check&lt;br&gt;2. Link to user stories check&lt;br&gt;3. Link to and check on IT change record status</td>
<td>- Adhere to WoW</td>
</tr>
<tr>
<td>Testing</td>
<td>- Facilitate capabilities for testing&lt;br&gt;- Facilitate audit reporting</td>
<td>- Creative work responsibility of Consumer&lt;br&gt;- Responsible for overseeing and follow up, in particular for (security) testing</td>
</tr>
<tr>
<td>Change deployment</td>
<td>- Ensure tollgate enforces related IT change record status check before deployment to production (<strong>tollgate</strong>, blocking)</td>
<td>- Adhere to WoW</td>
</tr>
</tbody>
</table>
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)

(*) 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.

<table>
<thead>
<tr>
<th>Classic view</th>
<th>Stating the objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td>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.</td>
</tr>
</tbody>
</table>

- 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
Questions

Look this new Agile thing: to deal with unpredictable events and things we cannot control in our projects.

We can prioritize, reduce the scope, change requirements at any time and increase the chances of success of the project.

Look, this is your new project, with fixed deadline, fixed scope and fixed quality: you can be “Agile” inside this triangle!!
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