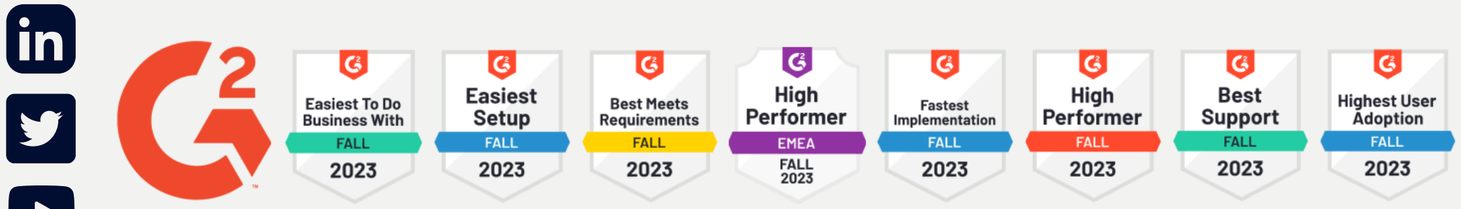
PRIVACYENGINE

10 Steps to a Compliant Privacy Program

Webinar Starting Shortly...

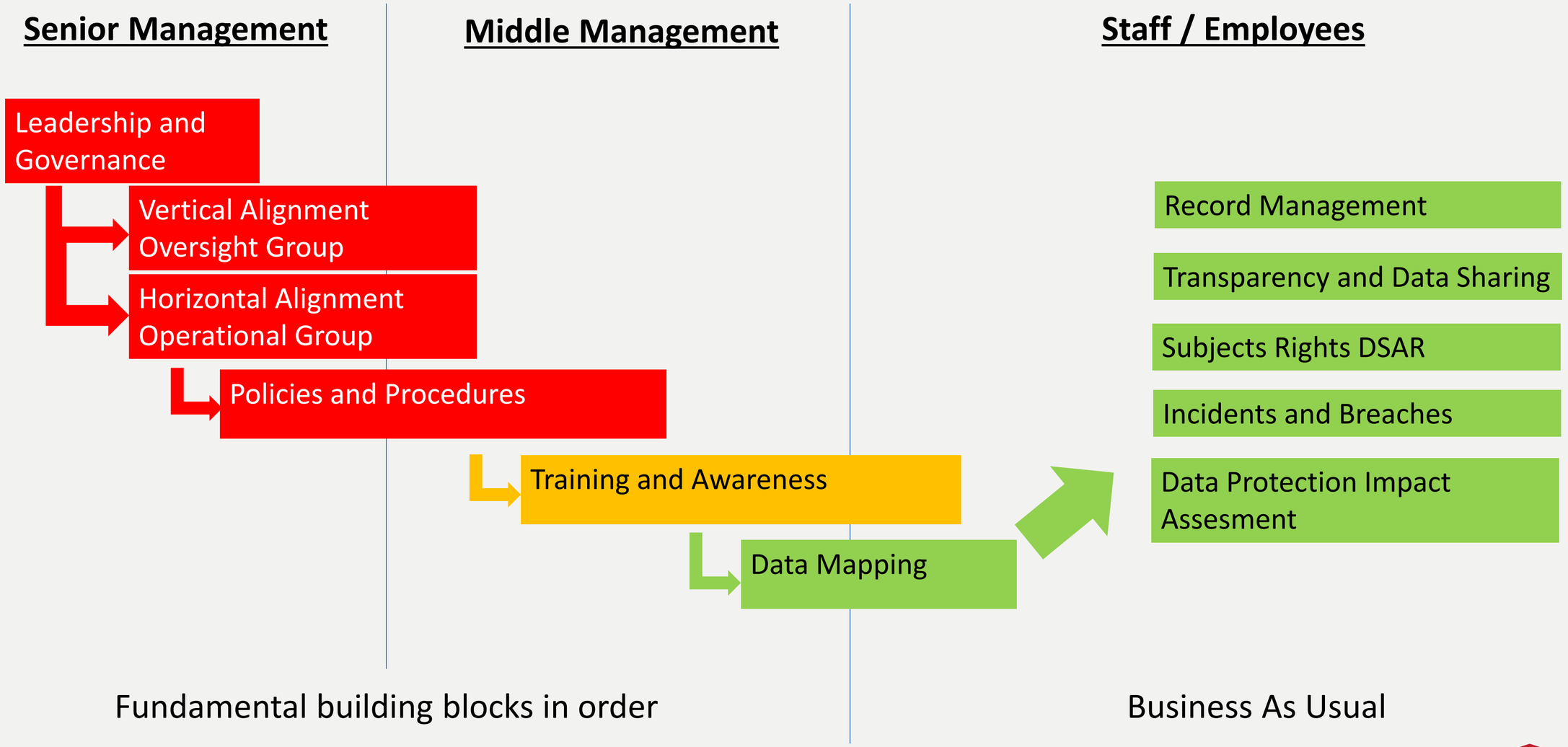
www.privacyengine.io



10 Steps to a Compliant Privacy Program

- Where to begin your privacy program journey
- The PrivacyEngine "Plan on a Page" - 10 steps to a complete program
- From the staff, via senior and mid management all the way to the board, how to implement rock solid compliance
- FAQ’s
- Creating your own privacy plan

Privacy Plan on a Page



PRIVACYENGINE

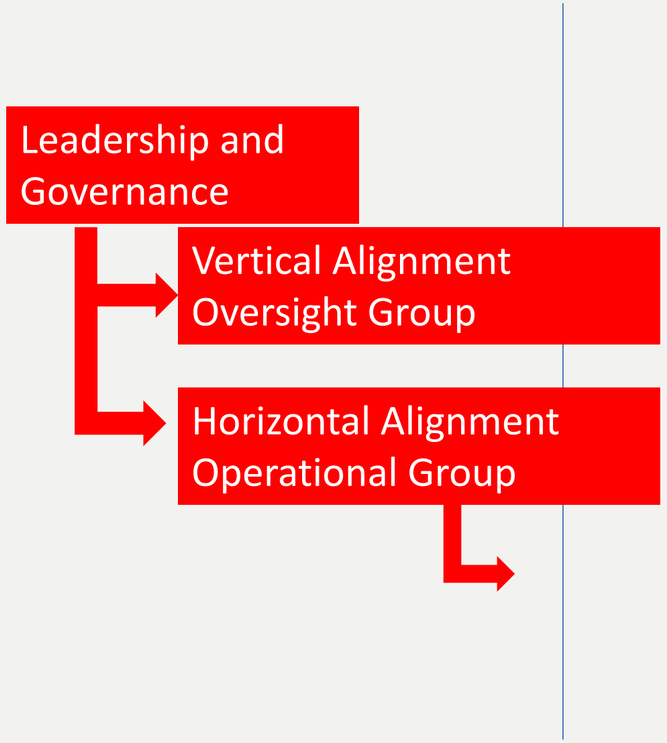
Alignment 33 KPIs	Policies & Procedures 17 KPIs	Training 21 KPIs	ROPA 33 KPIs	Individual Rights 42 KPIs	Transparency 31 KPIs	Contracts & data Sharing 31 KPIs	Risks & DPIAs 29 KPIs	Records Management 63 KPIs	Breach Response 39 KPIs
Organisational Structure	Direction and Support	Comprehensive Staff Training	Data Mapping	Informing individuals and identifying requests	Privacy Notice Content	Data Sharing Policies and Procedures	Identifying, Recording, and Managing Risks	Creating, Locating, and Retrieving Records	Detecting, Managing, and Recording Incidents and Breaches
Appointing a DPO	Review and Approval	Induction and Ongoing Education	Records of Processing Activities (ROPA)	Resources	Timely Privacy Information	Data Sharing Agreements	Data Protection by Design and by Default	Security for Transfers	Assessing and Reporting Breaches
Appropriate Reporting	Staff Awareness	Specialized Role Training	ROPA Requirements	Logging and tracking requests	Effective Privacy Information	Restricted Transfers	DPIA Policy and Procedures	Data Quality	Notifying Individuals
Operational Roles	Data Protection by Design and by Default	Monitoring and Verification of training	Good Practice for ROPAs	Timely Responses	Automated Decision-making and Profiling	Data Processors	DPIA Content	Retention Schedule	Reviewing and Monitoring
Oversight Groups		Proactive Awareness Building	Documenting Lawful Basis	Monitoring and Evaluating Performance	Staff Awareness	Processor Due Diligence Checks	DPIA Risk Mitigation and Review	Destruction	External Audit or Compliance Check
Operational Group Meetings			Lawful Basis Transparency	Inaccurate or Incomplete Information	Privacy Information Review	Processor Compliance Reviews		Information Asset Register	Internal Audit Programme
			Consent Requirements	Erasure	Tools Supporting Transparency and Control	Third Party Products and Services		Rules for Acceptable Software Use	Performance and Compliance Information
			Reviewing Consent	Restriction		Purpose Limitation		Access Control	Use of Management Information
			Risk-based Age Checks and Parental/Guardian Consent	Data Portability				Unauthorised Access	
			Legitimate Interest Assessment (LIA)	Rights Relating to Automated Decision-making and Profiling				Mobile Devices, Home or Remote Working, and Removable Media	
				Individual complaints				Secure Areas	
								Business Continuity, Disaster Recovery, and Back-ups	

Privacy Engine's 'Plan on a Page' is supported by **76 Goals/Initiatives** outlined above.

These are monitored, measured and reported utilising **339 metrics to assess Goals/Initiatives** under the 10 headings above.

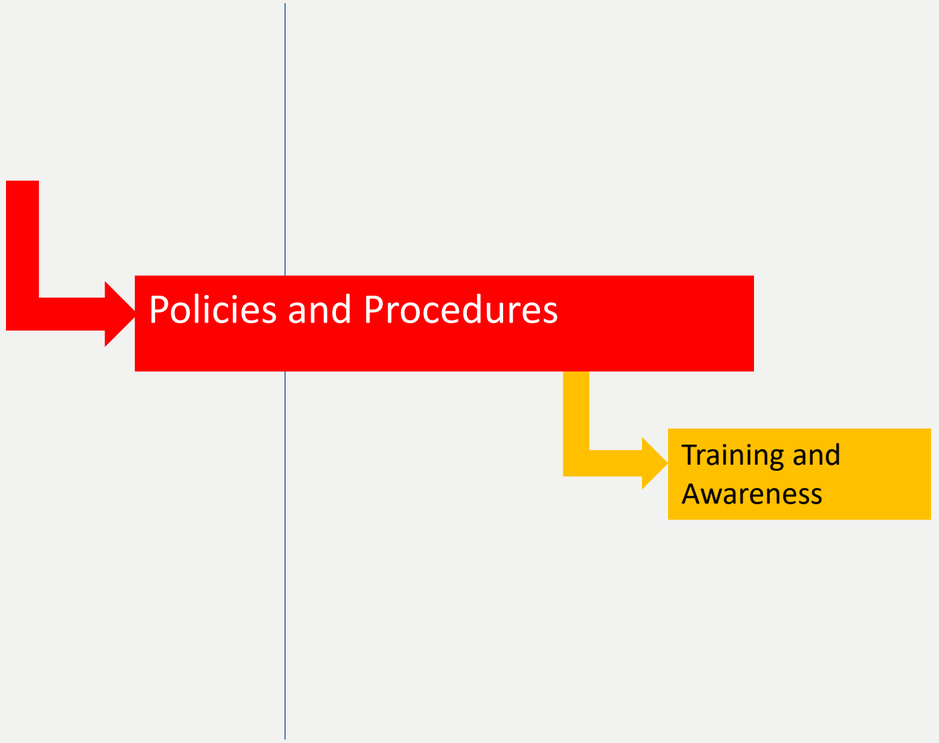
Alignment

- Leadership/Governance
  - Board Responsibility
    - EU/Irl : GDPR, NIS2, NCSC Baseline Standards
    - US : Rule 10 from Securities and Equities Commission (SEC)
    - A.I
- Organisational Group
  - SMTs, Oversight
  - Vertical Alignment
- Operational Group
  - DP Leads/Champions
  - Horizontal Alignment
  - Monthly reports and meeting



Policies and Procedures

- Direction and Support
- Review and Approval
  - Focus Groups
  - Policy must reflect factual evidence
- Data Protection by Design and Default



Policies

To be implementable it needs to:

- Clearly define the organisations commitment to the policy area (Board Approved)
- Have an implementation plan (Program Management)
- Be accompanied by policy instruments such as procedures, and clearly defined areas of responsibility

Must be situated in practice:

- Be based on consultation
- Have been tested at operational level
- Facilitate innovation
- Be routinely monitored and reviewed for effectiveness

Must be reflective of the Organisations priorities:

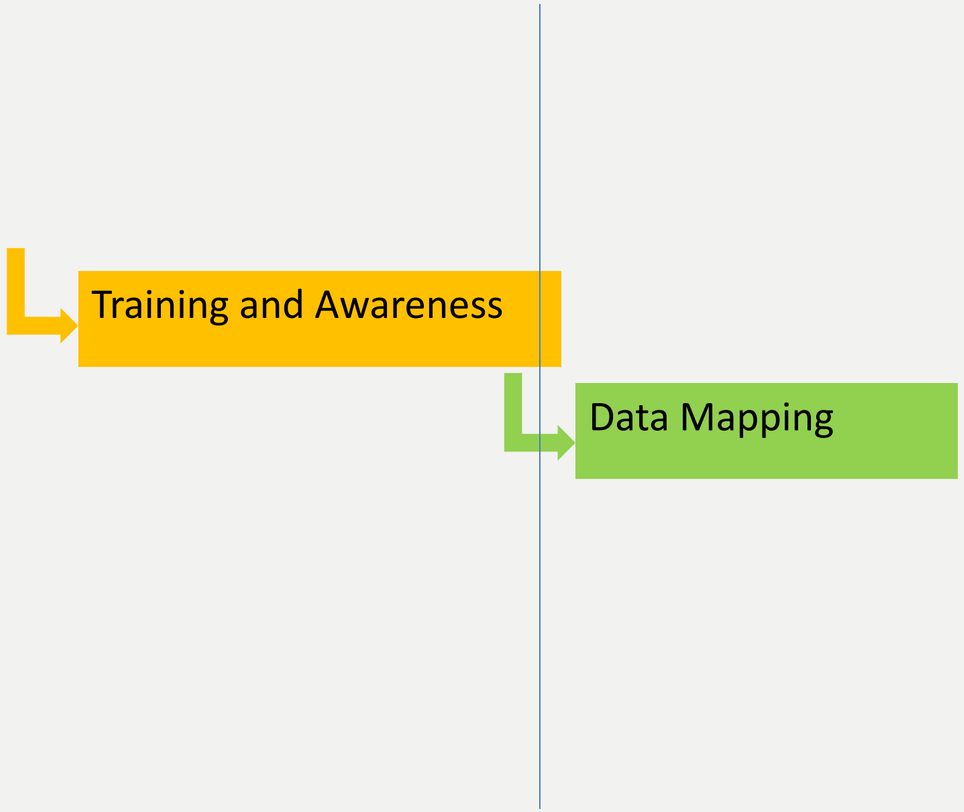
- Be guided by the Organisations vision and values (Awareness)
- Be in line with the Organisations strategic objectives (Business Goals)
- Allow the Organisation to meet its legal obligations (Strategic Risk)

Achieve compliance or assist your staff

Training and Awareness

- Know the difference
  - Training delivers skills
    - Internal/external
  - Awareness changes attitudes/culture
    - Top down

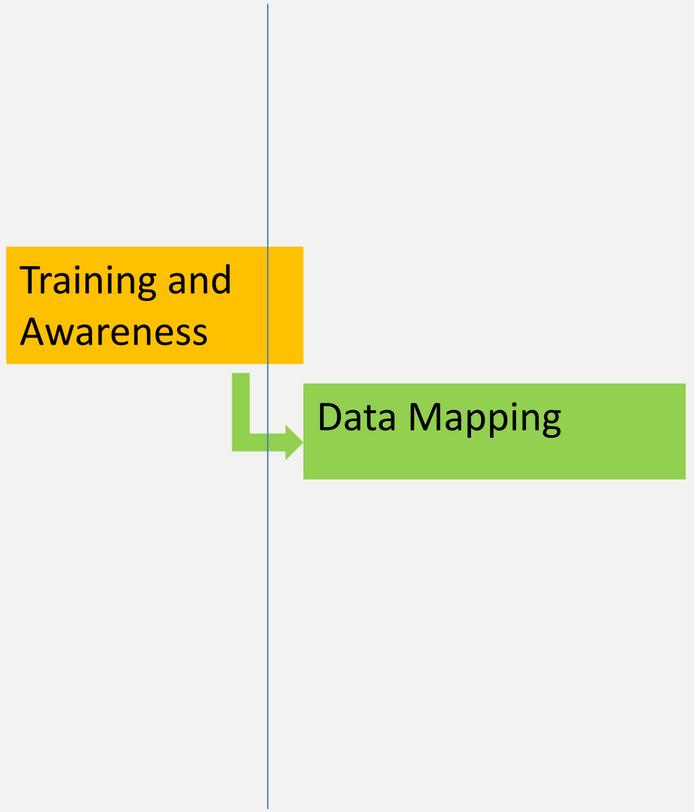
- Three required levels of training
  - Base line standard
  - Refresher/Incident lead
  - Risk based



Moving to Compliance

Data Mapping / R.O.P.A

- Organisational Support
- Operational execution
- Training and Awareness
- One-to-One interviews
- Process Owner or Information Asset Owner (IAO)
  - Role of the DPO
  - EDPB CEF on the Role of the DPO



Risk Based Approach

Where is Your Risk?

- Article 35 DPIA
  - Mitigate high level risk.
- Special Category
- Criminal Prosecutions
- Children
- ICO and EDPB lists

Examples of High-Level Risk

EDPB

1. Evaluation or Scoring
2. Automated-decision making with legal or similar significant effect
3. Systematic monitoring
4. Sensitive data or data of a highly personal nature
5. Data processed on a large scale
6. Matching or combining datasets
7. Data concerning vulnerable data subjects
8. Innovative use or applying new technological or organisational solutions
9. When the processing in itself “prevents data subjects from exercising a right or using a service or a contract”

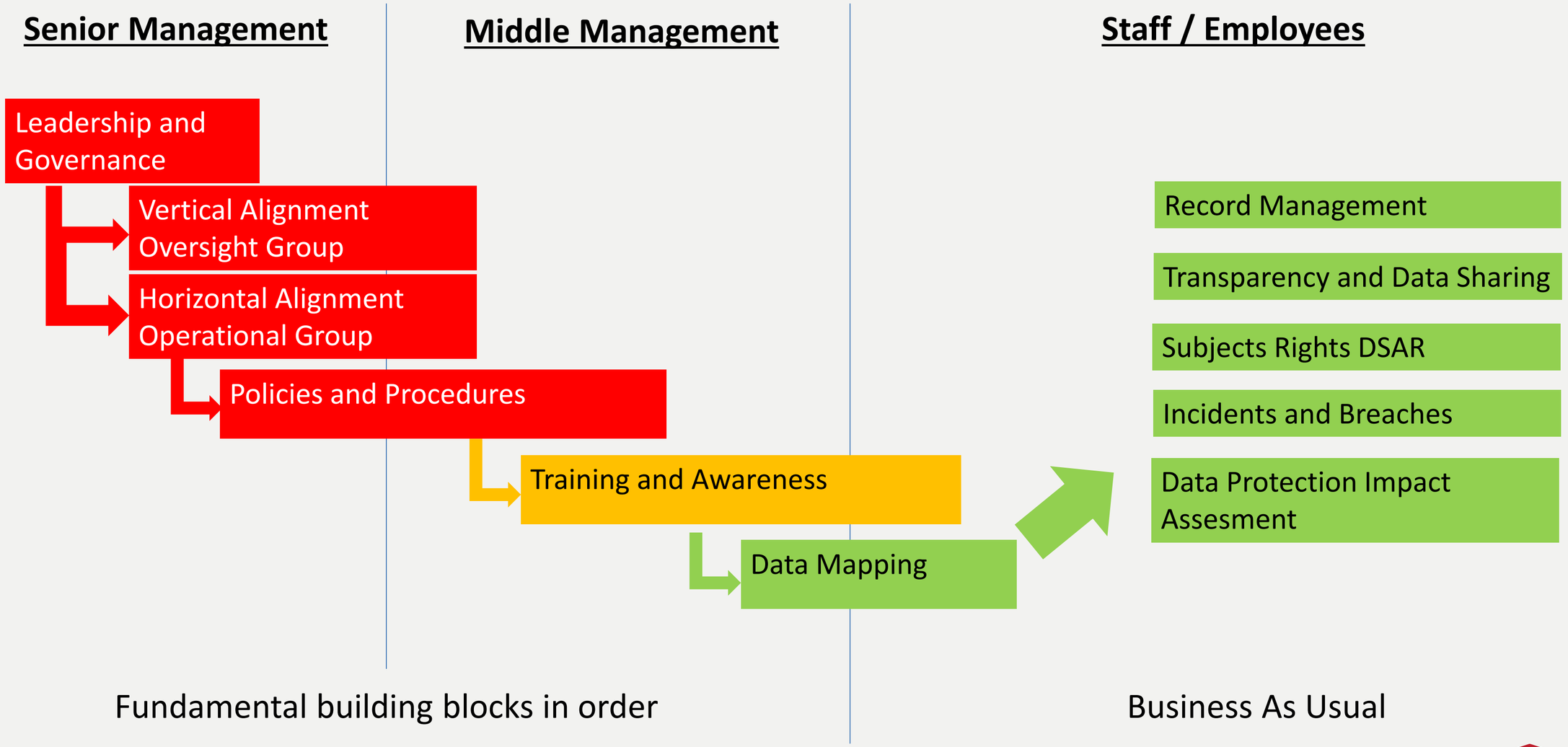
ICO

1. Innovative technology
2. Denial of service
3. Large-scale profiling
4. Biometrics
5. Genetic data
6. Data matching
7. Invisible processing
8. Tracking
9. Targeting of children or other vulnerable individuals
10. Risk of physical harm

Identifying your gaps?

- Third Parties
  - Due Diligence Questionnaire
  - Data Processing Agreement
- Lawful Basis
  - LIA
  - Defined Statutory, Regulatory, European or Member State Law
- Retention
  - Realistically defined

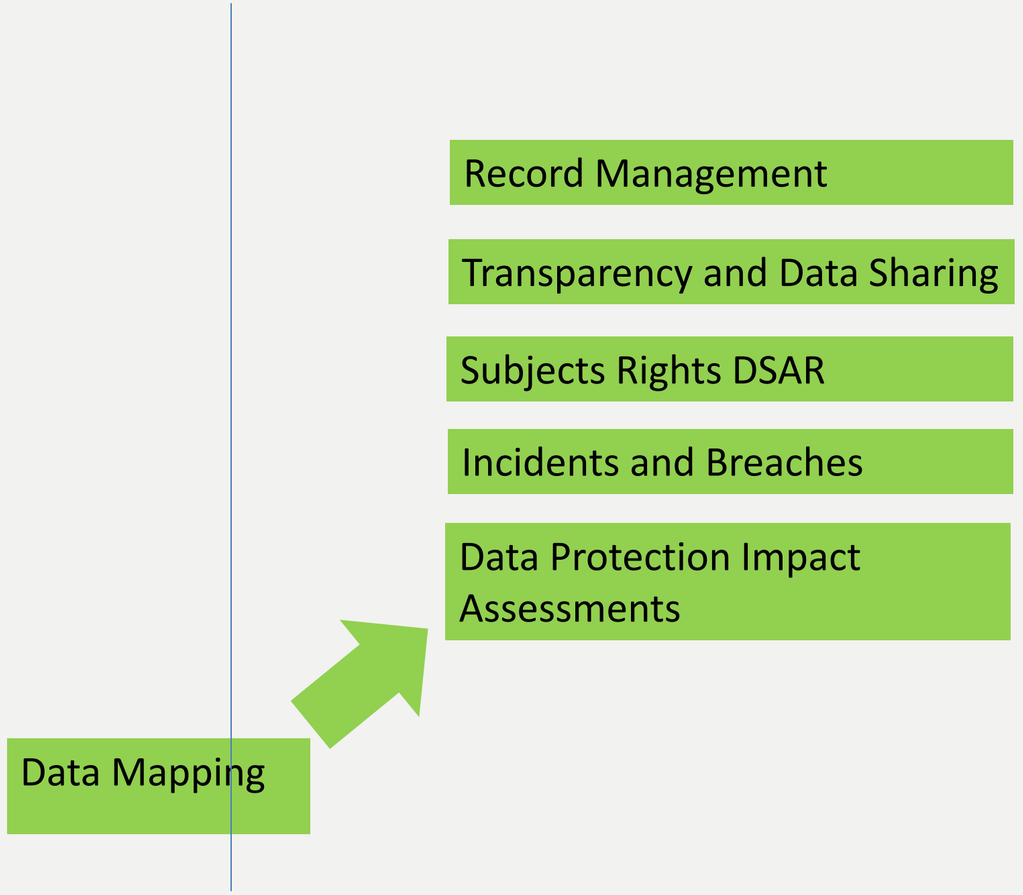
Privacy Plan on a Page



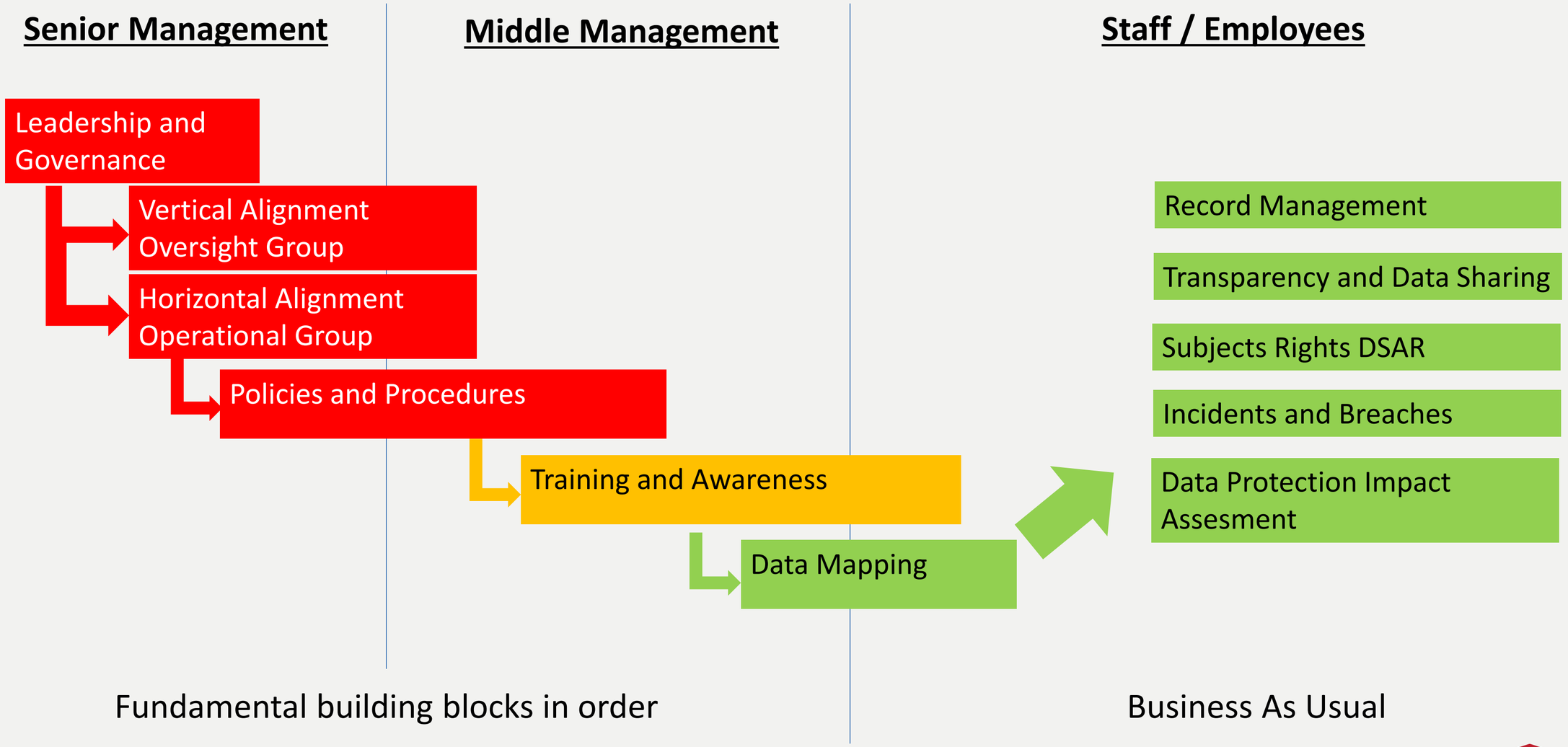
PRIVACYENGINE

Business as Usual (BAU)

- Records Management
- Transparency & Data Sharing
- Subject Rights
- Incidents and Breaches
- DPIAs



Privacy Plan on a Page



PRIVACYENGINE

Questions?

PRIVACYENGINE

Thank You!

Visit: https://www.privacyengine.io/services/
Email: nollag.conneely@privacyengine.io

Nollag Conneely
Head of Consulting
Consultancy | PrivacyEngine

www.privacyengine.io