# ISO27001: Why now? How to succeed?

PRESENTED BY **LAURENT DEHEYER** AND **EGIDE NZABONIMANA**

# Objectives

1. WHAT? INTRODUCTION TO ISO27001
2. WHY?
   1. BUSINESS LANDSCAPE
   2. KEY BENEFIT
3. HOW?
   1. CHALLENGES
   2. ENABLERS
   3. METHODOLOGY

# Your Guest

**Laurent Deheyer**

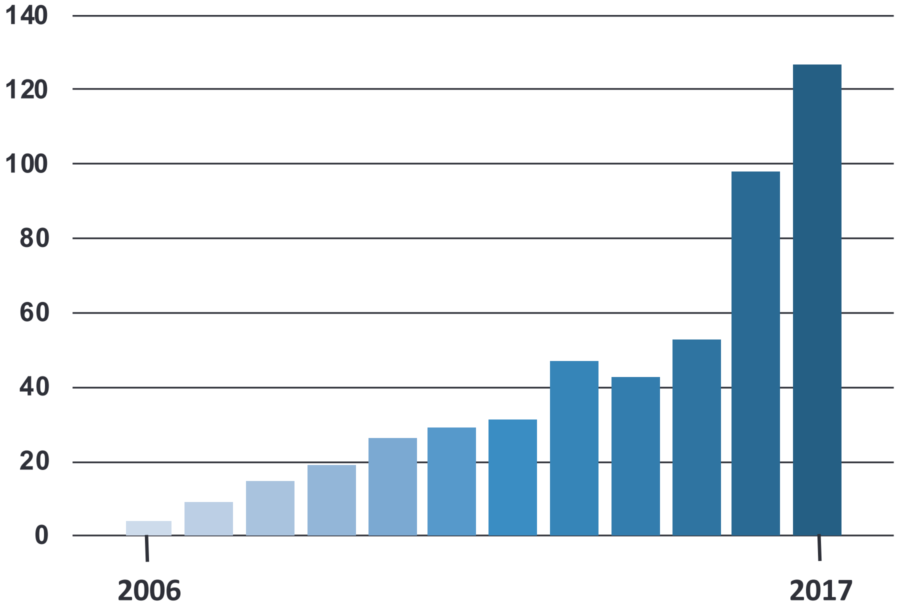
**Approach GRC Consulting Director**

**CISM – ISACA Member**

ISO 27001 Lead Implementer

Certified Data Protection Officer [GDPR]

# Number of ISO 27001 certifications is exploding in Belgium

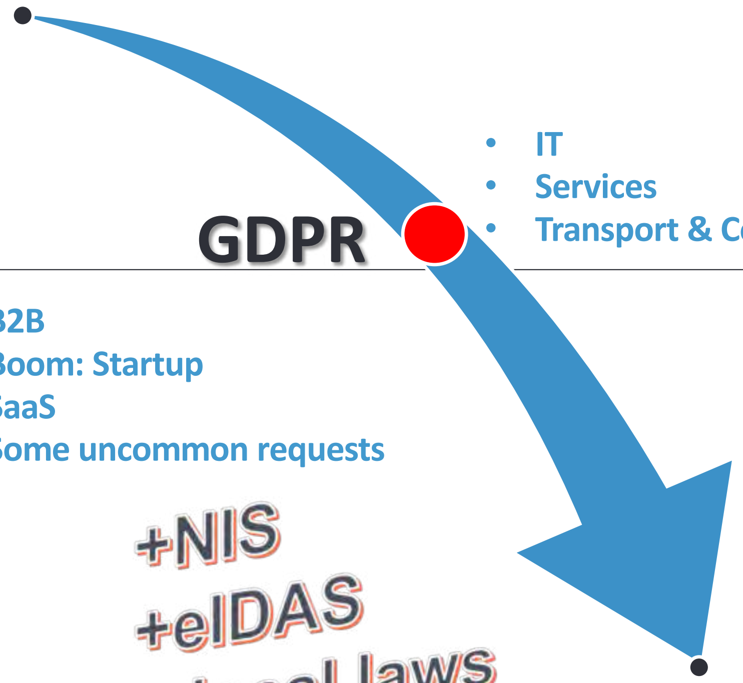


Source: [www.iso.org/the-iso-survey.html](www.iso.org/the-iso-survey.html)
ISO/IEC 27001-data per country and sector 2006 to 2017

APPROACH

# Trends

# ISO/IEC 27001



Organisations processing **company confidential data**

**GDPR**

- IT
- Services
- Transport & Communication

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

+NIS

+eIDAS

+ local laws

+...

+ ..

Organisations processing **personal data**

# ISO 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

ISO
27001:2013

# What do you want to protect?

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, ..**

Hardware

Intellectual Property

Applications

Employees

Information

# ISO27000 Family

ISO 27000 Family (Information Security)

## ISO 27001

ISMS Certification Standard

which is the reference for *certification* tackling the following subjects: Leadership, Performance, Improvement …

## ISO 27002

ISMS Code of Practice (Implementation Guidance)

describes a comprehensive set of information security control objectives and a set of generally accepted good practice security controls.

## ISO 27005

Risk Management

provides guidelines for information security risk management

# ISO27000 Family

ISO 27000 Family (Information Security)

## ISO 27001

ISMS Certification Standard

which is the reference for *certification* tackling the following subjects:

Leadership, Performance, Improvement …

Information Security Management System ISO 27001 Certified

## ISO 27701 - Privacy Information System Management

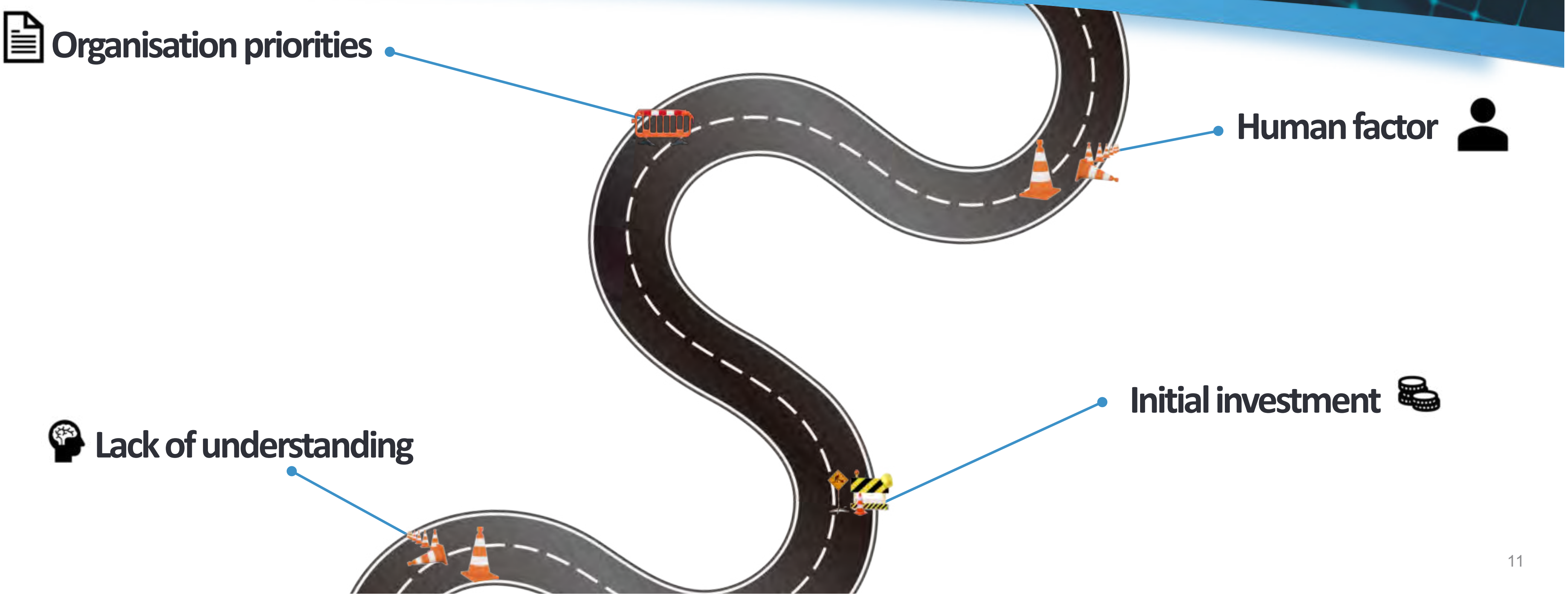
Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — **Requirements** and guidelines

ISO 27701: Will it Be the New GDPR Certification?

# Key benefits

- Compliance Management
- Market Demand
- Sales Efficiency
- Cyber Threats

# What are the roadblocks?



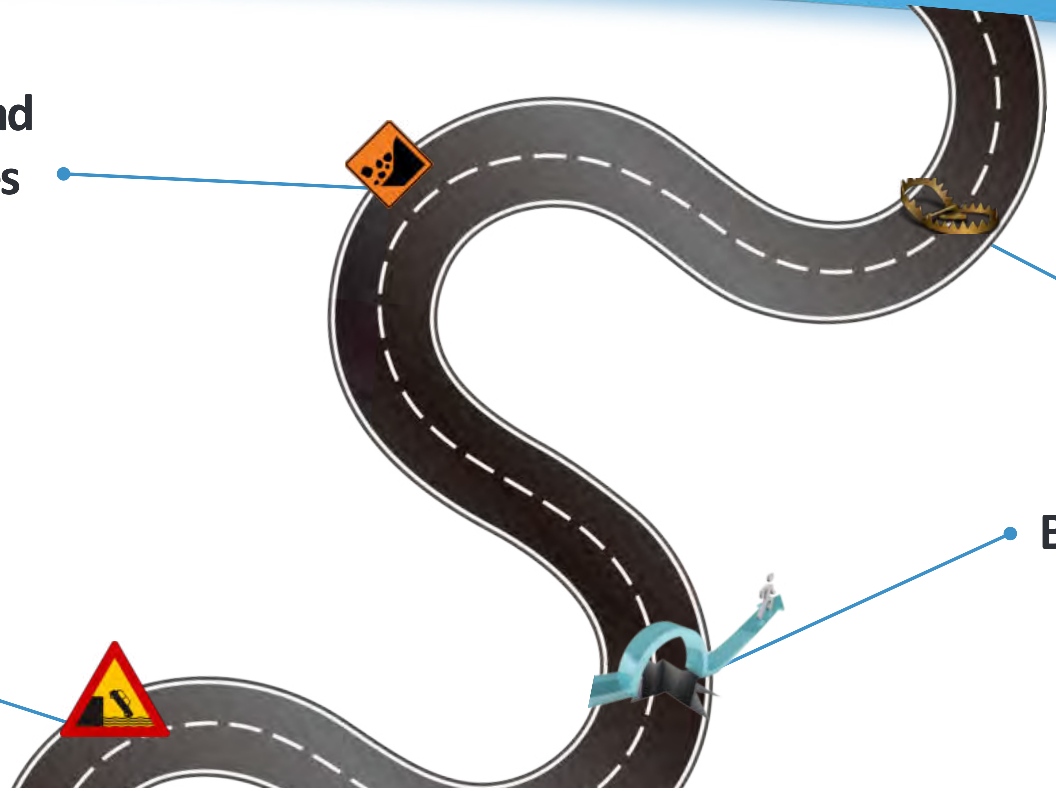
Organisation priorities

Human factor

Initial investment

Lack of understanding

# What are the pitfalls?



Lack of role and responsibilities

Technical vs. Organisational controls

Bad planning

The wrong scope

Stakeholders expecations

# Key Enablers

People

ISO 27001 Certified

CISM Certified Information Security Manager An ISACA Certification

Methodologies

COBIT 5

PRINCE2

GRC, Tools and Technologies

cases MONARC OPTIMISED RISK ANALYSIS

INTEGRITYGRC

Startup

Small & Medium

Large

# TOP  most difficult part during the projects

Survey from Approach's consultants based upon their experiences

## PHASE 1

- Scope definition
- Asset identification
- Management commitment

## ¨PHASE 2

- Change Management process and approval flows
- Data/Information classification
- Secure SDLC
- Business Continuity Management

# Question to ask during scope definition exercice

- 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?

# Top  more expensive items to consider

- Bring legacy system in compliance
- Implement proper vulnerability management system
- Develop robut secure SDLC processes
- Additional subscriptions from cloud service provider to include security controls

# Approach at a glance

# Our Portfolio of Solutions

How can **we help you ?**

| Governance, Risk & Compliance | Security Assessment | Secure Development | Infrastructure Security | Operational Security | Digital Identity & Trust Services |
|---|---|---|---|---|---|
| CISO as a Service | Penetration Testing | Secure Software Factory | Cloud Security | Cyber Emergency Services | Digital Identity Solutions |
| ISO 27001 Certification | Security Maturity Assessment | Staff Augmentation | Web Application Firewall | Forensics & Malware Analysis | IAM Solutions Integration |
| GDPR | Architecture Review | Secure Development Methodologies | System Hardening | Training & Coaching | Electronic Signatures |
| Business Continuity | Third Party Risk Assessment | Secure Code Review | Endpoint Security | Security Awareness | Other eIDAS Services |

# 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.

# Thank you !

Let's keep in touch

APPROACH

## APPROACH LOUVAIN-LA-NEUVE

7 rue Edouard Belin 1435 Mont-Saint-Guibert

## APPROACH ANTWERPEN

1-3 Rouaansekaai 2000 Antwerpen

☎ **Tel :** +32 10 83 21 10 ✉ **Email :** Sales@approach.be Website : www.approach.be

Linked in

ISO 27001 CERTIFIED VINÇOTTE

EU GDPR COMPLIANT