Donovan & Ho
ADVOCATES & SOLICITORS

Data Protection Impact Assessment (DPIA) Guidelines

Navigating Data Protection Impact Assessments

Donovan & Ho
ADVOCATES & SOLICITORS

What is a DPIA

An analytical process to systematically identify, assess, and mitigate risks before a new data processing operation begins. It helps organisations implement appropriate measures to minimise risks, safeguard personal data, and strengthen overall compliance frameworks.

Why Carry out a DPIA

- **Proactive Compliance:** Fulfills obligations under Personal Data Protection Act 2010 (Act).
- **Public Trust:** Demonstrates accountability to data subjects.
- **Global Adequacy:** Aligns with international privacy standards (e.g., EU, UK, Singapore, Japan).

The Key Parties Involved in a DPIA

Donovan & Ho
ADVOCATES & SOLICITORS

The Data Controller (Senior Management)

Role: Ultimate Responsibility.

Function: Makes the final decision to proceed with processing and ensures all identified risks are addressed and resourced.

The Data Protection Officer (DPO)

Role: Adviser & Supporter.

Function: Determines if a DPIA is required, provides regulatory advice, and develops bespoke assessment templates.

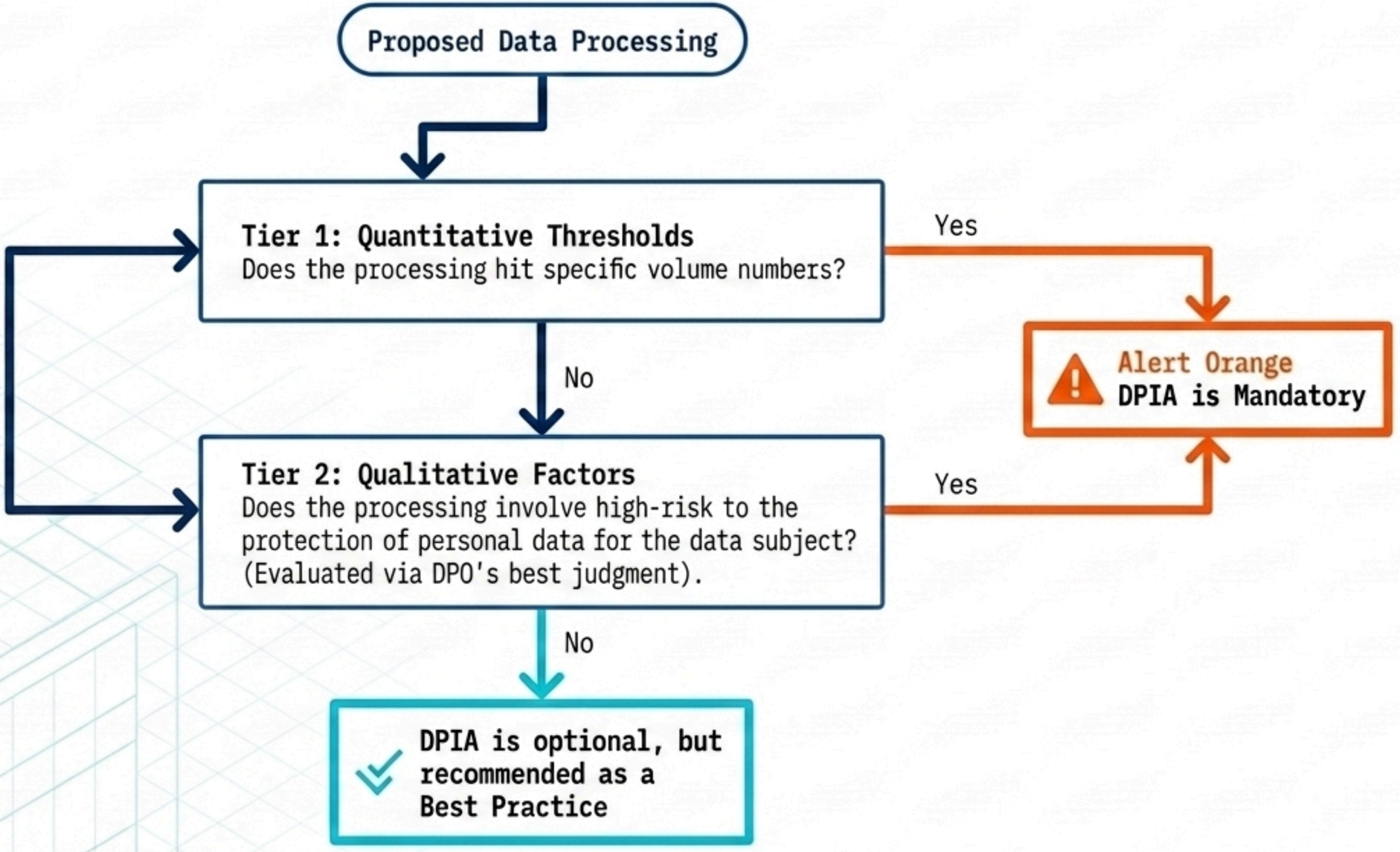
The DPIA Lead

Role: Execution.

Function: Plans and executes the assessment, gathering vital inputs from stakeholders (IT, Legal, Project Managers, and Data Processors).

The Trigger: Is a DPIA Required?

Donovan & Ho
ADVOCATES & SOLICITORS



Tier 1: Quantitative Thresholds

> 20,000 Data Subjects

Triggered when processing Personal Data expected to exceed this volume.

> 10,000 Data Subjects

Triggered when processing Sensitive Personal Data, including financial information data, expected to exceed this volume.

Donovan & Ho
ADVOCATES & SOLICITORS

Tier 2: Qualitative Factors

Legal/Significant Effects

Impacts the legal rights, financial status, health, reputation, or economic interests of data subjects.

Systematic Monitoring

Observation of data subjects, especially in commercial settings.

Innovative Technologies

Deploying new or significantly improved product (goods or services), new process, new marketing method or new organisational method in business practices.

Denial of Rights

Restricting a data subject's ability to withdraw consent or access personal data.

Location/Behavior Tracking

Continuous monitoring of a data subject's location or behavioural activities.

Vulnerable Individuals

Processing personal data of children or other vulnerable groups.

Automated Decision-Making

High-risk profiling without human intervention.

Examples

AI in Human Resources

Situation: An organization replaces manual reviews with an AI system that generates performance scores used for promotions or disciplinary actions.

The Trigger:
"Innovative Technology."
Significantly affects employment rights and professional reputation.

Retail Facial Recognition

Situation: A store uses facial recognition to identify loyalty members as they enter to provide personalized discounts.

The Trigger:
"Systematic Monitoring."
Uses biometric data in a commercial setting, posing a high risk of misidentification.

App-Based Tracking

Situation: A food delivery app tracks geolocation, browsing behavior, and order history to deliver targeted advertisements.

The Trigger:
"Behavioral Tracking."
Continuous profiling linked to commercial transactions.

Donovan & Ho
ADVOCATES & SOLICITORS

How to Carry Out A DPIA: The DEICA Framework

Phases 1 & 2: Describe and Evaluate

Step 1: Describe the Foundation

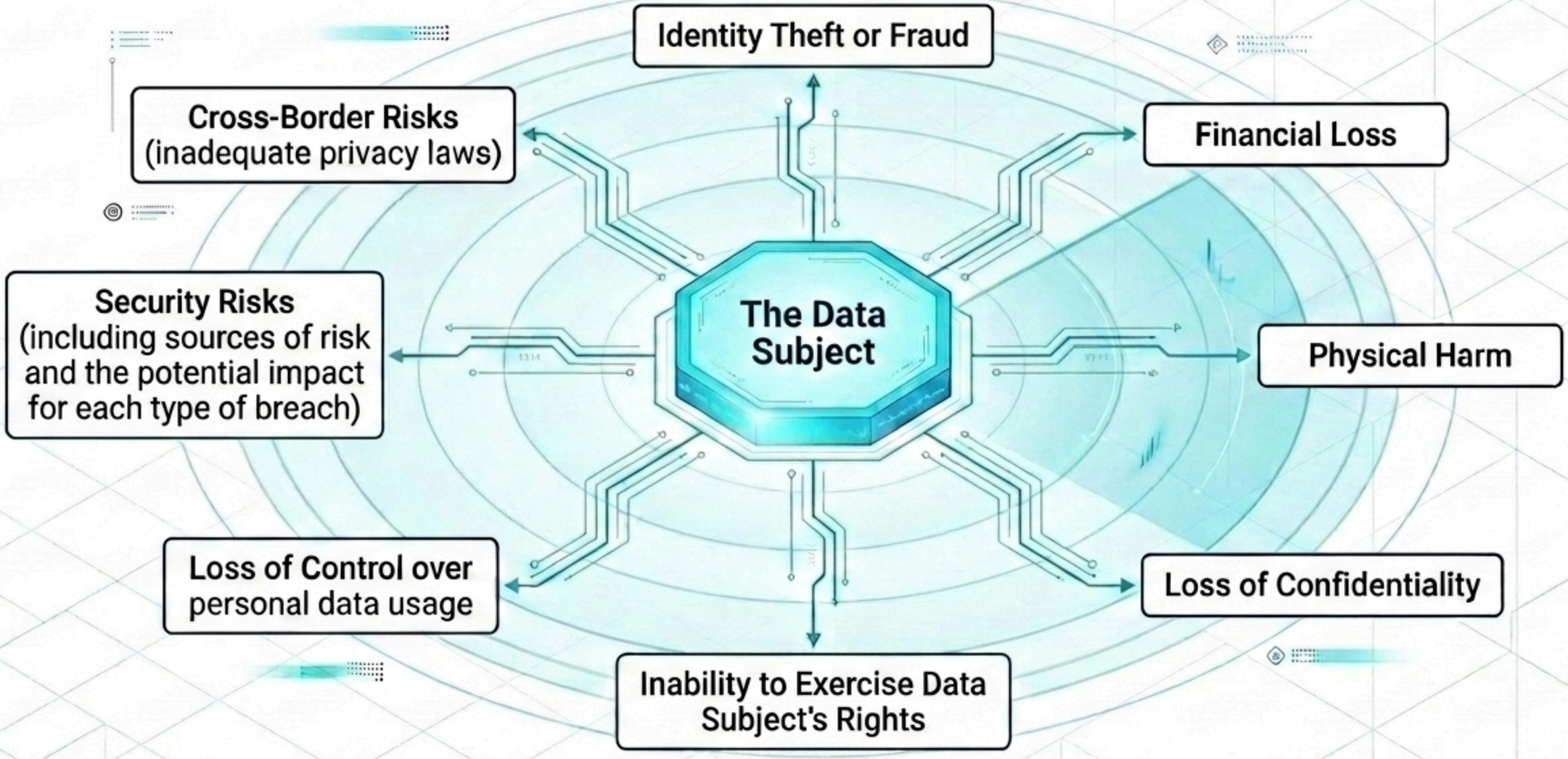
- **Nature:** How will personal data be collected, stored, and used?
- **Scope:** What the processing covers? (e.g. the volume and variety of personal data, the number of data subjects involved, and the geographical area covered).
- **Context:** What is the relationship with the data subject?
- **Purposes:** What is the reason why the organisation wants to process the personal data?

Step 2: Evaluate Proportionality

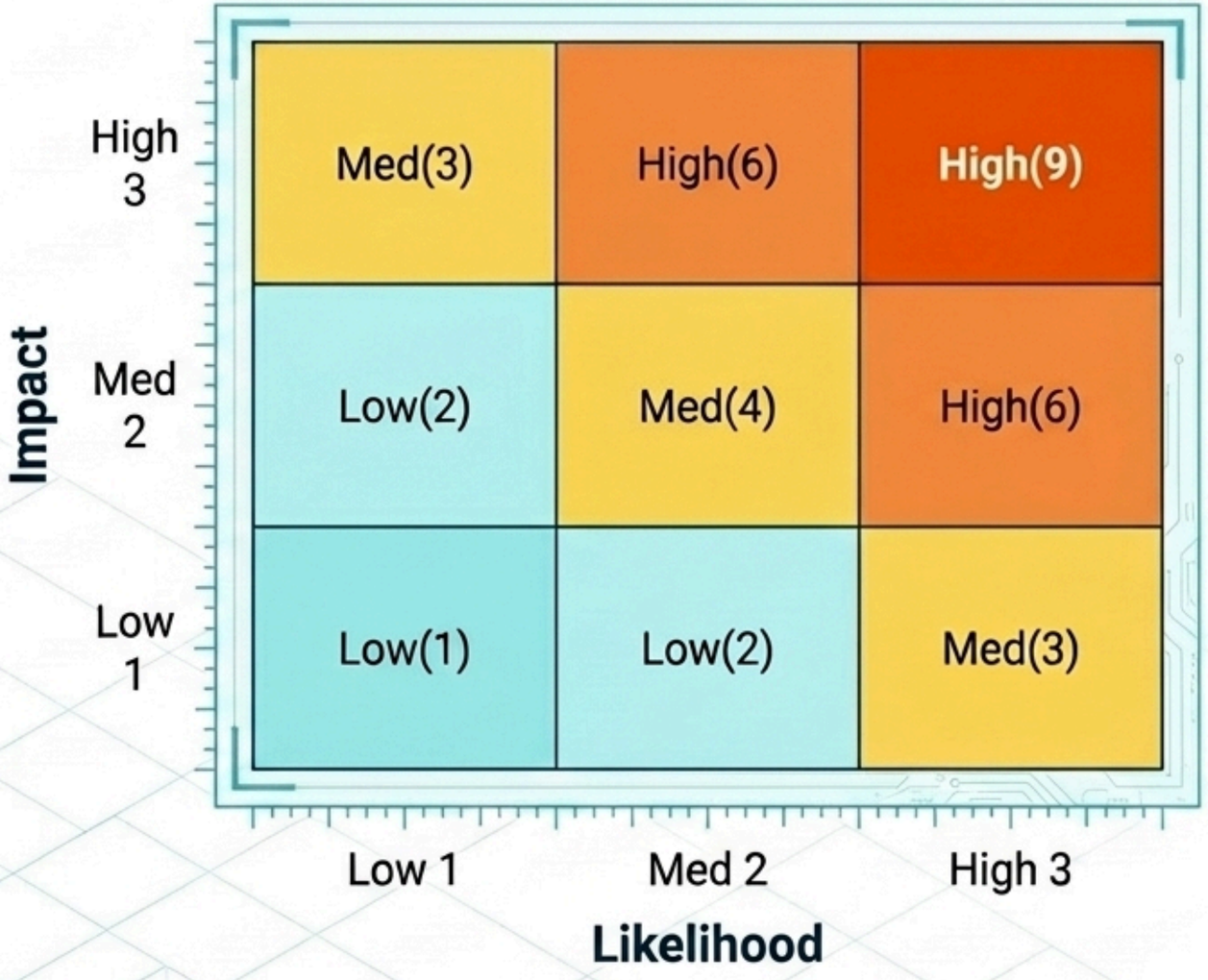
Does this process actually achieve the intended goal?

The Crucial Question: Is there another reasonable way to achieve this result without the proposed processing, or with less data?

Phase 3: Identify the Risks



Risk Assessment (3x3 Matrix)



Risk Response Action Thresholds

Low (1-2): Monitor.
Risk is manageable via standard operating procedures.

Medium (3-4): Mitigate.
Strengthen mitigation; implement additional controls.

High (6-9): Mandatory Action.
Robust risk treatment measures are required. A DPIA is triggered. ⚠

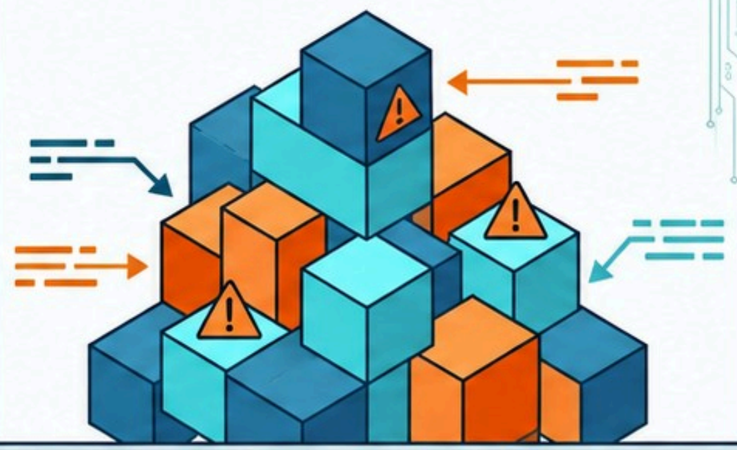
Donovan & Ho
ADVOCATES & SOLICITORS

Phases 4 & 5: Consider and Assess

Step 4: Consider Mitigation Measures

- Data Minimization (do not collect certain types).
- Shorter retention periods.
- Anonymization or pseudonymization.
- Transfer Impact Assessments (TIA) for cross-border transfers.
- Stricter contractual safeguards with third-party processors.

Identified Risk



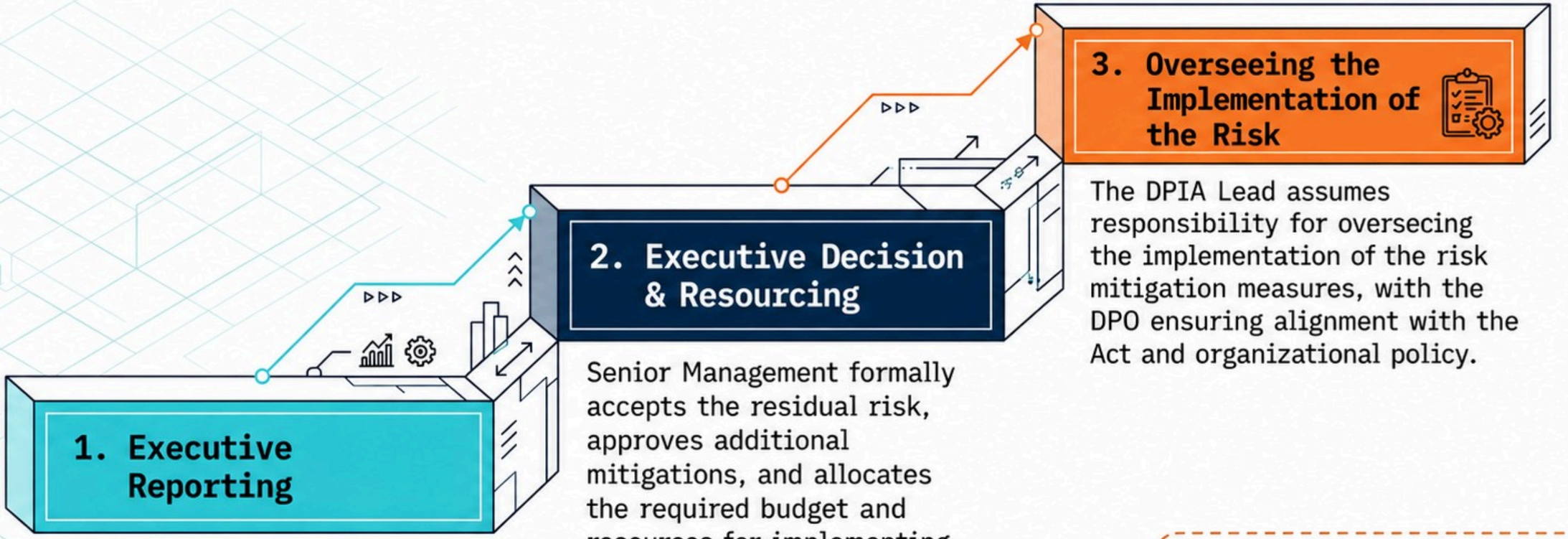
Step 5: Assess Residual Risk

After applying the measures from Step 4, recalculate the risk.

Determine the final, overall residual risk score of the entire operation (Low, Medium, or High).

Donovan & Ho
ADVOCATES & SOLICITORS

Post-DPIA:



1. Executive Reporting

If the residual risk is “High,” findings must be escalated to Senior Management.

(Best practice: Report all risk levels to maintain complete oversight).

2. Executive Decision & Resourcing

Senior Management formally accepts the residual risk, approves additional mitigations, and allocates the required budget and resources for implementing the risk mitigation measures.

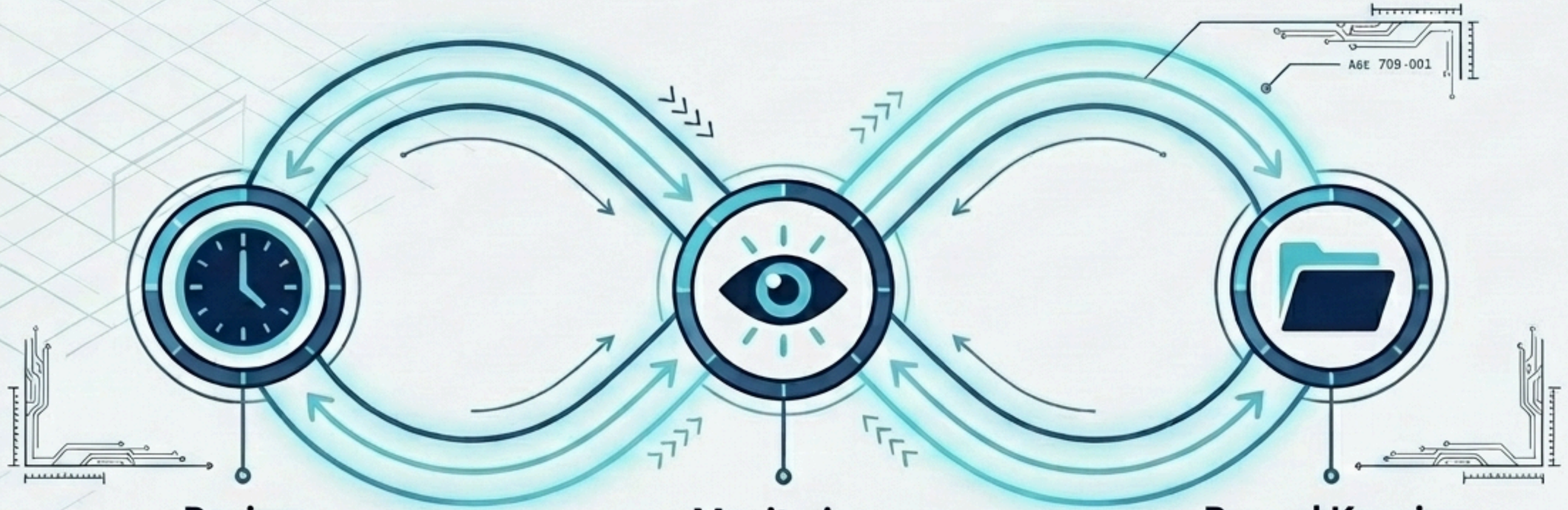
3. Overseeing the Implementation of the Risk

The DPIA Lead assumes responsibility for oversecing the implementation of the risk mitigation measures, with the DPO ensuring alignment with the Act and organizational policy.

Optional Step: Publication

Consider publishing a redacted version or summary of the DPIA to build public trust and demonstrate accountability.

Review, Monitoring and Record Keeping



Review

A completed DPIA is valid for two (2) years. Upon expiration, a refreshed DPIA must be conducted.

Monitoring

The DPIA Lead must actively monitor for changes in processing purposes or new technological vulnerabilities, adapting mitigations dynamically.

Record Keeping

All DPIA documentation must be maintained for at least two (2) years after the processing operation officially ceases.
Records must be available for Commissioner inspection.

Donovan & Ho
ADVOCATES & SOLICITORS

Key Implications for Companies

Market Trust

Companies that handle personal data responsibly earn compounding trust from customers, investors, and business partners.

Global Agility

Rigorous DPIAs ensure smooth collaboration with overseas partners and seamless expansion into regions with strict international regulations.

Operational Stability

Treating data protection as a built-in control creates resilient operations capable of withstanding the threats of a globally data-dependent business world.

This allows companies to improve data governance practices, strengthen internal risk controls, and build stronger trust across key stakeholders.