allied digital
IT managed.Responsibly.

GOVERNANCE IN

EMERGING TECHNOLOGIES & DATA SECURITY

Presented by:

Paresh Shah, Global CEO

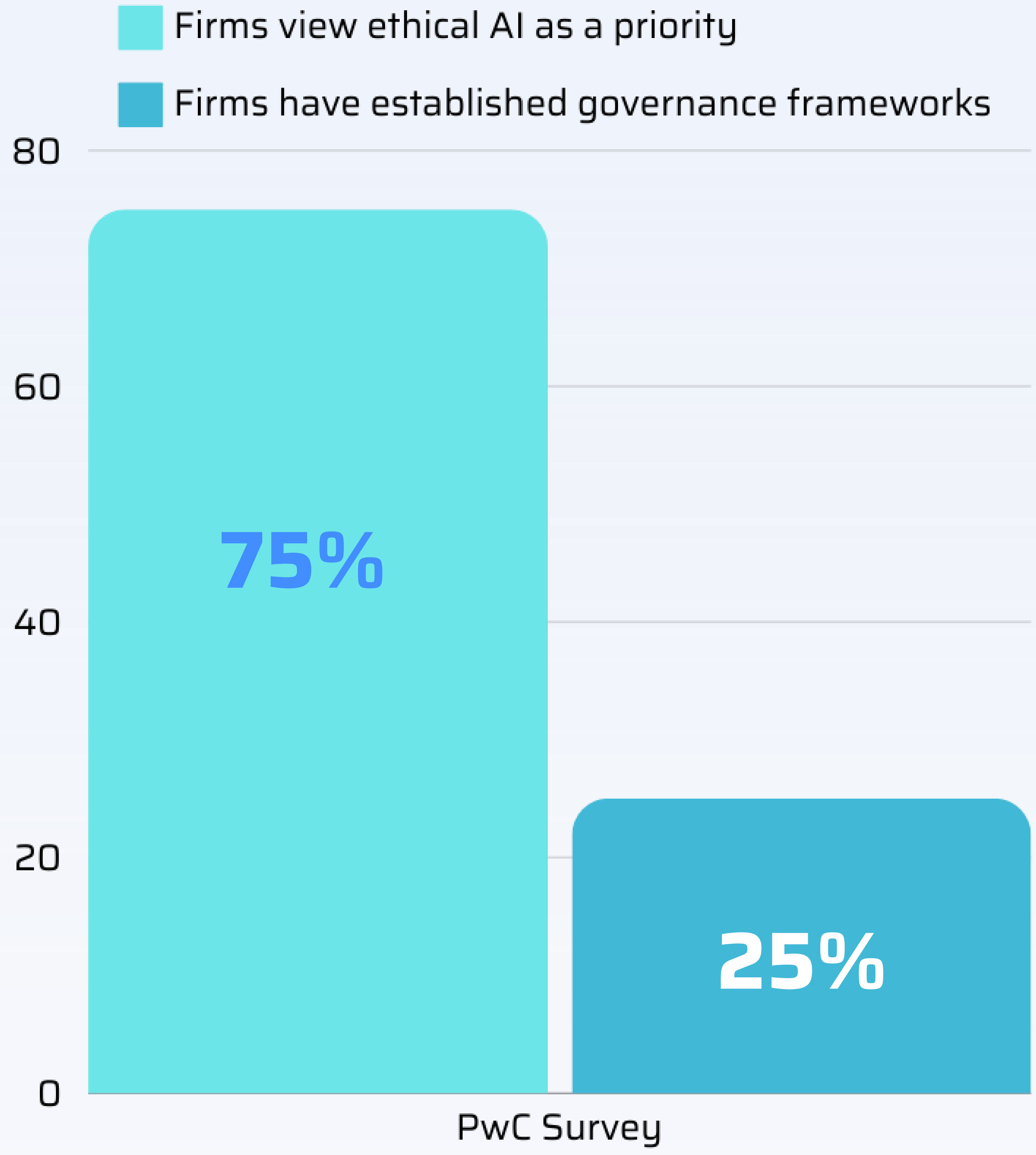
Allied Digital Services Limited

WHY GOVERNANCE AND DATA SECURITY ARE CRUCIAL

- **Rapid Technological Advancement:** Accelerating tech development is outpacing governance, creating regulatory gaps.

- **Risks of Unchecked Innovation:** Lack of governance may lead to ethical issues, security breaches, and social inequality.

- **Ensuring Responsible Development:** Strong governance and data security are crucial to align tech with societal values and promote fairness.



IDENTIFYING KEY EMERGING TECHNOLOGIES & THREATS

- **Artificial Intelligence (AI):** AI drives advancements across various sectors but raises concerns about data privacy and algorithmic bias.
  Threats – AI Driven cyberattacks, Data Poisoning

- **Blockchain:** Enhances security and transparency but requires robust governance to manage data privacy.
  Threats - Smart contract vulnerabilities

- **Quantum Computing:** Offers potential breakthroughs in cryptography but poses new challenges for data security.
  Threats - Breaking traditional encryption

IDENTIFYING KEY EMERGING TECHNOLOGIES & THREATS

- **5G and Beyond:** Enables advancements in IoT and smart cities but raises concerns about data security and privacy.
  Threats- Increased attack surface,
  Network slicing vulnerabilities

- **Internet of Things (IoT):** Connects devices and facilitates automation, demanding strong data security measures.
  Threats - Device vulnerabilities, Data interception

- **Augmented Reality (AR) and Virtual Reality (VR):** Transform user experiences but need careful consideration of data security.
  Threats: Extensive tracking of user behavior

IDENTIFYING KEY EMERGING TECHNOLOGIES & THREATS

- **Biotechnology:** Includes gene editing with significant ethical and data privacy concerns.

Threats: Privacy and security of individuals' genetic information

- **Autonomous Vehicles:** Innovations in transport and logistics require new governance models for safety and data protection.

Threats: Complex software and sensors that may fail or malfunction

- **Advanced Robotics:** Enhances automation but necessitates new safety and data security guidelines.

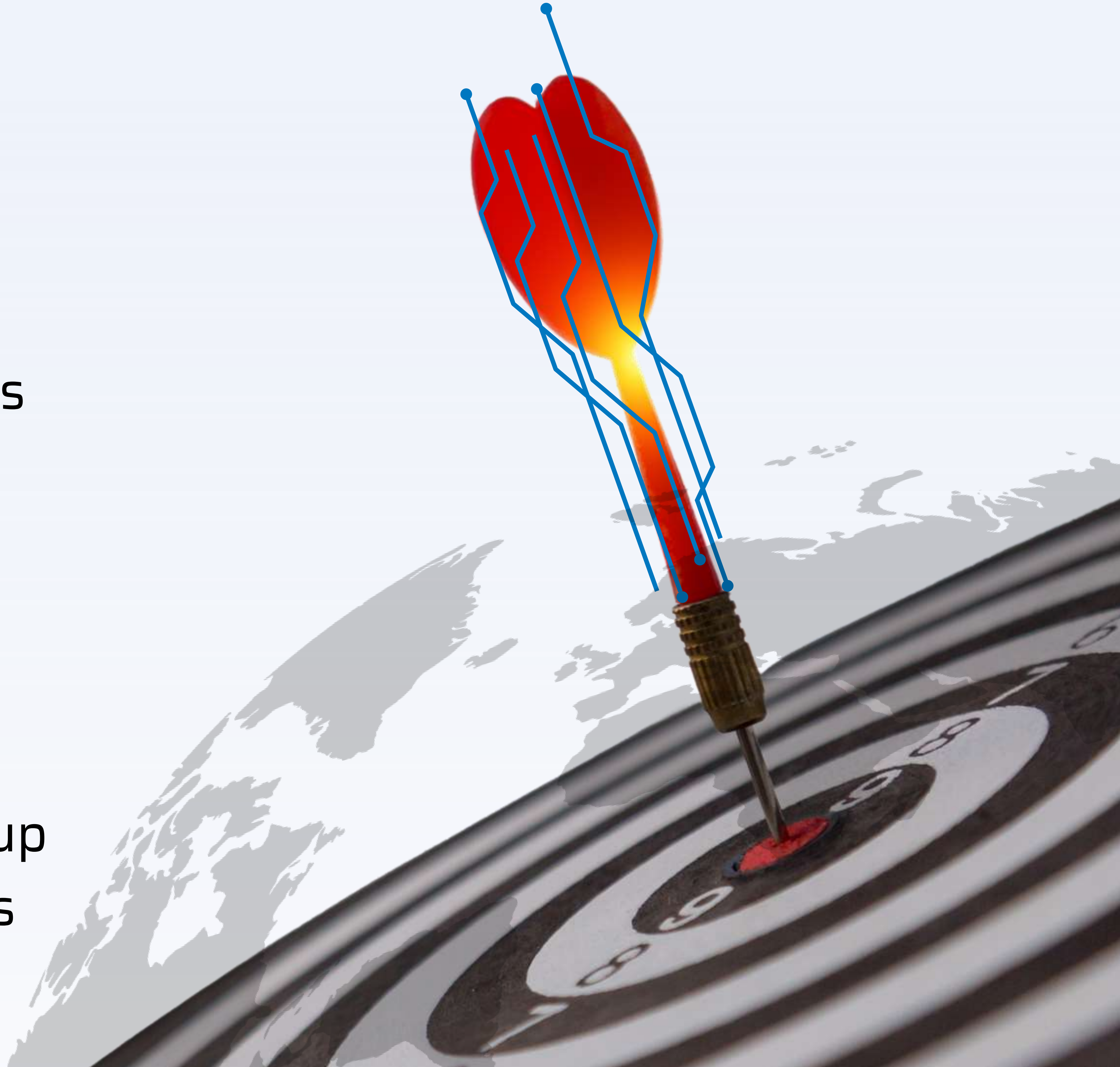
Threats: Highly autonomous robots could act in unpredictably ways

IMPACT OF EMERGING TECHNOLOGIES ON THE WORLD

- **Economic Impact and New Industries:** Technologies drive economic growth and job creation. For instance, AI is projected to add $15.7 trillion to the global economy by 2030.

- **Job Creation vs. Displacement:** While some jobs may be displaced, new roles will emerge. It's estimated that 75 million jobs may be lost, but 133 million new roles could be created.

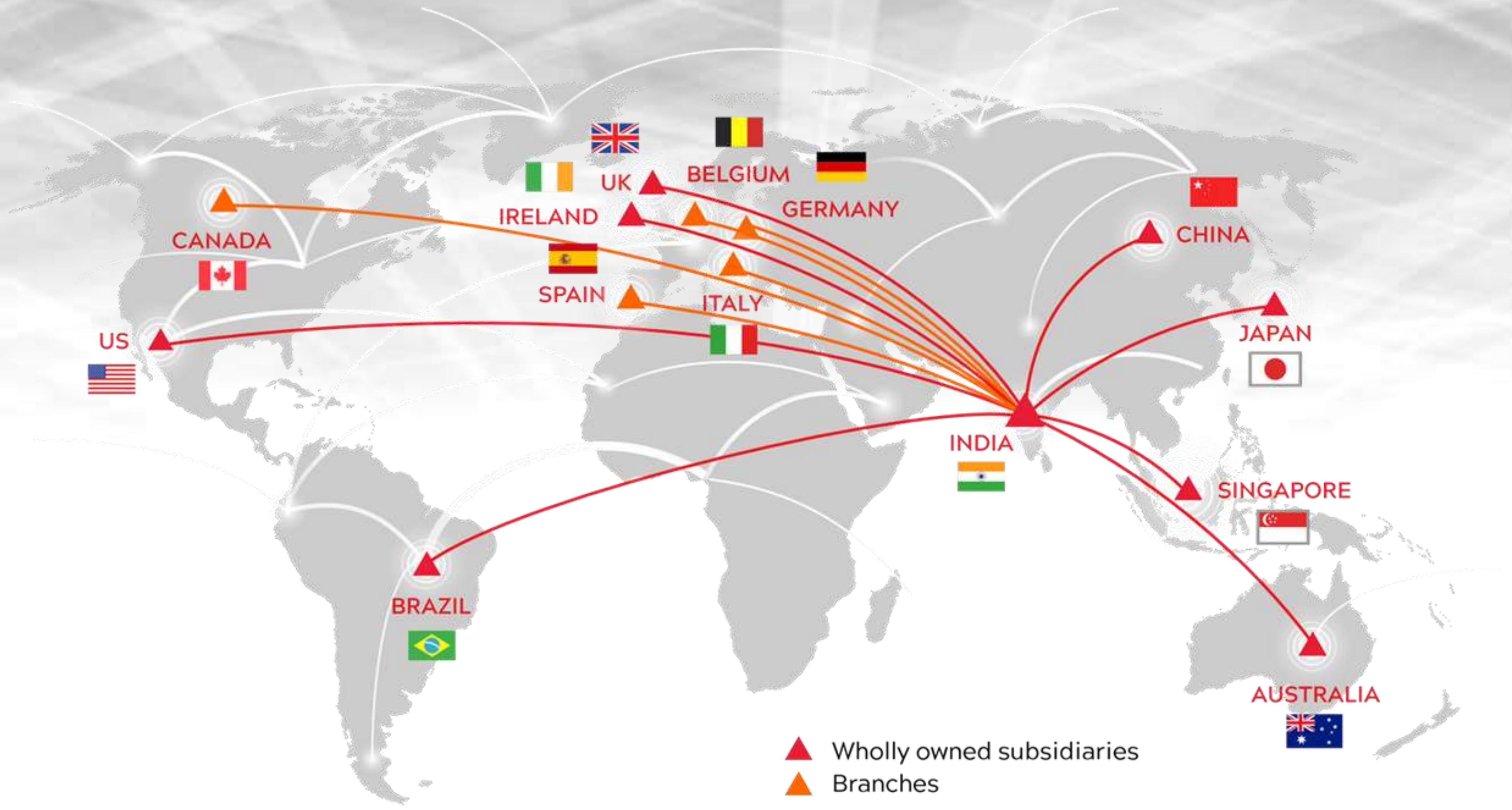
- **Environmental and Societal Effects:** Technologies can reduce carbon emissions by up to 20% by 2030 but also raise privacy concerns and contribute to the digital divide.



AI First Strategy

allied digital®

IT managed.Responsibly.



40 years of Legacy in IT Innovation

Cloud Services

Digital Engineering

Software Services

Cybersecurity

Infrastructure Management

Workplace Services

DEEP DIVE – AI DRIVEN SECURITY THREATS

- **AI-Driven Social Engineering Attacks**

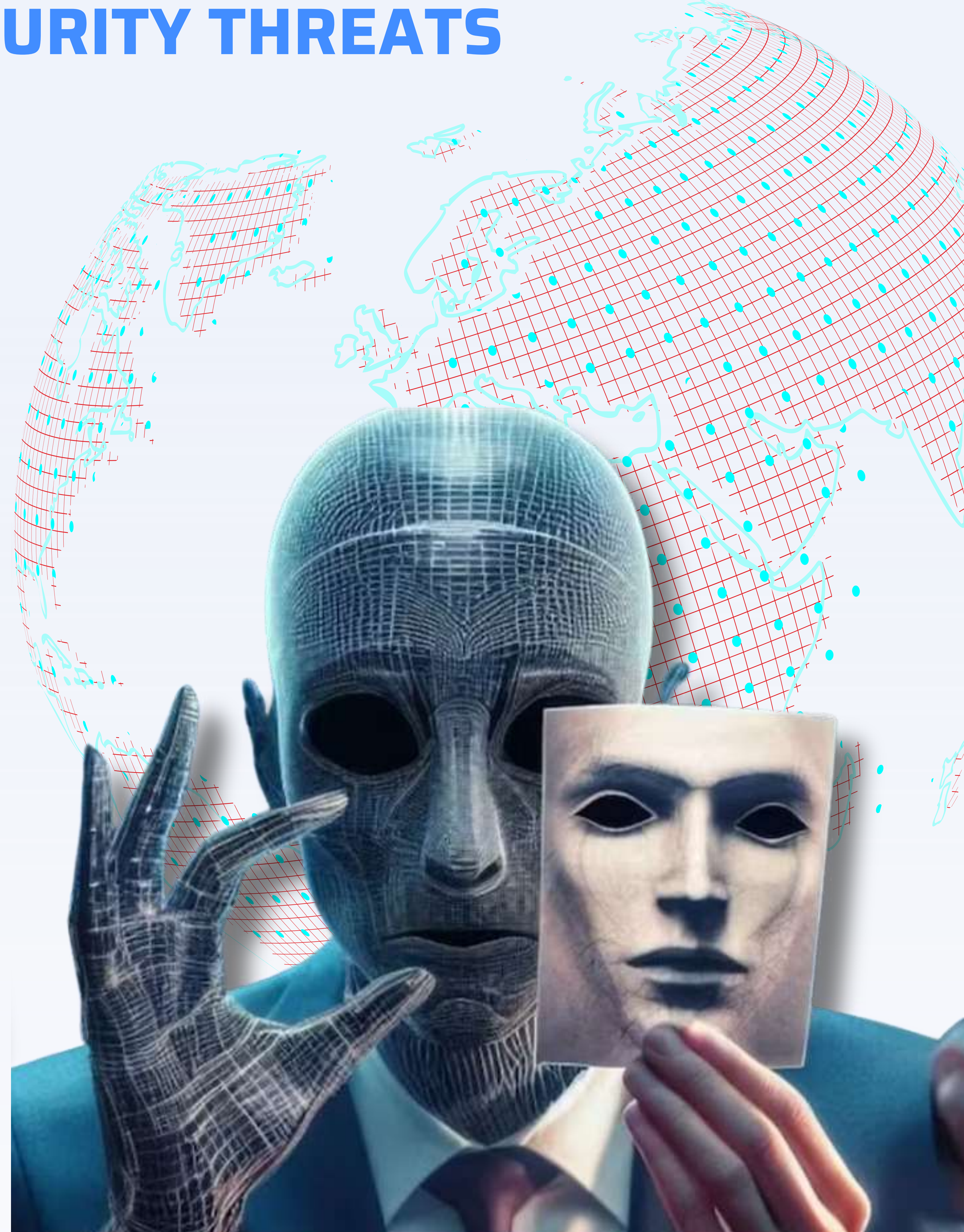
Threat: AI enhances the precision and effectiveness of social engineering tactics like phishing.
Example: AI can scrape data from social media and public sources to craft highly personalized phishing emails, increasing the likelihood of success.

- **Deepfakes**

Threat: AI-generated fake videos and audio recordings that are indistinguishable from reality.
Example: Deepfakes can be used to impersonate executives during video calls, leading to unauthorized and fraudulent transactions.

- **Adversarial AI/ML**

Threat: Exploiting AI systems by feeding them deceptive or misleading data.
Example: An attacker could manipulate traffic sign images to mislead and confuse autonomous vehicles, causing potential accidents



DEEP DIVE – AI DRIVEN SECURITY THREATS

- **AI-Enhanced Phishing Attacks**

Threat: Automating and refining phishing campaigns with AI to increase their effectiveness.
Example: AI can generate realistic phishing messages that are more likely to deceive even the most cautious recipients.

- **Malicious Generative AI**

Threat: Leveraging AI models to create harmful content, such as malicious code or disinformation.
Example: AI can be used to generate fake news articles or malicious code, spreading misinformation or causing significant harm.

- **AI-Optimized Ransomware Attacks**

Threat: AI can enhance ransomware tactics by identifying and targeting the most valuable data.
Example: AI algorithms can prioritize high-value targets within a network, maximizing the impact and damage of ransomware attacks.

DEEP DIVE – AI –DATA SECURITY – MITIGATING RISKS

- **Robust AI Models**: Developing AI systems that can detect and respond to adversarial inputs.
- **Continuous Monitoring**: Implementing real-time monitoring to identify and mitigate AI-driven threats.
- **Employee Training**: Educating employees about the risks and signs of AI-driven attacks.
- **Advanced Security Tools**: Using AI-based security tools to detect and prevent cyber attacks.

DEEP DIVE – AI –MODEL RELATED RISKS & MITIGATIONS

Adversarial Attacks

Attackers can subtly alter input data to deceive AI models, causing incorrect outputs.

Example: Tiny modifications to an image can lead to significant misclassifications in image recognition systems.

Mitigation: Enhance model resilience by developing defenses against adversarial inputs and incorporating adversarial training techniques.

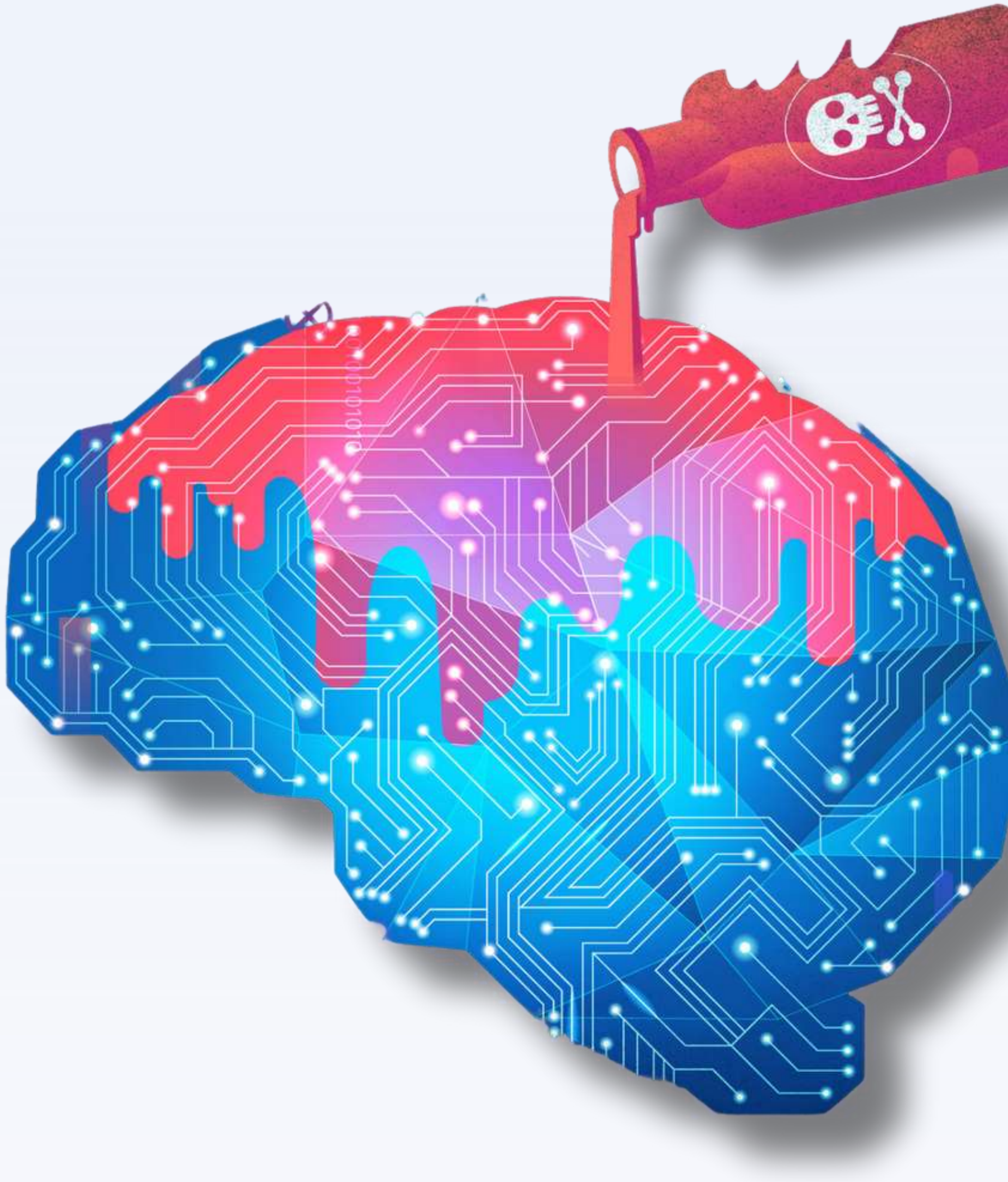
DEEP DIVE – AI -MODEL RELATED RISKS & MITIGATIONS

Data Poisoning

Malicious data is injected into the training set, corrupting the model's performance.

Example: Introducing biased or erroneous data to skew predictions or misguide the model.

Mitigation: Implement rigorous data validation, cleaning processes, and anomaly detection to safeguard training datasets.



DEEP DIVE - AI -MODEL RELATED RISKS & MITIGATIONS

Model Inversion Attacks

Attackers can extract sensitive information from the model’s outputs, potentially revealing private data.

Example: Inferring personal details used in training by analyzing the model's responses.

Mitigation: Employ differential privacy techniques to anonymize and protect sensitive information in the training data.

DEEP DIVE – AI –MODEL RELATED RISKS & MITIGATIONS

Model Stealing

Competitors can recreate proprietary models by querying and reverse-engineering the model's outputs.

Example: Replicating a patented model without access to the original data or architecture.

Mitigation: Limit the amount of detail provided by the model and monitor usage patterns for unusual or suspicious activity.

DEEP DIVE - AI -MODEL RELATED RISKS & MITIGATIONS

Bias and Fairness

AI models can inherit and perpetuate biases present in the training data, leading to unfair outcomes.

Example: Discriminatory practices in automated hiring systems due to biased data.

Mitigation: Regularly audit models for bias, ensure diverse and representative training datasets, and implement fairness-enhancing interventions.

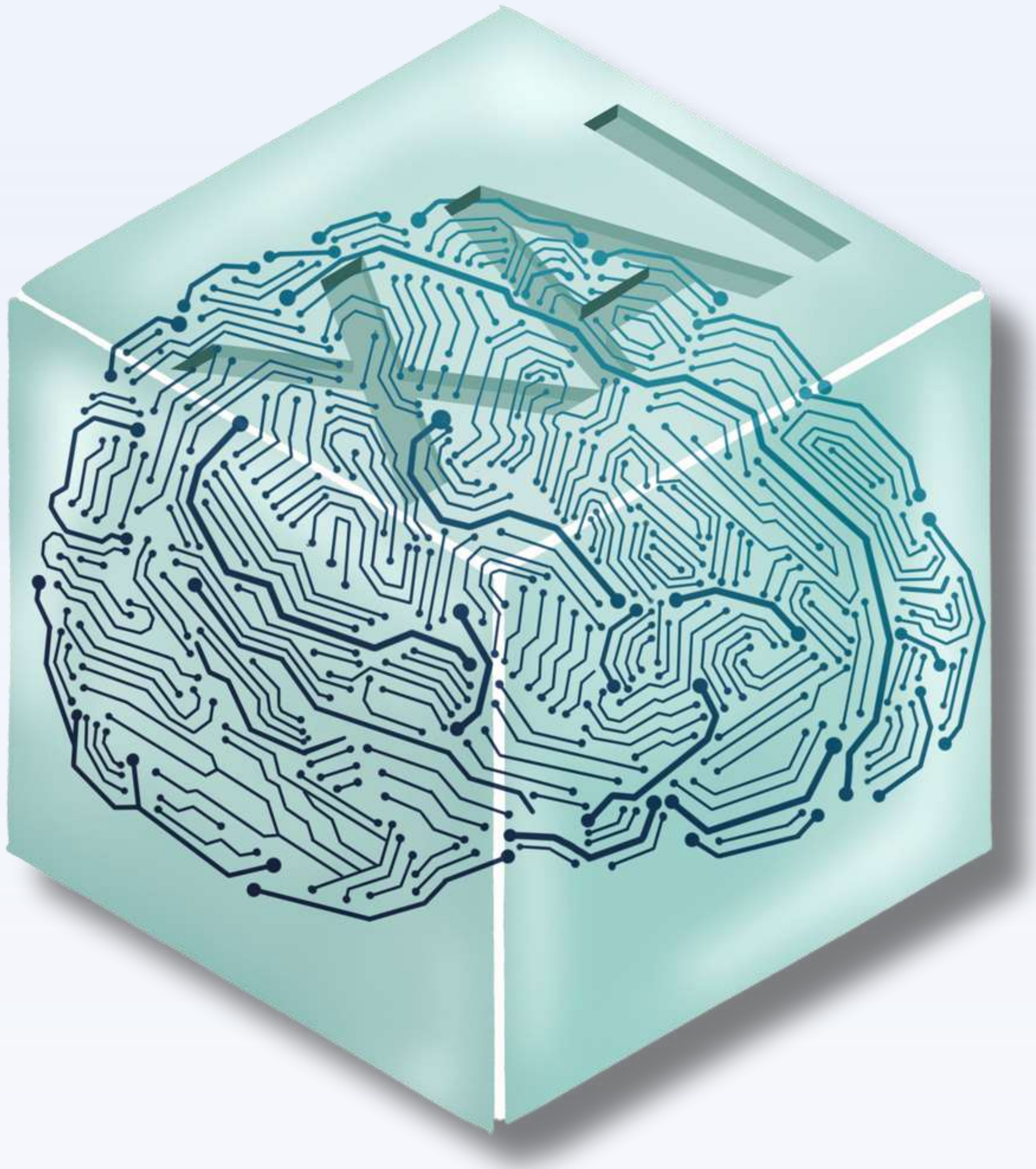
DEEP DIVE – AI –MODEL RELATED RISKS & MITIGATIONS

Explainability and Transparency

Many AI models operate as "black boxes," making it difficult to understand their decision-making processes.

Example: Deep neural networks often provide accurate results but lack transparency in how they reach those conclusions.

Mitigation: Develop and integrate explainable AI (XAI) techniques to make model decisions more understandable and interpretable.



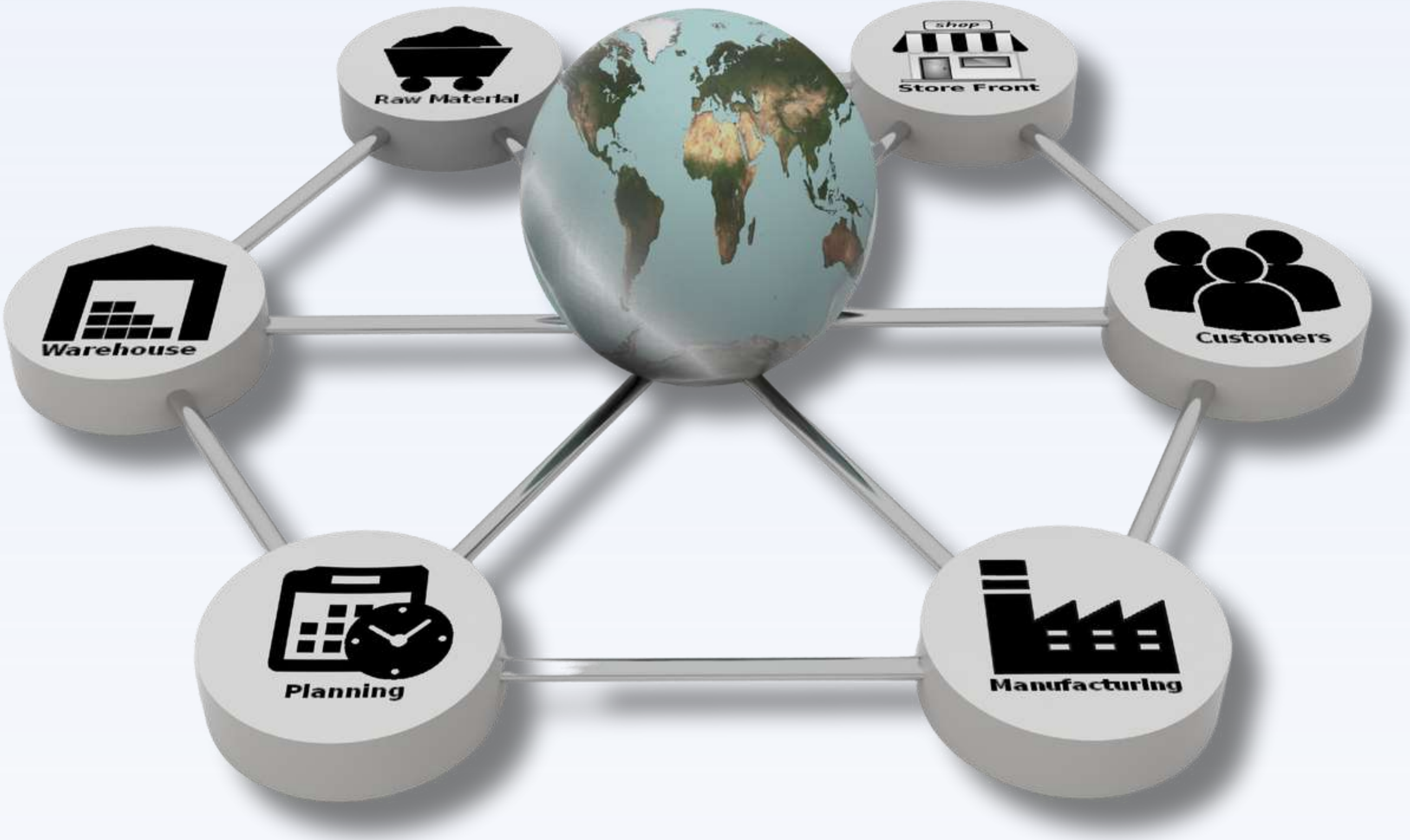
DEEP DIVE – AI -MODEL RELATED RISKS & MITIGATIONS

Security of AI Supply Chain

Ensuring the security and integrity of all components and data sources used in AI systems.

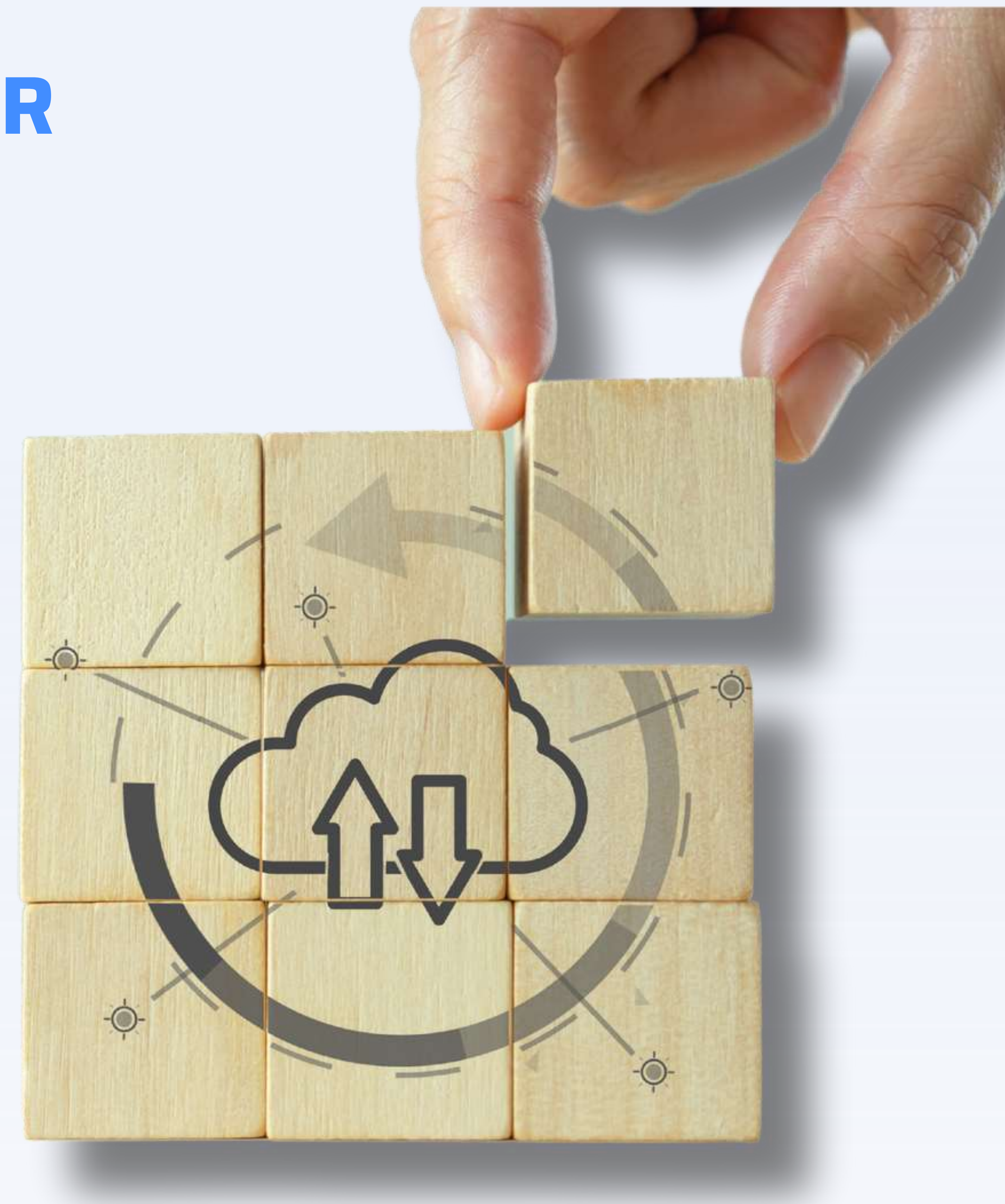
Example: Compromised third-party libraries or datasets can introduce vulnerabilities or malicious code.

Mitigation: Conduct thorough security assessments of all components, maintain rigorous supply chain management, and vet all external sources.



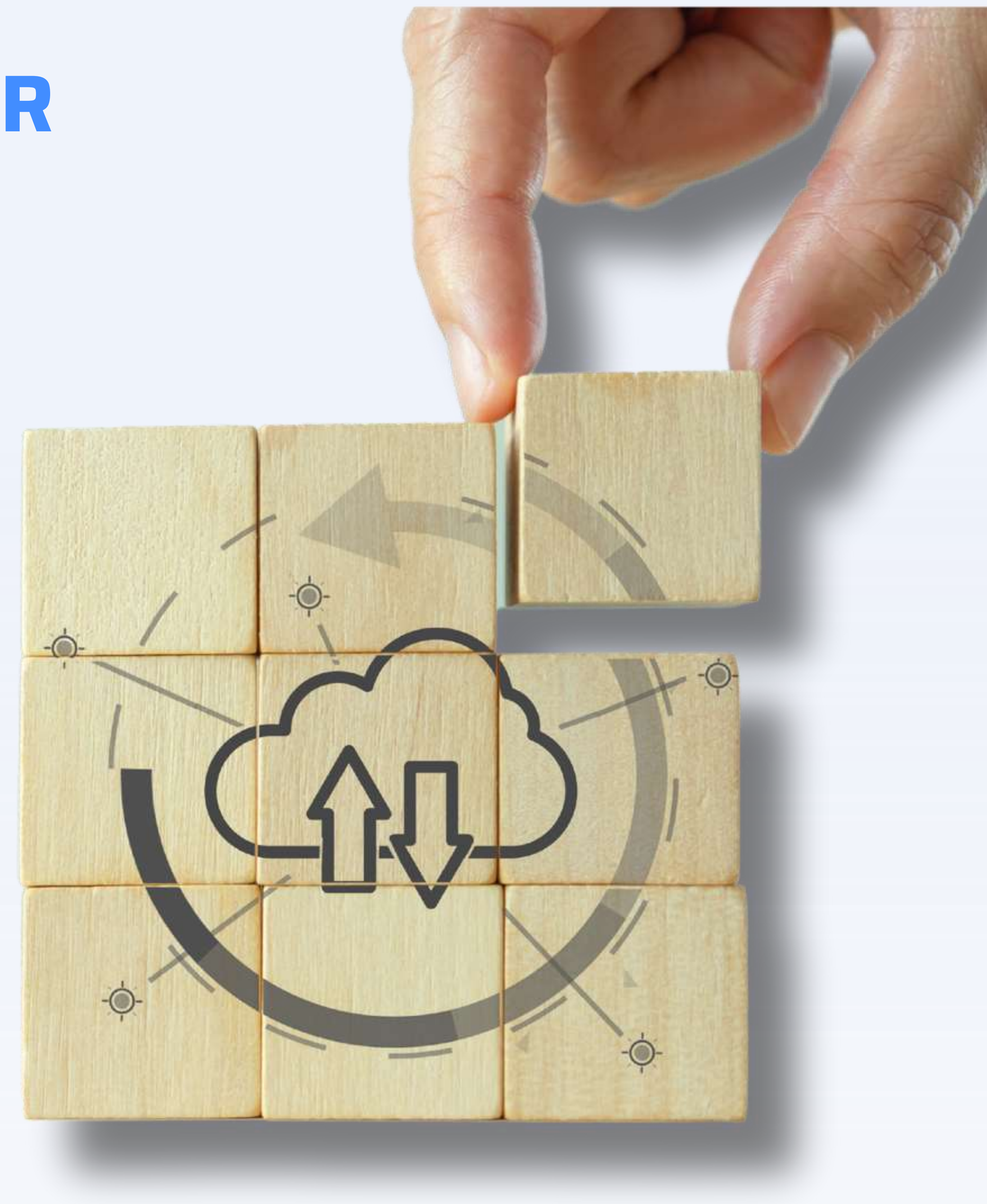
DATA CHALLENGES FACING THE PUBLIC SECTOR

- **Securing Data:** Protecting personally identifiable and classified information requires strict control over storage, access, and sharing.
- **Staying Within Budget:** Limited budgets constrain the acquisition of tools and skilled staff necessary for maintaining data quality, security, and privacy.
- **Changing Regulations:** Compliance with evolving privacy laws and regulations, including those with extraterritorial reach, is essential.

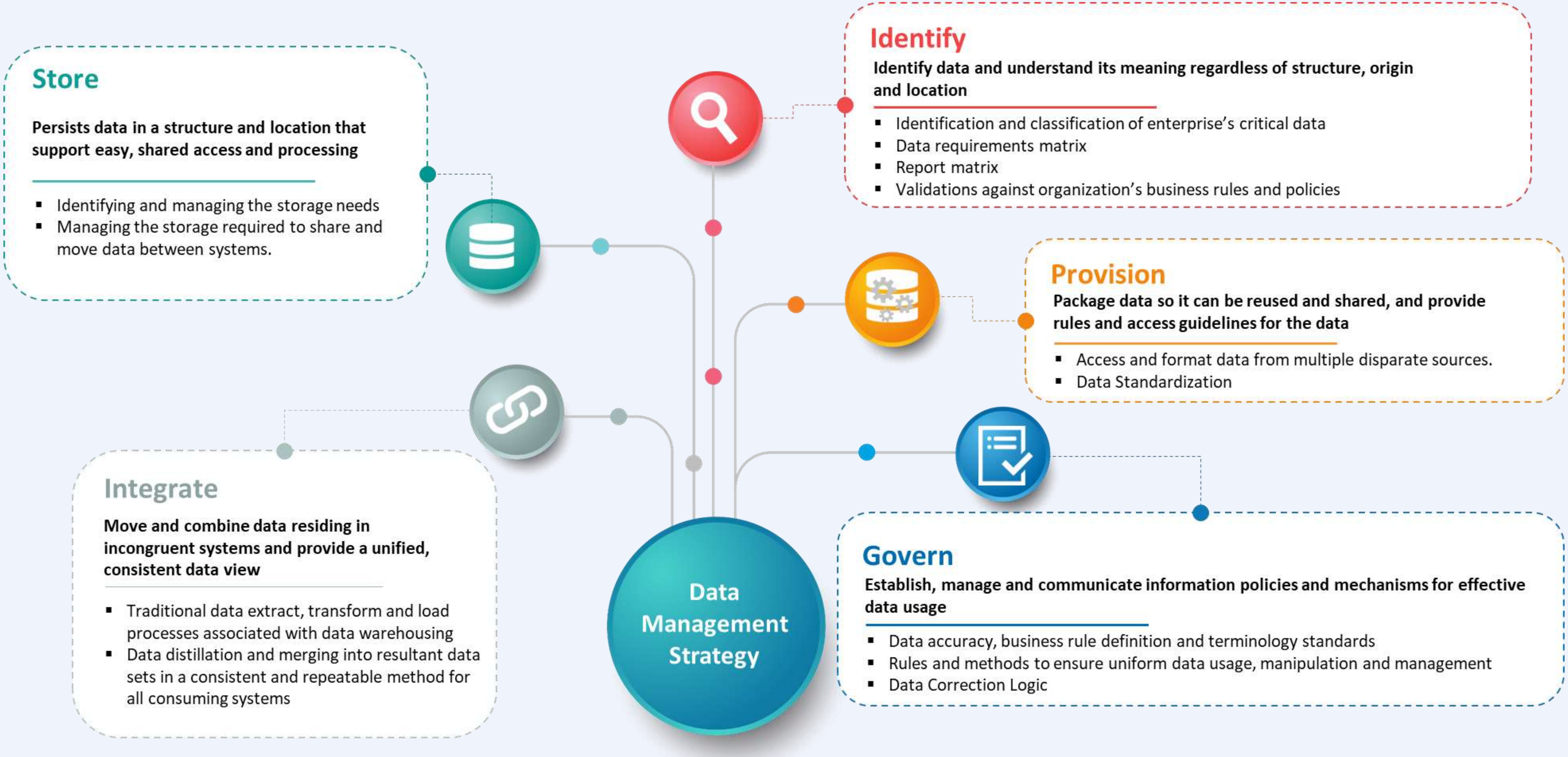


DATA CHALLENGES FACING THE PUBLIC SECTOR

- **Scattered Data:** Fragmented and dispersed datasets make it difficult to track and manage data across various registers.
- **Inaccessible, Paper-Based Systems:** Legacy paper records increase costs and administrative burdens, complicating data access and use.
- **Preventing Collaboration:** Data silos and paper-based systems hinder inter-agency coordination and data sharing.



DATA MANAGEMENT & GOVERNANCE STRATEGY



Store

Persists data in a structure and location that support easy, shared access and processing

- Identifying and managing the storage needs
- Managing the storage required to share and move data between systems.

Identify

Identify data and understand its meaning regardless of structure, origin and location

- Identification and classification of enterprise's critical data
- Data requirements matrix
- Report matrix
- Validations against organization's business rules and policies

Provision

Package data so it can be reused and shared, and provide rules and access guidelines for the data

- Access and format data from multiple disparate sources.
- Data Standardization

Integrate

Move and combine data residing in incongruent systems and provide a unified, consistent data view

- Traditional data extract, transform and load processes associated with data warehousing
- Data distillation and merging into resultant data sets in a consistent and repeatable method for all consuming systems

Govern

Establish, manage and communicate information policies and mechanisms for effective data usage

- Data accuracy, business rule definition and terminology standards
- Rules and methods to ensure uniform data usage, manipulation and management
- Data Correction Logic

WHAT WE MUST DO?

01

REGULATORY COMPLIANCE

Organizations must comply with various regulations that govern data security and privacy. This includes understanding and adhering to laws like GDPR, CCPA, and other regional data protection regulations

02

FRAMEWORKS AND STANDARDS

Implementing established frameworks and standards, such as those provided by NIST, can help organizations manage cybersecurity risks effectively. These frameworks offer guidelines on securing IoT devices, managing privacy in immersive technologies, and more

WHAT WE MUST DO?

03

BIAS AND FAIRNESS

Ensuring that emerging technologies do not introduce or perpetuate biases is essential. This involves creating unbiased algorithms and ensuring that data used in these technologies is representative and fair

04

GOVERNANCE FRAMEWORKS

Developing a robust governance framework that includes policies, procedures, and controls to manage data security is vital. This framework should be adaptable to the evolving nature of emerging technologies allied digital®

IT managed.Responsibly.

Allied Digital Services Limited

www.allieddigital.net | consult@allieddigital.net