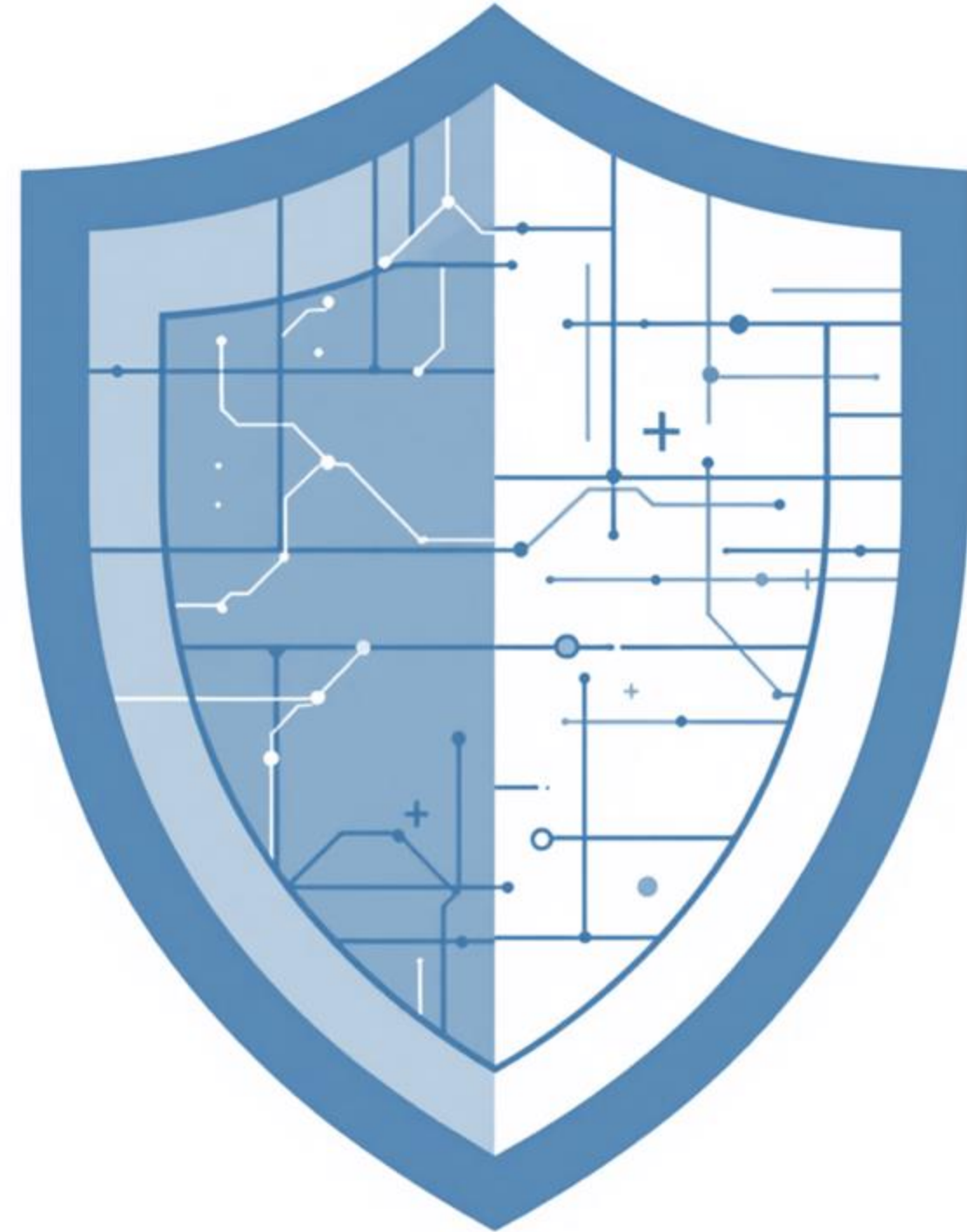


7 Steps in Privacy Risk Management

A systematic approach to protecting personal data and individuals' rights through comprehensive risk management.



What is Risk Management?

Risk management is a systematic application of management policies, procedures, and practices to the activities of communicating, consulting, establishing the context and identifying, analyzing, evaluating, treating, monitoring and reviewing risk.

— ISO 27000 Framework

The Complete Risk Management Process

01

Context Establishment

Define scope and criteria for risk management

02

Risk Identification

Determine potential losses and their causes

03

Risk Analysis

Assign levels based on likelihood and impact

04

Risk Evaluation

Compare risks against acceptance criteria

05

Risk Treatment

Implement measures to mitigate risks

06

Communication

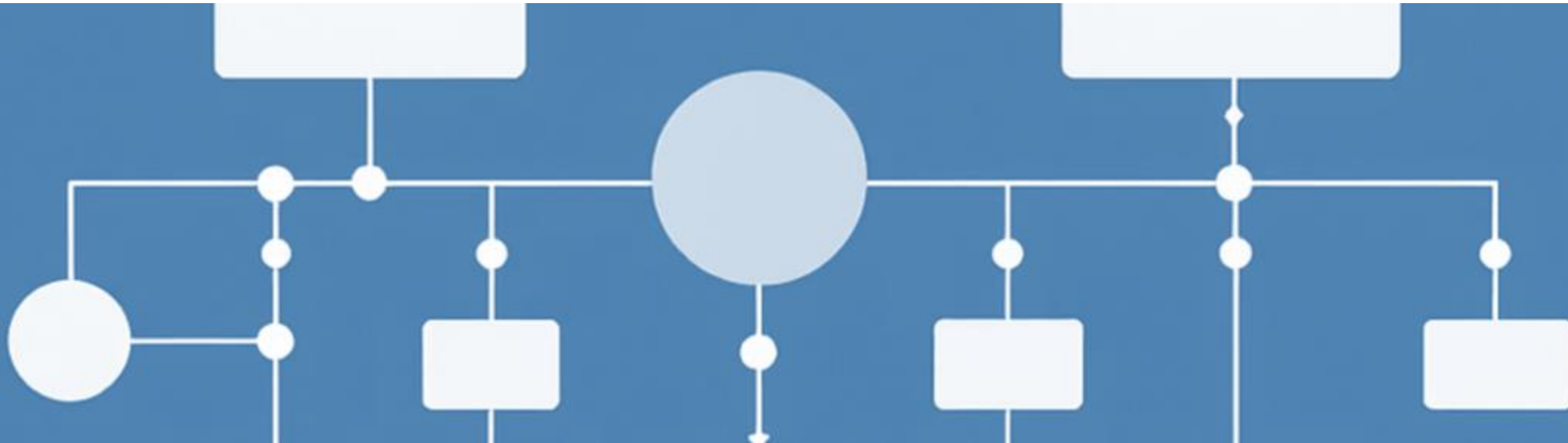
Share risk information with stakeholders

07

Monitoring & Review

Continuously track and update risk factors

Step 1: Context Establishment



Information Security

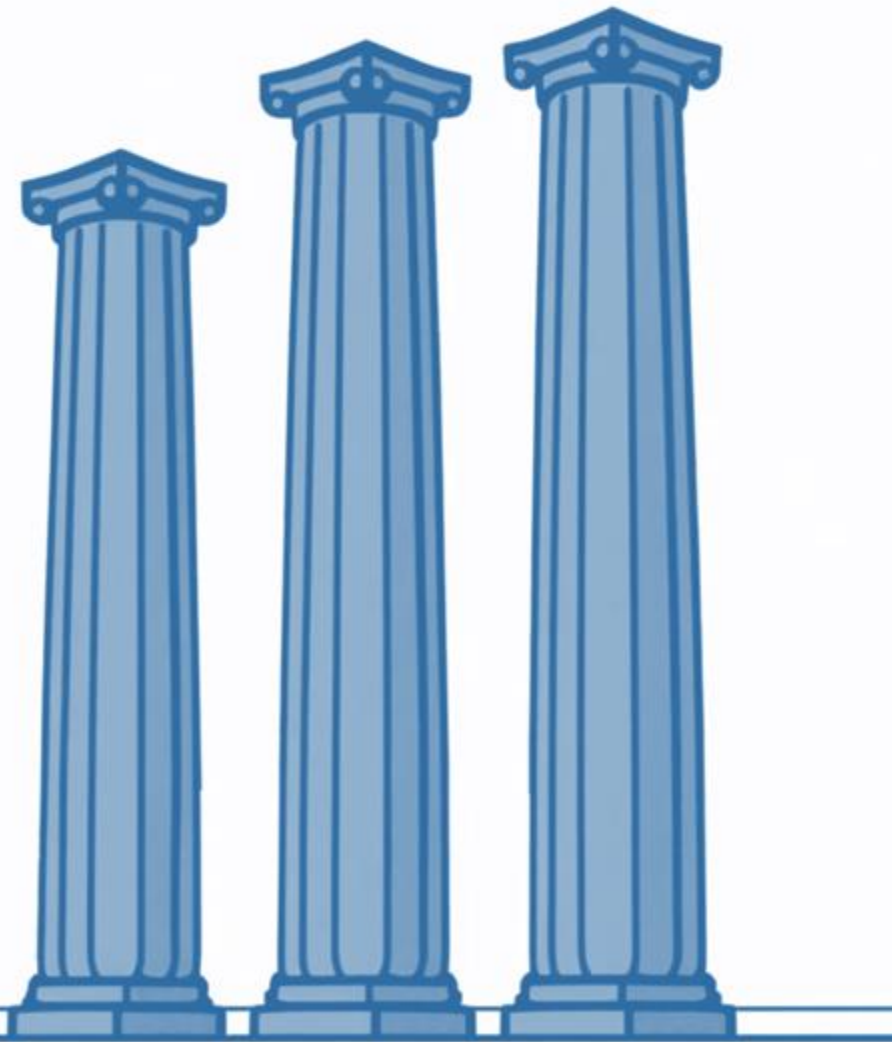
Defining context means outlining specific areas where risk management will be applied, including basic rules, scope, and organizational structure.

- Classification of information assets
- Operational and financial impacts
- Legal and regulatory breaches

Data Privacy

Scope focuses on records of processing activity, aligning with nature, scope, context, and purposes of processing personal data.

- Protecting individuals' privacy
- Meeting legal requirements
- Enhancing consumer trust



Three Essential Criteria

Risk Evaluation Criteria

Used to evaluate the criticality of the assets involved in processing activities.

Risk Impact Criteria

Used to describe the degree of damage caused by an incident to individuals' rights.

Risk Acceptance Criteria

Used to decide whether a risk is already at an acceptable level for processing.

Step 2: Risk Identification

Risk identification aims to determine what could cause potential loss and gain insight into how, where, and when



Assets

Personal data and special categories



Threats

Potential sources of harm



Controls

Existing protective measures



Vulnerabilities

System weaknesses



Consequences

Potential outcomes



Partner With GRC³ for DPDP Success

Contact:

Nidhi P. – Nidhi.p@grc3.io / +91 9004735605

Mayuri B. – mayuri.b@grc3.io / +91 8097235523


Pooja D. - pooja.d@securetain.com

Charu P. - charu.pel@grc3.io



In data privacy, risk levels depend on impact to natural persons. The risk level is determined by combining likelihood and severity using a risk assessment matrix.

Consequence: Impact severity on data subjects' rights and freedoms

 Risk Level = f(Likelihood, Severity)

[illegible]

Steps 4 & 5: Evaluation and Treatment

1

Risk Evaluation

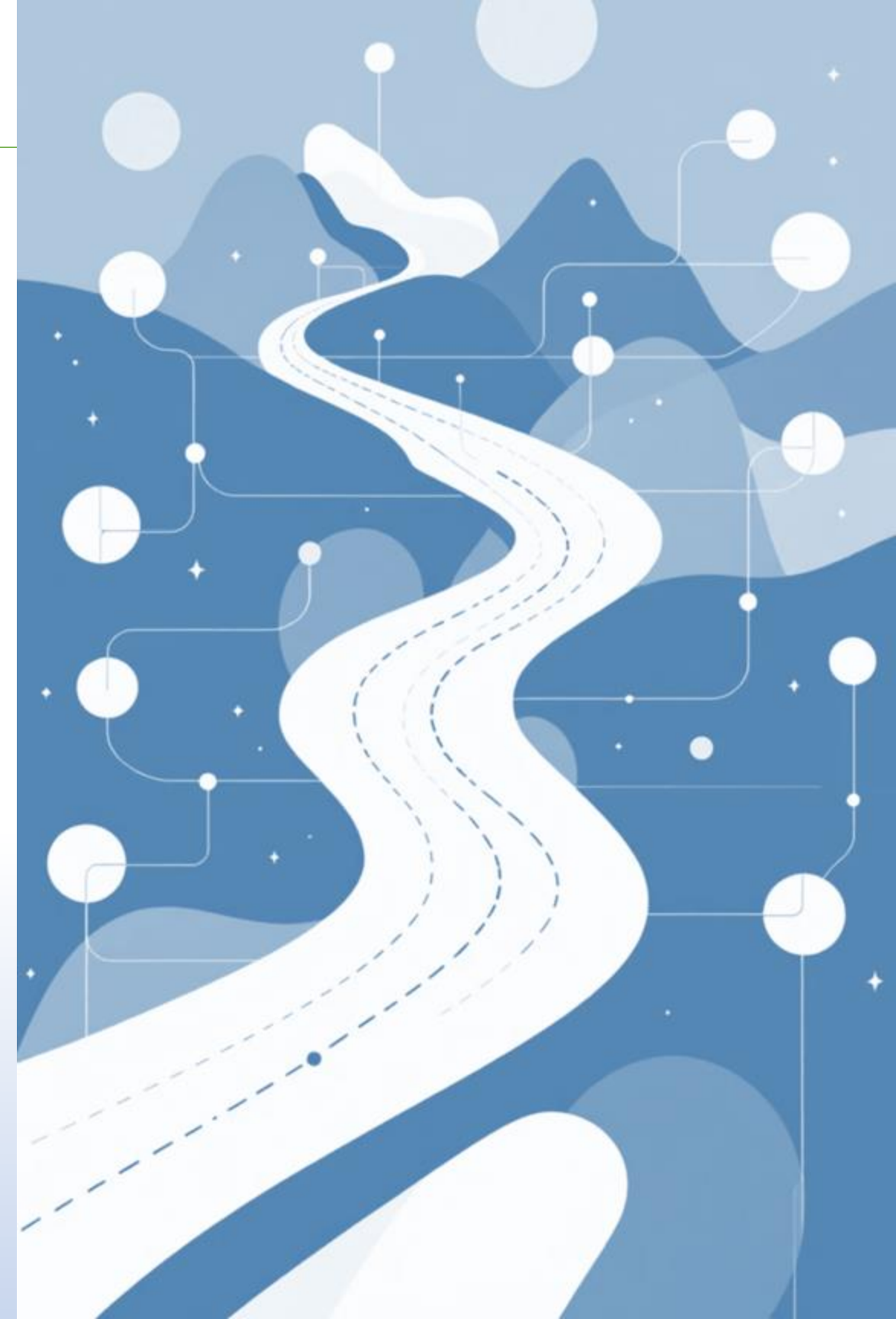
Compare risk levels against acceptance criteria. In data privacy, this determines "go" or "no go" for processing activities and may require consultation with authorities.

2

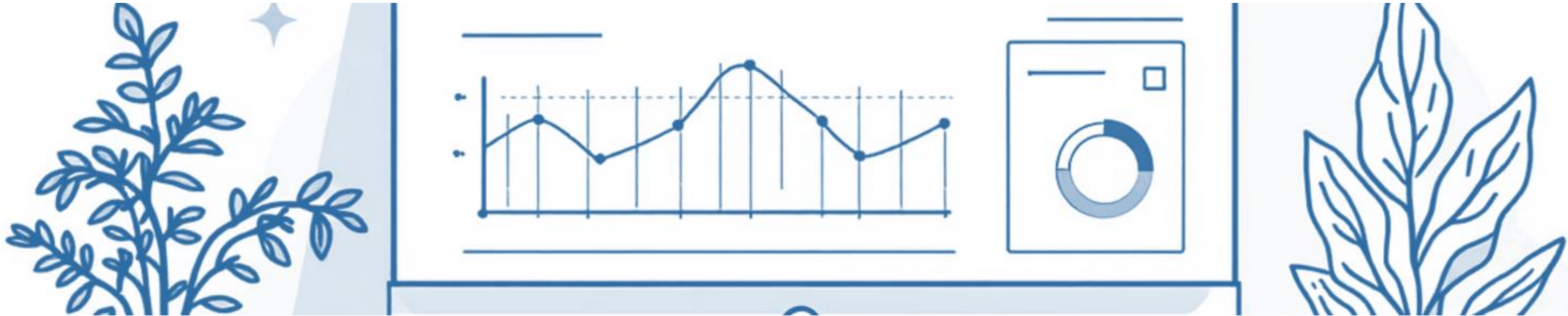
Risk Treatment Options

GDPR requires appropriate technical and organizational measures considering state of art, costs, and nature of processing to protect individuals' rights.

Unlike information security where risks can be accepted, transferred, or avoided, data privacy focuses primarily on risk mitigation to protect individuals' rights and freedoms.



Steps 6 & 7: Communication and Monitoring



Risk Communication & Consultation

Share information about risks between decision-makers and stakeholders, including existence, nature, likelihood, severity, and treatment of risks.

In data privacy, this extends beyond information security to include consultations with data protection authorities when processing poses high risk to individuals.

Risk Monitoring & Review

Risks are not static. Constant monitoring is necessary to detect changes in threats, vulnerabilities, likelihood, or consequences early enough.

Maintain an overview of the complete risk picture through continuous review of all risk factors.

Risk Management: Protecting Personal Data

Risk management serves as a systematic approach to navigating challenges within information security and data privacy. The journey from context establishment through monitoring ensures compliance with regulations like GDPR.



Systematic Process

Seven structured steps guide organizations through comprehensive risk management.



Individual Focus

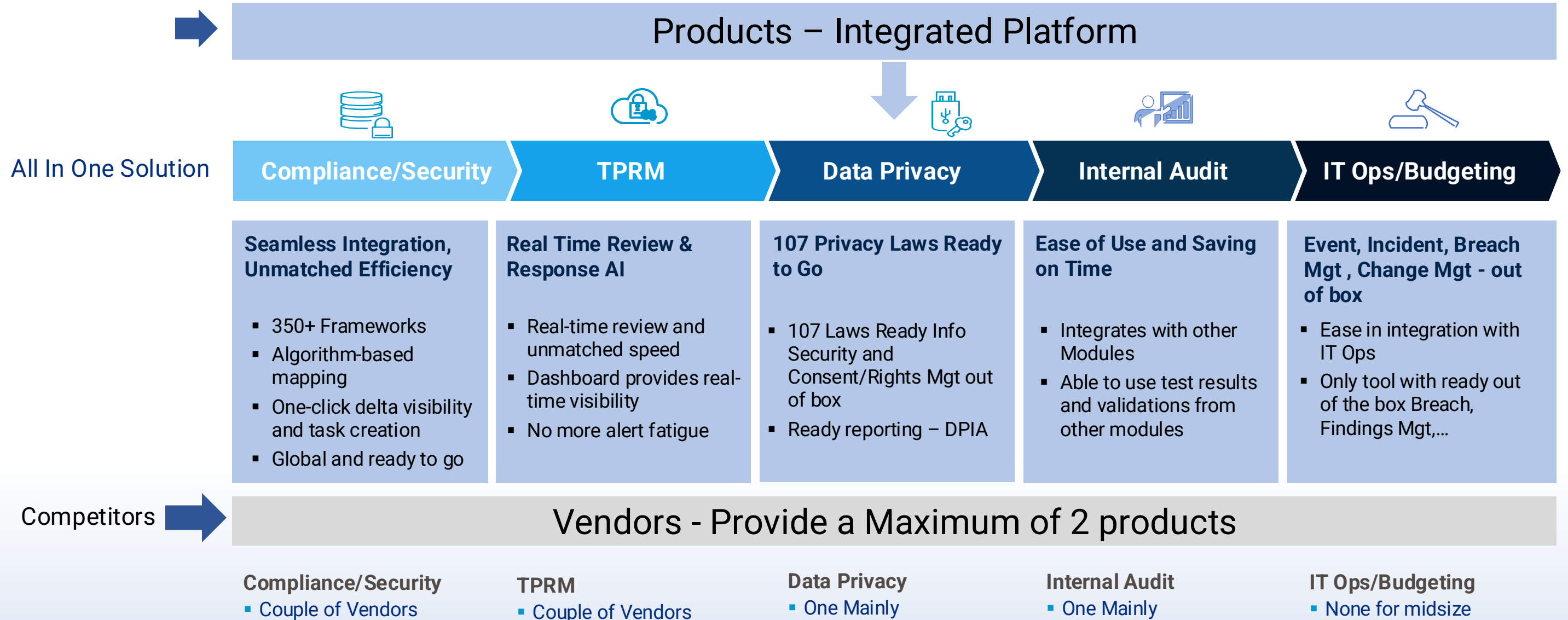
Data privacy uniquely considers impact on individuals' rights and freedoms.



Secure Digital Landscape

Tailored practices safeguard personal data and foster trust in the digital age.





← Multiple providers, limited frameworks, duplication of work, lack of integration, risks falling through the gaps, adoption challenges, costs, inadequate reporting, no centralized dashboard, inadequate service management and findings documentation →

Visual Dashboard

Continuous insight into all processing activities with clear program overview.

Automated Processes

Innovative SaaS platform designed to automate privacy workflows and minimize risks.

Cross-Departmental Cooperation

Support seamless collaboration ensuring compliance across your organization.

6

Product Lines

Comprehensive suite addressing key privacy challenges

20+

Multiple Modules

Each targeting specific compliance requirements

Commitment to Clients



Fast-Track Certifications



Integrated Risk & Compliance Platform



AI-Driven Efficiency



Build Credibility & Confidence



Expand to new territories faster with agility and built to scale

GRC³.io COMMITMENTS

**SPEED &
AGILITY**

**CUSTOMER
EXPERIENCE**

INNOVATION

