Cyber Security starts with Risk Aware Engineers!

DevOps Enterprise Summit London 2019

Jan-Joost Bouwman & Léon Janson

25 June 2019

a little bit about us

Jan-Joost Bouwman

- Risk Mngmt (coordinator SOx testing Domestic Bank NL)
- Previously: Change management

- Privately: birder and traveller
- Enjoys tweeting about IT conferences

Léon Janson

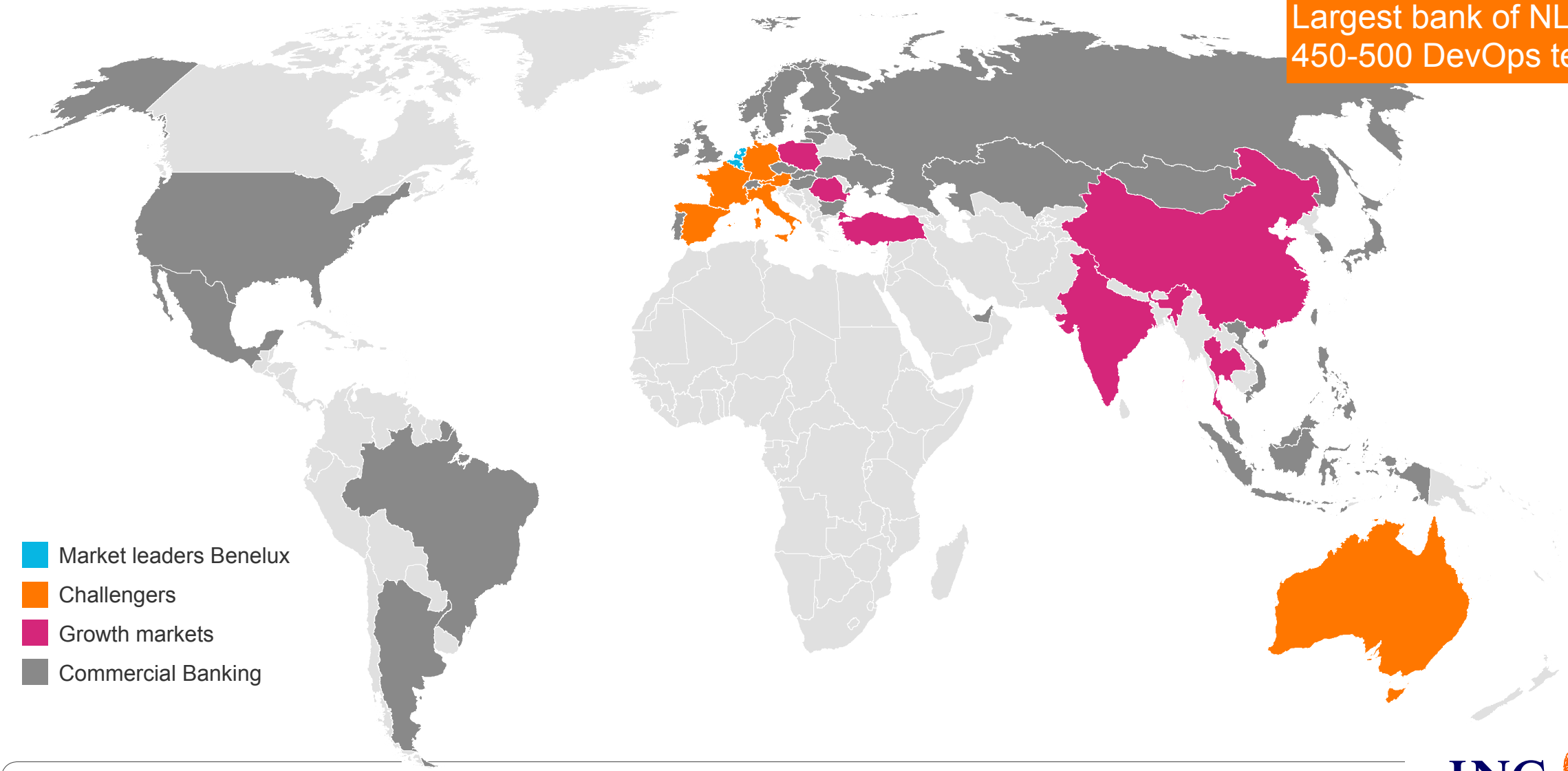
- IT (Risk) Mngmt at ING since late 90's
- Responsible for IT Risk DB NL
- Initiator Risk Awareness Days program

- Privately: married, father of two
- Coach for son's football team and referees daughter's hockey team

ING

Who is ING?

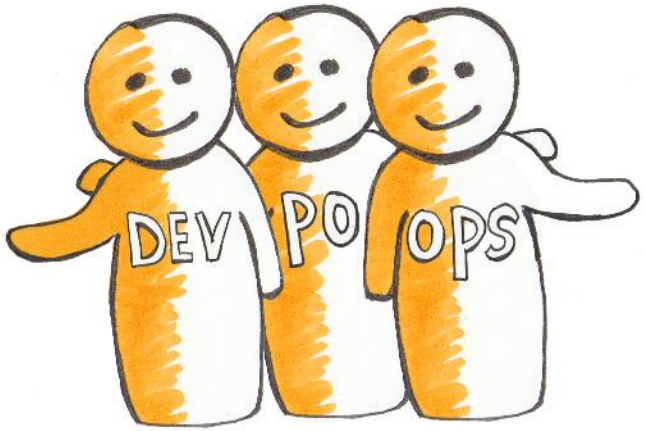
Over 40 countries
52,000+ employees
38 million Retail clients
12.2 primary
Largest bank of NL
450-500 DevOps teams

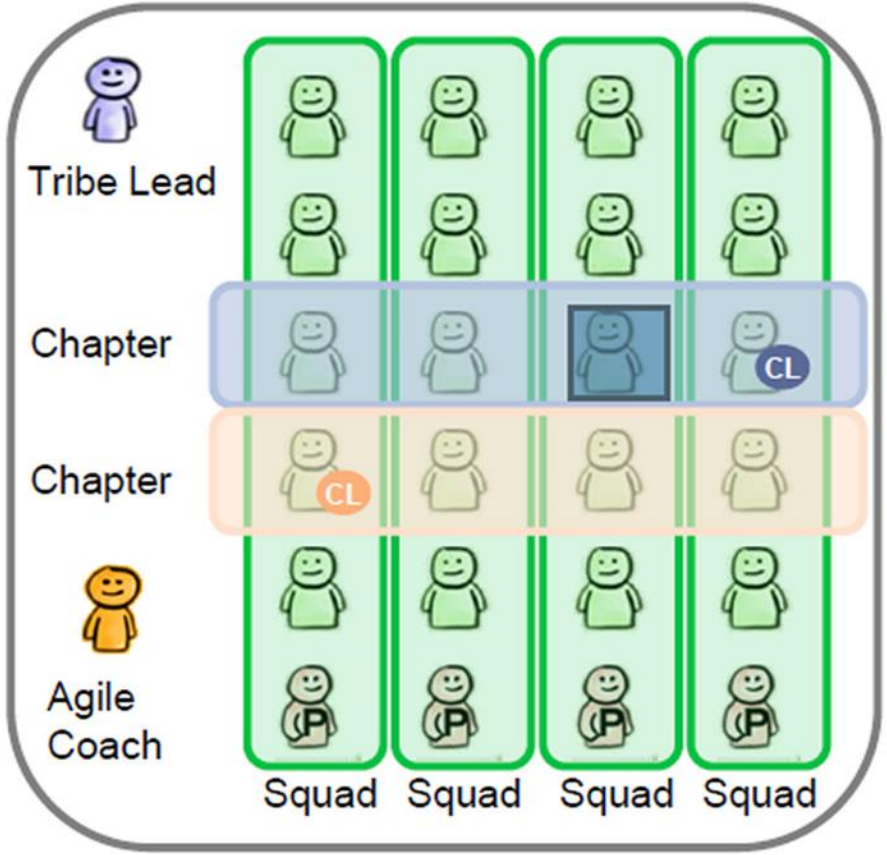


ING

Three phases of Agile

Agile (2011) => DevOps (2013) => BizDevOps (2015)

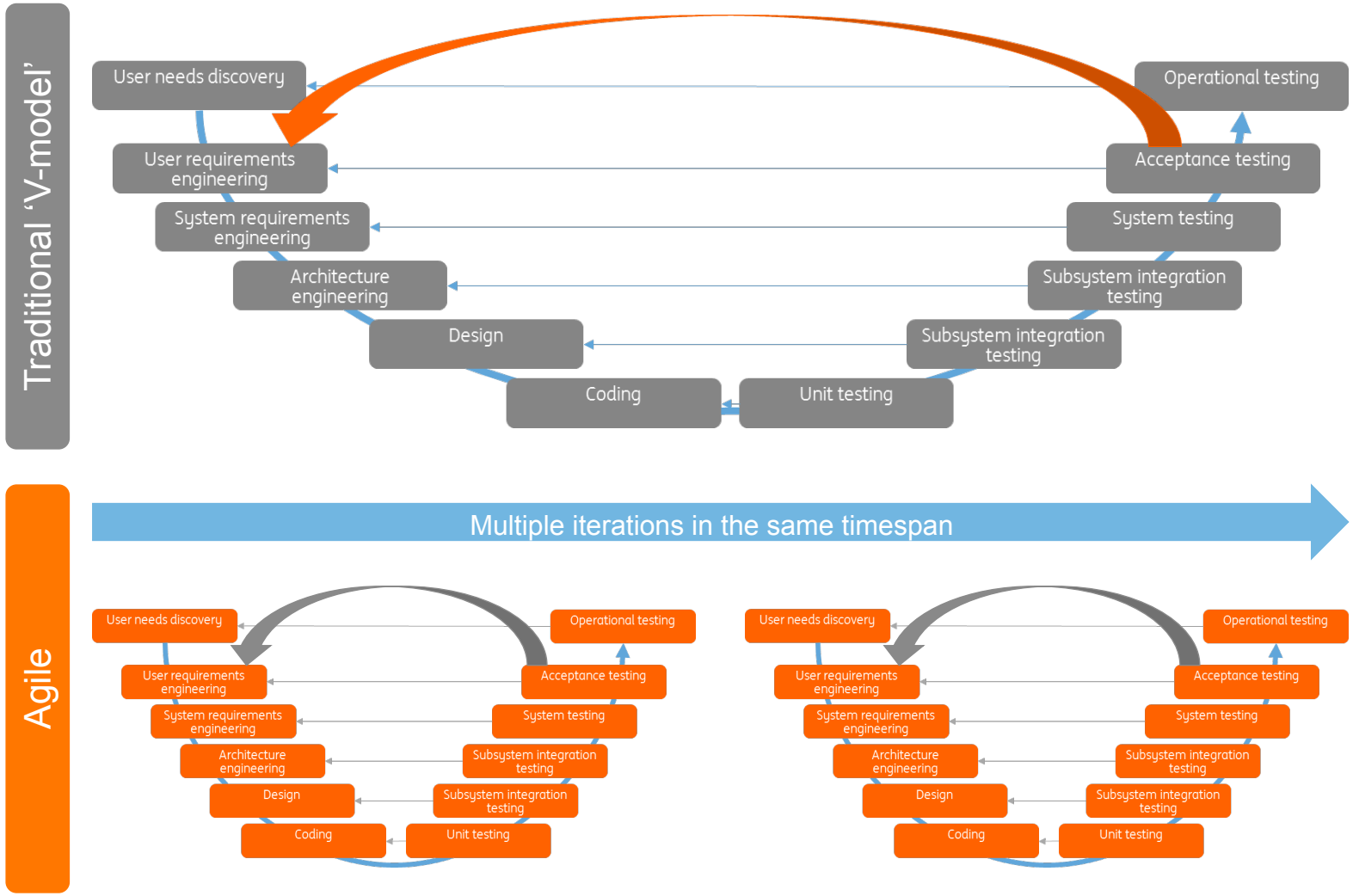




The Agile Way of Working reduces the risk of getting the design wrong due to quick iterations, but it also requires a ‘shift left’ to address risks during the design phase

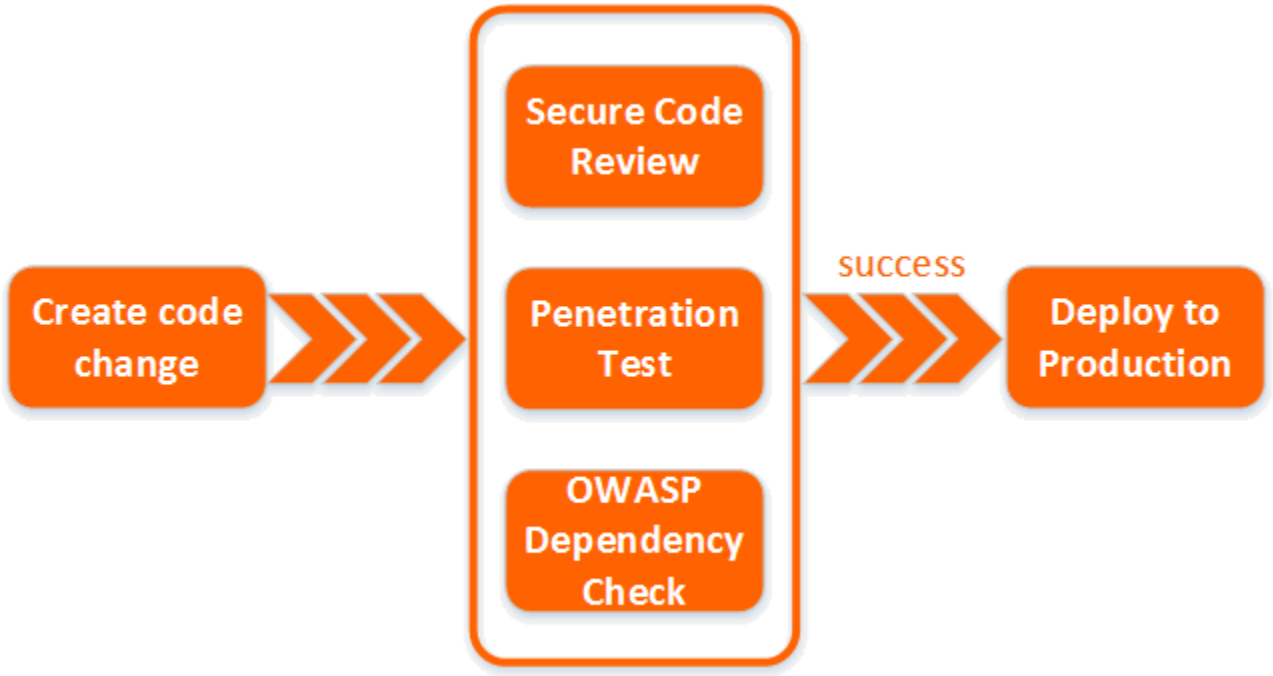
Shift Left

- In a shift-left approach, **testing is moved to the left** in the software development lifecycle
- Instead of testing at the end of the delivery lifecycle, **validation is performed during early stages already**, including the development of automated tests.
- Developers can **focus on quality right from the beginning,** making it easier to fix, rather than waiting for defects to be discovered late in the development life cycle



We call this ‘shift left’ Security by Design
It is also known as DevSecOps

Automation is essential, starting with testing



But it all starts with a Risk Aware Mind-set!

ING

What is Risk Awareness Day? | Concrete focus on Risk topics at your own desk in combination with central awareness discussions

Risk Awareness Days 2017

May 22	Credentials
Jul 3	Vulnerabilities
Sept 11	Data Breaches
Oct 9	Layered security
Nov 20	Domain Segmentation

Objectives:
- Create risk awareness
- (IT) Risk in the DNA of our employees
- Improve our security profile

How: Full day focus on (IT) Risk
- Introduction topic by senior management via webcast
- Clear run book giving teams concrete assignments
- Provide guidance to find relevant policies, standards, etc.
- Fun elements
- Active support by risk experts on the floor

Risk Awareness Days 2018

Feb 19	Security Monitoring
Apr 23	Privacy by Design
Jun 18	IAM Summer Clean up
Sept 17	Design for failure
Nov 19	Risk Action Day

Where:
- On the work floor
- Central locations for support and guidance

Participants: (>2500 and growing)
Domestic Bank IT departments NL and BE + growing number other departments

Mantra 1: "Celebrate Failure"
- Treat every identified or reported data issue as feedback (as a gift) → it will enable us to improve the Risk & Security of ING
- Look back at your backlog and identify and prioritize Risk Areas where we need to improve

Mantra 2: "Celebrate Success by Doing it Right"
- Operational Discipline is key for maintaining IT Risk Score
- Use Risk Journeys and ORM for correct implementation and quality levels
- Share best practices and look for automation opportunities where possible

Key succes factors for Risk Awareness Days

- Dedicated day where all engineers focus on IT Risk
- Clear Ground Rules: Be Risk Aware in sharing issues and practices
- Concrete topics that are relatable and relevant e.g. Credentials, Vulnerabilities
- Program with mixed learning
- Runbook and content guides providing Risk SPOCs and engineers clarity which actions to take
- Clear roles & responsibilities for all parties
  - Management and Product owners: leading and initiating
  - Risk SPOCs (1st line): guidance on content and trigger discussion to increase awareness
  - Engineers: learn and focus on making ING more secure

ING

Key ingredients

- Emphasis on Risk Awareness Day Mantras

- Learning
  - Webcast with motivating content based kick off
  - Webcast with external experts providing their insights
  - Workshops on content

- Fun
  - Kahoot Risk Quiz for the Risk Awareness Cup
  - Games: e.g Secure Code Warrior, IT Risk Game, Red/Blue team, etc.

- Content guides per Risk Awareness Day on Confluence
  - Links to more information & step-by-step instructions for teams

- Central locations with snacks & drinks to get answers and have discussions

Risk awareness day | Program September 17

Need a Power Break:
- Go to one of the central locations
- Energize your Risk appetite around 10.30 and 14.30 with snacks and drinks
- Discuss topics with Risk Experts

Time	Program
08.30	Start Risk Awareness Day: Prepare workplace, screens & get ready for webcast
09.00	Live Webcast: Peter Jacobs, Joe Katz: *"Be Resilient, design for failure"*
09.45	*Hunt & Fix*: (1) Focus on changes without downtime: All changes between 9-5 and (2) Design for 100% availability: Analyse your set up and enhance your resilience (e.g. active-active solutions)
	Learn & play: ***Please subscribe a.s.a.p.*** Workshops*: SRE Workshops, APT Scenario analysis, Sec Mon with Tech PL, Disaster Recovery* Games: *Red Blue team game, Secure code Warrior*
12.15	Energizer: Kahoot Risk Quiz
12.30	Free time: Have lunch – stretch your legs
13.30	Live Webcast: Ad van der Graaff & Léon Janson: *""IT Resilience, what does it take?""*
14.00	*Hunt & Fix* : (1) Create transparency and deliver evidence for IT Resilience (e.g. Availability, capacity & performance plans) and (2) Be Resilient: Operational discipline on risk controls (e.g. vulnerabilities) *Learn & play:* see morning sessions. ***Please subscribe a.s.a.p.*** via Risk Awareness Day mailbox
16.45	Wrap up: Share tips & best practices via Confluence and register user stories (#RiskawDay)
17.00	End of Risk Awareness Day

Wrap up

- Short cycles of DevOps/CD → Security by Design by shift left is essential
- Security is just as important for a DevOps team as coding or testing
- The role of Risk managers shifts from control to coach
- Automation is a big enabler, but it all starts with a Risk Aware mind-set
- The approach we chose: Risk Awareness Days
- Key elements: relatable and relevant; webcasts and workshops; actionable items; (cyber)security competitions and quizzes.
- **A mix of Information, Engineering and Fun creates the biggest impact on Risk Awareness**