DPO.pro

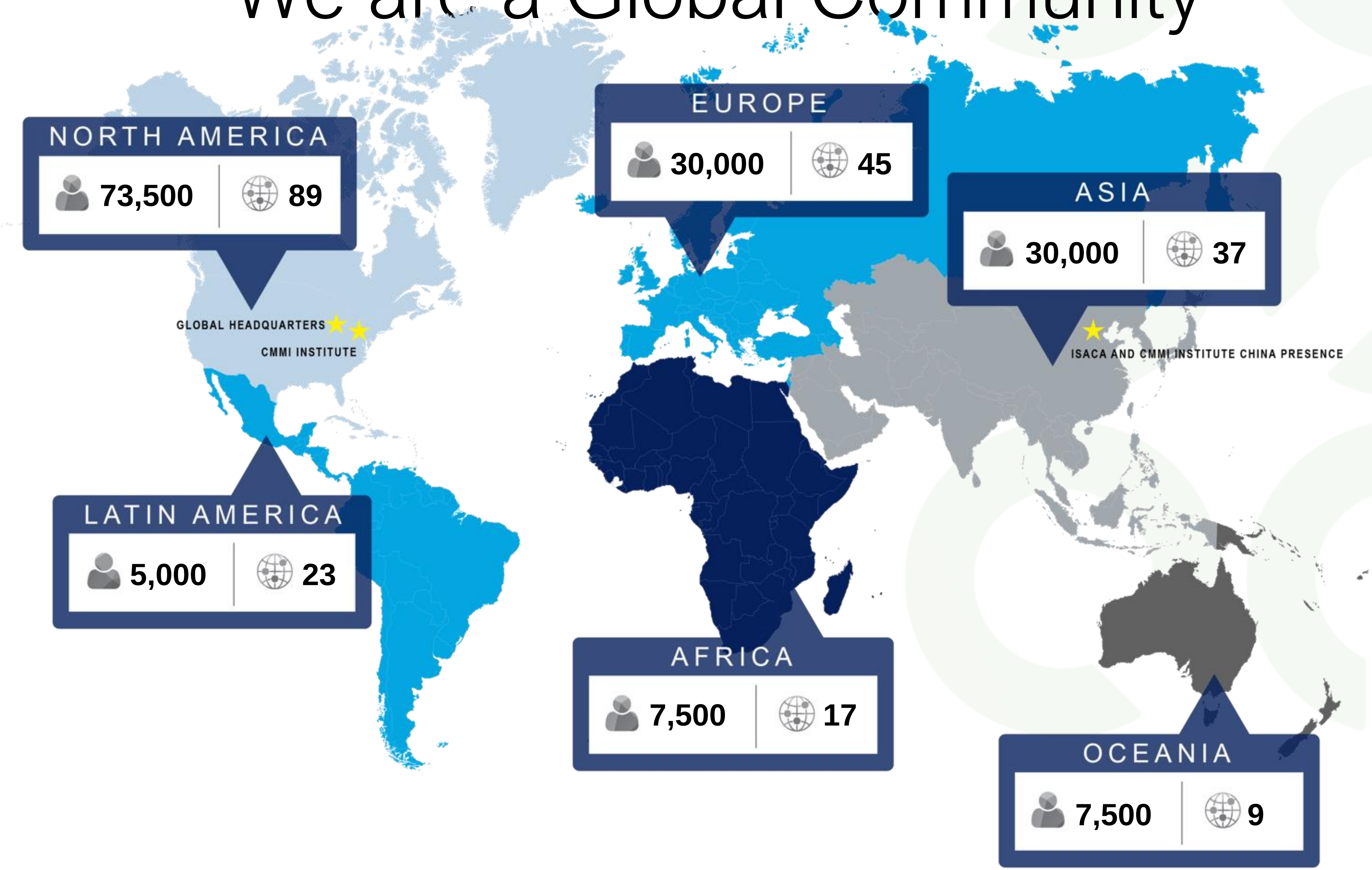
ISACA
Belgium Chapter

Data Protection
institute

INTRO BY EGIDE NZABONIMANA

HOW TO AUDIT GDPR ?

We are a Global Community



150,000+
MEMBERS

220
CHAPTERS

Note: Number of members is rounded to the nearest thousand.

ISACA

ISACA Certifications

CISA Certified Information Systems Auditor. An ISACA® Certification

CISM Certified Information Systems Manager. An ISACA® Certification

CGEIT Certified in the Governance of Enterprise IT. An ISACA® Certification

CDPSE Certified Data Privacy Solutions Engineer. An ISACA® Certification

CRISC Certified in Risk and Information Systems Control. An ISACA® Certification

CSX-P CSX Cybersecurity Practitioner. An ISACA® Certification

ADDITIONAL ISACA BUSINESSES AND BRANDS:

CMMI®

COBIT® 5
AN ISACA® FRAMEWORK

Best Professional Certification Program SC
Awards 2020

Best Professional Certification Program Finalist
SC Awards 2020

Global Knowledge's 2020 Highest-Paying IT Certifications

#3 CISM

#4 CRISC

#7 CISA

ISACA

What do you benefit from joining the ISACA Belgium Chapter

1 A strong network of local professionals in Belgium

2 ISACA Frameworks

Access to the updated frameworks in advance

Access to the framework details and toolbox

3 Events/Webinars

Access to worldwide events at a discounted price

Early access to events with limited places

4 Community

Access to a community of experts exchanging information on certifications and documents

Access to an international forum to discuss ISACA related subjects

How to be aware of ISACA Belgium events or updates

Contact a person from the ISACA Belgium chapter

There are many ISACA Belgium chapter person available to answer any question you have regarding the events, the certifications, local events…

You can even connect with a bigger network of professional sin the field via the chapter

Subscribe to the ISACA Belgium Chapter Newsletter

Registering to the newsletter give access to the upcoming events and notify as well for any updates

In case of any changes in the venue or in the event per se, you are warned in advance

You get updates from the board of directors

DPO.pro

ISACA Belgium Chapter

Data Protection institute

19 OCTOBER

INTRO BY EGIDE NZABONIMANA

HOW TO AUDIT GDPR ?

HYBRID EVENT : @ P&V IN BRUSSELS & LIVE WEBINAR

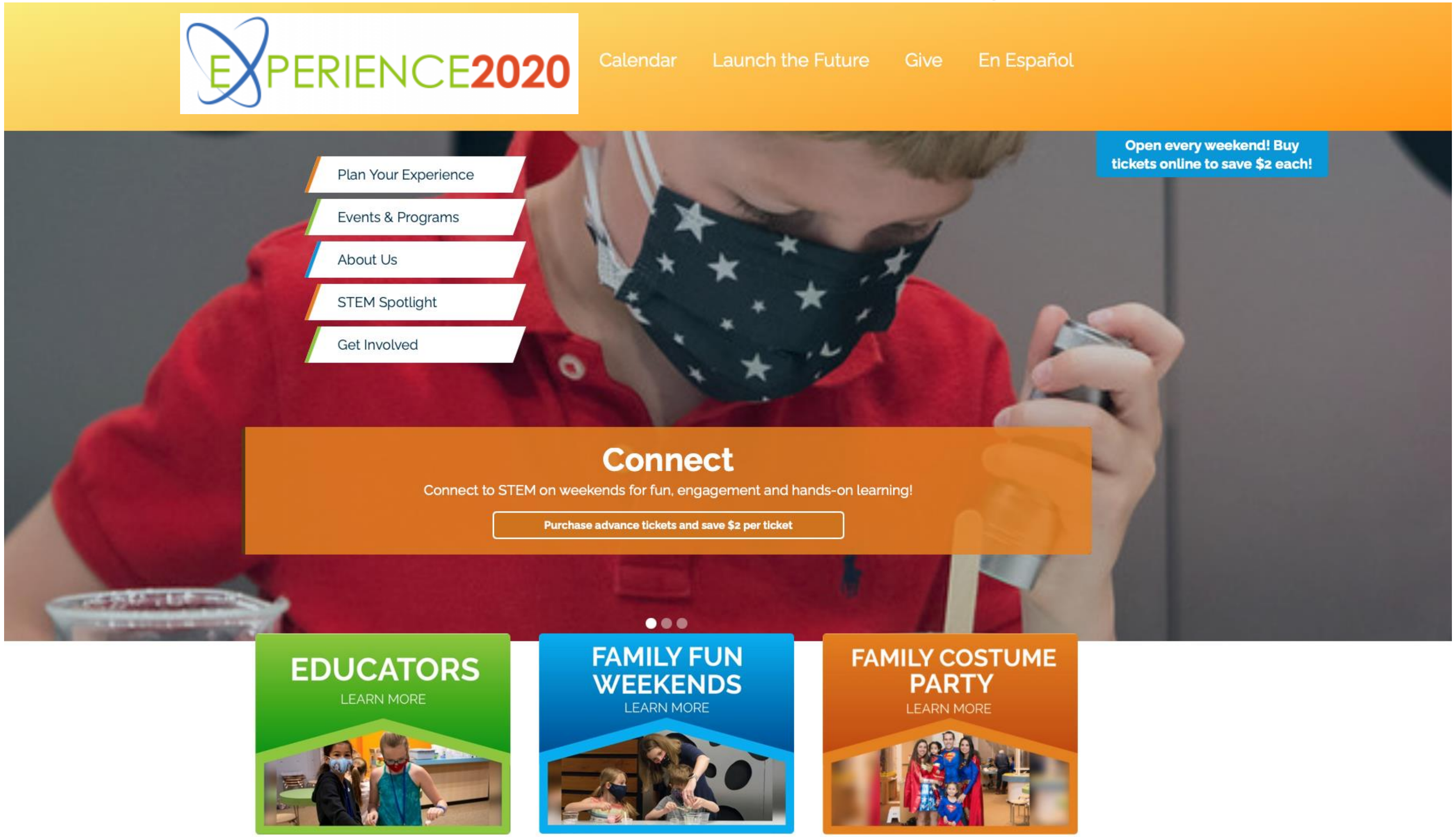
GDPR AUDIT: WHAT ARE WE TALKING ABOUT?

AUDITING GDPR RELATED RISKS

PETER BERGHMANS

PATRICK SOENEN

Introduction - Casestudy



Open every weekend! Buy tickets online to save $2 each!

Connect

Connect to STEM on weekends for fun, engagement and hands-on learning!

Experience 2020 is a hands-on science center designed for children
5 – 17 years of age.

They offer:

- fascinating and interactive exhibits
- programs and camps that bring the physical sciences to life.

What can be the goal of the audit?

DPO | CISO | CEO | R&C manager | Internal auditor | Data subject

Remember: DPO has 3 tasks, as defined by art. 39 GDPR:

- To inform
- To provide advice
- To monitor compliance

What can be the goal of the audit?

DPO | CISO | CEO | R&C manager | Internal auditor | Data subject

The DPO of Experience2020 might be interested in:

- Are all processing activities “in line” (compliant) with GDPR
- Is everyone aware?
- Are processes regarding data subject rights running in a compliant manner?

What can be the goal of the audit?

DPO | **CISO** | CEO | R&C manager | Internal auditor | Data subject

The CISO of Experience2020 might be interested in:

- Is personal data well secured?
- Are new exhibits designed in a secured manner (security and privacy be design)?
- Are suppliers working in a secure way (DP-agreements)?

What can be the goal of the audit?

DPO | CISO | **CEO** | R&C manager | Internal auditor | Data subject

The CEO of Experience2020 might be interested in:

- Are we vulnerable to fines?
- (Do we need to bother anyway)?

What can be the goal of the audit?

DPO | CISO | CEO | **R&C manager** | Internal auditor | Data subject

- Can we show accountability?
- Is GDPR part of the overall risk assessment of the company?

What can be the goal of the audit?

DPO | CISO | CEO | R&C manager | **Internal auditor** | Data subject

- To what extend is GDPR implemented in that way that it it covers risks and opportunities of business and stakeholders?

What can be the goal of the audit?

DPO | CISO | CEO | R&C manager | Internal auditor | **Data subject**

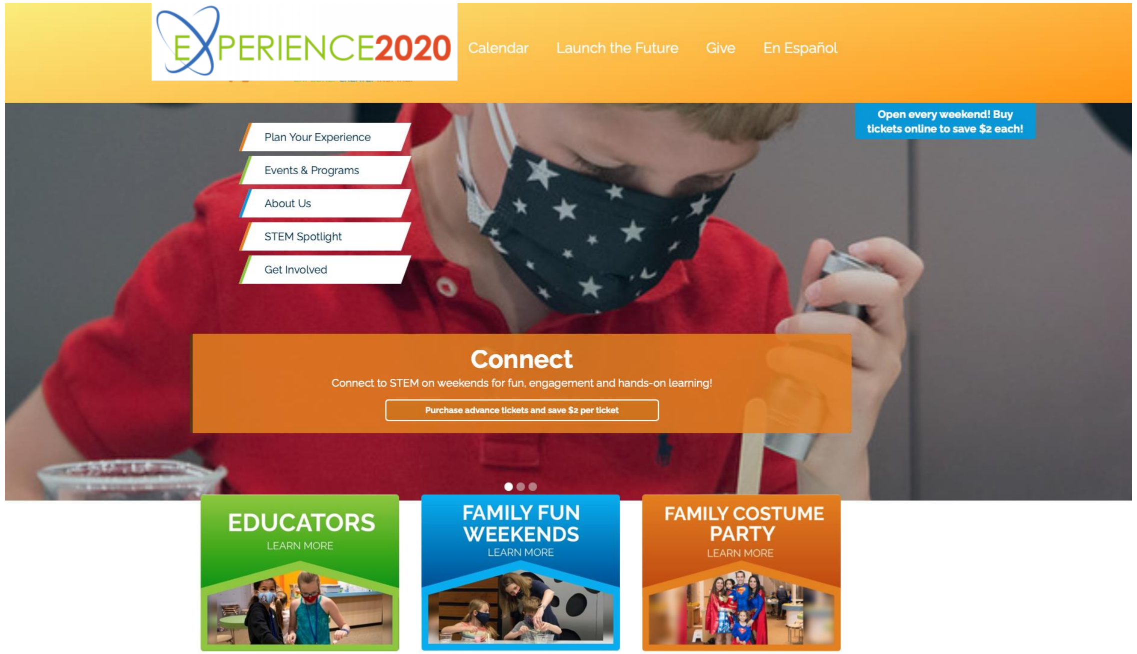
- Are cookies on the website of Experience 2020 compliant to ePrivacy directive?
- Are exhibits collecting sensitive data?

Scoping is key in GDPR audits

Defining the audit scope, methodology and goals is needed

GDPR is complex as it contains

- A technical dimension
- A legal dimension
- An ethical dimension
- Operational dimension
- Accountability is core in GDPR



Open every weekend! Buy tickets online to save $2 each!

Connect

Connect to STEM on weekends for fun, engagement and hands-on learning!

Purchase advance tickets and save $2 per ticket

Types of GDPR audits

1. Common types of audit in GDPR
2. Other types of evaluations/audits
3. What is ‘risk-based approach’?

Type of audits

Management system audit

Scope: Organisation

Plan-Do-Check-Act related to management system

Framework based on set of controls

Type 1

Product/services based auditing

Scope: Product and services

Technical, legal and organisational scope

Audit schema (ToE)

Type 2

Risk based (internal audit)

Scope: (part of) organisation

- Governance
- Risk
- Controls

Risk based auditing

Type 3

Type of audits

Management system audit

Scope: Organisation

Plan-Do-Check-Act related to management system

Framework based on set of controls

Type 1

View organization from a management system perspective

Link organization and management system is being looked at

PDCA approach means that you look at how the system is set up and how the feedback loop works

Typical: Audit is done via fixed steps (ISO 19011)

Controls come from standards (like ISO 27701)

- Standard that defines the management system
- Standard containing the controls

Type of audits: result type 1

Management system audit

Scope: Organisation

Plan-Do-Check-Act related to management system

Framework based on set of controls

Type 1

- Is the management system of Experience 2020 running?
  - Is the management involved?
  - Are budgets and resources available?
  - Are risks identified and managed?
  - Are controls implemented?
  - Are review meetings and audits running?

- Are controls in place?

Type of audits: result type 1

Management system audit

Scope:
Organisation

Plan-Do-Check-Act related to management system

Framework based on set of controls

Type 1

- Are controls in place?
  - Example control 6.5.3.1 implemented?
    - *Experience 2020 uses removable physical media and/or devices that permit encryption when storing PII. Unencrypted media should only be used where unavoidable, and in instances where unencrypted media and/or devices are used, Experience2020 should implement procedures and compensating controls (e.g. tamper-evident packaging) to mitigate risks to the PII.*

Type of audits: result type 1

Management system audit

Scope: Organisation

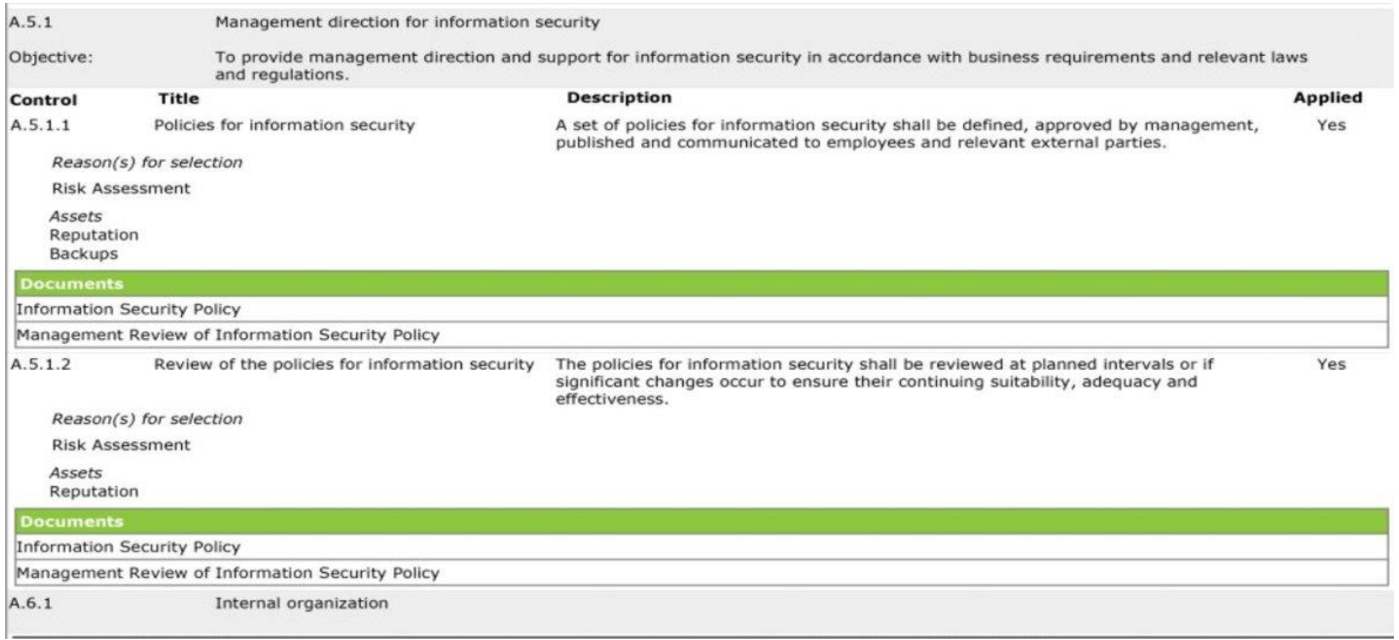
Plan-Do-Check-Act related to management system

Framework based on set of controls

Type 1

- Focus on **ACCOUNTABILITY**
- Certificates such as ISO 27701 (ISO 27001)

Result will be a statement of applicability



A.5.1	Management direction for information security		
Objective:	To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.		
Control	**Title**	**Description**	**Applied**
A.5.1.1	Policies for information security	A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.	Yes
	Reason(s) for selection Risk Assessment *Assets* Reputation Backups		
Documents			
Information Security Policy			
Management Review of Information Security Policy			
A.5.1.2	Review of the policies for information security	The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	Yes
	Reason(s) for selection Risk Assessment *Assets* Reputation		
Documents			
Information Security Policy			
Management Review of Information Security Policy			
A.6.1	Internal organization		

Type of audits

Product/services based auditing

Scope: Product and services

Technical, legal and organisational scope

Audit schema (ToE)

Type 2

Not the organization, but a product or service is screened

A schedule is drawn up prior to the audit

The audit activities are described in ISO 17065

TOMs and legal

Type of audits: result type 2

Product/services based auditing

Scope: Product and services

Technical, legal and organisational scope

Audit schema (ToE)

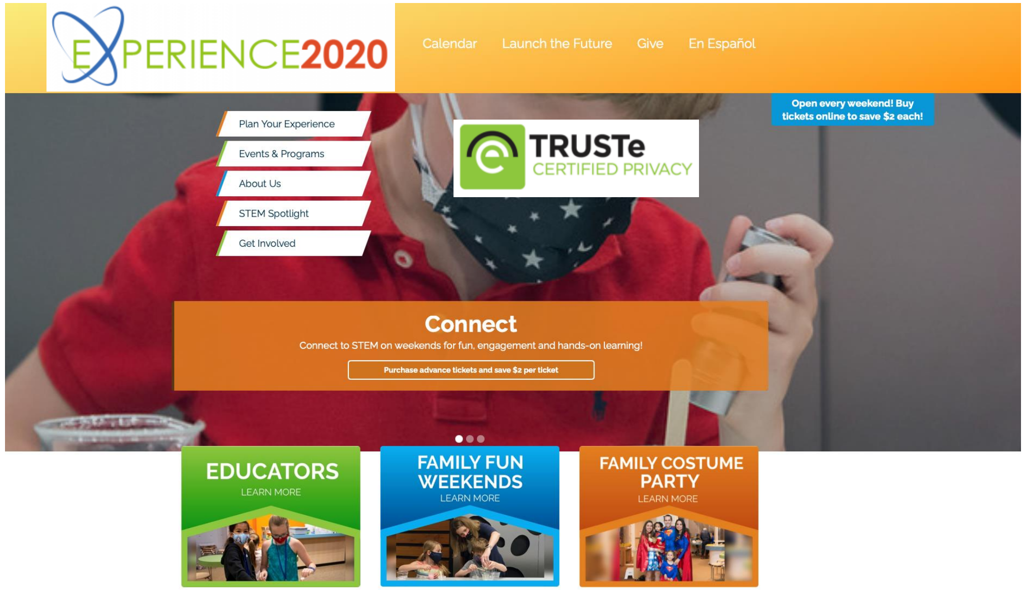
Type 2

Is a product or service running in a compliant way?

In depth results (legal/TOMs)

GDPR articles 42 and 43 => certification is possible

Seals are possible



Open every weekend! Buy tickets online to save $2 each!

Connect to STEM on weekends for fun, engagement and hands-on learning!

Type of audits

Risk based (internal audit)

Scope: (part of) organisation

- Governance
- Risk
- Controls

Risk based auditing

Type 3

- Auditing organization from a holistic approach
- Integration of a GDPR audit into a wider GRC framework
- Typical frameworks are ERM/COSO (IFACI – see next presentation)
- Typical standards are
  - IPPF (International Professional Practices Framework) of IIA
  - More abstract in thinking
  - Broader scope

Type of audits results type 3

Risk based (internal audit)

Scope: (part of) organisation

- Governance
- Risk
- Controls

Risk based auditing

Type 3

- Focus on business risks
- Not an evaluation of the process activities
- Also focus on ACCOUNTABILITY

Types of GDPR audits

1. Common types of audit in GDPR
2. **Other types of evaluations/audits**
3. What is ‘risk-based approach’?

Other types of evaluation/audit

Inspection | Forensic audit | Other

Inspection department of the GBA/APD

- In scope vs out of scope inspections
- Reports will be sent to litigation chamber

Other types of evaluation/audit

Inspection | **Forensic audit** | Other

Fraud: In Belgium IFA is the institute for fraud auditors.

They publish a guide on how to deal with fraud and the role of audit in this.

Code of conduct?

Other types of evaluation/audit

Inspection | **Forensic audit** | Other

Forensic audit & GDPR? Can be executed

- after a case of fraud
- but also after an incident
  - At the processor see processing agreement
  - At own organization:
    - see also cyber policy
    - Watch out for the role of DPO
    - Interaction with police services: investigative powers?

Other types of evaluation/audit

Inspection | Forensic audit | **Other**

- Intentions of the evaluation/audit may influence the way GDPR will be evaluated

i.e. GDPR check during the Due diligence

Other types of evaluation/audit

Inspection | Forensic audit | **Other**

- Data Protection Officer also has the task to evaluate GDPR (art 39 par 1b):

  to monitor compliance with

  - this Regulation
  - with other Union or Member State data protection provisions
  - and with the policies of the controller or processor in relation to
    - the protection of personal data, including the assignment of responsibilities
    - awareness-raising and training of staff involved in processing operations
    - and the related audits;

Types of GDPR audits

1. Common types of audit in GDPR
2. Other types of evaluations/audits
3. What is ‘risk-based approach’?

Risk based approach

Protection of personal data: fundamental right cfr Article 8 Charter of Fundamental Rights.

- Any processing operation, from collection to use and disclosure, should respect this key right.
- Rights granted to data subject by EU law should be respected regardless level of the risks

There can be different levels of accountability obligations depending on risk

- There should be recognition that not every accountability obligation is necessary in every case
- Form of documentation of processing activities can differ according to risk posed by processing
- However controllers should always be accountable

DPO.pro ISACA Belgium Chapter Data Protection institute

AUDITING GDPR RELATED RISKS

PATRICK SOENEN

GENERAL SECRETARY

DPO.pro

Manage and audit GDPR risks

DPO.pro

https://www.dpopro.be/

Support a thriving community of DPOs

Promote and represent the DPOs

Inform DPOs at the top

DPO Connect

https://www.dpoconnect.be/

- Forum
- FAQ
- Library
- News

DPO.pro

European Commission

Autorité de protection des données
Gegevensbeschermingsautoriteit

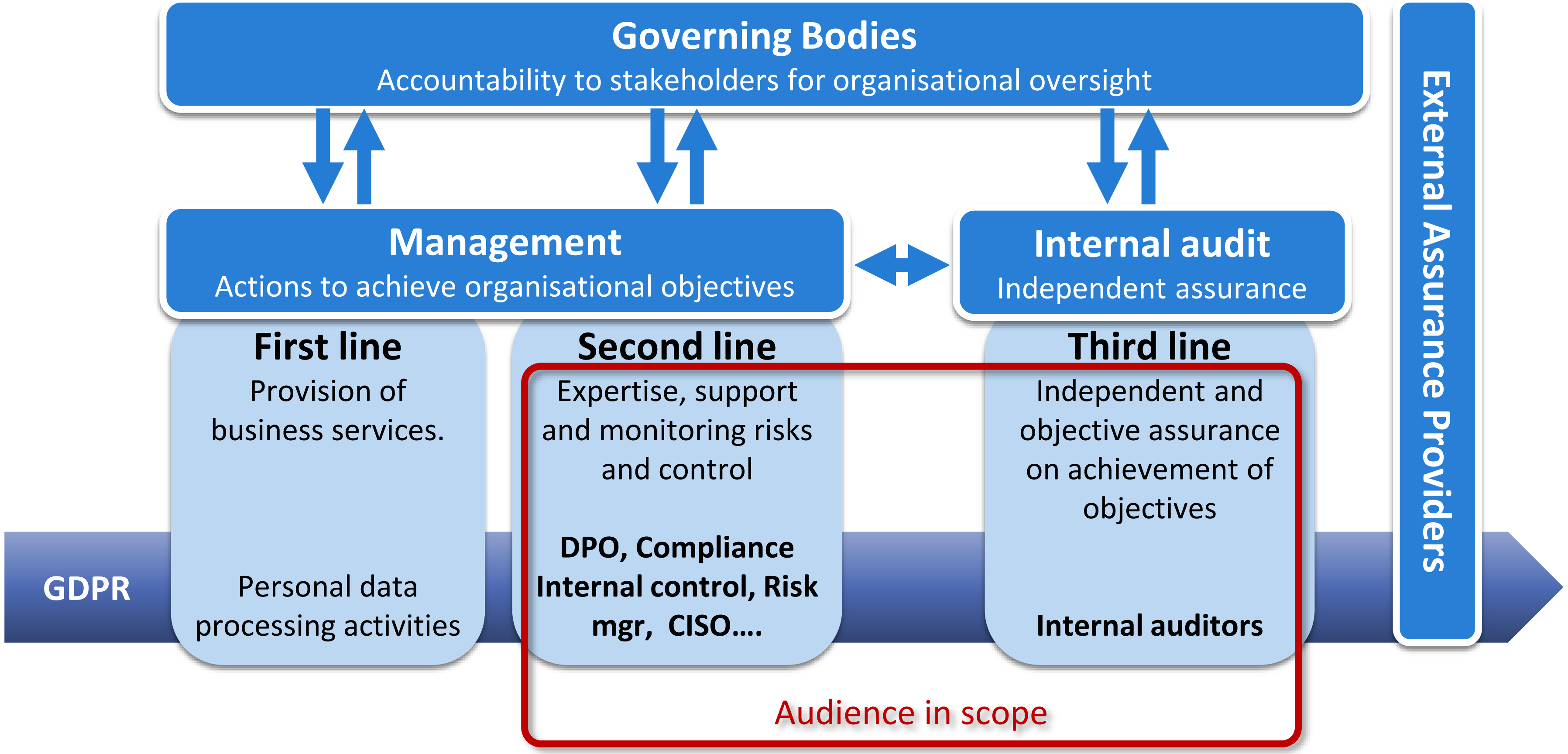
VUB VRIJE UNIVERSITEIT BRUSSEL

Audience

THE IIA'S THREE LINES MODEL

An update of the Three Lines of Defense

The Institute of Internal Auditors Global


Governing Bodies
Accountability to stakeholders for organisational oversight
Management
Actions to achieve organisational objectives
Internal audit
Independent assurance
External Assurance Providers
GDPR
First line
Provision of business services.
Personal data processing activities
Second line
Expertise, support and monitoring risks and control
DPO, Compliance Internal control, Risk mgr, CISO....
Third line
Independent and objective assurance on achievement of objectives
Internal auditors
Audience in scope

Audit / Assurance ?

A specific type of **assurance engagement**

In which an audit and assurance **professional**

Conducts a formal independent and systematic inspection or **examination**

Of a **subject matter** →

Against a recognised and appropriate **standard** →

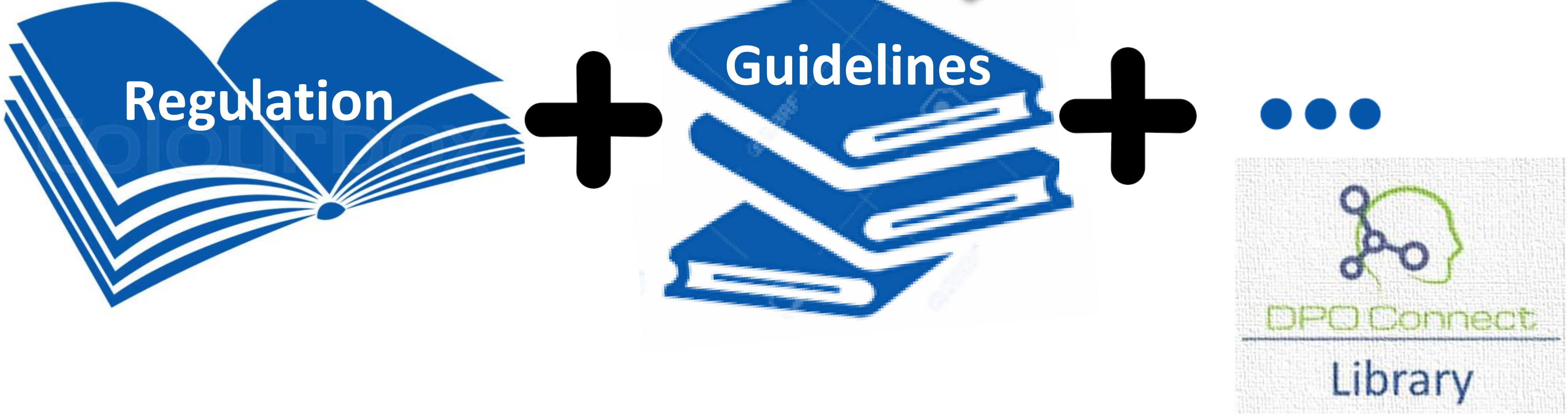
That must meet specific **criteria** →

GDPR

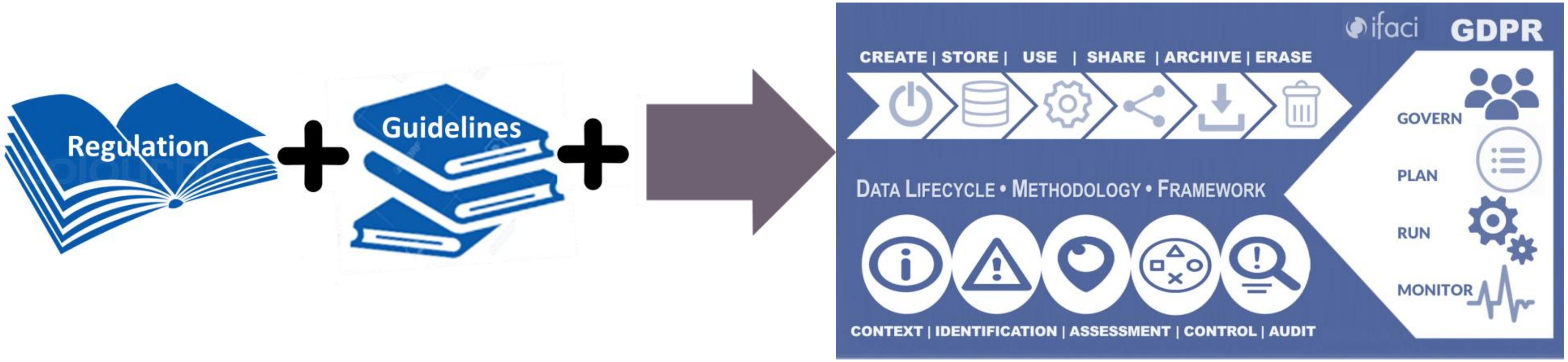
Compliance? Risk?

Audit / Assurance ?

Against a recognised and appropriate **standard**



Origin


Regulation
+
Guidelines
+
ifaci GDPR
CREATE | STORE | USE | SHARE | ARCHIVE | ERASE
DATA LIFECYCLE • METHODOLOGY • FRAMEWORK
CONTEXT | IDENTIFICATION | ASSESSMENT | CONTROL | AUDIT
GOVERN
PLAN
RUN
MONITOR

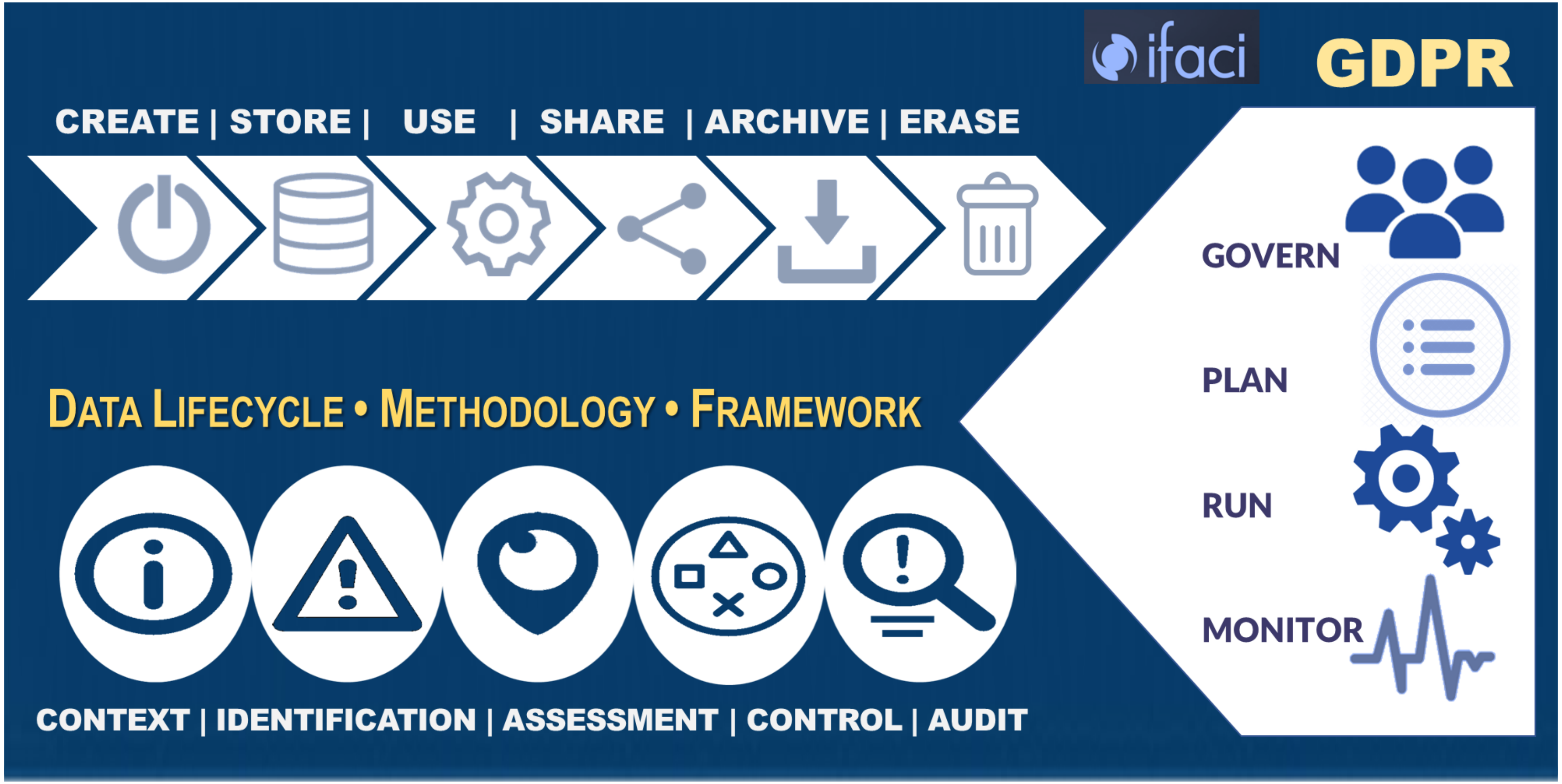
- Methodology and a framework to **manage and audit GDPR risks**

- Developed by a workgroup @ IFACI - French IIA chapter (2018 – 2020)

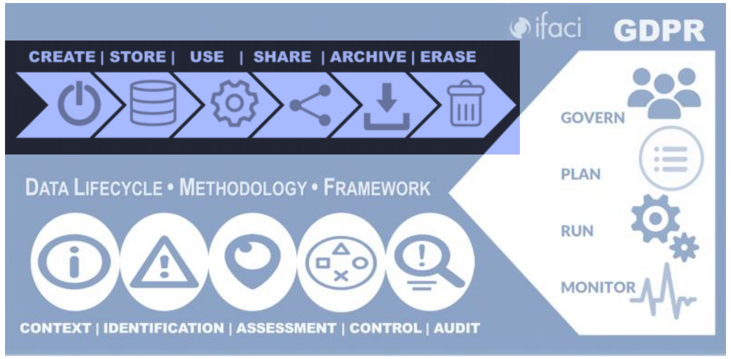
ifaci institut français de l'audit et du contrôle internes

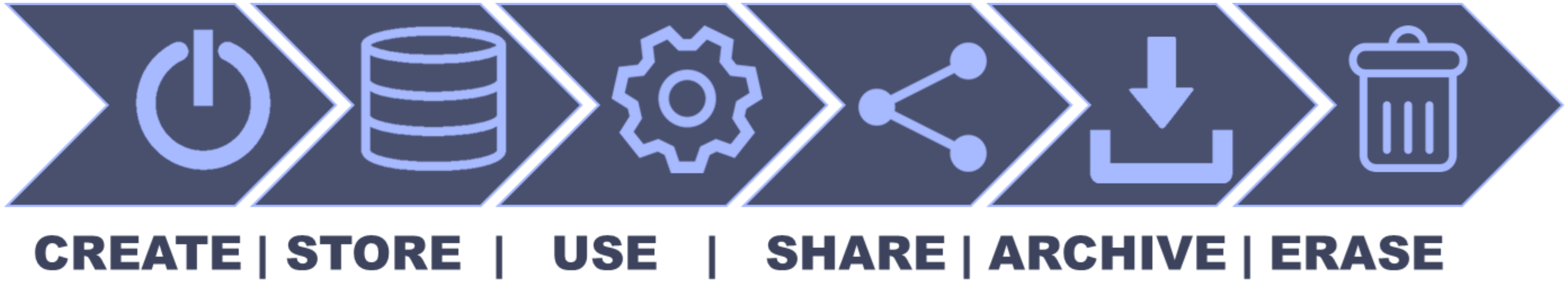
GROUPE DE TRAVAIL RGPD

Overview - Framework & Methodology


ifaci
GDPR
CREATE | STORE | USE | SHARE | ARCHIVE | ERASE
DATA LIFECYCLE • METHODOLOGY • FRAMEWORK
CONTEXT | IDENTIFICATION | ASSESSMENT | CONTROL | AUDIT
GOVERN
PLAN
RUN
MONITOR

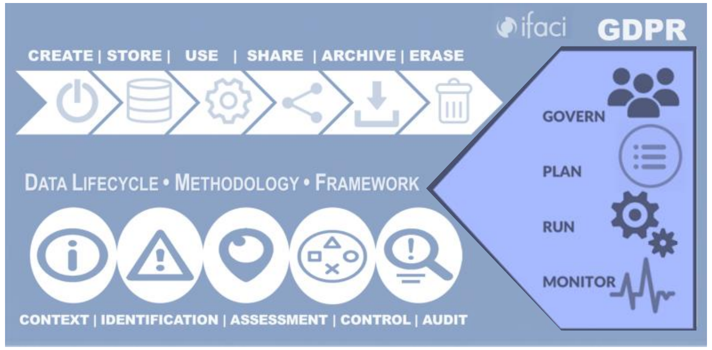
… covering the personal data lifecycle

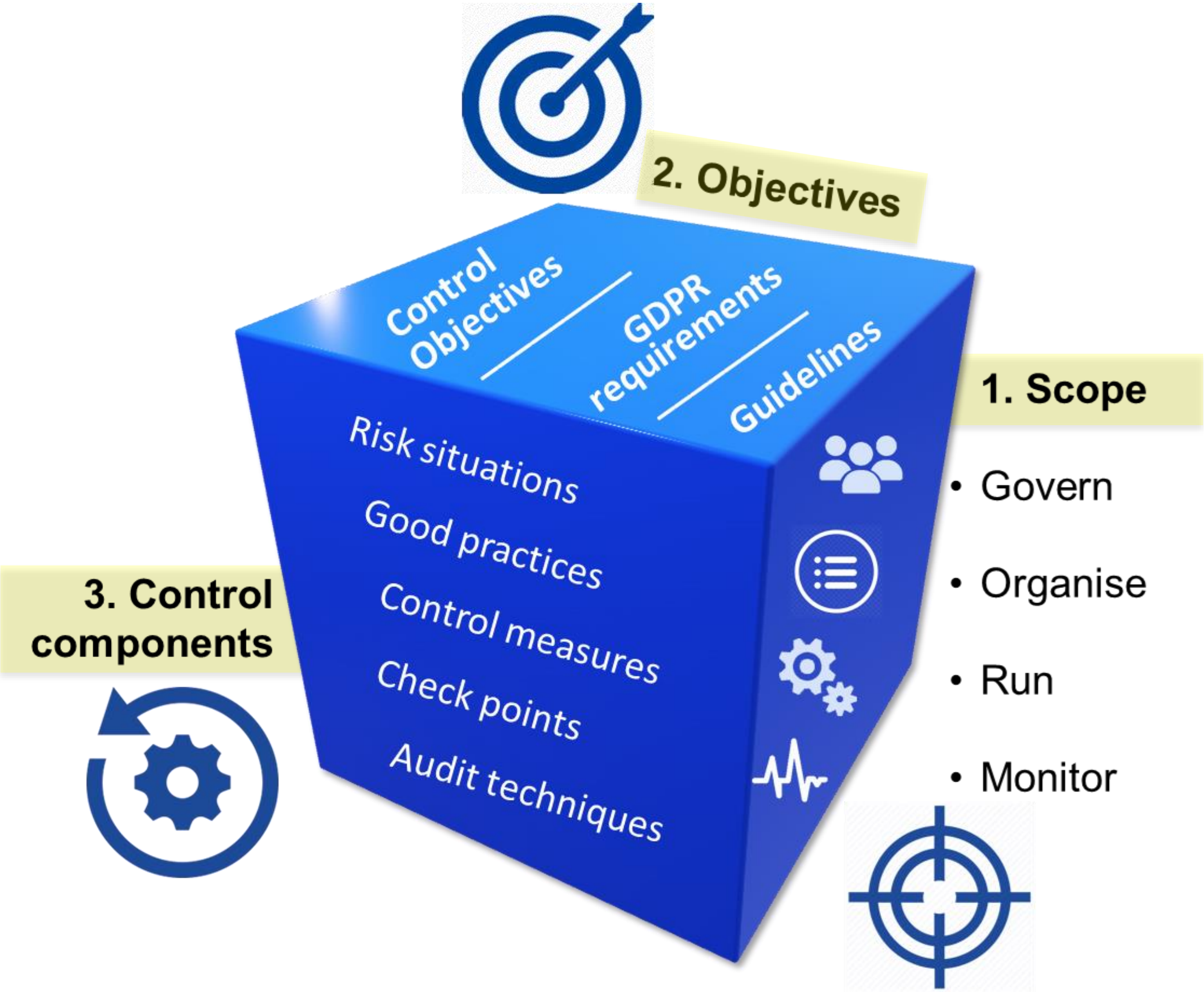

ifaci
GDPR
CREATE | STORE | USE | SHARE | ARCHIVE | ERASE
GOVERN
PLAN
RUN
MONITOR
DATA LIFECYCLE • METHODOLOGY • FRAMEWORK
CONTEXT | IDENTIFICATION | ASSESSMENT | CONTROL | AUDIT



- Data
  - Personal
  - Sensitive
- Processing
  - From collection…
  - To deletion

GDPR Framework


ifaci GDPR
CREATE | STORE | USE | SHARE | ARCHIVE | ERASE
DATA LIFECYCLE • METHODOLOGY • FRAMEWORK
GOVERN
PLAN
RUN
MONITOR
CONTEXT | IDENTIFICATION | ASSESSMENT | CONTROL | AUDIT



2. Objectives

Control Objectives / GDPR requirements / Guidelines

1. Scope

- Govern
- Organise
- Run
- Monitor

3. Control components

Risk situations

Good practices

Control measures

Check points

Audit techniques

GDPR Framework - Scope

1. Scope

- Govern
- Organise
- Run
- Monitor

4 domains *21 topics*

	A. Govern	
	Governance bodies, roles & responsibilities, policies ensuring adequate personal data protection within the organisation.	4 topics
	B. Organise	
	Processes to implement according GDPR requirements.	7 topics
	C. Run	
	Processes and procedures to deploy to get GDPR operational.	7 topics
	D. Monitor	
	Oversight, review, monitoring and inspection measures	3 topics

GDPR Framework - Scope

1. Scope

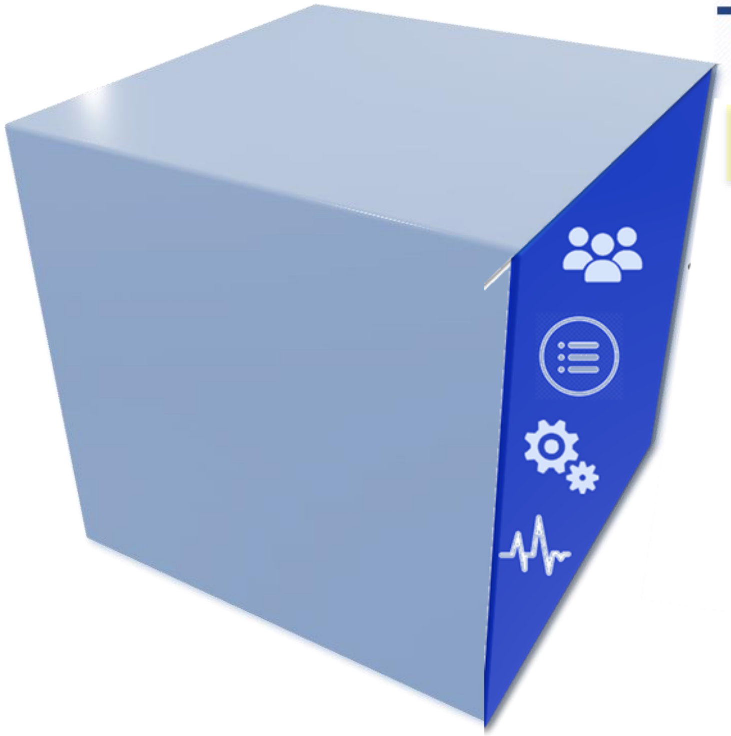
- Govern
- Organise
- Run
- Monitor

👥	A. Govern
	A1. Commitment of the Data Controller
	A2. Data protection policies & organisation
	A3. Governance bodies, roles & responsibilities
	A4. Data Protection Officer (DPO)
☰	B. Organise
⚙	C. Run
🟥	D. Monitor

1. Scope

- Govern
- Organise
- Run
- Monitor

GDPR Framework - Scope

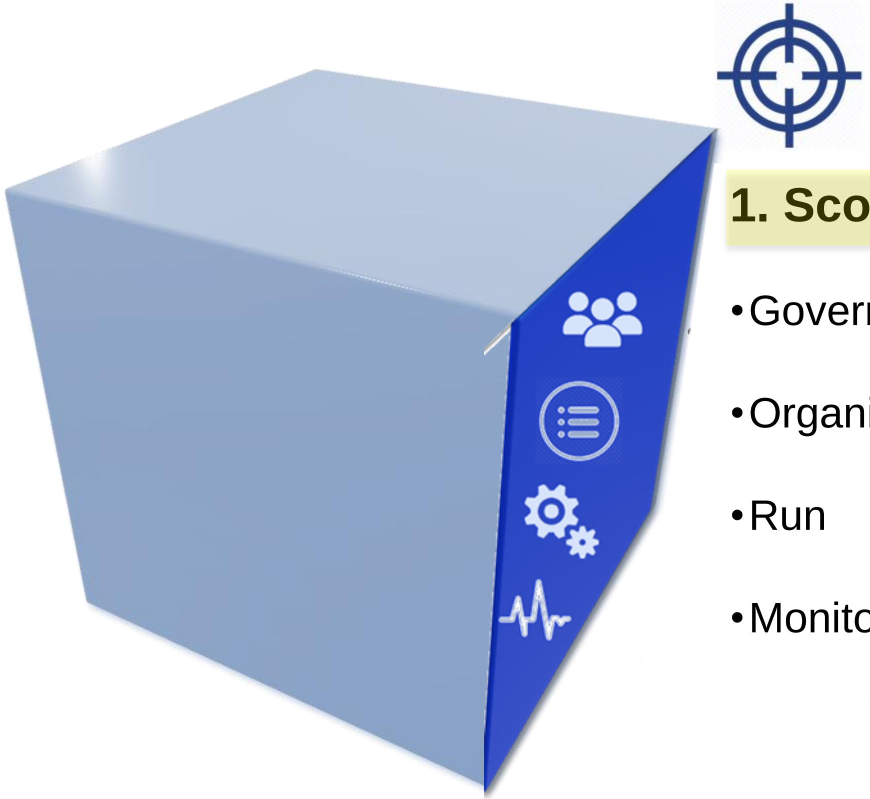


1. Scope

- Govern
- Organise
- Run
- Monitor

	A. Govern
	B. Organise
	B1. Lawfulness of processing
	B2. Records of processing activities
	B3. Data Protection Impact Analysis (DPIA)
	B4. Privacy by Design and by Default
	B5. Use and retention of personal data
	B6. Controller - Processor relationships
	B7. Transfers outside the European Economic Area
	C. Run
	D. Monitor

GDPR Framework - Scope



1. Scope

- Govern
- Organise
- Run
- Monitor

A. Govern

B. Organise

C. Run

C1. Steering and implementation

C2. Rights of the data subject

C3. Information and transparency

C4. Awareness raising and training

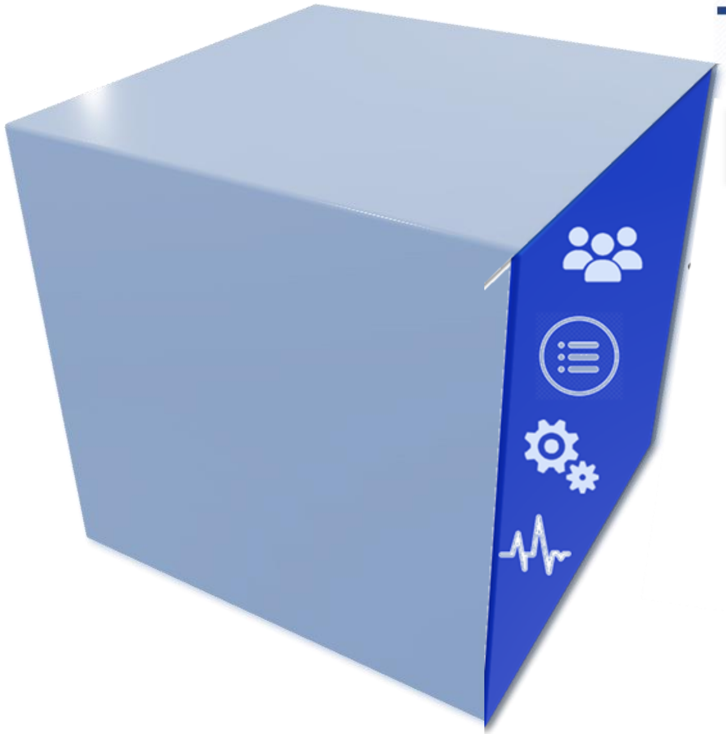
C5. Business and service continuity management

C6. Data breach management and notification

C7. Personal data proteccion and security

D. Monitor

GDPR Framework - Scope



1. Scope

- Govern
- Organise
- Run
- Monitor

A. Govern

B. Organise

C. Run

D. Monitor

D1. Monitoring and review by the DPO

D2. Review by the lines of defense

D3. Inspection by the Data Protection Authority

GDPR Framework - Objectives

2. Objectives
Control Objectives
GDPR requirements
Guidelines

Sample

Domain A. Govern

Topic A1. Commitment of the Data controller

Control objectives

Business objective, goal to reach

Set the tone at the top by ensuring adequate governance bodies and establishment of a privacy charter

GDPR requirements

based on the regulation

Art 4 - (7) Controller
Art 24 - Responsibility of the controller
Art 26 – Joint controllers

Guidelines

from EDPB or G29.

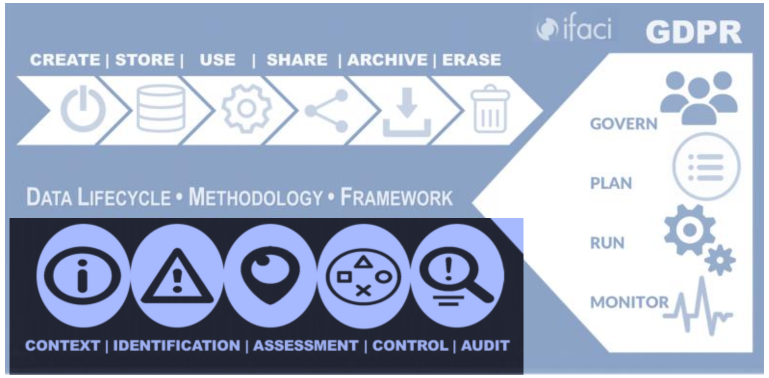
- EDPS guidelines on the concepts of controller, processor ….
- Guidelines 7/2002 on the concepts of controller and processor … (EDPB)
- …

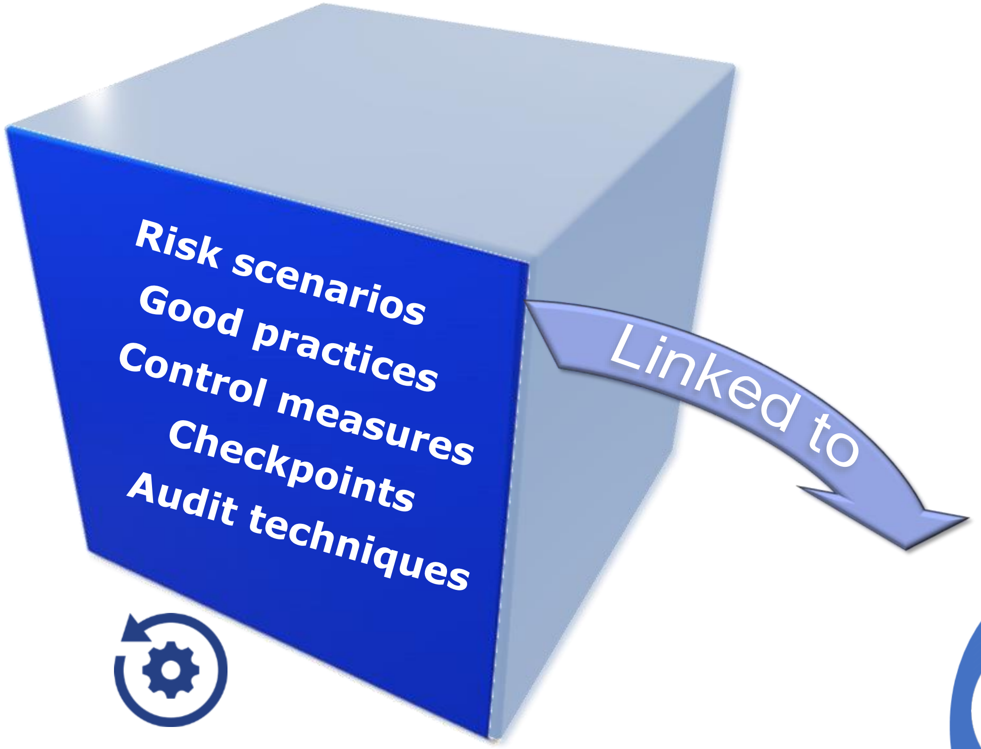
GDPR Framework - Controls

Risk scenarios
Good practices
Control measures
Checkpoints
Audit techniques
3. Control components

- Risk scenarios
  description of a potential risk event
- Good practice
  Action proven to provide positive results
- Control measures
  Actions to reduce the risk level within acceptable levels (appetite)
- Checkpoints
  Verifications and indicators to ensure the operational effective of the control measures
- Audit techniques
  Methods to collect evidence on the measures effectiveness

GDPR Framework - Controls


ifaci GDPR
CREATE | STORE | USE | SHARE | ARCHIVE | ERASE
DATA LIFECYCLE • METHODOLOGY • FRAMEWORK
GOVERN
PLAN
RUN
MONITOR
CONTEXT | IDENTIFICATION | ASSESSMENT | CONTROL | AUDIT



Risk scenarios
Good practices
Control measures
Checkpoints
Audit techniques

Linked to

Methodology

Context setting	Risk identification	Risk analysis	Control measures	Audit execution

← Based on ISO 31000 →

Methodology – 1. Context setting

- **Understand** the personal data business environment
  - Personal data processed
  - Processing activities
  - Roles and responsibilities
  - Risk culture
  - Risk Appetite (Risk acceptance criteria)
  - Control environment
  - ……

Methodology – 2. Risk analysis

Identify risks
based on hypothetical risk situations:

Sample A1

Domain A. Govern
Topic A1. Commitment of the Data controller

  - Lack of commitment by governance bodies (tone @ top)
  - Deficiency of allocated resources
  - No formalised governance/management processes
  - Non-existence or no/low visibility of a data protection approach
- Good practices
  - Code of conduct, privacy charter …
  - Data protection policies
  - “Data protection” on agenda of the executive committee
  - ……

DPO.pro ISACA Belgium Chapter Data Protection institute

Methodology – 3. Risk analysis

- **Impact criteria:** financial reputation performance

- **Risk level** = Highest Frequency x impact

Frequency → **Impact ↓**	Trivial	Low	Moderate	High	Sure
Critical	🟥	🟥	🟥	🟥	🟥
Strong	🟦	🟥	🟥 **Significant exposure**	🟥	🟥
Medium	🟩	🟦	🟦	🟥	🟥
Low	■	🟩	🟦 **Medium exposure**	🟦	🟦
Negligible	■ **Negligible exposure**	■	🟩 **Low exposure**	🟩	🟦

Methodology – 4. Control Measures

Risk scenarios
Good practices
Control measures
Checkpoints
Audit techniques

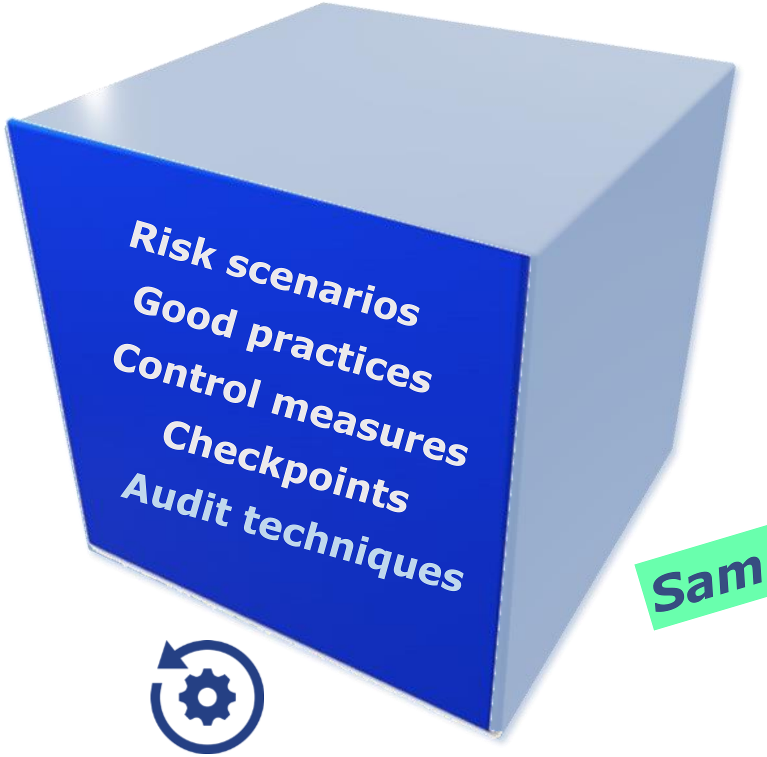
RISK MITIGATION

Sample A1

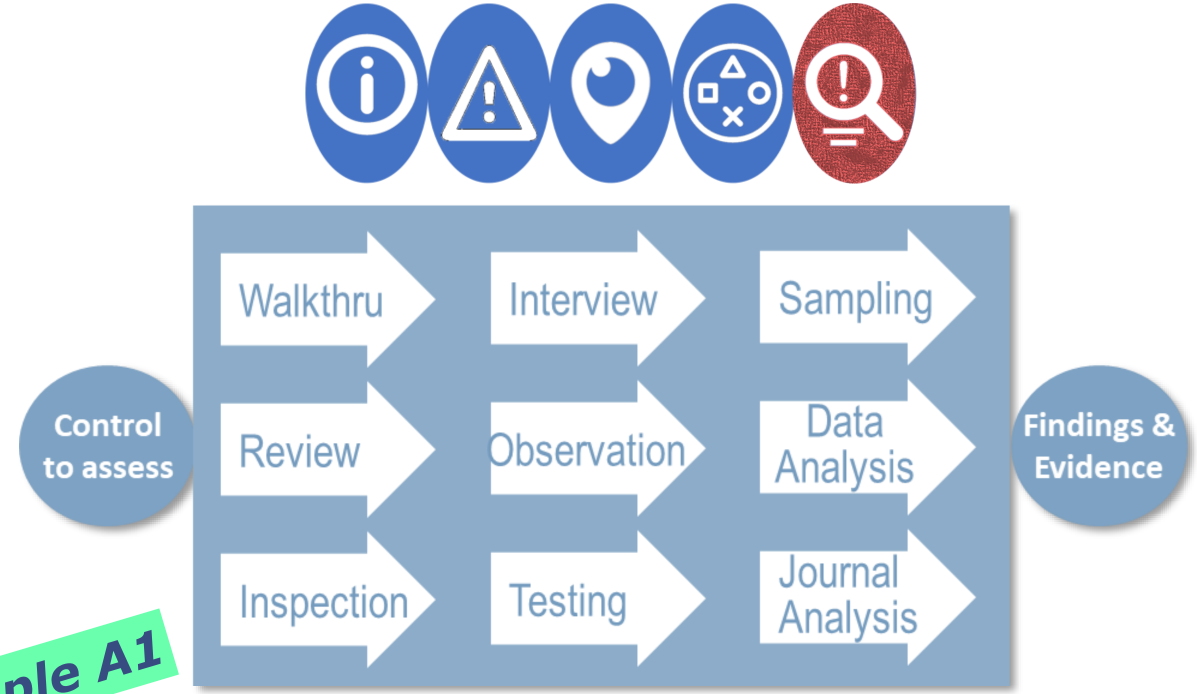
Domain A. Govern
Topic A1. Commitment of the Data controller

- Management communication
- Budget allocated to GDPR / DPOR
- Management meeting minutes
- DPO presentations @ executive mgt
- Annual DPO report to controller
- ….

Methodology – 5. Audit



Risk scenarios
Good practices
Control measures
Checkpoints
Audit techniques



Control to assess

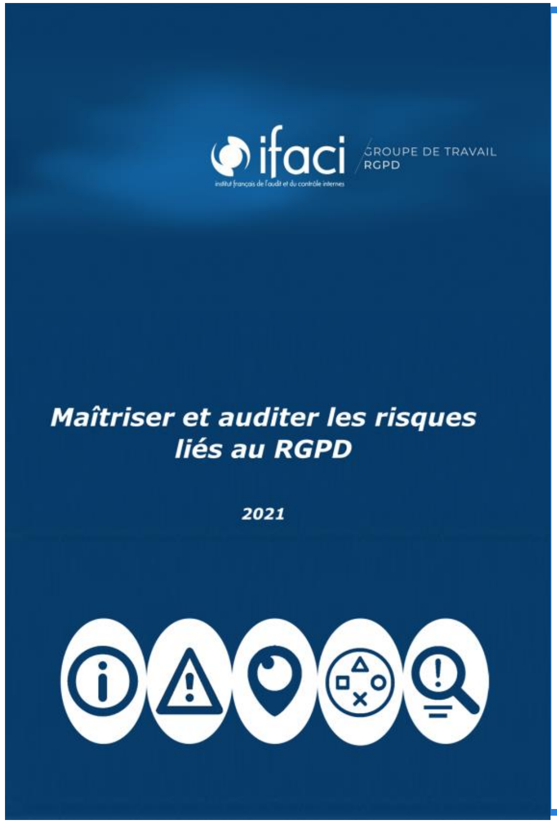
Walkthru
Interview
Sampling
Review
Observation
Data Analysis
Inspection
Testing
Journal Analysis

Findings & Evidence

Sample A1

- Interview : executive mgt, governance bodies…
- Review : privacy charter, policies…
- Assessment : budget, process practices
- Review : Executive mgt minutes, DPO report to mgt
- ….

Methodology - Tools



ifaci GROUPE DE TRAVAIL RGPD

Maîtriser et auditer les risques liés au RGPD

2021

Introduction

Methodological approach

GDPR Framework

Case study

Appendices

- ISO 27001
- ISO 27701
- Glossary
- References…

Available to IIA members on Workplace (French)

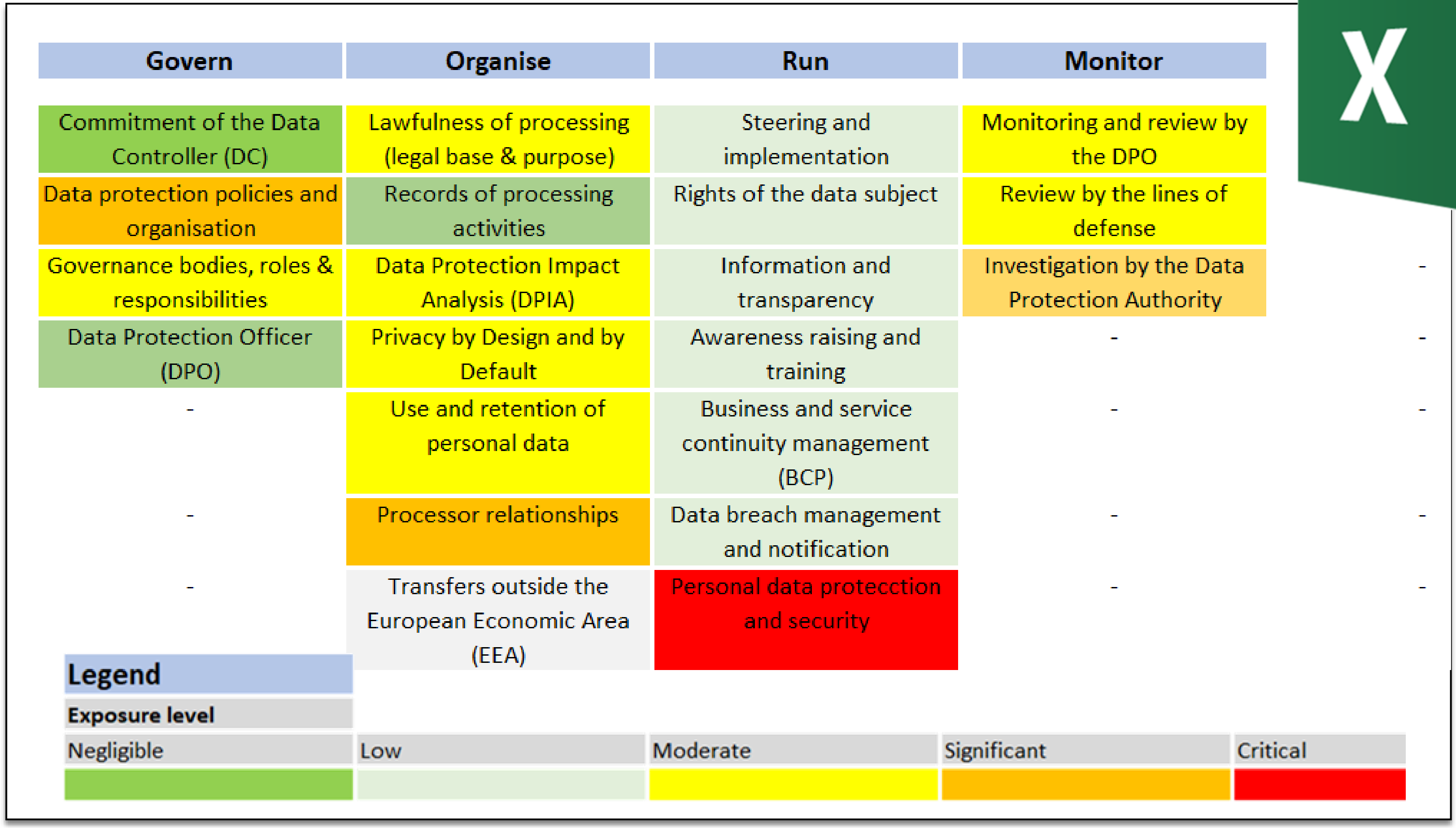
Excel Tool

- Risk identification
- Risk analysis
- Control measures
- Audit

Upcoming end 2021

Methodology - Tools

Sample chart : risk level per topic



Govern	Organise	Run	Monitor	
Commitment of the Data Controller (DC)	Lawfulness of processing (legal base & purpose)	Steering and implementation	Monitoring and review by the DPO	
Data protection policies and organisation	Records of processing activities	Rights of the data subject	Review by the lines of defense	
Governance bodies, roles & responsibilities	Data Protection Impact Analysis (DPIA)	Information and transparency	Investigation by the Data Protection Authority	-
Data Protection Officer (DPO)	Privacy by Design and by Default	Awareness raising and training	-	-
-	Use and retention of personal data	Business and service continuity management (BCP)	-	-
-	Processor relationships	Data breach management and notification	-	-
-	Transfers outside the European Economic Area (EEA)	Personal data protecction and security	-	-

Legend

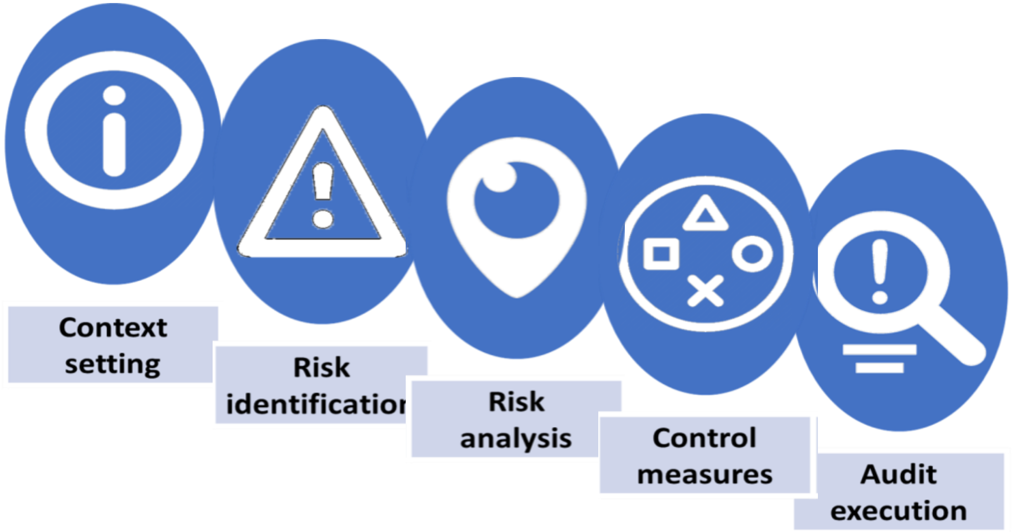
Exposure level

Negligible	Low	Moderate	Significant	Critical
🟩	⬜	🟨	🟧	🟥

Upcoming in 2022

- ISACA / DPO-pro **cooperation** for events / workshops
- **Training** " GDPR audit pro" by DP-Institute – 2 days – Spring 2022
  1. Presentation of the GDPR Framework
  2. Case study per phase

ASSIST+



  3. Application of GDPR by the Internal Audit

HOW TO AUDIT GDPR ?

Q&A