



# ISO/IEC 27000 family

PRESENTED BY LAURENT DEHEYER

# Objectives

1. WHAT? INTRODUCTION TO ISO27000
2. WHY?
  1. BUSINESS LANDSCAPE
  2. KEY BENEFIT
3. HOW?
  1. CHALLENGES
  2. ENABLERS
  3. METHODOLOGY



# Your Guest



**Laurent Deheyer**

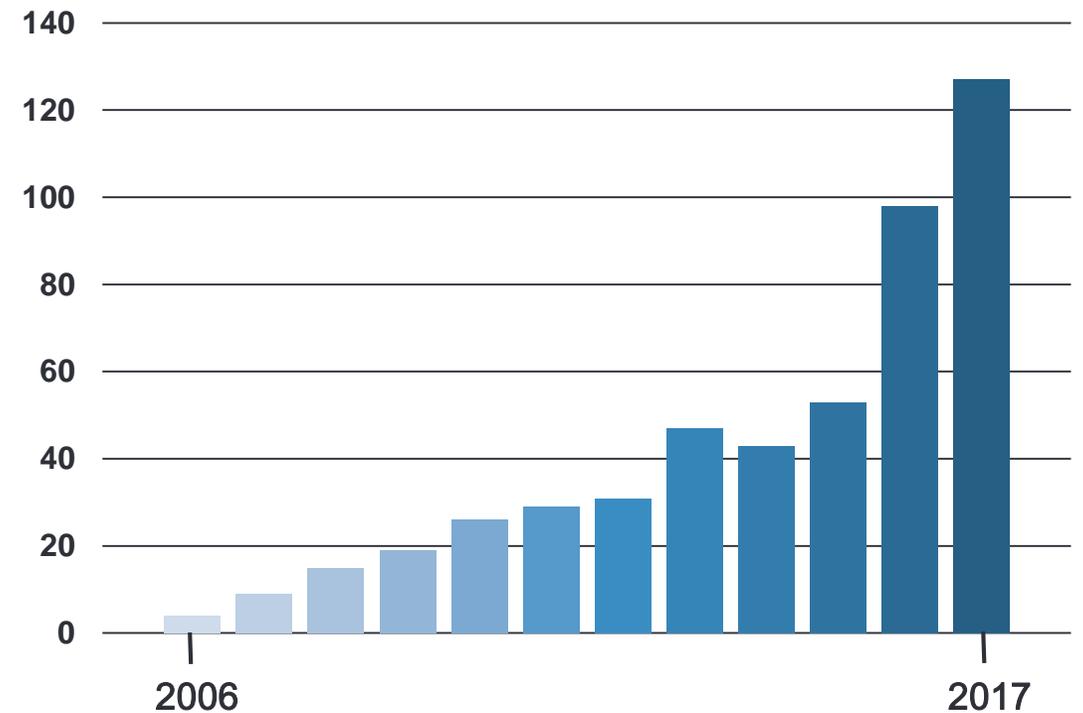
**Approach GRC Consulting Director**

CISM – ISACA Member

ISO 27001 Lead Implementer/Certified Trainer

Certified Data Protection Officer [GDPR]

# Number of ISO/IEC 27001 certifications is exploding in Belgium



Source: [www.iso.org/the-iso-survey.html](http://www.iso.org/the-iso-survey.html)  
//IEC 27001-data per country and sector 2006 to 2017

# Trends

## ISO/IEC 27001

Organisations processing company confidential data

**GDPR**

- IT
- Services
- Transport & Communication

- B2B
- Boom: Startup
- SaaS
- Some uncommon requests

+NIS  
+eIDAS  
+ local  
+ sector  
+ ..

Organisations processing personal data

# ISO/IEC introduction

- **ISO: International Organization for Standardization**
- Worldwide federation of national standards bodies from 146 countries, one from each country, e.g., – NBN - Institut Belge de Normalisation (Belgium)
- ISO was established in 1947 ([www.iso.ch](http://www.iso.ch) )
- Mission: to promote the development of standardization and related activities in the world with a view to facilitating the international exchange of goods and services, and to developing cooperation in the spheres of intellectual, scientific, technological and economic activity.
- 2.937 technical bodies
- ISO's work results in international agreements which are published as **International Standards (IS)**
- 20 500 standards and standards-type documents

# ISO/IEC 27001 is about managing Information Security

- Internationally recognized Standard
- Part of ISO27000 family
- Set the specification for an **Information security management system (ISMS)**
- Based upon **Information Risk Management**
- Focus on **Continuous Improvement**
- Certification by accredited body - valid 3 years, re-audit every year



Note: newly release 27001:2017 → includes very minors changes

# What do you want to protect?

CONFIDENTIALITY, INTEGRITY, AVAILABILITY of organisations ASSETS

You want to protect your **'assets'**. There are several definitions for the term 'asset', generally speaking an asset could be defined as *'an item of value'* for a company in order to run its business, including **servers, laptops, smartphones people, confidential/private information, Intellect Property, applications, customer's data, ..**



# ISO/IEC 27K-series

→ 47 published standards to date



# ISO27701 Privacy Certification- Context & Implementation Guidance

- ISO27701- an international standard for Privacy Information Management System, PIMS
- ISO27701- provides **guidance** to implement & continually improve **measures** to ensure privacy of PII
- **Integrates** related requirements & guidance of below standards/regulation
  - GDPR- a regional regulation (with international scope) on personal data (**little guidance, not certifiable**)
  - ISO29100- an international privacy protection **framework**
  - ISO29151- an international **code of practice** for PII
  - ISO27001/2- international standard on **Information Security**
- ISO27701- comprises **clauses & Annexes** that are sequentially aligned with ISO27001/2, the GDPR, ISO29100, etc
- PIMS (ISO27701)- **certifiable** (subject to or together with 27001 ISMS certification).
- ISO27001 plus ISO27701 certifications meet privacy & information security requirements of the GDPR (*but it does not amount to GDPR certification because there is still no official certification for the GDPR*)
- Terminology- (a) ISO27701 **privacy/PII** = GDPR **protection/data** (b) ISO27701 **PII principal** (sometimes data subject) = GDPR **data subject** (c) ISO27701 **PII Controller (or Privacy Stakeholder)** = GDPR **data Controller** (d) ISO27701 **PII Processor** = GDPR **data Processor**

# Key benefits

Compliance  
Management



Market  
Demand



Sales  
Efficiency



Cyber  
Threats



# What are the roadblocks?

 Organisation priorities

Human factor 

 Lack of understanding

Initial investment 

# What are the pitfalls?



Lack of role and responsibilities

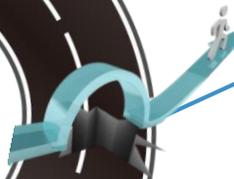


Technical vs. Organisational controls



Bad planning 

 The wrong scope  
Stakeholders expectations



# Key Enablers



People



Methodologies



PRINCE2



GRC, Tools and Technologies



INTEGRITYGRC



Startup



Small & Medium

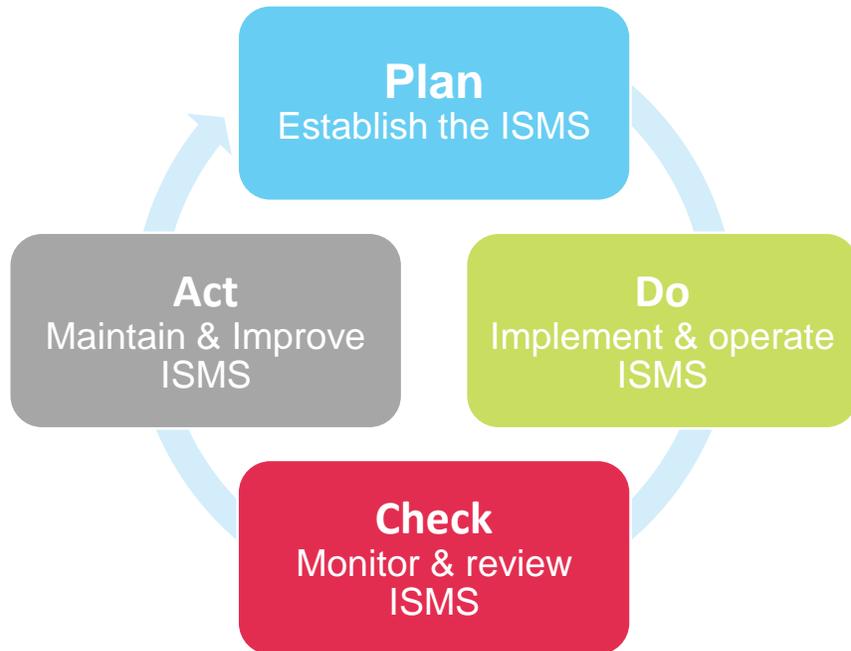


Large

# Methodology

STRIVE FOR A SUCCESSFULL IMPLEMENTATION

The overall methodology used is based on the PDCA model (Plan, Do, Check, Act):



This model is not dedicated for security, it is widely used to implement standards like ISO 9000 (Quality), ISO 14001 (Environment)...

# TOP most difficult parts during the projects

Survey from Approach's consultants based upon their experiences

## PLAN

- Scope definition
- Asset identification
- Management commitment

## DO

- Change Management
- Data/Information classification
- Secure SDLC
- Business Continuity Management

# Question to ask during scope definition exercise

- What is the business needs?
- Do you have a clear organisational chart?
- How many people would be affected inside the company?
- For multi-site organisation, can you map services delivered from which locations?
- Can you identify the business applications and processes supporting the service in scope for you certification?
- Can you define what should NOT be in scope, identify the boundaries and interfaces?



# BACKUP

# General information on ISO

- General information at: [www.iso.org](http://www.iso.org) on
- ISO Code of Conduct [http://www.iso.org/iso/codes\\_of\\_conduct.pdf](http://www.iso.org/iso/codes_of_conduct.pdf)  
(Implementation suggestions for ISO Code of Conduct  
[http://www.iso.org/iso/suggestions\\_for\\_implementation\\_of\\_the\\_iso\\_code\\_of\\_conduct.pdf](http://www.iso.org/iso/suggestions_for_implementation_of_the_iso_code_of_conduct.pdf))
- Standards <http://www.iso.org/iso/home/standards.htm>  
(benefits, certification, management system standards, education about standards)
- About ISO <http://www.iso.org/iso/home/about.htm>  
(structure, members, consumers, conformity assessment, developing countries, training)
- Standards development [http://www.iso.org/iso/home/standards\\_development.htm](http://www.iso.org/iso/home/standards_development.htm) (technical committees, deliverables, who develops standards, why get involved?, resource area)
- News [http://www.iso.org/iso/home/news\\_index.htm](http://www.iso.org/iso/home/news_index.htm)
- ( ISO standards in action, ISO Magazines, events, media Kit)
- ISO store <http://www.iso.org/iso/home/store.htm>

# ISO27001 vs ISAE3402 SOC2

## ISO27001

- Focus on Risk Management
- Best Practices (guidelines)
- Certificate
- All processes

« looking forward »

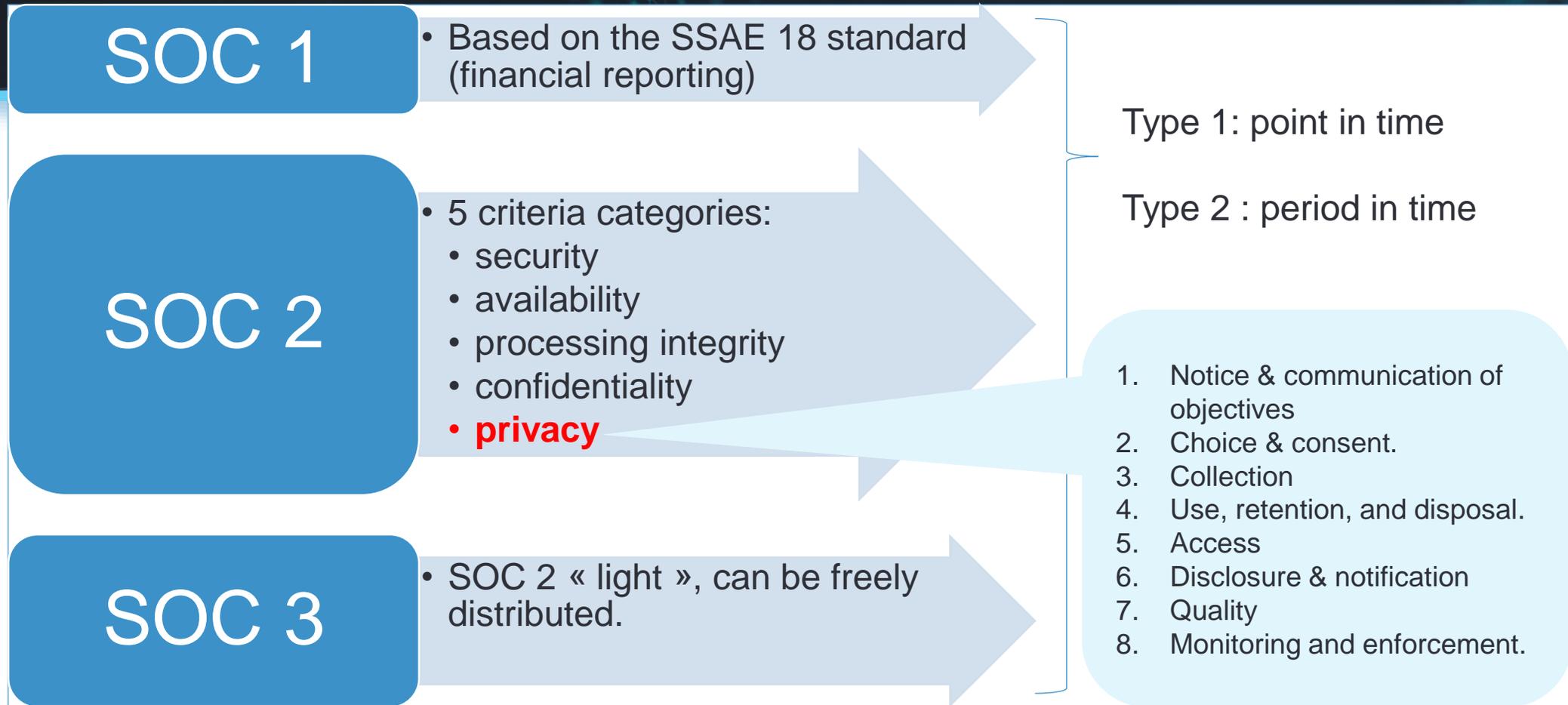
## ISAE3402 SOC2

- Focus on Risk Management
- Principles (trust services)
- Report (type 1 / type 2)
- Selection of processes

« looking backward »

# Privacy with SOC 2

Service Organisation Control Reports (AICPA)





# Approach at a glance

# Our Business at a Glance

Approach **in a few words**



## Our Company

Founded in 2001  
Private company



## Our Mission

We deliver state-of-the-art solutions  
to your cyber security challenges



## Success Stories

+400 satisfied customers  
across all industries



## Sustainable Growth

2018 Revenue: 7,1 M€  
Average annual growth: +10%



## Certification & Compliance

ISO 27001 certified  
GDPR compliant



## Our Locations

Antwerpen  
Louvain-la-Neuve

# Why Approach ?

## Global Approach to Cyber Security



### Expertise & Talent

60+ certified professionals



### Methodologies

Pragmatic proven methods tailored to your context and needs



### Assets

Advanced tooling and trusted partners



We cover the **entire cyber security value chain**, from governance and strategy through to resilient technical designs, architectures and implementations.



Because we have our own **software factory**, we are uniquely positioned to develop highly secure solutions for our clients.

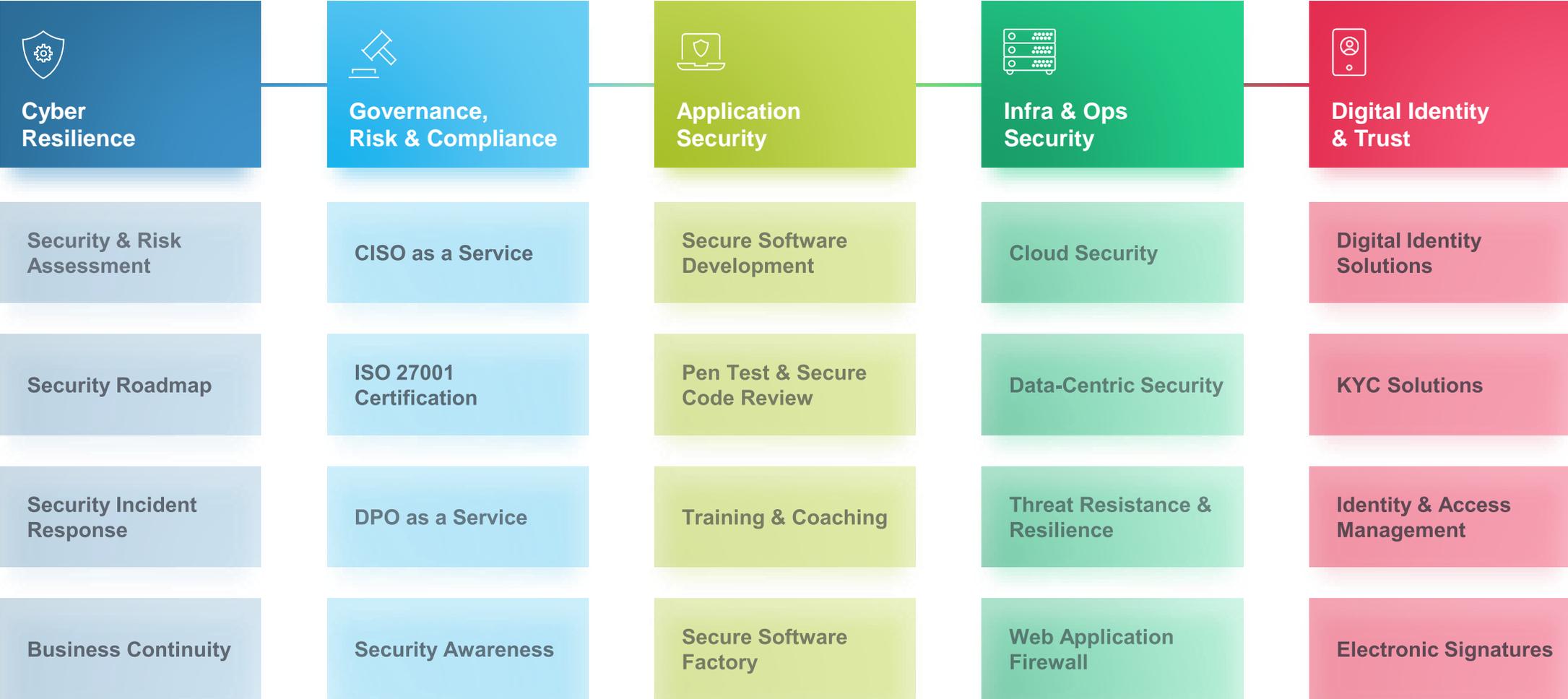
# Get Access to the **Cyber Security Ecosystem**

## The Approach Network



# Our Portfolio of Solutions

How can we help you?



# Some of our Customers

... and how we help them

Public sector	Financial & fintechs	Health care	Others
<p>Pen Test, Security Review</p> 	<p>Staff Augmentation (DEV, SOC, CERT)</p> 	<p>GDPR, ISO27001, HIPPA</p> 	<p>CSIRT GDPR</p> 
<p>WAF</p> 	<p>Architecture, Mobile App Security</p> 	<p>Risk Management, Policies</p> 	<p>Training Architecture Review</p> 
<p>GDPR program</p> 	<p>Supplier Risk Management</p> 	<p>Mobile Applications</p> 	<p>Software Factory</p> 
<p>CISOaaS, Security audits</p> 	<p>Security Review, Pen Test</p> 	<p>Security Assessment</p> 	<p>PKI, GDPR, ISO 27001</p> 
<p>Cyber Security Consulting</p> 	<p>Staff Augmentation (PKI, SOC, GDPR)</p> 		<p>Secure Software Factory, WAF</p> 
	<p>Secure Software Factory, eIDAS, Mobile Apps</p> 		<p>Software Factory</p> 

# Thank you !

Let's keep in touch



## APPROACH LOUVAIN-LA-NEUVE

7 rue Edouard Belin 1435 Mont-Saint-Guibert

☎ **Tel** : +32 10 83 21 10 ✉ **Email** : [Sales@approach.be](mailto:Sales@approach.be) 🌐 **Website** : [www.approach.be](http://www.approach.be)

[Linked in](#)

## APPROACH ANTWERPEN

1-3 Rouaansekaai 2000 Antwerpen



# What our customers say about us

## Testimonials



*In **Approach**, we found the ideal partner to build the breakthrough technology and processes we need for a highly secure itsme® solution*

**Kris DE RYCK**

Belgian Mobile ID CEO

**Belgian Mobile ID**



***Approach** is uniquely positioned to support ISABEL securing tomorrow digital banking and corporate identity solutions.*

**Jean DE CRANE**

Isabel Group CEO

**isabel  
group**



*Thanks to **Approach**, we were able to provide our partners and customers with a solution combining high security and smooth integration.*

**Stéphane RIES**

LuxTrust Deputy CEO & COO

**LUXTRUST®**  
Enabling a digital world