Building Responsible Innovation via Data Governance Excellence

May 2024

Overview

Data Governance and Responsible Innovation

How effective governance delivers responsible innovation by default.

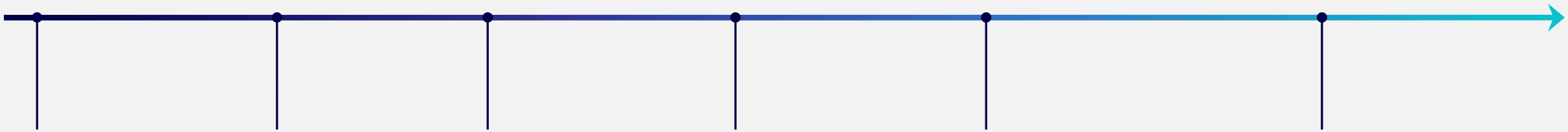
Good Governance

How instantaneous assurance can enable rapid implementation, powering market differentiation

Building Comprehensive Quality Management Systems

Key principles for creating transparent and encyclopaedic knowledge about processing activities to delivers robust governance and compliance.

EU AI Act Key dates



Entry into force

20 days after publication in official journal of the EU

+ 6 Months

Prohibitions on unacceptable risk AI

+ 12 Months

Obligations on providers of general purpose AI models come into effect.
Appointment of member state competent authorities
Annual Commission review of, and possible amendments to, the list of prohibited AI.

+ 18 Months

Commission implementing act on post-market monitoring.

+ 24 Months

Obligations on high-risk AI systems specifically listed in Annex III, which includes AI systems in biometrics, critical infrastructure, education, employment, access to essential public services, law enforcement, immigration and administration of justice.
Member states have to have implemented rules on penalties, including administrative fines.
Member state authorities to have established at least one operational AI regulatory sandbox.
Commission review, and possible amendment of, the list of high-risk AI systems.

+ 36 Months

Obligations for high-risk AI systems that are not prescribed in Annex III but are intended to be used as a safety component of a product, or the AI is itself a product, and the product is required to undergo a third-party conformity assessment under existing specific EU laws, for example toys, radio equipment, in vitro diagnostic medical devices, civil aviation security and agricultural vehicles.

By the end of 2030

Obligations go into effect for certain AI systems that are components of the large-scale IT systems established by EU law in the areas of freedom, security and justice, such as the Schengen Information System.

EU AI Legislation – a three-part plan

Prevention of harm

AI Act
- Prevent harm by AI systems
- Risk-based approach
- Prohibit AI with unacceptable risk
- Transparency and governance
- Regulatory fines (6% turnover)

AI Liability Directive
- Claims by natural or legal persons
- Claims against any person (providers, developers, users)
- Claims for any type of damage
- Presumption of harm causation
- Provide easier access to evidence

Fault-based liability

Strict liability (no fault)

Revised Product Liability Directive
- Claims by natural persons only
- Claims against manufacturers
- Claims for material losses
- “Products” include software/AI
- Evidence disclosure requirements
- Burden of proof presumptions

Provision of compensation

There are currently three different pieces of proposed EU legislation (the AI Act, the AI Liability Directive, and the Revised Product Liability Directive) which are designed to be complimentary.

- The **AI Act** will introduce risk-based regulation of AI systems, giving regulators the power to issue fines for non-compliance (but not to compensate affected parties).
- The **AI Liability Directive** will enable non-contractual compensation claims against any person (providers, developers, users) for harm caused by AI systems which is due to the fault or omission of that person (where ‘person’ can also be a legal entity).
- The **Revised Product Liability Directive** will enable civil compensation claims against manufacturers (and importers) for harm caused by defective software and AI products or which incorporate software and AI systems.

Diagram source: https://digiphile.law/

cognizant

Rules and risks

The EU AI Act has both rules-based and risk-based elements.

Rules are binary – you can or cannot do something.

Risks are interpretable. They require the application of guidelines, frameworks and codes of conduct.

Article 5

Lays out what uses of AI are forbidden:

- Uses that aim to influence behaviour, i.e. subliminal, manipulative, or deceptive AI-aided techniques or using AI to exploit a person or group's vulnerabilities.
- Use of biometric information to ascertain a person's race, sexual orientation, beliefs or trade union membership.
- Social scoring – tracking a person's behaviour in a way that could result in their unfavourable treatment in an unrelated situation.
- Real-time facial recognition/remote biometric identification (RBI) in public places. Exception is law enforcement for specific investigations/missing person search provided appropriate legal authorisation has been obtained.
- Using AI to estimate a person's likelihood to commit a crime based solely on personal characteristics i.e. predictive policing.
- AI cannot be used to create databases of facial images by scraping the internet or CCTV videos. (see ClearviewAI).
- Tools that infer a person's emotions in the workplace or an educational environment.

How to address high-risk AI

By following appropriate data governance practices:

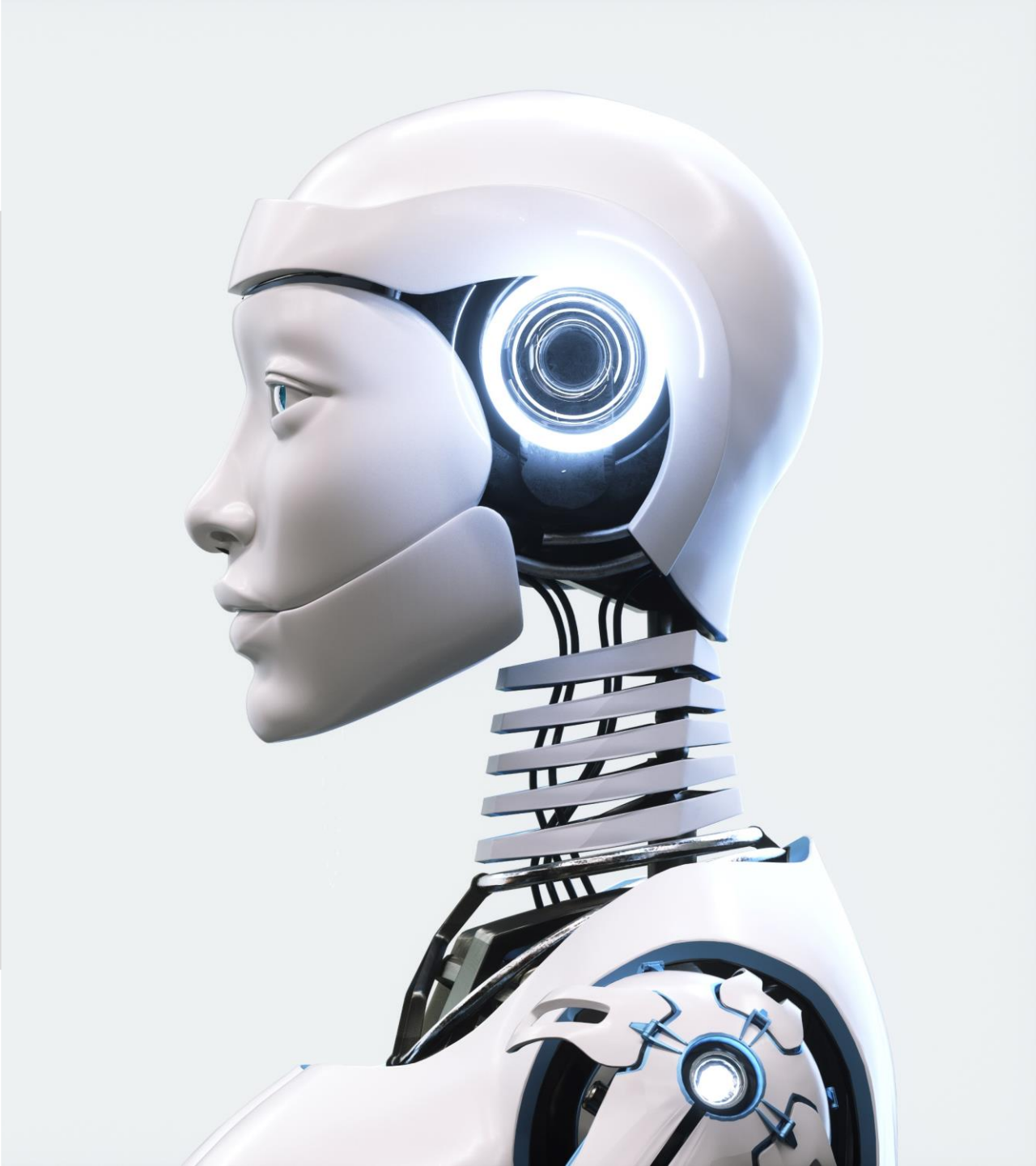
- Ethical collection of datasets for training.
- Documentation
- Fundamental Rights Impact Assessment (FRIA)

High Risk AI Systems

Annex III

Includes:

- Biometrics
- Facial recognition (not explicitly forbidden by Art. 5)
- Critical infrastructure components
- Education and the workplace
- Access to public service, benefits or essential private services like banking and insurance
- Uses related to law enforcement, migration, justice and elections



Ensuring Compliance

Importance of Compliance

Compliance with regulations is critical for building responsible innovation, ensuring that organisations adhere to relevant laws and avoid costly legal penalties and reputational damage.

Key Steps for Compliance

Organisations can take a number of key steps to ensure compliance with relevant regulations, including monitoring regulatory developments, implementing training and compliance programs, and building a culture of data governance excellence.

General Purpose AI

AI Act definition

"Models" that underpin AI tools – not the customer-facing apps, but the software architecture that is integrated into different providers' products.

e.g. ChatGPT, Gemini, CoPilot

1. Documentation

Developers will need to keep detailed technical documentation

2. Partners

Developers will need to help companies or people deploying their models understand the tools' functionality and limits.

3. Copyright

Developers will need to provide a summary of the copyrighted material (e.g. text and images) that has been used to train the models.

4. Enforcement

Developers must cooperate with European Commission and national enforcing Authorities when it comes to compliance with the rulebook.

5. Labelling

Some general purpose models with be labelled as "systemic risk" because of their reach and power – including the ability to cause catastrophic events.
These systems must have mitigation strategies in place

6. Reporting

Developers of models labelled "systemic risk" must report all incidents to the Commission's AI Office.

The importance of good governance

Responsible Innovation	It ensures that AI is developed and used in a way that is ethical, transparent, and beneficial for society.
Data Governance Excellence	Good governance is crucial for data governance excellence. It ensures that data is properly managed, stored, and used, and that privacy and security are protected.
Effective Change Control Processes	Change control is a critical component of an effective quality management system. Effective data governance is the critical factor in ensuring changes can be implemented friction-free and at pace.

Instantaneous assurance and rapid deployment are outcomes of holistic risk management systems. Combined with a comprehensive Quality Management System they power market differentiation

Risk Management

Risk Management Framework

A risk management framework is a structured approach to identifying, assessing, and managing risks associated with data governance and AI. It helps organizations build responsible innovation and data governance excellence.

Key Components of a Risk Management Framework

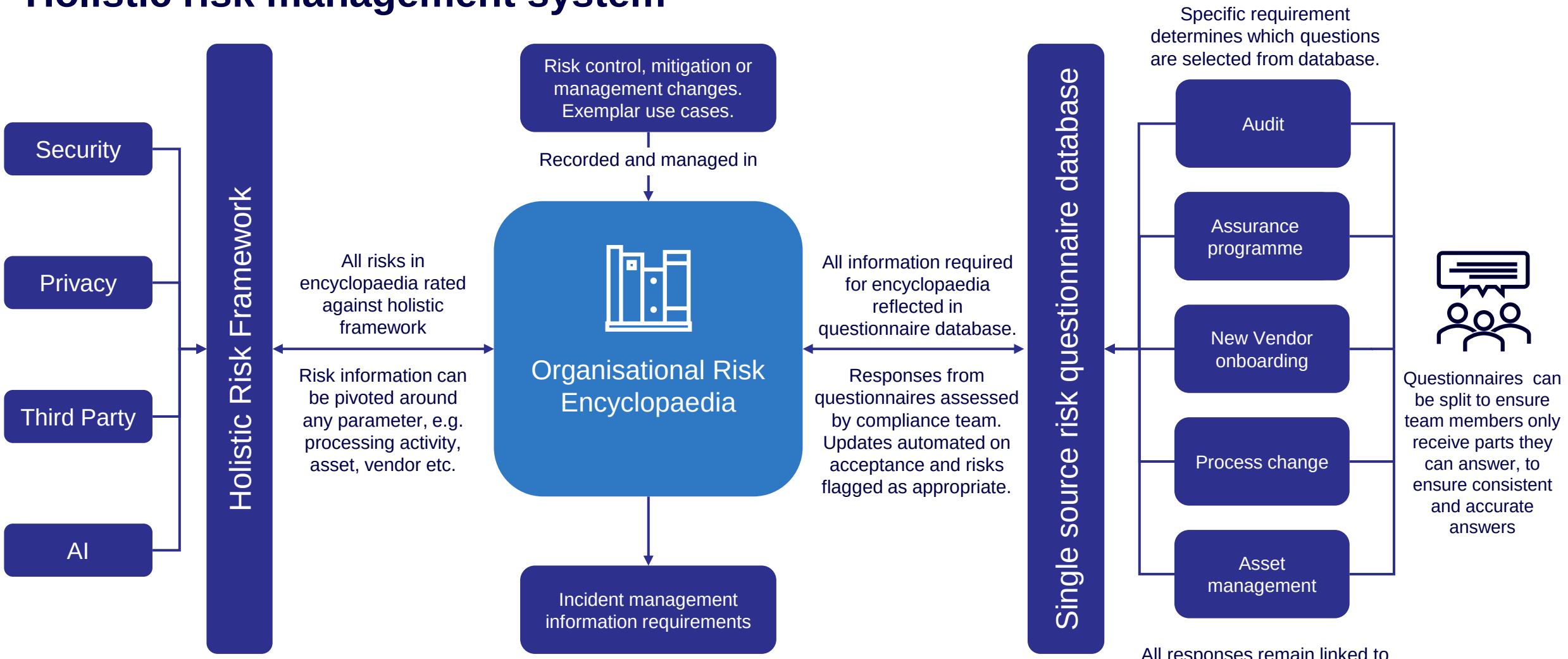
A risk management framework typically includes the following key components:

- Risk identification
- Risk Assessment
- Risk Mitigation
- Risk Monitoring
- Reporting

Identifying and Mitigating Risks

A risk management framework can help organizations identify and mitigate risks associated with data governance and AI, such as data privacy, security breaches, algorithmic bias, and ethical concerns.

Holistic risk management system

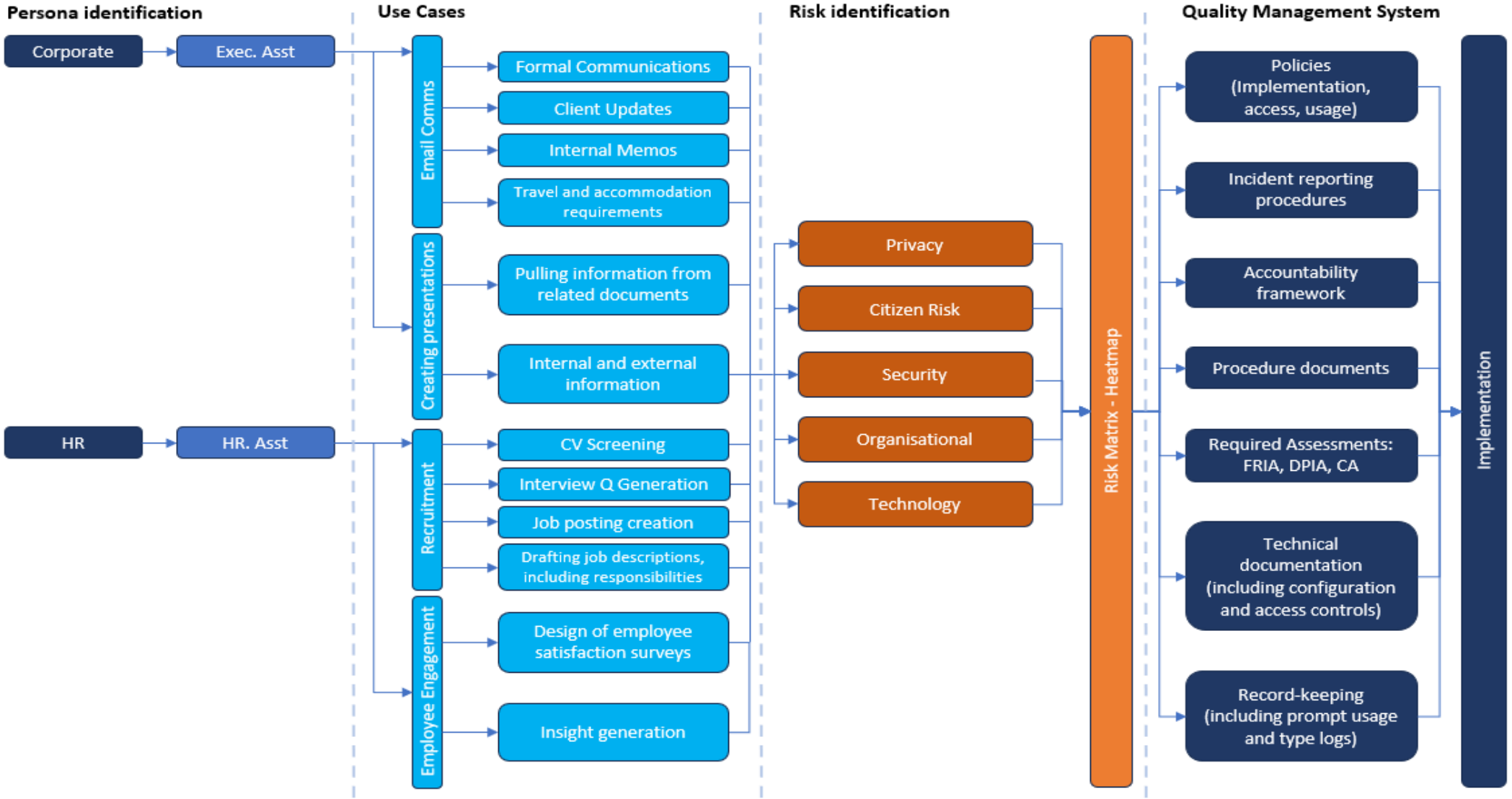


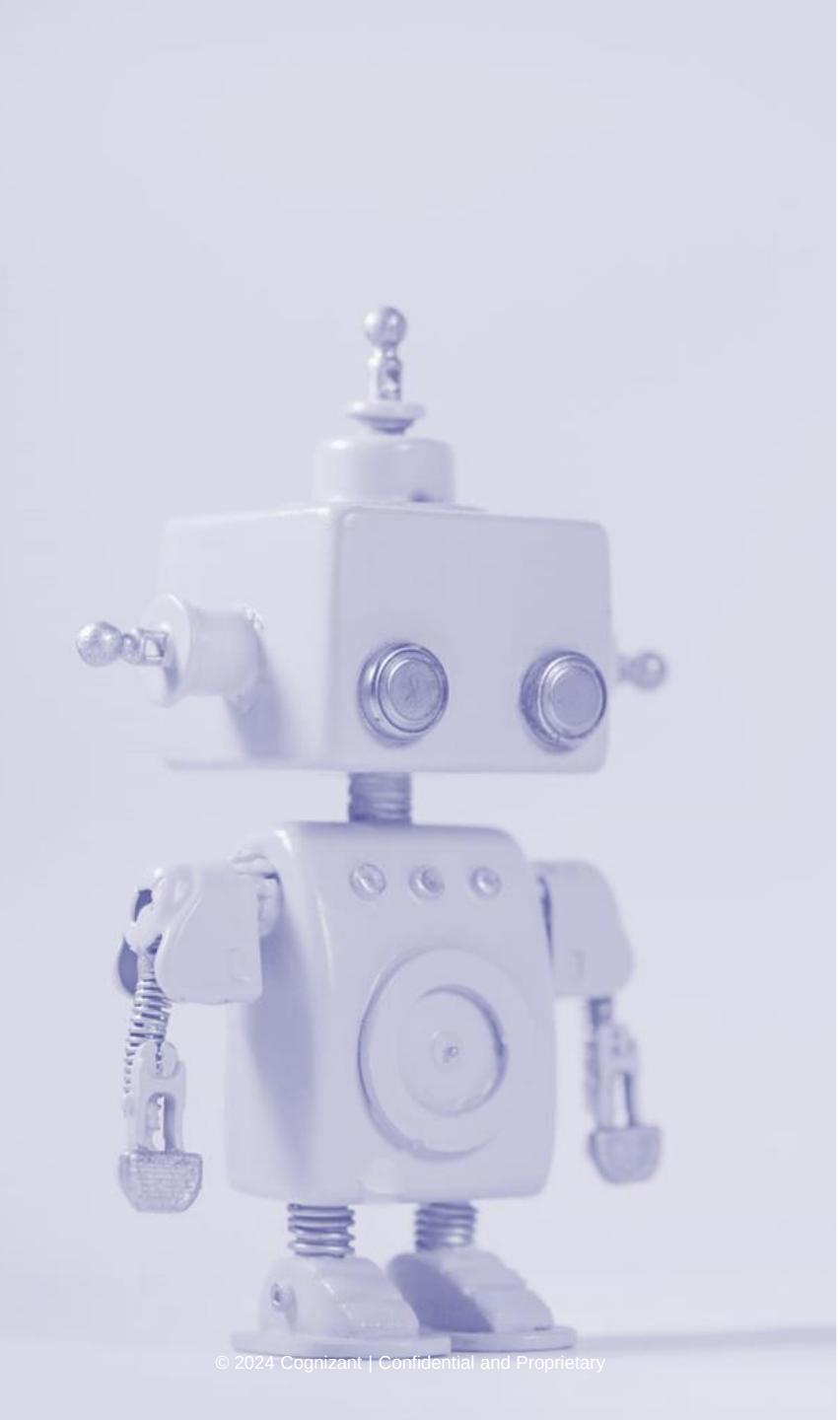
Implementing controls

Access controls	Critical component of any compliance program, helping orgasizations ensure that only authorized individuals have access to sensitive data or systems.
Data Retention, deletion and remediation	Data retention policies help manage the lifecycle of data, from creation to destruction, ensuring that data is retained only as long as necessary and is disposed of securely.
Auditing, assurance and monitoring	Auditing and monitoring are essential controls that help organizations detect and deter noncompliance. These activities help identify potential issues and enable corrective action before they become significant problems

Controls are dependent on good data governance. Without it, none of the controls which deliver frictionless compliance can be put in place.

Triage process for risk in AI project implementation





In conclusion…

- Data governance is foundational for responsible innovation.
- Together, these factors are critical to the successful implementation of AI.
- Building comprehensive quality management systems that deliver robust and transparent governance can enable instantaneous assurance, frictionless compliance and rapid implementation, ultimately delivering powerful market differentiation.

cognizant

Thank you

Hellen Beveridge LL.M FIP

hellen.beveridge@cognizant.com
+44 (0) 7901 101945