DATA PRIVACY AND INFORMATION GOVERNANCE

Presented by
Rishi Maharaj
Executive Director
EquiGov Institute

EquiGov Institute

About EquiGov Institute

The EquiGov Institute Ltd (EGI) is a social enterprise incorporated in October 2018 and based in Trinidad, and Tobago. We develop practical solutions and create space for critical thinking, combining values-driven consultancy, training, research and learning across key themes such as information access, transparency, governance, data privacy, and monitoring and evaluation.

EquiGov Institute

Core Capabilities

Our consulting and training services focus on our clients' most critical issues and opportunities. We bring deep, functional expertise, capture value across boundaries and between the silos of any organization.

- **Data Privacy**
  - **Privacy Risk Assessment and Policy Development**
  - **Global Privacy Regulation Compliance**
  - **Privacy Office Consulting**

- **Governance**
  - **Access to Information**
  - **Public Procurement and Transparency**
  - **Whistleblowing**

- **Monitoring and Evaluation**
  - **Evaluation and Research**
  - **Monitoring Support**
  - **Capacity Building**

EquiGov Institute

Strategic Partners

FUTURE LAW
ENGINEERING A BETTER WORLD

pill
PROCUREMENT
INNOVATION
& LEADERSHIP LAB

Cloud Carib

PINAKA
CONSULTING LTD

Microsoft

EquiGov Institute

"It takes 20 years to build a reputation and five minutes to ruin it." --

—Warren Buffett

EquiGov Institute

Digital Economy and Data

Data &
Digital Economy

Data is the new Oil. Data is just like crude. It's valuable, but if unrefined it cannot really be used.

– Clive Humby,

We have for the first time an economy based on a key resource [Information] that is not only renewable, but self-generating. Running out of it is not a problem, but drowning in it is.

– John Naisbitt

EquiGov Institute

Data is exploding across the digital estate

EquiGov Institute

Personal Information captured by Data

Our personal digital footprint, an ineradicable record of every electronic interaction, just keeps increasing. Your email traffic, internet search history, geotagged images on our smartphone and social media sites, retail purchases, loyalty program transactions, invoice payments, toll road payments and medical records all add to the unique tread that makes up the footprint.

People's day-to-day movements are often so predictable that even anonymised location data can be linked back to identified individuals with relative ease when it is correlated with other outside information. Apparently our movement patterns are so repetitive and predictable that as few as 4 data points that include date and time are enough to identify an individual.

EquiGov Institute

Data Protection Laws

Let’s Dispel Some Myths

EquiGov Institute

Privacy ≠ Secrecy

Privacy is *not* about having something to hide

EquiGov Institute

Privacy = Control

EquiGov Institute

What is Data/Privacy Protection

- **Data protection is about safeguarding our fundamental right to privacy, which is enshrined in international and regional laws and conventions.**

- **Data protection is commonly defined as the law designed to protect your personal information, which is collected, processed and stored by "automated" means or intended to be part of a filing system**

EquiGov Institute

General Views on Privacy

- General belief: privacy is a fundamental human right that has become one of the most important rights of the modern age

EquiGov Institute

My Definition of Data Protection

We have a right to protection from UNREASONABLE INTRUSION into areas of affairs for which no explicit consent was given or for which we have a REASONABLE EXPECTATION OF PRIVACY

EquiGov Institute

GENERAL DATA PROTECTION REGULATION

What is GDPR

- **A new and updated EU wide legal framework focusing on personal data privacy which became effective on May 25th, 2018.**

- **The main goals of GDPR aims primarily to give control to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.**

EquiGov Institute

EquiGov Institute

Rights enshrined under GDPR

Know Your (Customers') Rights: 8 Ways GDPR Expands EU Privacy Rights

The Right to Be Informed
Individuals have a right to know who is processing their personal data

The Right to Access
Individuals have the right to access any personal data that has been collected about them

The Right to Rectifications
Individuals have the right to require organizations to correct inaccurate personal data

The Right to Be Forgotten
Individuals have the right to have their personal data deleted and to prevent further collection

The Right to Restrict Processing
Individuals have the right to require organizations to restrict the processing of specific categories of personal data

The Right to Data Portability
Individuals have the right to require organizations to transfer personal data to a recipient of their choice

The Right to Object
Individuals have the right to consent, or withdraw consent, to the processing of their personal data

Rights in Relation to Automated Decision Making and Profiling
Individuals have the right to opt out of the use of their personal data by automated systems, such as artificial intelligence

GDPR Global Reach

- **Data processors located outside the EU that handle the personal information of EU residents will have to abide by it.**

- **The broad territorial scope of the GDPR is enshrined in Article 3. Under Article 3, the GDPR applies to the processing of personal data of EU data subjects.**

- **Additionally as part of its international trading deals, which would also incorporate data flows, any country wanting to sign a trade deal with the EU will have to sign up to respecting GDPR and also have implemented within its jurisdiction similar legislative provisions.**

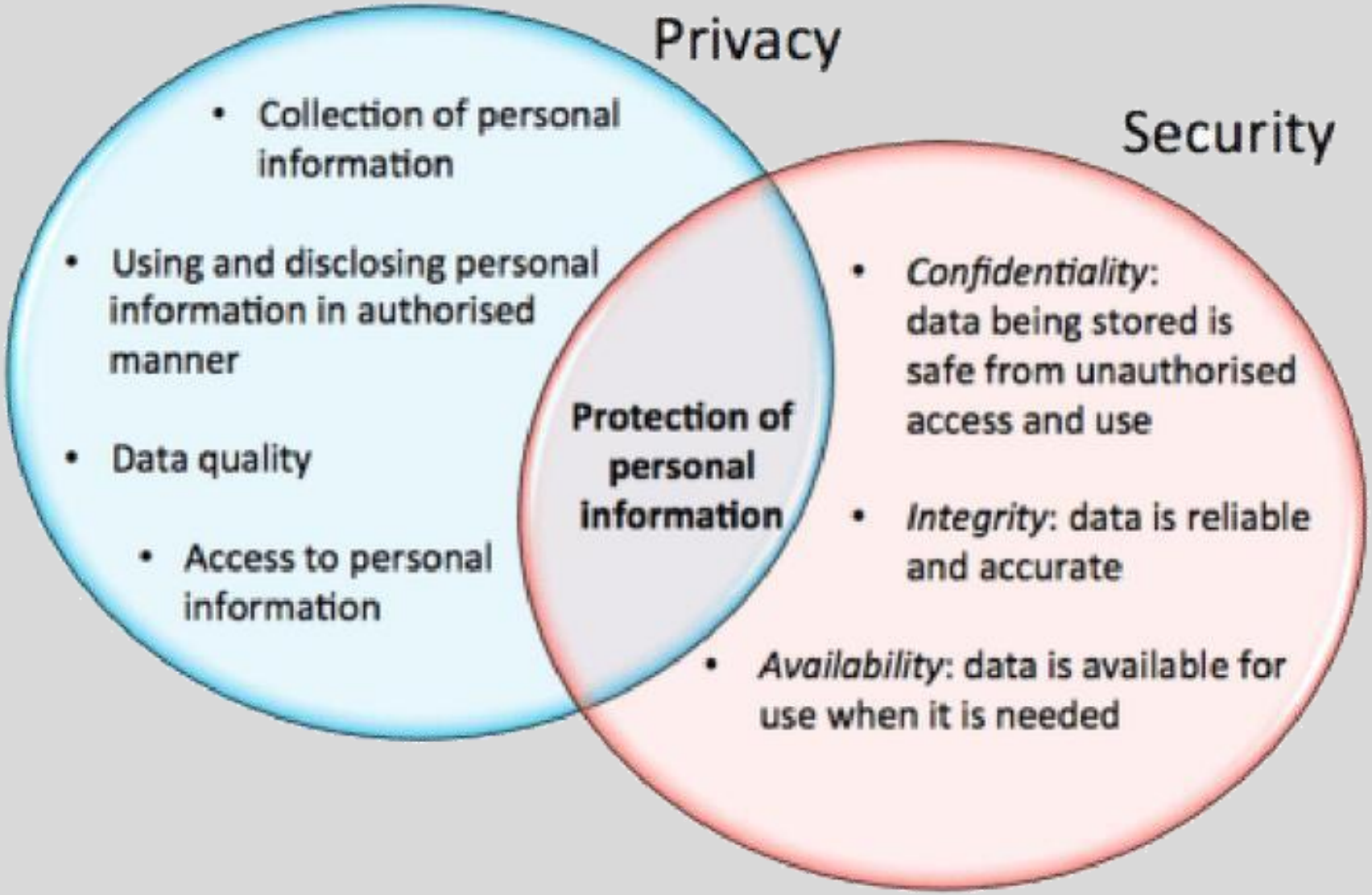
A RISK BASED APPROACH TO DATA PROTECTION

PRIVACY RISK

"Risk Management should be enterprise wide and engrained into the business culture of the organization".
Julie Dickerson

EquiGov Institute

EquiGov Institute



A RISK-BASED APPROACH IS KEY

- Most data protection laws are all about safeguarding the information your company collects, creates, uses and shares, whether it's collected from your employees, customers or third-party vendors.
- Because this information originates from so many different systems and locations, you must take a risk-based approach to data protection to best assess and mitigate your company's top risks.

EquiGov Institute

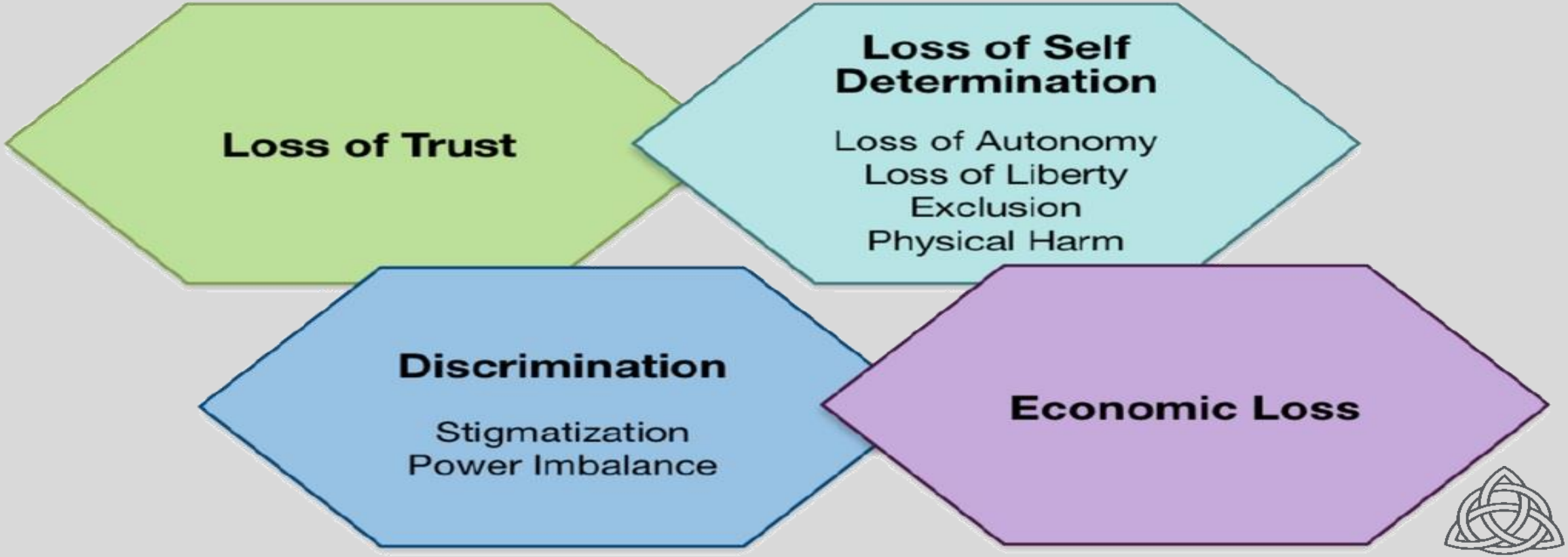
PRIVACY RISK

- Privacy risk is defined as the "potential loss of control over personal information".

- These Risks are a function of:
  - The **Threat** of an occurrence of adverse event; and
  - The **Vulnerability** to attack

EquiGov Institute

Processing Personal Information Can Create Problems for Individuals



EquiGov Institute

RISK AND WHAT IT MEANS FOR DATA PRIVACY

RISKS TO INDIVIDUALS

the potential for

***damage** or*

distress

RISKS TO ORGANISATIONS

financial and/or reputational

impact of a data breach.

EquiGov Institute

RISK THREATS, VULNERABILITIES AND IMPACT

THREAT

Threat is anything that can exploit vulnerability, intentionally or accidentally, and obtain, damage, or destroy an asset.

VULNERABILITY

Vulnerability refers to the inability (of a system or a unit) to withstand the effects of a hostile environment.

IMPACT OF THE RISK

Risk impact is the consequence of risk events if they are realized.

EquiGov Institute

Risk = Threats x Vulnerabilities

Risk

- business disruption
- financial losses
- loss of privacy
- damage to reputation
- loss of confidence
- legal penalties
- impaired growth
- loss of life

=

Threats

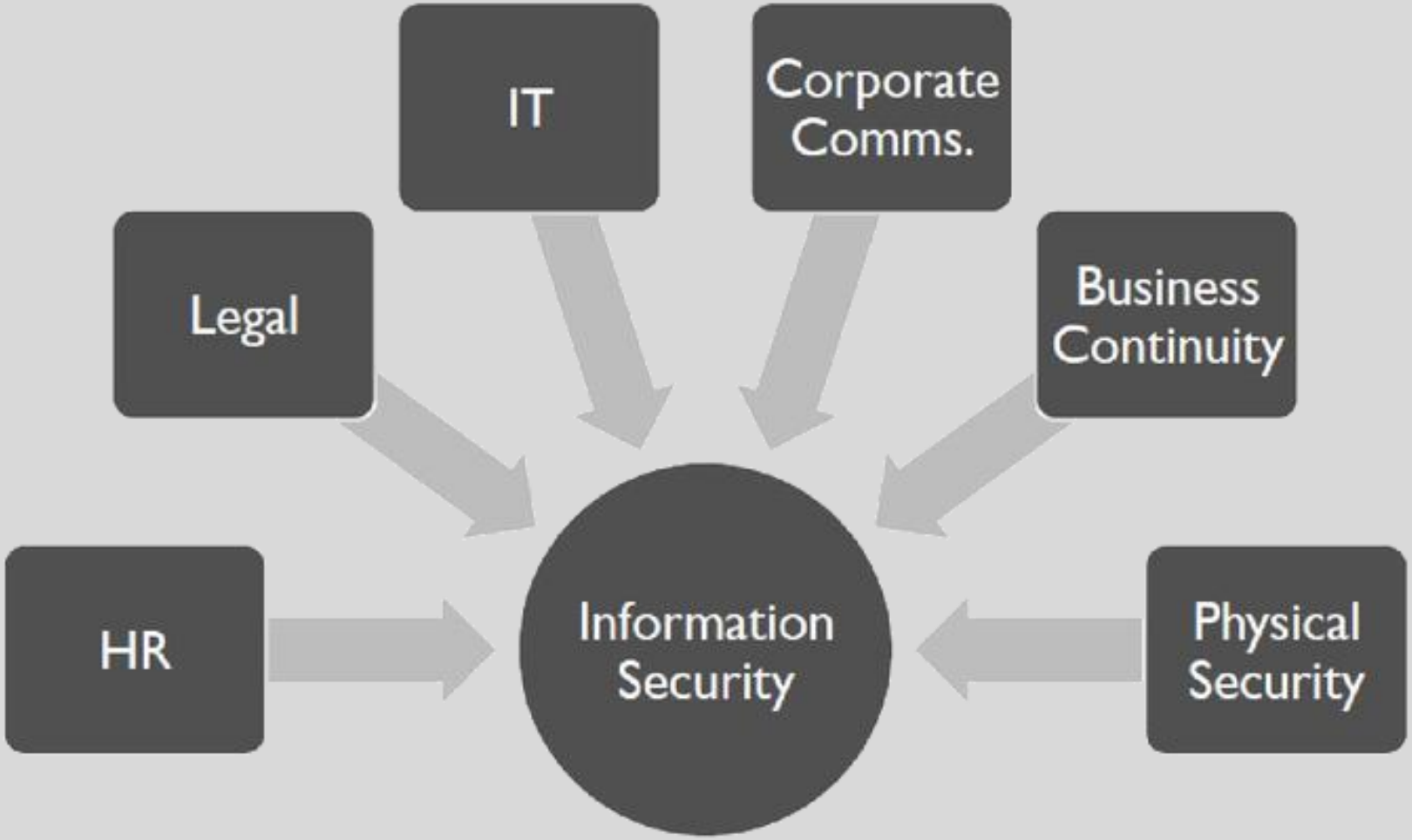
- angry employees
- dishonest employees
- criminals
- governments
- terrorists
- the press
- competitors
- hackers
- nature

X

Vulnerabilities

- software bugs
- broken processes
- ineffective controls
- hardware flaws
- business change
- legacy systems
- Inadequate BCP
- human error

Information Security Risks, Threats and Vulnerabilities



EquiGov Institute

PRIVACY IMPACT ASSESSMENT

EquiGov Institute

1

WHAT IS A PRIVACY IMPACT ASSESSMENT

3

UNDERTAKE A PRIVACY IMPACT ASSESSMENT

2

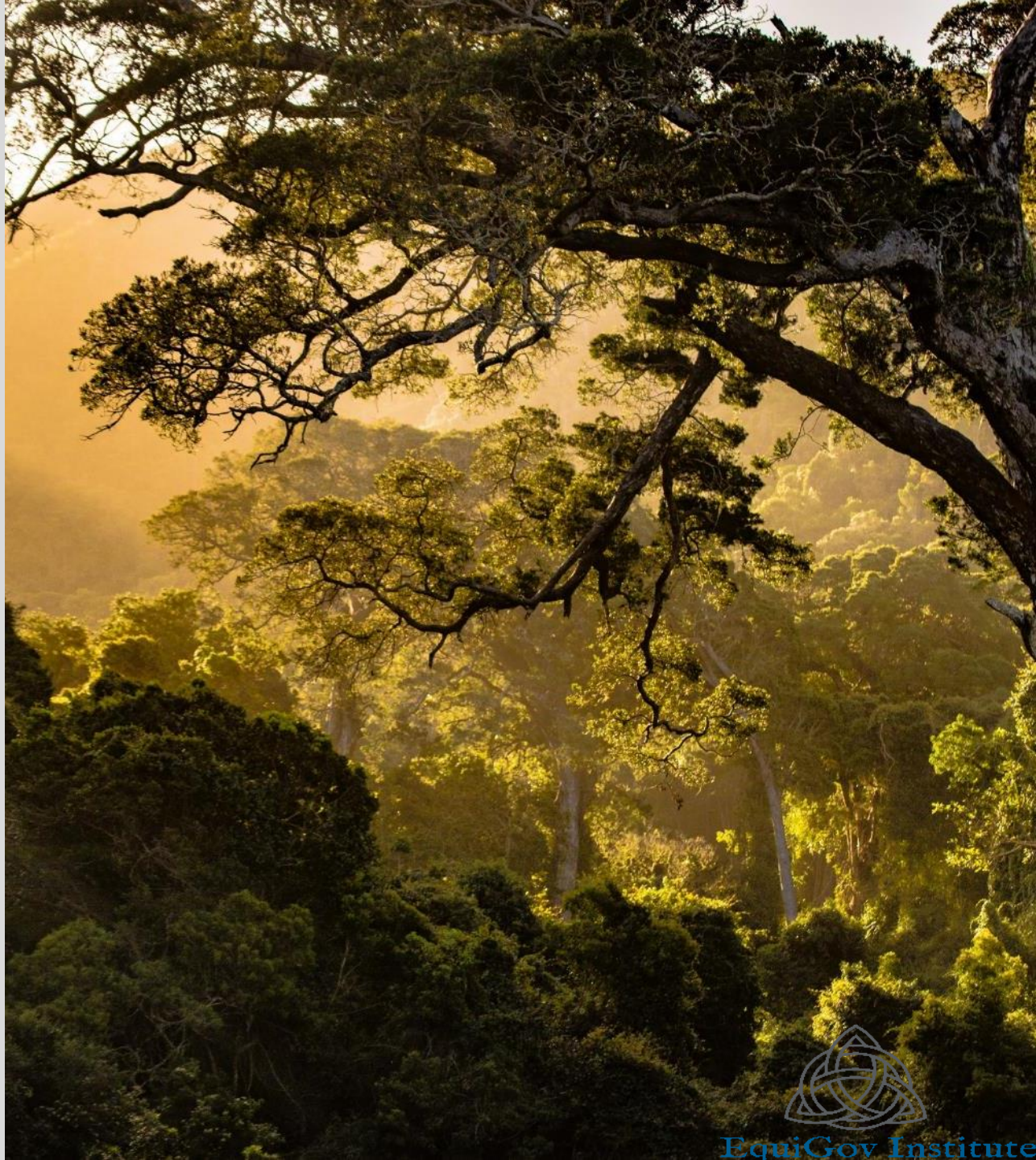
IS IT NECESSARY

EquiGov Institute

WHAT IS A PIA

- A privacy impact assessment is a systematic assessment of a project that identifies the impact that the project might have on the privacy of individuals, and sets out recommendations for managing, minimising or eliminating that impact.

- PIAs are an important component in the protection of privacy, and should be part of the overall risk management and planning processes of APP entities.



WHAT A PIA CAN ACHIEVE

- A PIA can identify problems and opportunities early and make it easier and cheaper to address them. It's much simpler to build in good privacy management throughout the process, rather than trying to bolt it on at the end.
- It will not be possible to identify and eliminate every risk, or identify every opportunity, and a PIA does not aim to do so. However, it gives you a good chance of identifying the most serious and the most likely problems.

EquiGov Institute

IS A PIA NECESSARY?

- Non-compliance with the letter or the spirit of relevant privacy laws, potentially leading to a privacy breach and/or negative publicity;
- Loss of credibility through lack of transparency in response to public concern about handling personal information;
- Damage to reputation;
- identification of privacy risks at a late stage resulting in unnecessary costs or inadequate solutions.

EquiGov Institute

PROJECTS THAT MAY BENEFIT FROM A PIA?

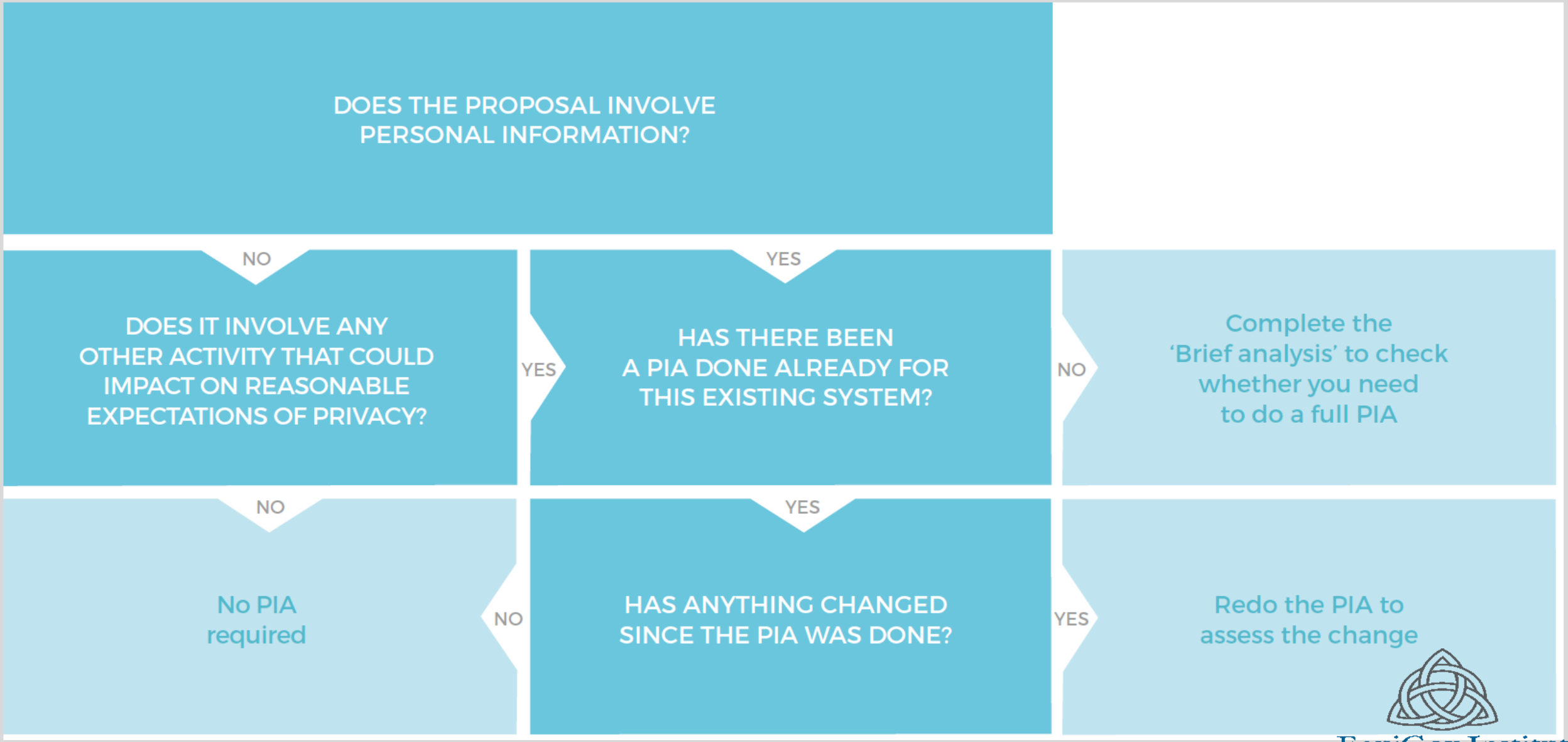
- involves personal information – that is, information about identifiable individuals,
- involves information that may be used to identify or target individuals
- may result in surveillance of individuals, or intrusions into their personal space or bodily privacy
- may otherwise affect whether people's reasonable expectations of privacy are met.

EquiGov Institute

Can you think of any projects within your own organization that can benefit from a PIA?

EquiGov Institute

Flowchart: An initial filter



EquiGov Institute

THE PIA PROCESS

01 Identify need for a PIA

02 Describe information flows

03 Identify privacy risks

04 Identify privacy solutions

05 Identify privacy solutions

06 Integrate PIA outcomes into project plan

EquiGov Institute

Privacy by Design

EquiGov Institute

Positive-Sum Model: *The Power of "And"*

Change the paradigm
from a zero-sum to
a "positive-sum" model:
Create a win-win scenario,
not an either/or (vs.)
involving unnecessary trade-offs
and false dichotomies …

replace "vs." with "and"

EquiGov Institute

Privacy by Design:
The 7 Foundational Principles

1. ***Proactive*** not ***Reactive: Preventative***, not Remedial;
2. Privacy as the ***Default*** setting;
3. Privacy ***Embedded*** into Design;
4. ***Full*** Functionality: Positive-Sum, not Zero-Sum;
5. End-to-End **Security: Full** Lifecycle Protection;
6. Visibility **and** Transparency: Keep it **Open**;
7. Respect for User Privacy: Keep it **User-Centric**.

PbD

www.privacybydesign.ca

Privacy by Design

The 7 Foundational Principles

Ann Cavoukian, Ph.D.
Information & Privacy Commissioner
Ontario, Canada

Privacy by Design is a concept I developed back in the 90's, to address the ever-growing and systemic effects of Information and Communication Technologies, and of large-scale networked data systems.

Privacy by Design advances the view that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must ideally become an organization's default mode of operation.

Initially, deploying Privacy-Enhancing Technologies (PETs) was seen as the solution. Today, we realize that a more substantial approach is required — extending the use of PETs to PETS *Plus* — taking a positive-sum (full functionality) approach, not zero-sum. That's the "*Plus*" in PETS *Plus*: positive-sum, not the either/or of zero-sum (a false dichotomy).

Privacy by Design extends to a "Trilogy" of encompassing applications: 1) IT systems; 2) accountable business practices; and 3) physical design and networked infrastructure.

Principles of *Privacy by Design* may be applied to all types of personal information, but should be applied with special vigour to sensitive data such as medical information and financial data. The strength of privacy measures tends to be commensurate with the sensitivity of the data.

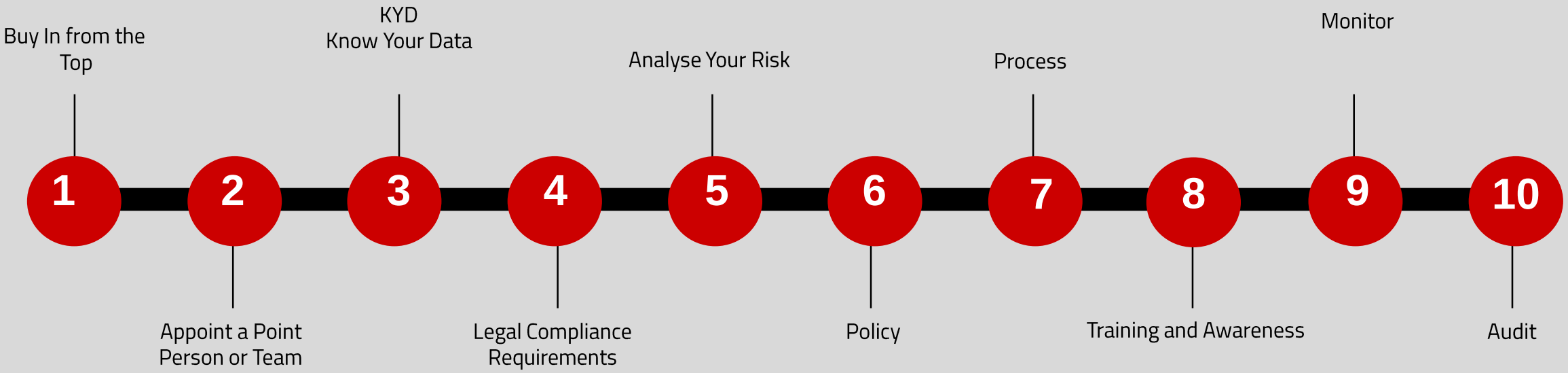
The objectives of *Privacy by Design* — ensuring privacy and gaining personal control over one's information and, for organizations, gaining a sustainable competitive advantage — may be accomplished by practicing the following 7 Foundational Principles *(see over page)*:

www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf

EquiGov Institute

WHAT STEPS CAN YOUR ORGANISATION TAKE

Ten Steps to Designing, Building and Sustaining a Data Protection Management Programme



EquiGov Institute

Step One

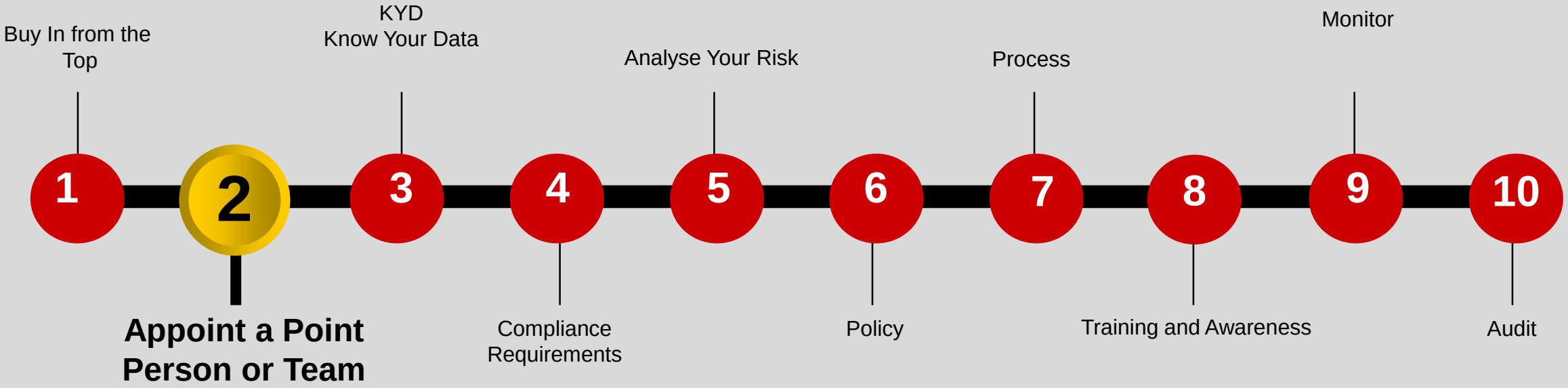
EquiGov Institute

Buy in From the Top

Top management should:

- ✓ **convey to all staff of their support to cultivate a personal data privacy respectful culture and commitment to the implementation of PMP through staff meetings or internal circulars;**
- ✓ **appoint a Point Privacy Officer;**
- ✓ **endorse the programme controls and the whole PMP;**
- ✓ **allocate adequate resources (including finance and manpower) to implement PMP;**
- ✓ **actively participate in the assessment and review of PMP;**
- ✓ **report to the Board on the programme regularly.**

Step Two



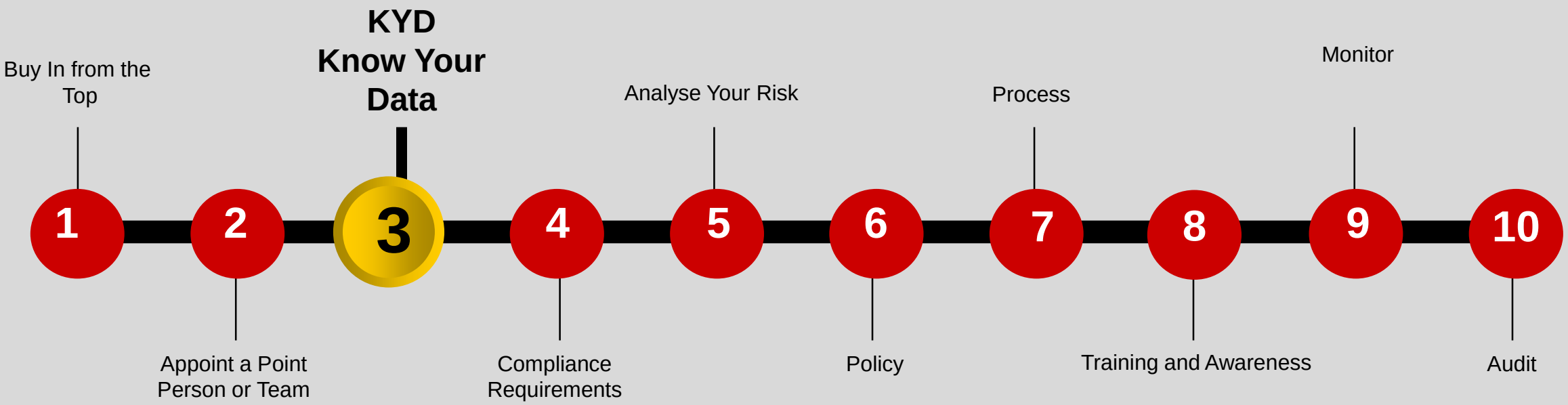
EquiGov Institute

Appoint a Point Person or Team

- Depending on your organization's size, or on the sort of data it collects/stores, some regulations will require a formal DPO, but even if this is not mandatory, doing so will make creating a solid Data Privacy Strategy much easier.

- On more practical terms, having a person in charge of your Data Privacy Efforts will make sure the next steps (creating a data inventory, mapping requirements, analysing risks, creating both policies and procedures, monitoring compliance) are adequately executed.

Step Three



EquiGov Institute

Know Your Data

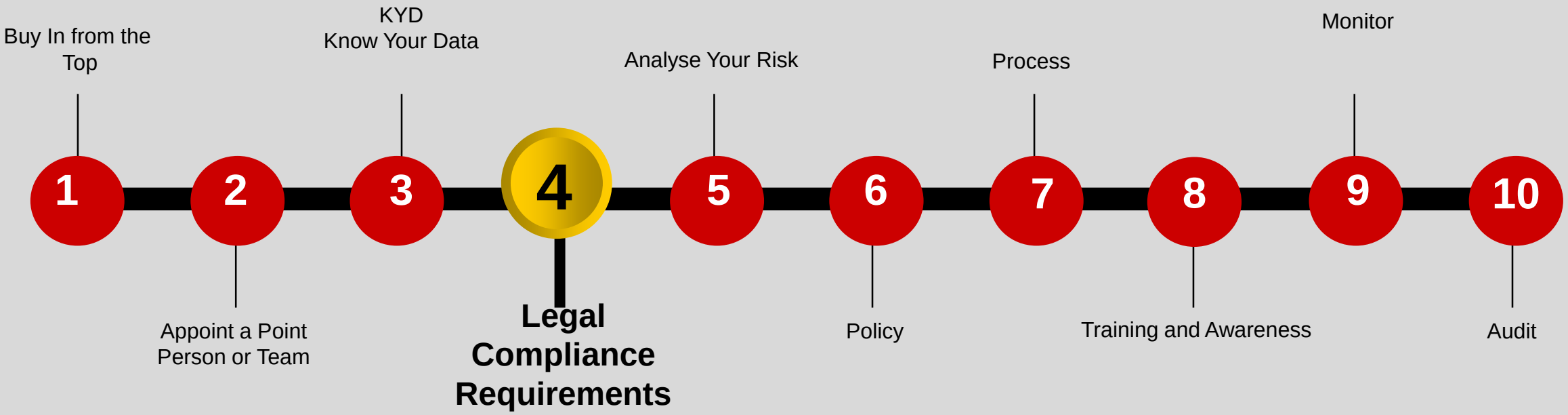
- It is not possible to protect that which you do not know.
- Once you have the approval for your new Data Privacy Strategy, someone (or even a whole team) should be assigned the task of creating a data inventory.
- This should include every piece of information stored or processed by your company, both electronically and/or hard copies.
- The idea is understanding what sort of data is collected, where and how it is stored, what is it used for, if it is shared with another organization or group, and how long is it kept before being disposed.

Know Your Data 5 W's

- ✓ WHY … is personal data processed?
- ✓ WHOSE … personal data is processed?
- ✓ WHAT … personal data is processed?
- ✓ WHEN … is personal data processed?
- ✓ WHERE … is personal data processed?

EquiGov Institute

Step Four



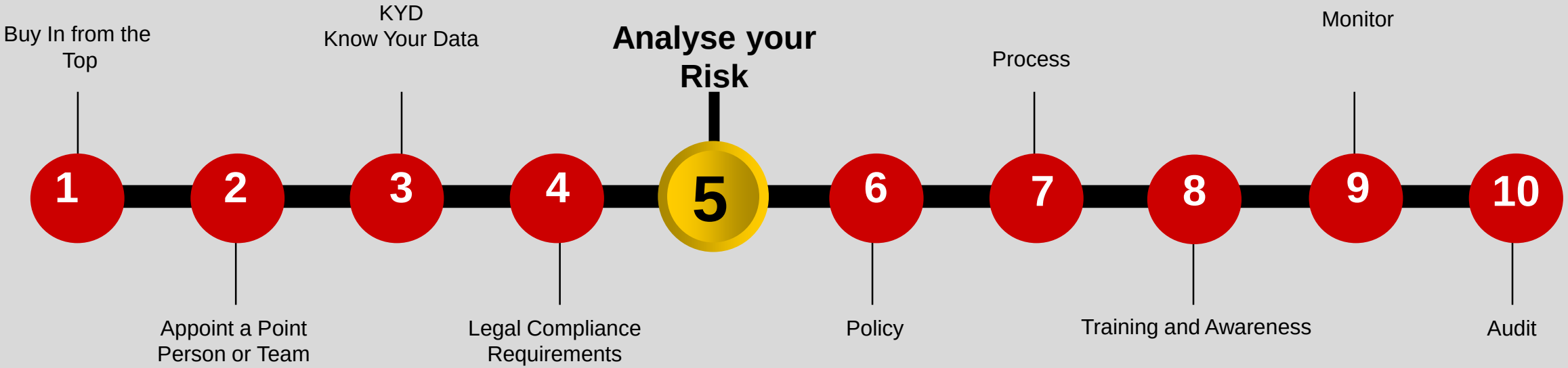
EquiGov Institute

Legal Compliance Requirements

Now that you know your data, it is time to understand its privacy requirements. Requirements will be dependent on what sort of data your company is storing/processing and your line of business. For example, since May 2018, the General Data Protection Regulation (GDPR) is mandatory for any organization (including the ones located outside of the EU) that offer goods or services to, or monitor the behavior of, EU data subjects.

EquiGov Institute

Step Five



EquiGov Institute

Analyse your Risk

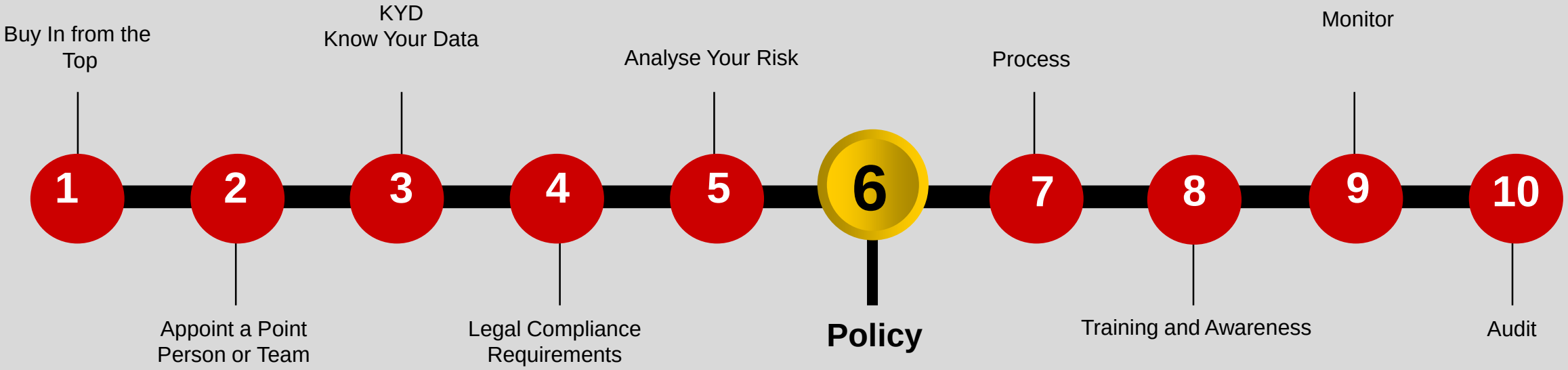
- A risk-based approach is your safest bet for making sure every data privacy vulnerability, threat source, and their joint impact is properly understood so it can be adequately treated.

- Privacy risk is defined as the “potential loss of control over personal information

- Impact assessment is an important part of any PMP to ensure that the privacy policies and practices of organisations are and remain compliant with respective laws.

EquiGov Institute

Step Six



EquiGov Institute

Policy

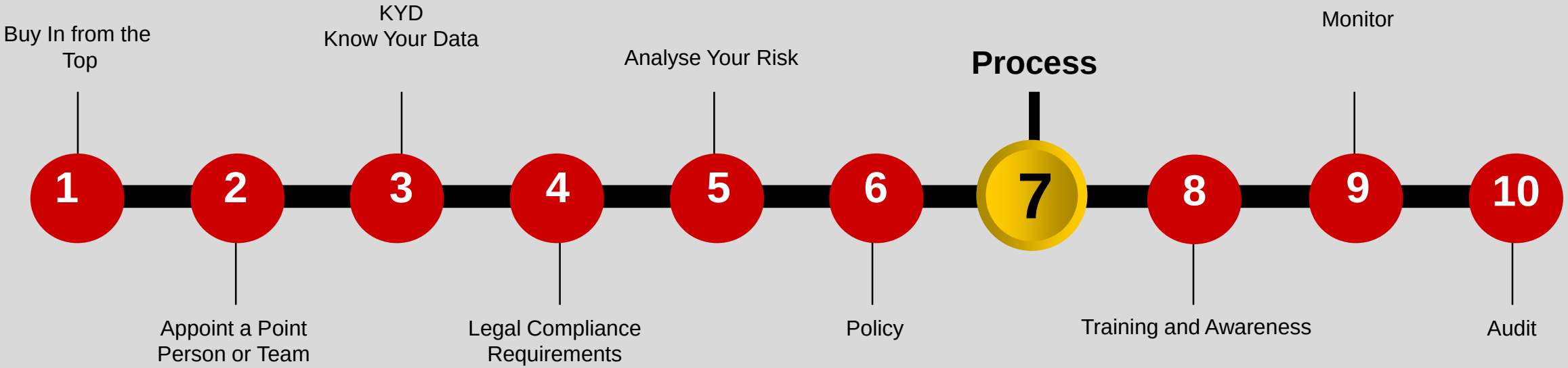
- The principles in a personal data protection policy sets the tone and provides guidance for the organisation's treatment of personal data.

- Organisations should develop and communicate a personal data protection policy for both its internal stakeholders (e.g. staff) and external parties (e.g. customers). This will provide clarity to internal stakeholders on the responsibilities and processes on handling personal data in their day-to-day work.

- Policies also demonstrate accountability to external parties by informing them on the ways in which the organisation handles personal data.

EquiGov Institute

Step Seven



EquiGov Institute

Process

- Process will help with any day-to-day tasks.

- Some common procedures such as the necessary steps for customer consent, retention of records, secure data disposal, international data transfer, and complaints, amongst others.

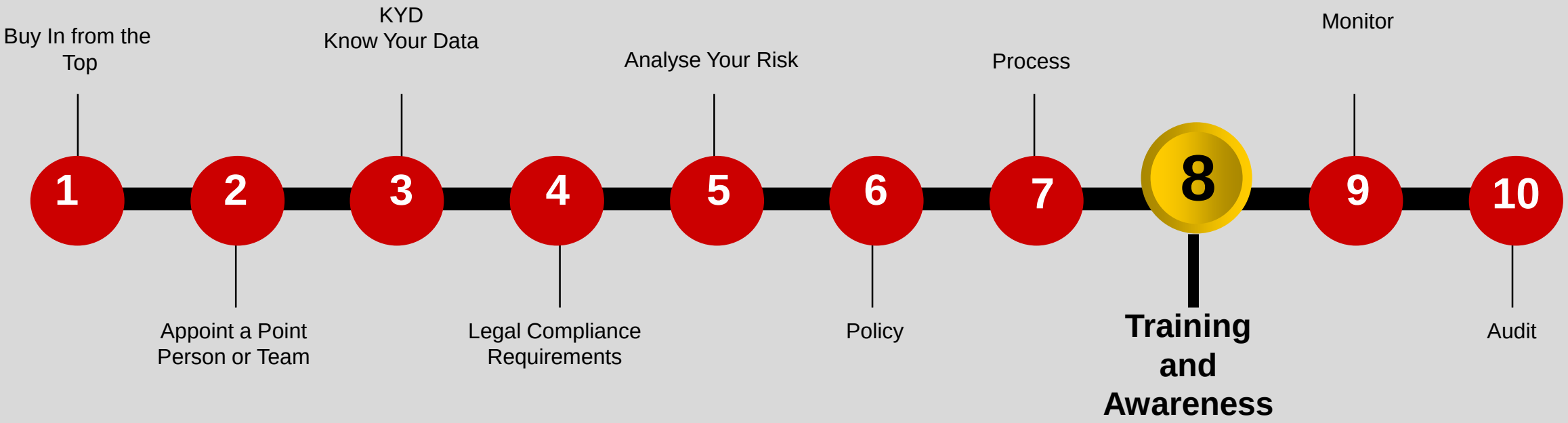
- One way to translate data protection policies to business processes is by adopting a Privacy by Design (PbD) approach in which organisations consider the protection of personal data from the earliest possible design stage of any project, and throughout the project's operational lifecycle. This can be as simple as putting data protection considerations in the foreground of any project development instead of as an afterthought.

Process

- **Establish a process for data breach incidents**
  - **Personal data breaches can occur due to various reasons such as malicious activity, human error or computer system error. Organisations should develop and implement a personal data breach management process to address breach incidents. The plan may include the following set of activities –**

    - C- Containing the breach
    - A – Assessing the risk
    - R – Reporting the incident
    - E – Evaluating the response and recovery to prevent future breaches

Step Eight



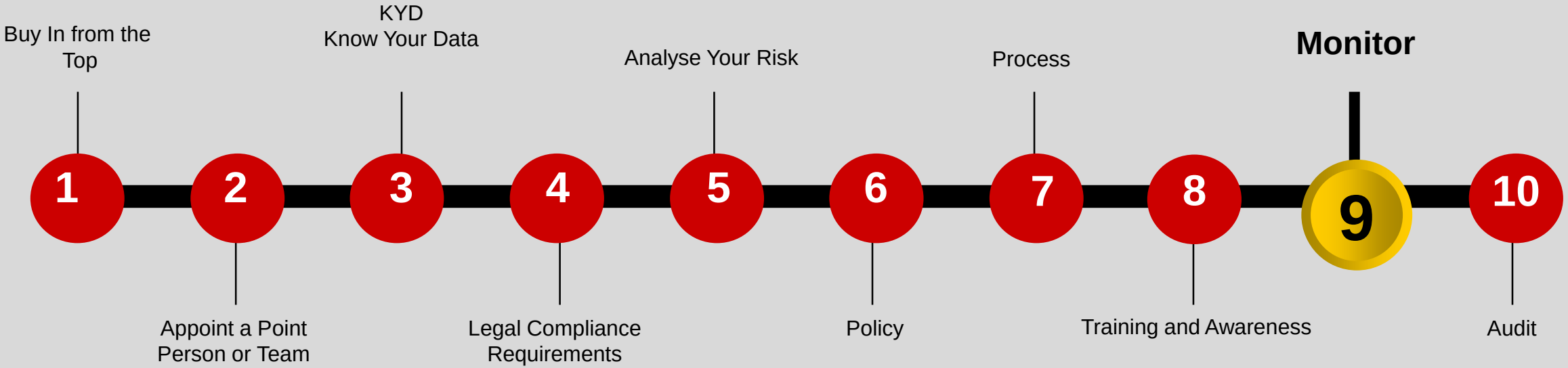
EquiGov Institute

Training and Awareness

- A sound PMP requires all members of an organisation to be aware of, and be ready to act on personal data protection obligations. Organisation should provide employees with up-to-date training and education tailored to specific needs. The organisation should also document its training processes and measure participation and effectiveness.

- It is not possible do have significant corporate cultural change without educating every involved party. For instance, while normal employees should at least understand the basic requirements for working with private data, some specialized functions, including IT staff, Security team, Legal, Auditors, and even the Point Person, may require advanced training, especially if they are expected to follow specific procedures.

Step Nine



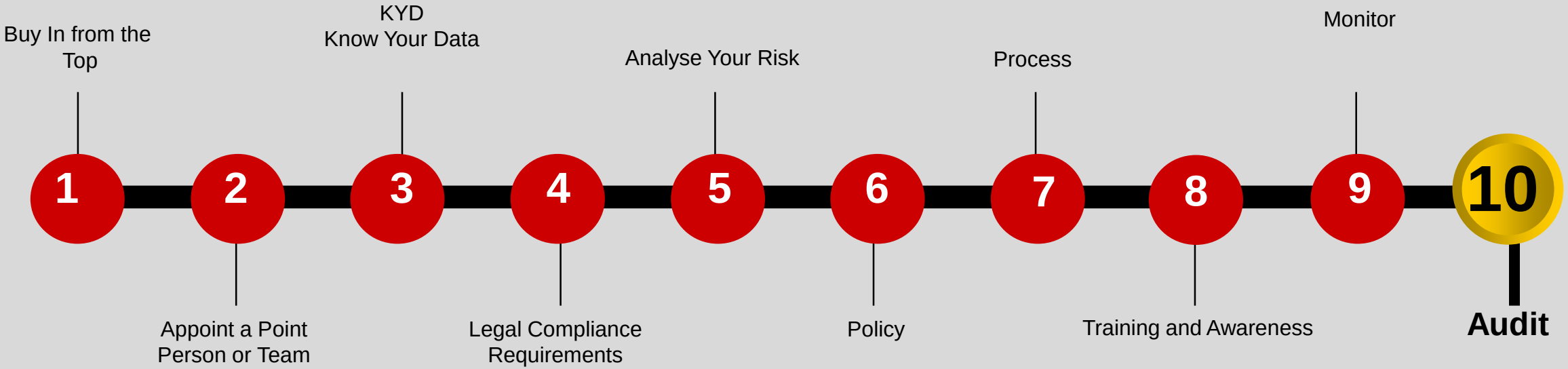
EquiGov Institute

Monitor

- **The effectiveness of programme controls should be monitored, periodically audited, and where necessary, revised. Organisations may consider the following factors before determining whether the programme controls should be revised:**

    - **What are the latest threats and risks?**
    - **Are the programme controls addressing new threats and reflecting the latest complaint or audit findings?**
    - **Are new services being offered that involve increased collection, use or disclosure of personal data?**
    - **Is training necessary and if yes, is it taking place, is it effective, are policies and procedures being followed, and is the programme up to date?**

Step Ten



EquiGov Institute

Audit

- The aims of Data Protection Audits address the wider aspects of data protection including:
  - Mechanisms for ensuring that information is obtained and processed fairly, lawfully and on a proper basis
  - Quality Assurance - ensuring that information is accurate, complete and up-to-date, adequate, relevant and not excessive
  - Retention - appropriate weeding and deletion of information
  - Documentation on authorised use of systems, e.g. codes of practice, guidelines etc.
  - Compliance with individual's rights, such as subject access
  - Compliance with the data protection legislation in the context of other pieces of legislation such as the Human Rights Act, FOI Act etc.

The Bottom Line

Privacy should be viewed as a **business** issue, not a ***compliance*** issue

Think strategically and transform privacy into a competitive business advantage

EquiGov Institute

Cost of Taking the Reactive Approach to Privacy

Proactive

Class-Action Lawsuits

Damage to One's Brand

Loss of Consumer Confidence and Trust

EquiGov Institute

Thank You

EquiGov Institute