Cyber Security starts with Risk Awareness!

ISACA NL Webinar

Jan-Joost Bouwman

24 March 2021

a little bit about me

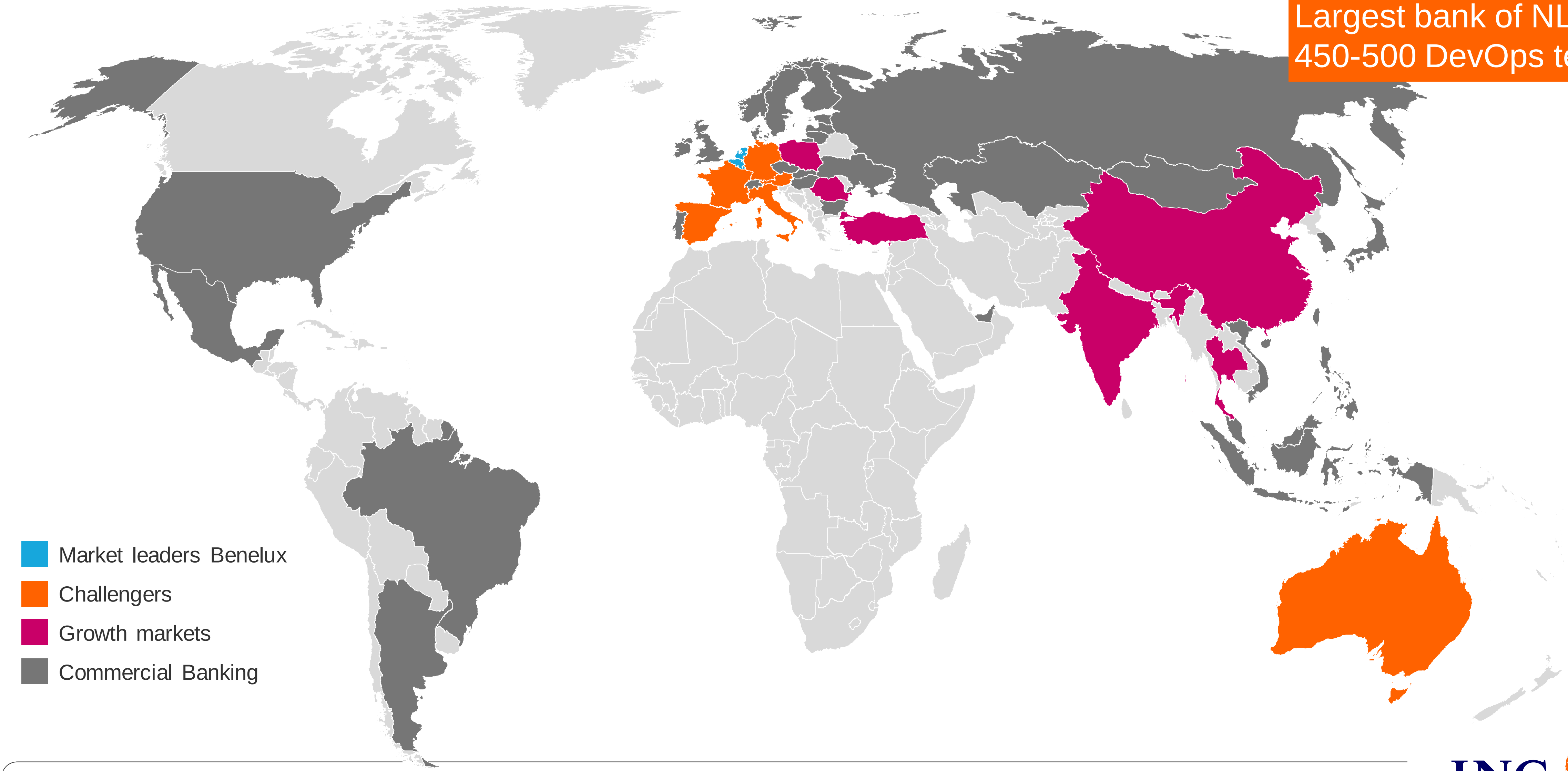
Jan-Joost Bouwman

- Risk Mngmt (coordinator SOx testing Domestic Bank NL)
- Previously: Change management
- 20+ years experience in IT
- Enjoys speaking at conferences about DevOps and Risk Management @ING
- Enjoys helping engineering colleagues to speak at conferences as well

- Privately: birder and traveller
- Enjoys tweeting about IT conferences
- Twitter handle: @JanJoostBouwman

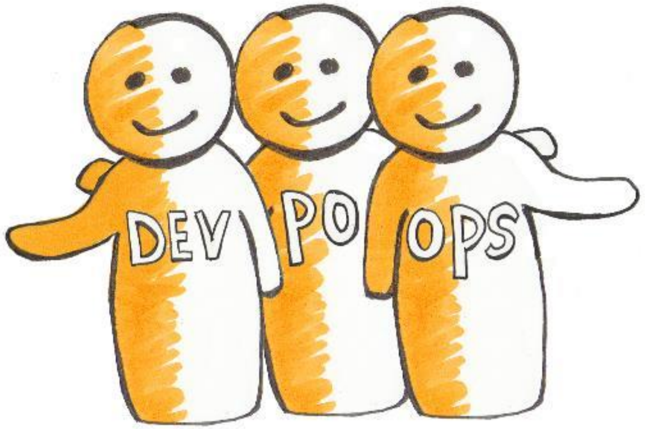
Who is ING?

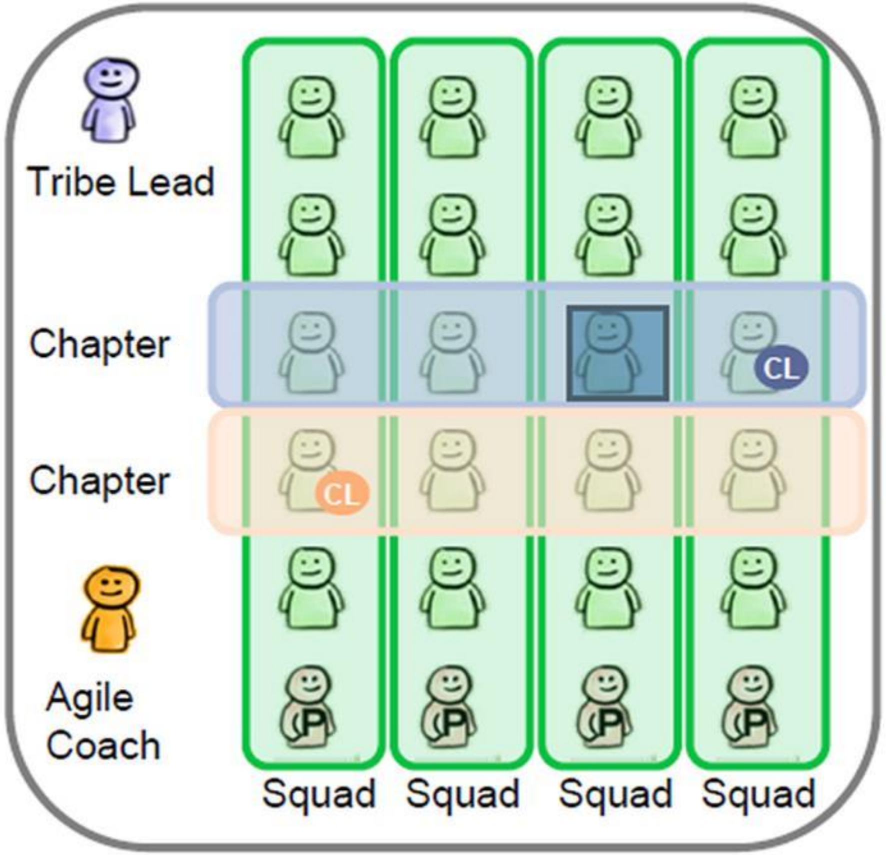
Over 40 countries
52,000+ employees
38 million Retail clients
12.2 primary
Largest bank of NL
450-500 DevOps teams



Three phases of Agile

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

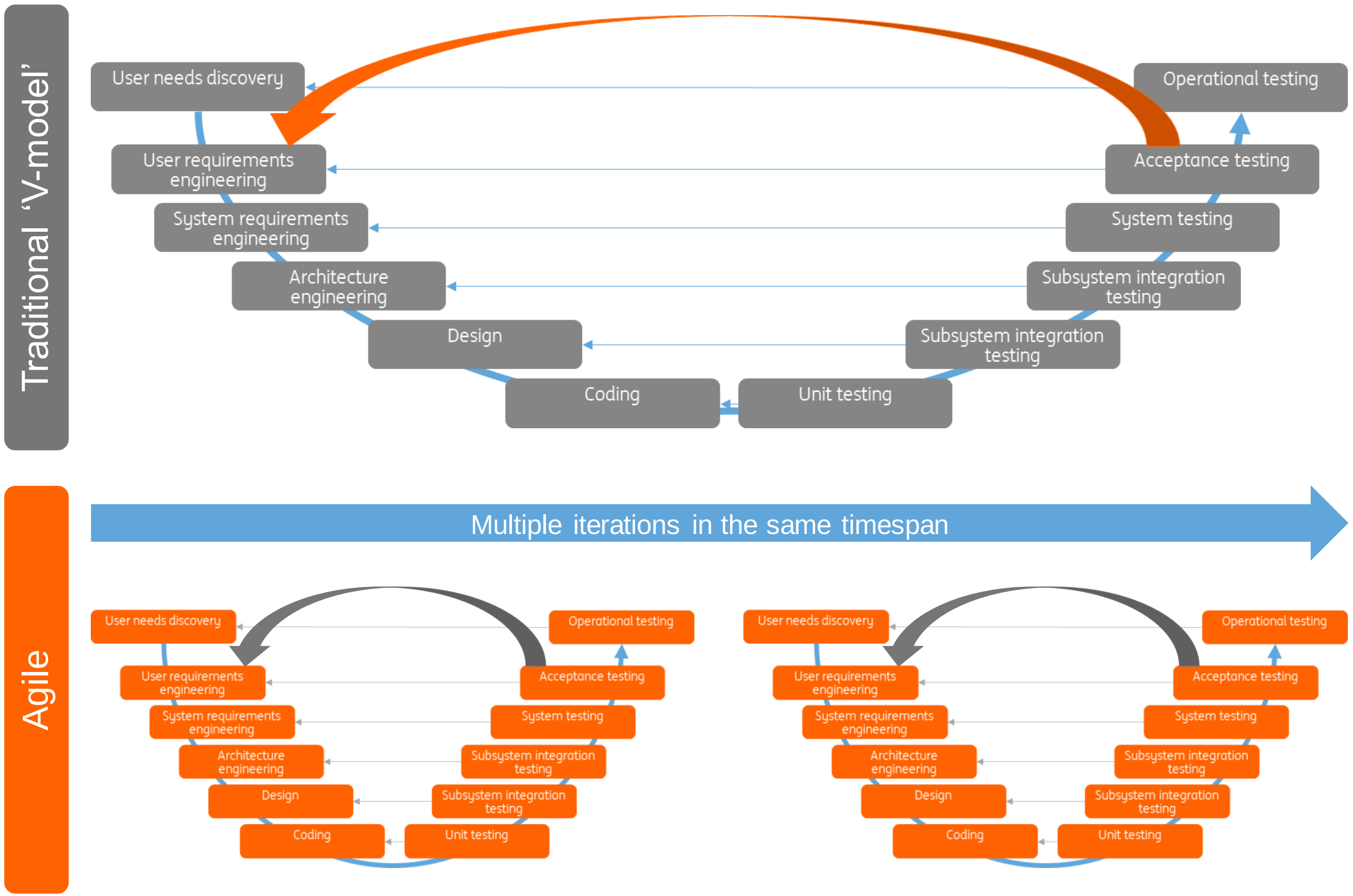




The Agile Way of Working reduces the risk of getting the design wrong due to quick iterations, but it also requires a ‘shift left’ to address risks during the design phase

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



Traditional ‘V-model’

User needs discovery

User requirements engineering

System requirements engineering

Architecture engineering

Design

Coding

Unit testing

Subsystem integration testing

Subsystem integration testing

System testing

Acceptance testing

Operational testing

Agile

Multiple iterations in the same timespan

User needs discovery

User requirements engineering

System requirements engineering

Architecture engineering

Design

Coding

Unit testing

Subsystem integration testing

Subsystem integration testing

System testing

Acceptance testing

Operational testing

User needs discovery

User requirements engineering

System requirements engineering

Architecture engineering

Design

Coding

Unit testing

Subsystem integration testing

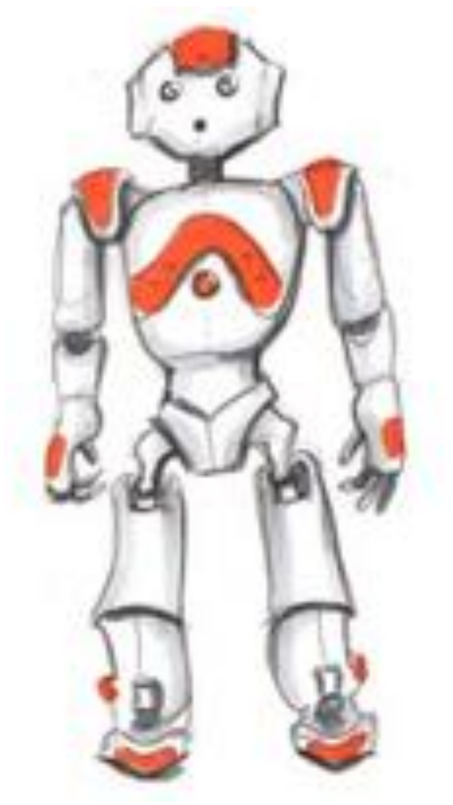
Subsystem integration testing

System testing

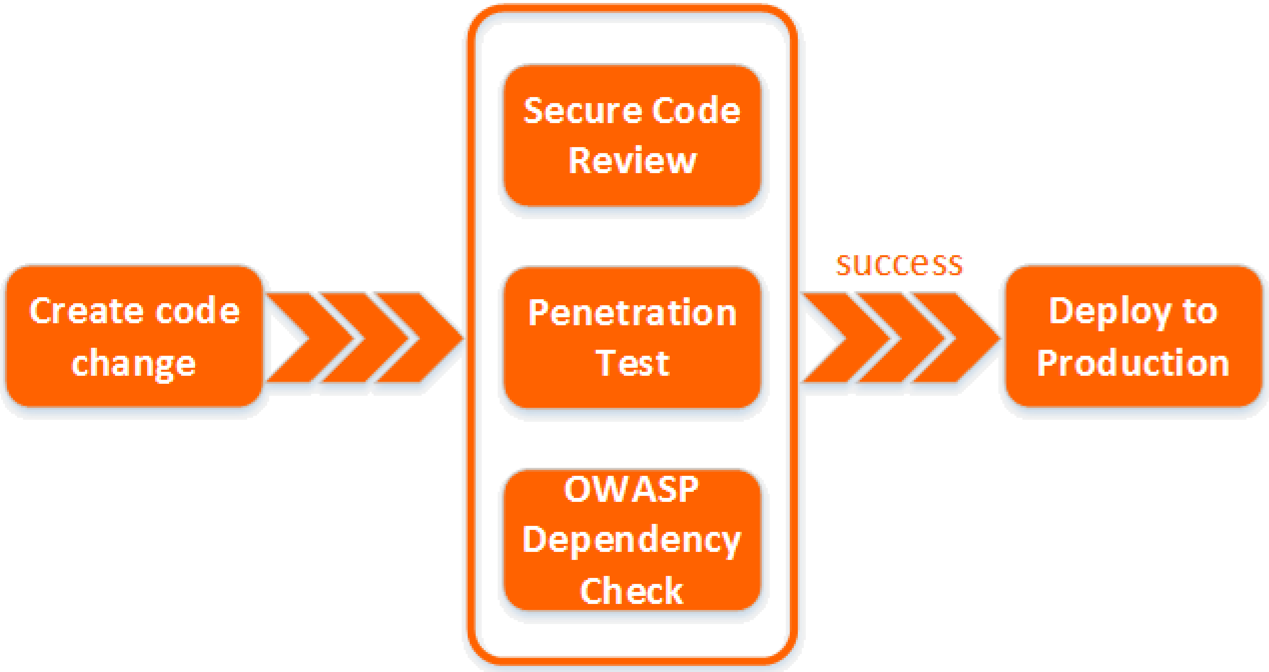
Acceptance testing

Operational testing

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!

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

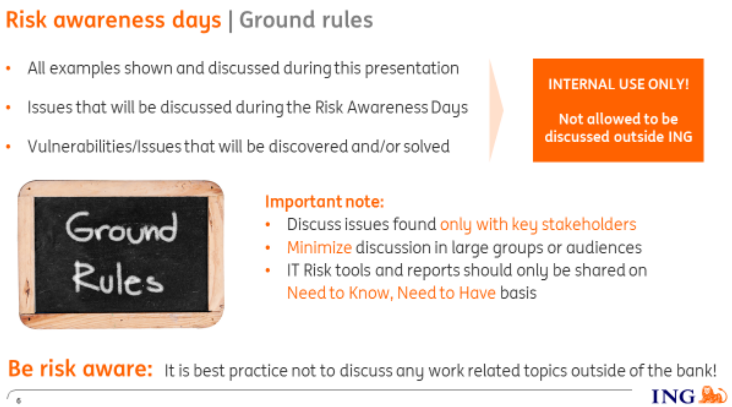
Mantra 1: “Celebrate Failure”

- 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



Risk awareness days | Ground rules

- All examples shown and discussed during this presentation
- Issues that will be discussed during the Risk Awareness Days
- Vulnerabilities/Issues that will be discovered and/or solved

INTERNAL USE ONLY!

Not allowed to be discussed outside ING

Ground Rules

Important note:

- Discuss issues found only with key stakeholders
- Minimize discussion in large groups or audiences
- IT Risk tools and reports should only be shared on Need to Know, Need to Have basis

Be risk aware: It is best practice not to discuss any work related topics outside of the bank!

6

- 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

Key ingredients

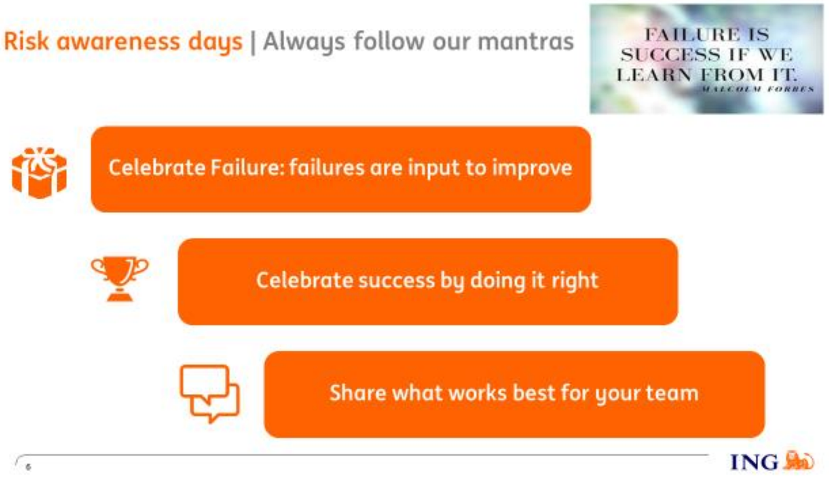
- Emphasis on Risk Awareness Day Mantras

- 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

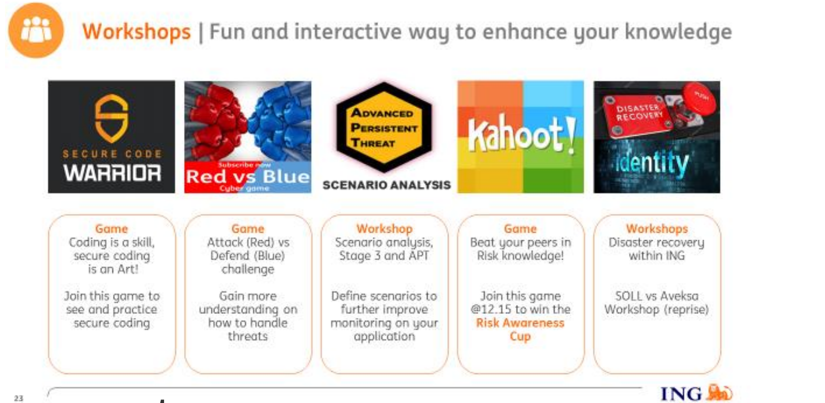


Risk awareness days | Always follow our mantras

Celebrate Failure: failures are input to improve

Celebrate success by doing it right

Share what works best for your team



Workshops | Fun and interactive way to enhance your knowledge

Game	Game	Workshop	Game	Workshops
Coding is a skill, secure coding is an Art! Join this game to see and practice secure coding	Attack (Red) vs Defend (Blue) challenge Gain more understanding on how to handle threats	Scenario analysis, Stage 3 and APT Define scenarios to further improve monitoring on your application	Beat your peers in Risk knowledge! Join this game @12.15 to win the Risk Awareness Cup	Disaster recovery within ING SOLL vs Aveksa Workshop (reprise)

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

LET’S GET AN IMPRESSION!

Evolution in scope

2017 (IT DBNL only)

- Credentials
- Vulnerabilities
- Prevent Data Breaches – Data Protection
- Layer our Security – OCD 3.0
- Domain Segmentation

Evolution in scope

2017 (IT DBNL only)

- Credentials
- Vulnerabilities
- Prevent Data Breaches – Data Protection
- Layer our Security – OCD 3.0
- Domain Segmentation

2018 (IT NL + BE)

- Security Event Monitoring
- Privacy by Design in IT
- Summer Clean Up
- IT Resilience
- Risk Action Day!

Evolution in scope

2017 (IT DBNL only)

- Credentials
- Vulnerabilities
- Prevent Data Breaches – Data Protection
- Layer our Security – OCD 3.0
- Domain Segmentation

2018 (IT NL + BE)

- Security Event Monitoring
- Privacy by Design in IT
- Summer Clean Up
- IT Resilience
- Risk Action Day!

2019 (Business and IT, NL + BE)

- Safe Bank is our #1 Priority!
- Data (Ab)Use – Keep our Data Safe!
- KYC – Together we can keep out illegal activities

Evolution in scope

2017 (IT DBNL only)

- Credentials
- Vulnerabilities
- Prevent Data Breaches – Data Protection
- Layer our Security – OCD 3.0
- Domain Segmentation

2018 (IT NL + BE)

- Security Event Monitoring
- Privacy by Design in IT
- Summer Clean Up
- IT Resilience
- Risk Action Day!

2019 (Business and IT, NL + BE)

- Safe Bank is our #1 Priority!
- Data (Ab)Use – Keep our Data Safe!
- KYC – Together we can keep out illegal activities

2020 – oops, we are all working from home now

- Only one RAWD: Sourcing
- All remote, talks only
- Combined with other security events that couldn't go ahead as planned, including one with OWASP BE as a Security Week

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**
- **Remote you can reach more people, but it will be less interactive**