The role of tools and frameworks

Trustworthy AI Standardization Workshop

Singapore, 2023-10-27

Dr Martin Saerbeck

Add value.
Inspire trust.

AI Quality is the key for organizations to leverage the full potential of AI while managing the risks

AI has found successful applications across all significant industry sectors, acting as a disruptive force that **reshapes organizational structures and competitive landscapes**.

The expansive deployment of AI and its potential risks to individuals, society, and the environment, have **spurred governments into regulating AI usage**.

Shift in focus from AI development and AI deployment to **compliance, reputational, technical, and legal risks**.

What is AI Quality?

It refers to the degree to which an AI System satisfies requirements throughout its life cycle

The assurance of AI Quality overcomes key challenges for adopters and developers

Complying with regulation

- Do I understand my roles and responsibilities?
- Do I understand my exposure, liabilities?
- Is the AI system and its usage compliant?

AI Quality is imperative for systems to align with industry standards and regulations

Demonstrating responsible use of AI

- Can I demonstrate the AI system does not violate expected ethical principles?
- Can my AI system cause harm?
- Is the AI system aligned with the values of my organisation?

AI Quality helps ensure and demonstrate that AI systems are ethical

Scaling AI

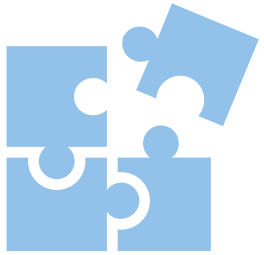
- Is the AI system fit and trustworthy for large-scale deployment?
- Is my organisation prepared for widespread adoption?
- Are all risks mitigated comprising safety, security, legal, ethics, performance, and sustainability?

AI Quality enables organisations to utilise the full potential of AI while managing the associated risks

A unified approach to AI quality

Harmonized and Specific

Taps on standards, regulations, and other frameworks that are relevant for specific AI solutions, and does not follow a rigid, fixed approach.



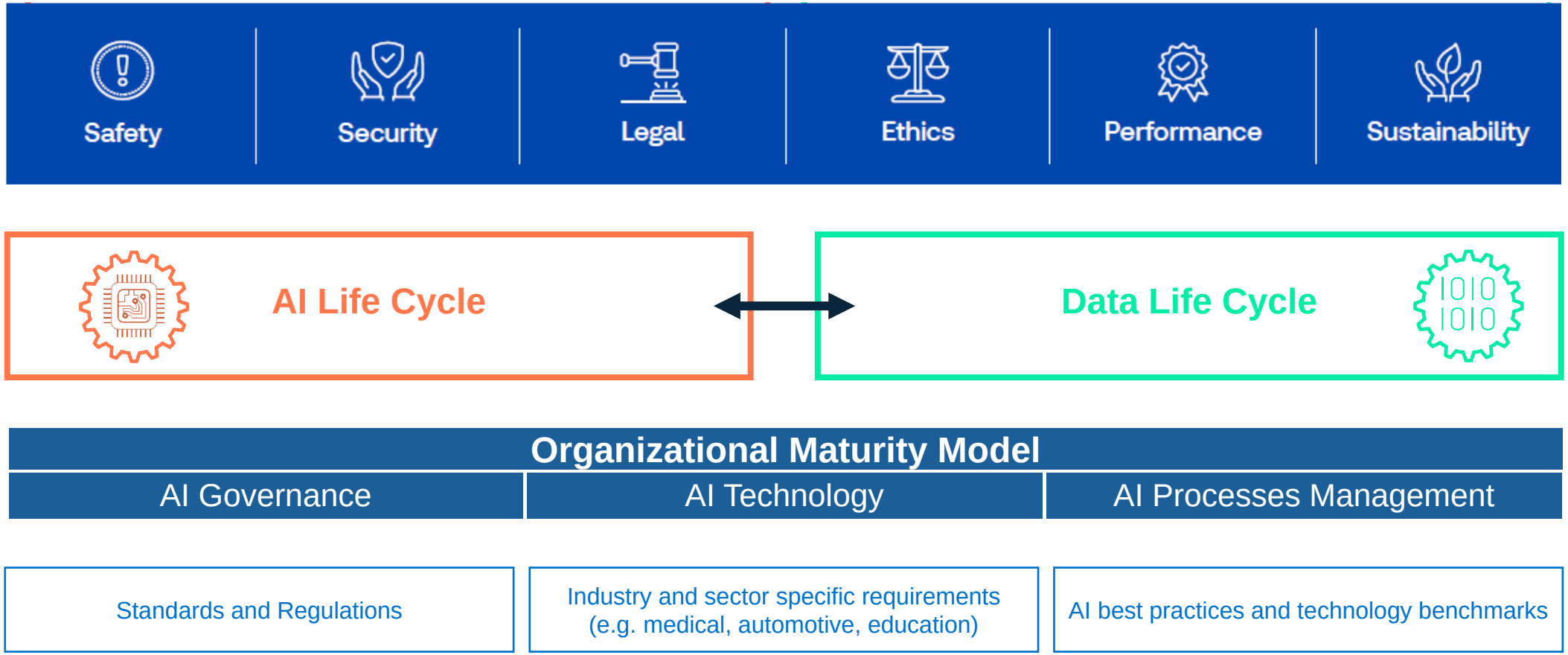
Comprehensive and Sufficient

Covers the entire spectrum of an AI Quality Management System (AIQMS), whereas other frameworks and providers focus only on specific aspects, e.g., governance, technical testing, ethical aspects.

Versatile

Can be utilised equally for advisory, assessment, and certification purposes.

Harmonized quality approach



Element 1: Quality Profile

6 pillars include all AI risks

Safety

Has the AI system the potential to directly or indirectly harm anyone/anything?

- Predictability
- Testability
- Traceability
- ...

Legal

Is the AI system and usage compliant with regulations?

- Obligations
- Governance
- Auditability
- ...

Performance

Is the system fit for use? Are unsubstantiated claims made?

- Suitability
- Efficiency
- Reliability
- ...

Security

Does the AI system increase cybersecurity risks?

- Confidentiality
- Authenticity
- Recoverability
- ...

Ethics

Does it violate accepted ethical principles for impacted stakeholders?

IEEE CERTIFAIED AI ETHICS

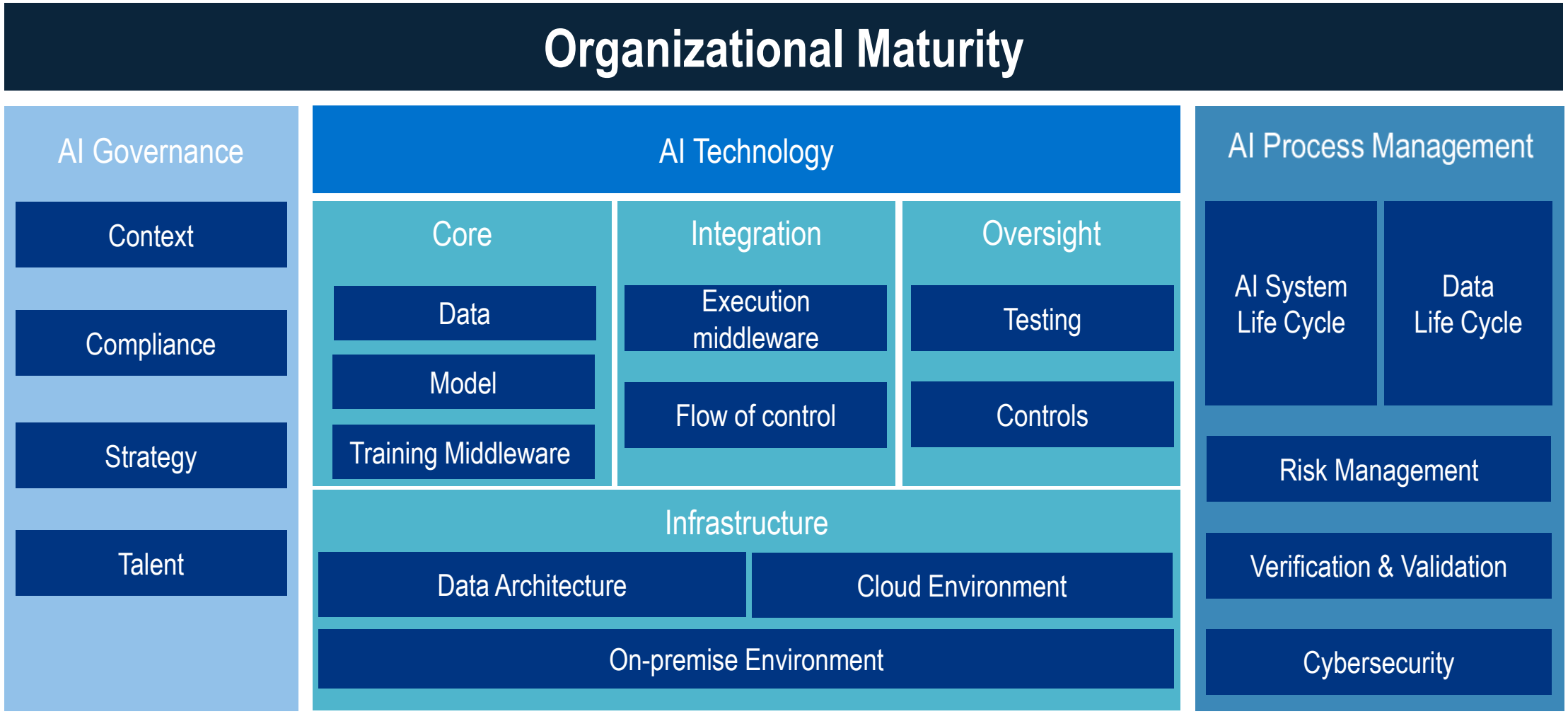
- Transparency
- Non-discrimination
- Accountability
- ...

Sustainability

Has the development or operation been conducted with environmental considerations?

- Resource footprint
- Proportionality
- Reusability
- ...

Element 3: Process, Technology, Organisation



Methodology to identify and assess quality requirements

AI Quality Model
Risk Assessment
Life cycle process audits
Product Tests

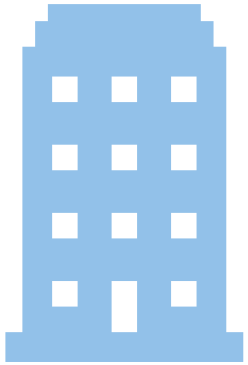
AI Application and Intent → **AI Quality Framework** → **Company specific quality profile**

Meet requirements for compliance and market access
Identify risks when adopting AI at scale
Demonstrate responsible us of AI

Standards
Regulations
Best Industry Practices

Contextualised quality and risk profile
Organisational maturity readiness profile
Roadmap to quality management system

Use Case - Assessing AI System of AV Software



The Company

The Company is a software solution provider to drive automated vehicles

The Product

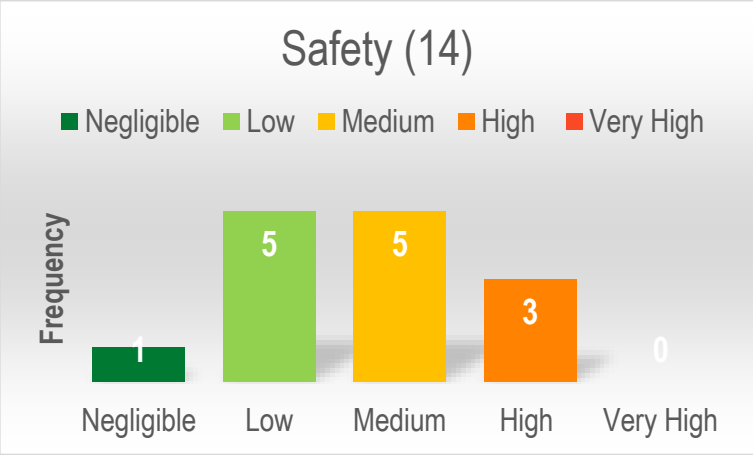
Autonomous vehicles use synchronized sensors to detect objects through traditional and data-driven algorithms.

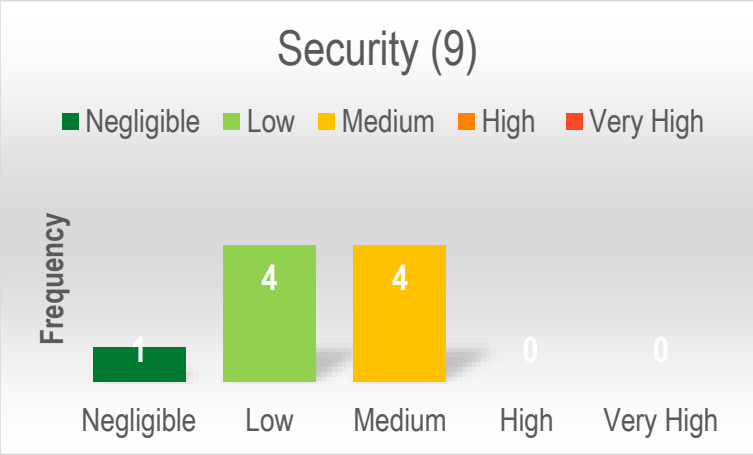
Neural networks aid in detecting drivable space.

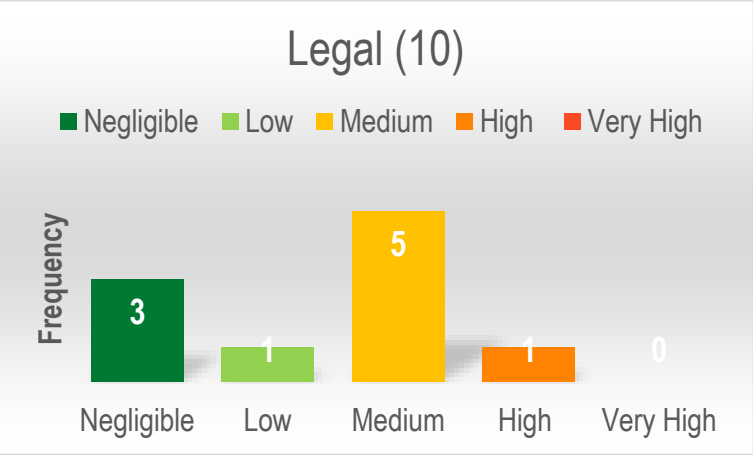
The Challenge

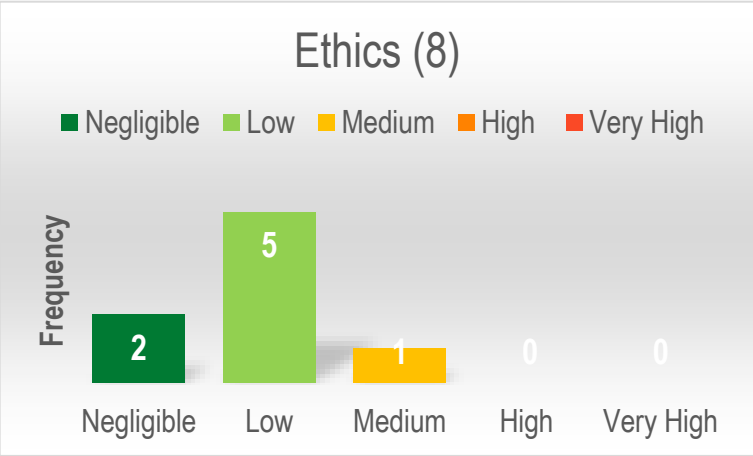
Evaluate the preparedness of the organization to ensure the quality of their AI system

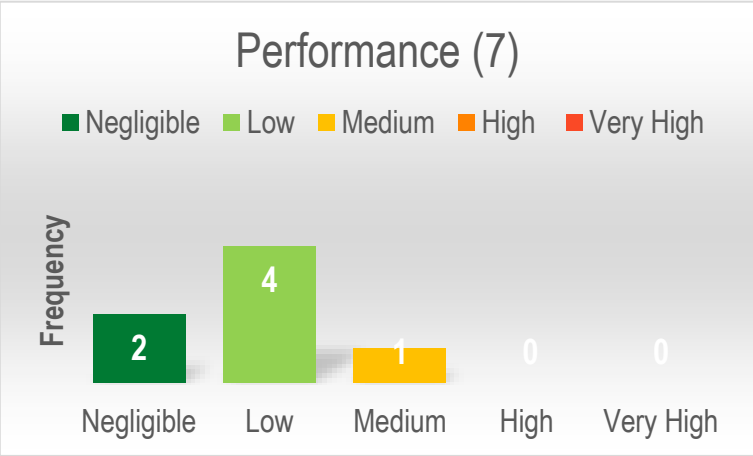
Risk profiling over all quality pillars

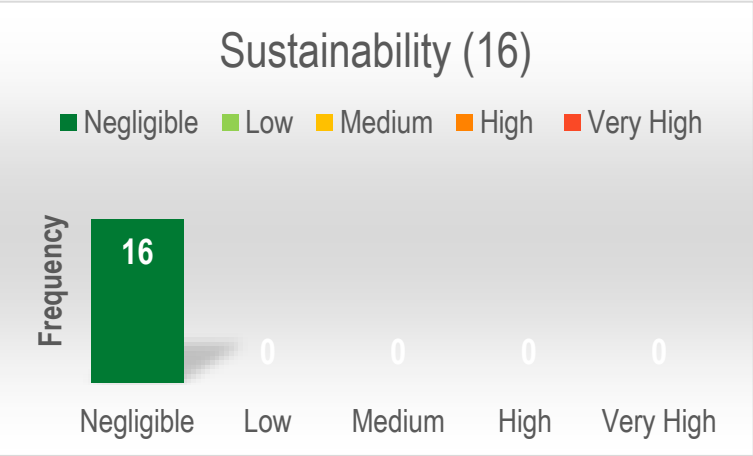








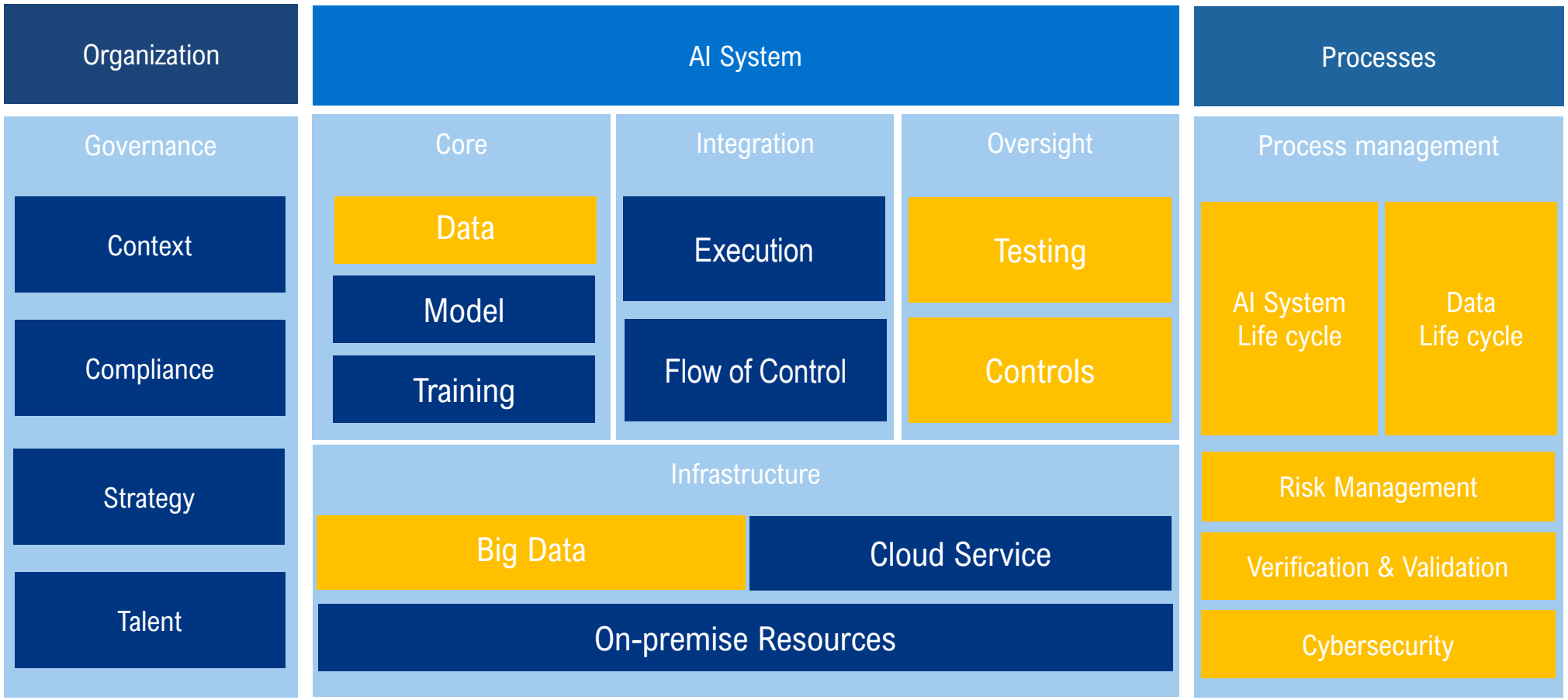




Results are for illustration only

Organisational maturity analysis

The operational maturity analysis identifies areas that need to be addressed to assure the quality of the respective AI application.



Results are for illustration only

Conclusion

1. **AI Evolution**
   From development to trustworthiness, AI is now central to business strategy

2. **Core Challenges**
   Compliance, Responsible Use, Scaling AI

3. **Quality Assurance**
   Vital for AI trustworthiness and addressing challenges

4. **Harmonized Approach**
   Navigate the diverse AI landscape with standards and best practices

5. **Frameworks and tools**

Risk	Safety, security, ethics, legal, performance, and sustainability
Life Cycle	AI System Life Cycle, Data Life Cyle, DevOps
Governance	Process, Technology, and Organization
Controls	Testing, Monitoring, Audit, Compliance management

6. **Way forward**
   A unified AI approach ensures trust, competitiveness, and reliability

Thank you

Dr. Martin Saerbeck
CTO, TUV SUD Digital Service
andreas.hauser@tuvsud.com