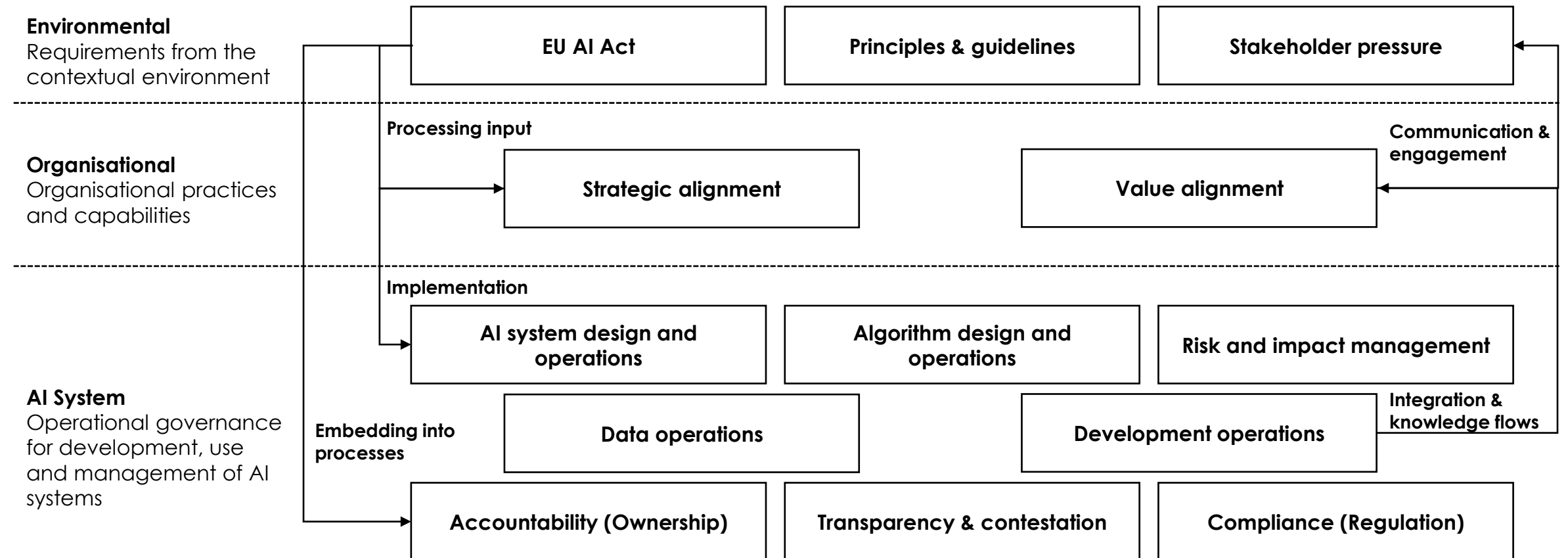# EU AI Act Governance Model

JUNE 2023

For Public Use

# Target model of organizational AI governance

Hourglass metaphor denotes the flow of governance requirements from the environmental layer to AI systems through the mediating organizational layer.

Environmental
Requirements from the contextual environment

Organisational
Organisational practices and capabilities

AI System
Operational governance for development, use and management of AI systems

| EU AI Act | Principles & guidelines | Stakeholder pressure |

Processing input

Communication & engagement

| Strategic alignment | | Value alignment |

Implementation

| AI system design and operations | Algorithm design and operations | Risk and impact management |

Embedding into processes

Integration & knowledge flows

| Data operations | Development operations |

| Accountability (Ownership) | Transparency & contestation | Compliance (Regulation) |

Framework

To successfully address the proper management of EU AI Act compliance a number of components operate in a coordinated manner and in line with the defined strategy and the following framework that defines its key elements.
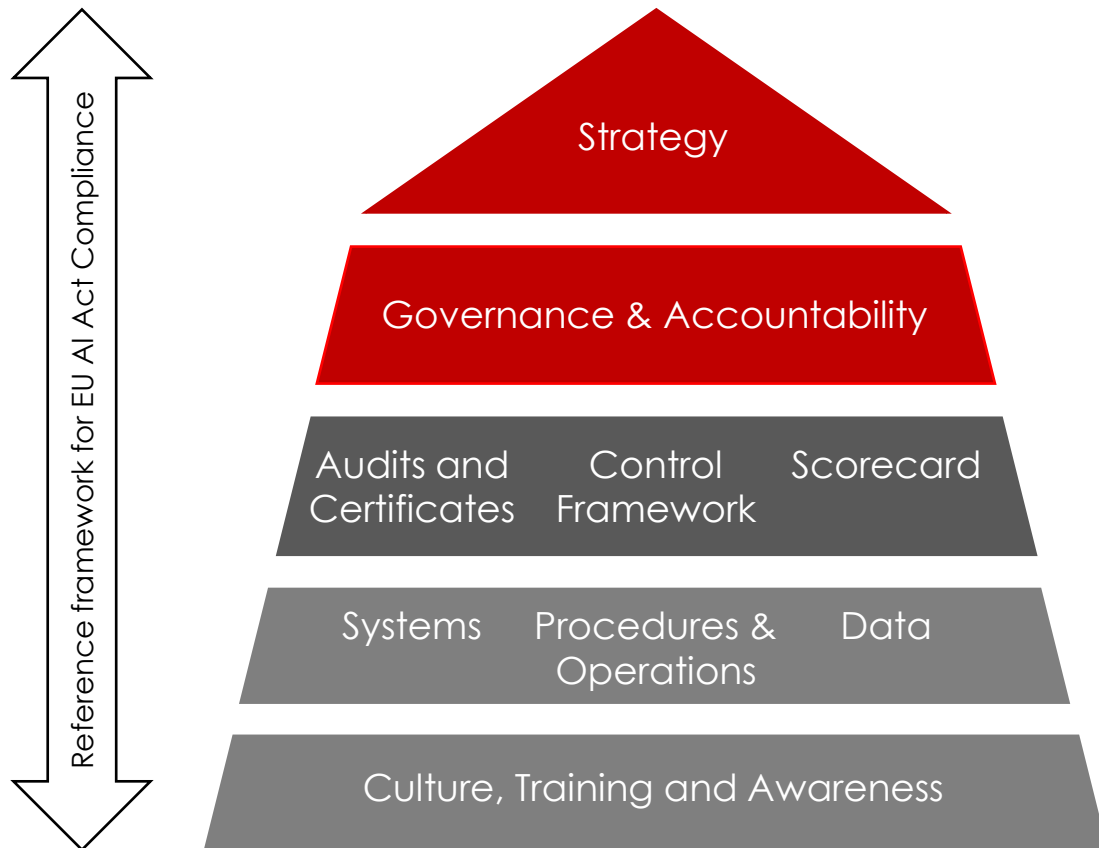
Governance Layer
- Governance structure which organises and appropriately establishes the roles and responsibilities.
- Policies and general framework to all components of the reference framework.

Monitoring and Control Layer
- Control model based on 3 LoD.
- Scorecard that enable the decision making.
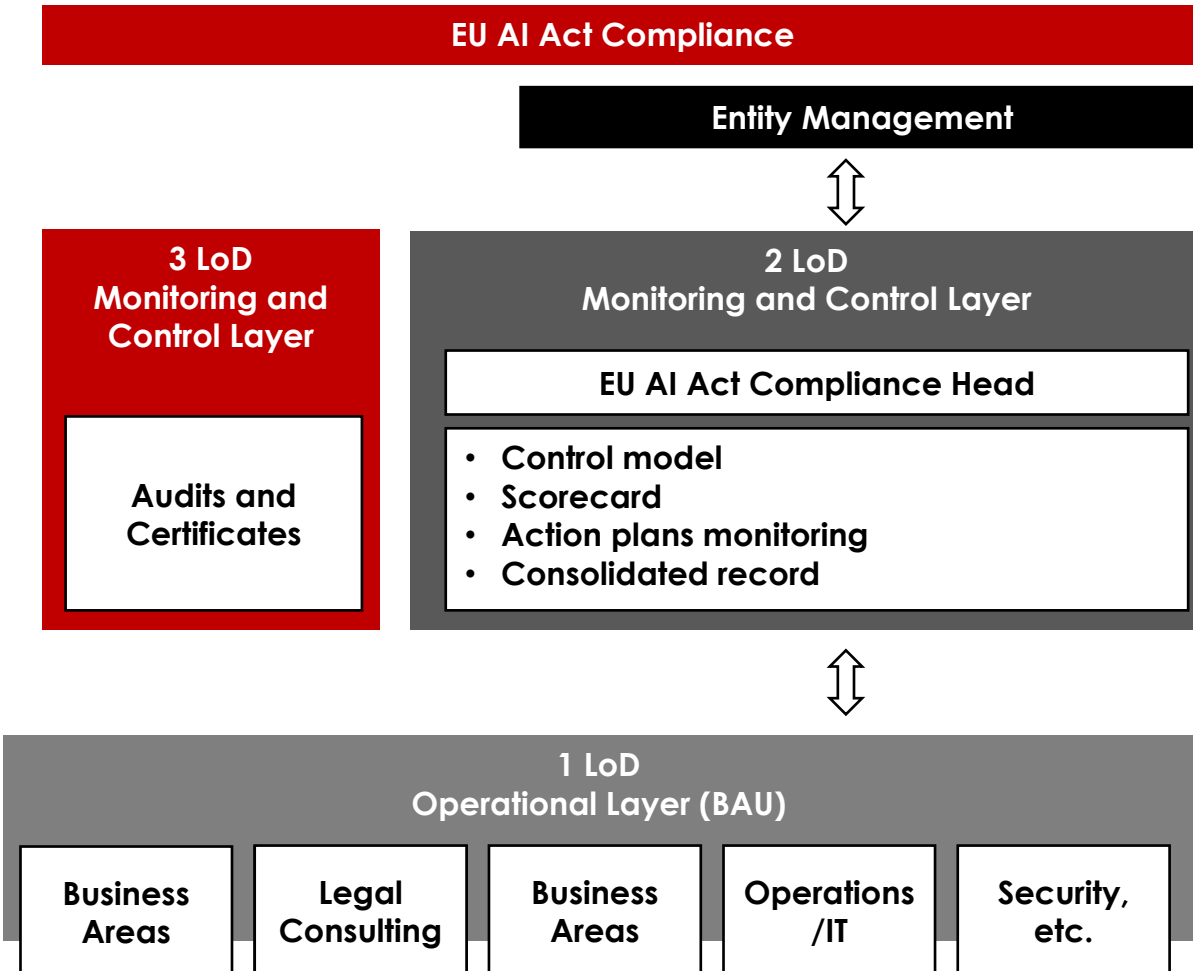- Following up of the mitigating actions plans

Operational Layer
- Set of processes, procedures and operations that provide operational support to EU AI Act compliance. They must be properly coordinated with the monitoring and control layer, in accordance with the governance layer.

Reference framework for EU AI Act Compliance

Strategy

Governance & Accountability

Audits and Certificates   Control Framework   Scorecard

Systems   Procedures & Operations   Data

Culture, Training and Awareness

Lines of Defence (LoD)

The EU AI Act governance model at a entity-level fits into the corporate/group governance level.

EU AI Act Compliance

Entity Management

⇕

3 LoD Monitoring and Control Layer	2 LoD Monitoring and Control Layer
Audits and Certificates	**EU AI Act Compliance Head** • **Control model** • **Scorecard** • **Action plans monitoring** • **Consolidated record**

⇕

1 LoD
Operational Layer (BAU)

Business Areas	Legal Consulting	Business Areas	Operations /IT	Security, etc.

3 LoD
Independent view on the organization compliance degree of the AI system management, taking as a reference the EU AI Act, as well as existing policies and procedures.

2 LoD
Monitoring of privacy activities management to be carried out by the 1 LoD. This 2 LoD must ensure that AI risks are managed in accordance with the risk appetite formulated by the entity management and will promote a solid culture of risk and compliance across the organization.
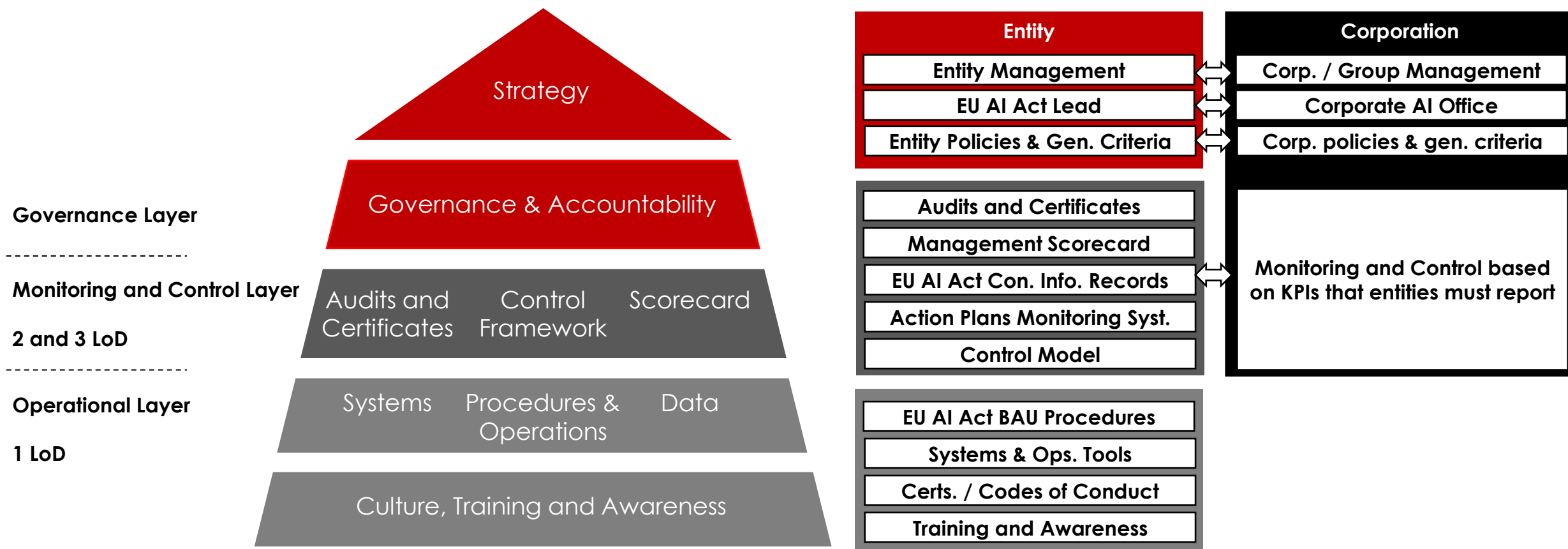
1 LoD
Business and support units, as responsible for the execution of the business as usual (BAU) activities according to the defined policies and procedures. They must be properly trained and aware about privacy matters and existing policies and procedures and provided with sufficient resources to do so effectively.

4

Lines of Defence (LoD)

The EU AI Act governance model at a entity-level fits into the corporate/group governance level.

Strategy

Governance & Accountability

Governance Layer

- - - - - - - - - - - - - - - - - -

Monitoring and Control Layer

2 and 3 LoD

- - - - - - - - - - - - - - - - - -

Audits and Certificates   Control Framework   Scorecard

Operational Layer

1 LoD

Systems   Procedures & Operations   Data

Culture, Training and Awareness

Entity	Corporation
Entity Management	**Corp. / Group Management**
EU AI Act Lead	**Corporate AI Office**
Entity Policies & Gen. Criteria	**Corp. policies & gen. criteria**

Entity	Corporation
Audits and Certificates	**Monitoring and Control based on KPIs that entities must report**
Management Scorecard	
EU AI Act Con. Info. Records	
Action Plans Monitoring Syst.	
Control Model	

EU AI Act BAU Procedures
Systems & Ops. Tools
Certs. / Codes of Conduct
Training and Awareness

EU AI Act Heads

Three main figures display the highest level of responsibility in terms of EU AI Act compliance.

EU AI Act Compliance	Champion
Local	

Local

EU AI Act Compliance	Champion

EU AI Act maximum authority
• Point of contact for the regulator and AI system stakeholders
• Cooperation with the regulator
• AI system advice
• Control and monitoring
• Training
• FRIAs advice
• Realization of prior consultations to the Supervisory Authority
• Monitoring of processing activities record
• Assess on AI system breach communication
• Assess on third-party management
• Monitoring of AI system use exercise
	SME in the unit or entity
	• Internal point of contact as first level of support.
	• Channel for resolving and/or addressing questions and support requests:
	    • To the corporate AI office, in the case of units and corporate entities.
	    • To the AI Officer/Head/Heads of the jurisdiction, in the case of other entities.
	• Responsible for the internal distribution of criteria, procedures, and other instructions

Corporate AI Office

Corporate

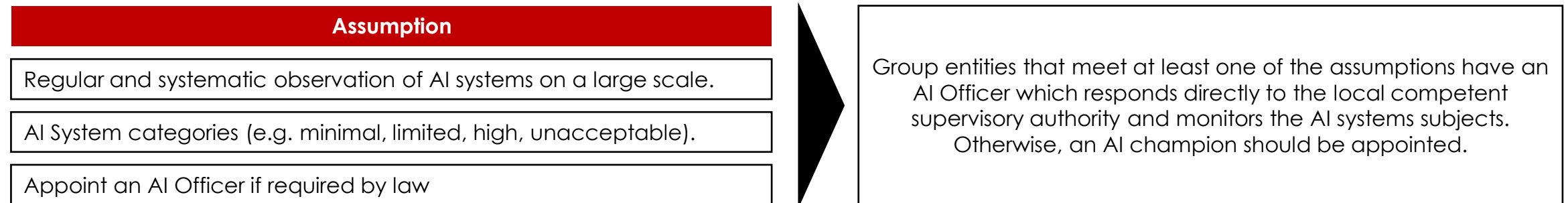|	
EU AI Act compliance global supervisor • Monitoring the EU AI Act compliance of the Group • Consolidated reporting to group senior management • Point of communication with regulators at a global level • Impact assessment of security incidents at a global level • AI system global risks assessment • Facilitate corporate criteria and be the point of contact at a corporate level for the entity's AI officers	**Support the AI Officer/Head and champions of the units and corporate entities** • Provide expert advice on the regulation and support the AI Officer/Heads and champions on the execution of their functions

EU AI Act Heads

Each entity or unit subject to EU AI Act provisions has appointed a head of AI, which may be a AI Officer/Head or a "champion" on the basis of the following criteria.

1. **Group subsidiaries.**

For those subject to GDPR requirements, a DPO is formally appointed should any of the following assumptions are met:

Assumption
Regular and systematic observation of AI systems on a large scale.
AI System categories (e.g. minimal, limited, high, unacceptable).
Appoint an AI Officer if required by law

Group entities that meet at least one of the assumptions have an AI Officer which responds directly to the local competent supervisory authority and monitors the AI systems subjects. Otherwise, an AI champion should be appointed.

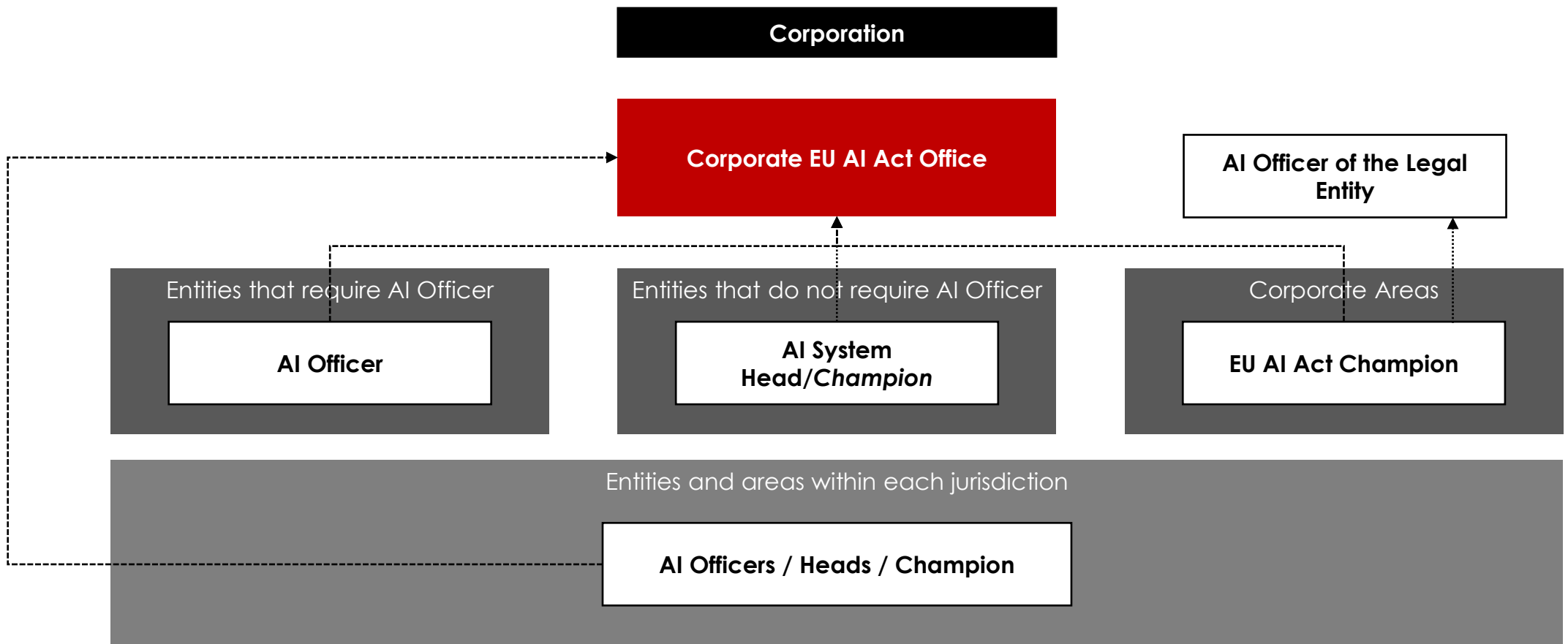Likewise, on those jurisdictions outside the EEA, EU AI Act heads have been appointed.

2. **Units and corporate areas.**

Units that interact with AI systems have appointed a champion figure that supports the AI Office/Head of the entity to which they belong.

Organisational structure

The governance model has the following organizational structure and relationship model among the EU AI Act responsible figures:

Functions and responsibilities

- **R – Responsible:** Responsible for the execution of task
- **A – Accountable:** Responsibility for that task to be executed
- **C – Consulted:** Figure that must be consulted to perform the task
- **I – Informed:** Figure that must be informed of the implementation of the task

Components/Roles		Corp/Group. Management	Corporate AI Office	Entity Management	AI Officer/Head	Champion (if applicable)	Area resp. for AI system int.	AI system activity stakh.	Other areas
Governance model	Definition	I	I	C, I	R, A	C, I	I	I	I
Representation and institutional aspects	Point of contact	I*	I	I*	R, A	C	C		
	Coop.	I*	I	I*	R, A	C	C		
Operational aspects	Definition	I*	C, I	A, C	R	C, I	I	I	I
	Reg. chang.	I*	C, I	C	R, A	C, I	I	I	I
	Provide advice		C		R, A	R**	C, I	I	I
	BAU procedur.	I*	I	I*	A, C	C	I	C	R
	Identif. & eval.				A, C	A, C**	R	C	
	Risk method.	I*	I	I*	A, R	I	I		C (p.e Risks)
	Risk assessmt.		I	I*	A, C	A, C**	R	C	C (p.e CISO, Risks, Legal)
	Prior consult.		I	C, I	A, R	C	C, I		
	Update mainten. Record.		I	I*	A, I	C, I	R	C	C (p.e CISO, Risks, Legal)

*At discretion of the AI Officer/AI Office; **Responsibility in the first instance, shared with the AI Officer in the case it cannot be assured; ***Units without AI Officer

9

Functions and responsibilities

- **R – Responsible:** Responsible for the execution of task
- **A – Accountable:** Responsibility for that task to be executed
- **C – Consulted:** Figure that must be consulted to perform the task
- **I – Informed:** Figure that must be informed of the implementation of the task

Components/Roles		Corp/Group. Management	Corporate AI Office	Entity Management	AI Officer/Head	Champion (if applicable)	Area resp. for AI system int.	AI system activity stakh.	Other areas
Operational aspects	Ensuring compl.				A	I	R	R	R (p.e CISO, Business etc)
	Risk identi.				A	I	R	R	R (p.e. CISO)
	Risk eval. and comm.	I	I	I	R, A	R***, A, C	C	C	C (p.e CISO, Business etc)
	Third-party approval		I, C	I*	A, I	I	C	C	R (p.e. Procurement)
	Third-party mngmnt.			I*	A, I	I	C	C	R (p.e. Legal)
	Third-party comp. monitoring			I*	A, I	I	C	C	R (p.e. Procurement)
	Attention to requests			I*	A	A	C	C*	R (p.e. Legal)
	Ops. & IT changes implemnt.			I*	A, C	C**	R	I	R (p.e. IT)
	BAU Ops. Execution			I*	A	A	R	I	R
	Execution of training & awareness			I*	A	A	C		R (p.e. Training)

*At discretion of the AI Officer/AI Office; **Responsibility in the first instance, shared with the AI Officer in the case it cannot be assured; ***Units without AI Officer

10

Functions and responsibilities

- **R – Responsible:** Responsible for the execution of task
- **A – Accountable:** Responsibility for that task to be executed
- **C – Consulted:** Figure that must be consulted to perform the task
- **I – Informed:** Figure that must be informed of the implementation of the task

Components/Roles		Corp/Group. Management	Corporate AI Office	Entity Management	AI Officer/Head	Champion (if applicable)	Area resp. for AI system int.	AI system activity stakh.	Other areas
Internal Control Model for each entity/area	Control model definition		I	I	A, C	A, C**	C	C	R (Comp. and 1 LoD areas)
	Controls execution				A, I	A, I	I		R (Controls respons.)
	Comp. monitoring	I*	I	I*	A, R	A, C, I	I	C	C (Controls respons.)
Scorecard (Corporation-Subsidiary relationship model)	Definition of scorecard mangmnt. System		A, R		C, I	C, I			
	Indicators reporting		I	I*	A, R	R**			
	Indicators analysis	I*	A, R		A, C, I	A, C, I			
Relevant aspects and critical incident management	Relevant aspects and critical incident mangmnt.	I*	C, I	C, I	A, R	A, C	C	C	C

*At discretion of the AI Officer/AI Office; **Responsibility in the first instance, shared with the AI Officer in the case it cannot be assured; ***Units without AI Officer

Operational AI governance components

Governance Components and Tasks	Description
A. AI system T1. AI system repository and AI ID T2. AI system pre-design T3. AI system use case T4. AI system user T5. AI system operating environment T6. AI system architecture T7. AI system deployment metrics T8. AI system operational metrics T9. AI system version control design T10. AI system performance monitoring design T11. AI system health check design T12. AI system verification and validation T13. AI system approval T14. AI system version control T15. AI system performance monitoring T16. AI system health checks	Ensuring that the AI system is developed, operated, and monitored in alignment with the organization's strategic goals and values.

Operational AI governance components

Governance Components and Tasks	Description
B. Algorithms T17. Algorithm ID T18. Algorithm pre-design T19. Algorithm use case design T20. Algorithm technical environment design T21. Algorithm deployment metrics design T22. Algorithm operational metrics design T23. Algorithm version control design T24. Algorithm performance monitoring design T25. Algorithm health check design T26. Algorithm verification and validation T27. Algorithm approval T28. Algorithm version control T29. Algorithm performance monitoring T30. Algorithm health checks	Ensuring that the algorithms used by an AI system are developed, operated, and monitored in alignment with the organization's strategic goals and values.

Operational AI governance components

Governance Components and Tasks	Description
C. Data operations T31. Data sourcing T32. Data ontologies, inferences, and proxies T33. Data pre-processing T34. Data quality assurance T35. Data quality metrics T36. Data quality monitoring design T37. Data health check design T38. Data quality monitoring T39. Data health checks	Ensuring that data are sourced, used, and monitored in alignment with the organization's strategic goals and values.

Operational AI governance components

Governance Components and Tasks	Description
D. Risk and impacts T40. AI system harms and impacts pre-assessment T41. Algorithm risk assessment T42. AI system health, safety, and fundamental rights impact assessment T43. AI system non-discrimination assurance T44. AI system impact minimization T45. AI system impact metrics design T46. AI system impact monitoring design T47. AI system impact monitoring T48. AI system impact health check	Identifying, managing, and monitoring potential risks and impacts caused by the AI system to align the system with the organization's strategic goals and values.

Operational AI governance components

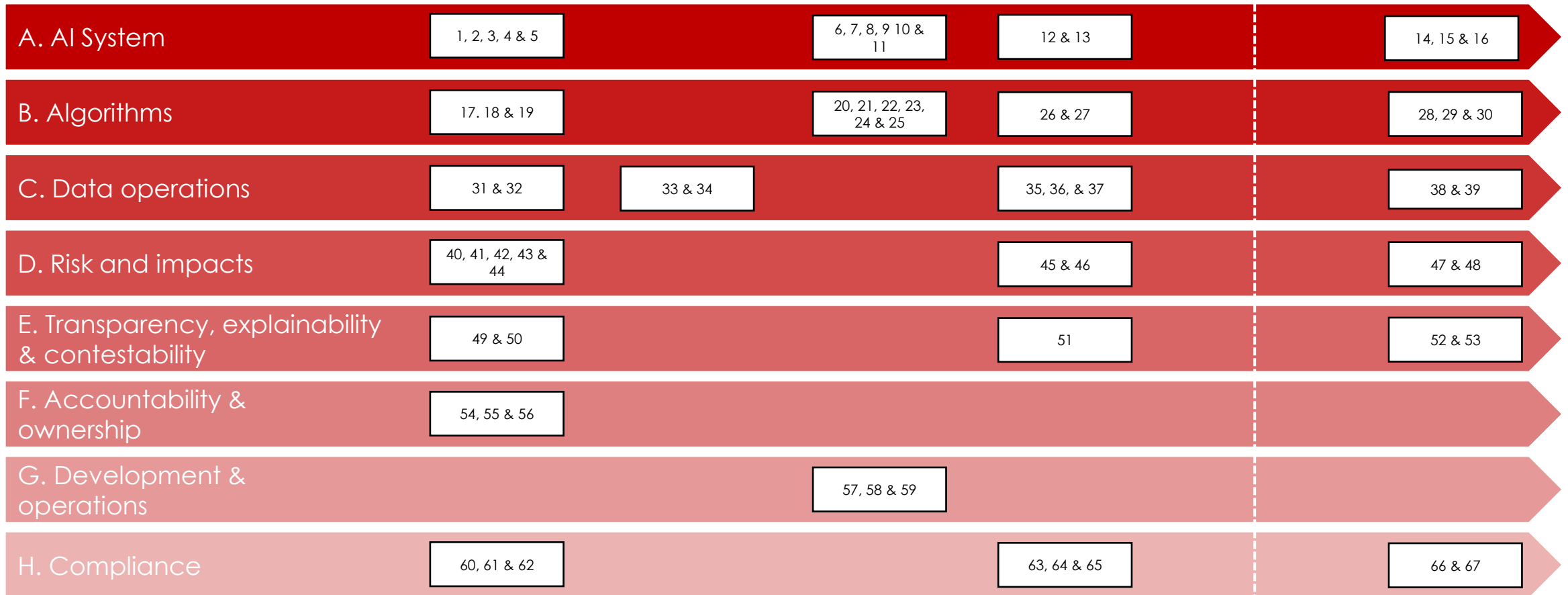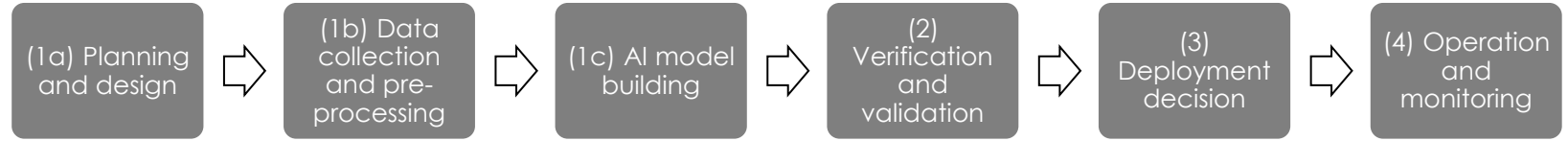| Governance Components and Tasks	Description
E. Transparency, explainability, and contestability (TEC) T49. TEC pre-design T50. TEC design T51. TEC monitoring design T52. TEC monitoring T53. TEC health checks	Ensuring that the AI system transparency, explainability, and contestability is aligned with the organization's strategic goals and values.
F. Accountability and ownership T54. Head of AI T55. AI system owner T56. Algorithm owner	Ensuring necessary decision rights and responsibilities to govern the AI system and its algorithmic components to align the system with the organization's goals and values.
G. Development and operations T57. AI development T58. AI operations T59. AI governance integration	Designing and implementing appropriate workflows and organizational structures for developing AI systems

Operational AI governance components

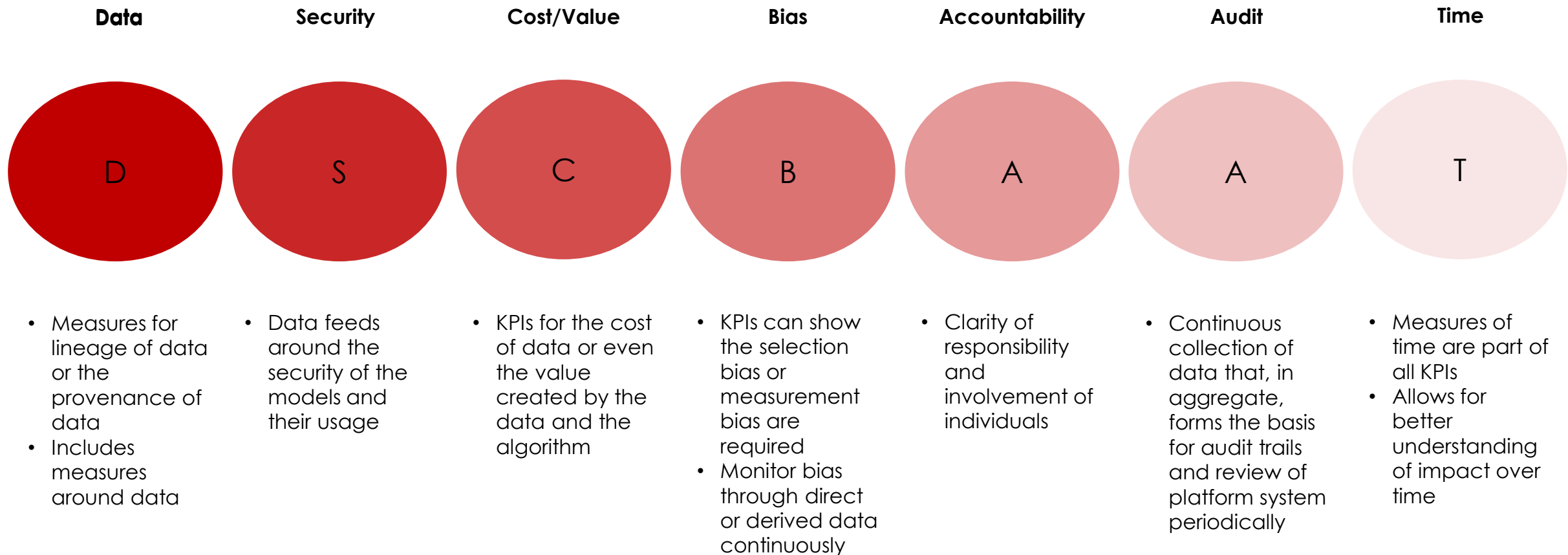| Governance Components and Tasks	Description
H. Compliance T60. Regulatory canvassing T61. Regulatory risks, constraints, and design parameter analysis T62. Regulatory design review T63. Compliance monitoring design T64. Compliance health check design T65. Compliance assessment T66. Compliance monitoring T67. Compliance health checks	Understanding the regulatory environment of an AI system and ensuring its compliance with the relevant regulations.

AI system lifecycle and operational AI governance components

	(1a) Planning and design	(1b) Data collection and pre-processing	(1c) AI model building	(2) Verification and validation	(3) Deployment decision	(4) Operation and monitoring
A. AI System	1, 2, 3, 4 & 5		6, 7, 8, 9 10 & 11	12 & 13		14, 15 & 16
B. Algorithms	17. 18 & 19		20, 21, 22, 23, 24 & 25	26 & 27		28, 29 & 30
C. Data operations	31 & 32	33 & 34		35, 36, & 37		38 & 39
D. Risk and impacts	40, 41, 42, 43 & 44			45 & 46		47 & 48
E. Transparency, explainability & contestability	49 & 50			51		52 & 53
F. Accountability & ownership	54, 55 & 56					
G. Development & operations			57, 58 & 59			
H. Compliance	60, 61 & 62			63, 64 & 65		66 & 67

Measuring EU AI Act governance

Businesses must be able to measure EU AI Act governance by considering facts and data-driven KPIs:

Data	**Security**	**Cost/Value**	**Bias**	**Accountability**	**Audit**	**Time**
D	S	C	B	A	A	T

Data
- Measures for lineage of data or the provenance of data
- Includes measures around data

Security
- Data feeds around the security of the models and their usage

Cost/Value
- KPIs for the cost of data or even the value created by the data and the algorithm

Bias
- KPIs can show the selection bias or measurement bias are required
- Monitor bias through direct or derived data continuously

Accountability
- Clarity of responsibility and involvement of individuals

Audit
- Continuous collection of data that, in aggregate, forms the basis for audit trails and review of platform system periodically

Time
- Measures of time are part of all KPIs
- Allows for better understanding of impact over time

DISCLAIMER

This Presentation may contain information, text, data, graphics, photographs, videos, sound recordings, illustrations, artwork, names, logos, trade marks, service marks, and information about us, our lines of services, and general information may be provided in the form of documents, podcasts or via an RSS feed ("the Information").

Except where it is otherwise expressly stated, the Information is not intended to, nor does it, constitute legal, accounting, business, financial, tax or other professional advice or services. The Information is provided on an information basis only and should not be relied upon. If you need advice or services on a specific matter, please contact us using the contact details for the relevant consultant or fee earner found on the Presentation.

The Presentation and Information is provided "AS IS" and on an "AS AVAILABLE" basis and we do not guarantee the accuracy, timeliness, completeness, performance or fitness for a particular purpose of the Presentation or any of the Information. We have tried to ensure that all Information provided on the Presentation is correct at the time of publication. No responsibility is accepted by or on behalf of us for any errors, omissions, or inaccurate information on the Presentation. Further, we do not warrant that the Presentation or any of the Information will be uninterrupted or error-free or that any defects will be corrected.

Although we attempt to ensure that the Information contained in this Presentation is accurate and up-to-date, we accept no liability for the results of any action taken on the basis of the Information it contains and all implied warranties, including, but not limited to, the implied warranties of satisfactory quality, fitness for a particular purpose, non-infringement, compatibility, security, and accuracy are excluded from these Terms to the extent that they may be excluded as a matter of law.

In no event will we be liable for any loss, including, without limitation, indirect or consequential loss, or any damages arising from loss of use, data or profits, whether in contract, tort or otherwise, arising out of, or in connection with the use of this Presentation or any of the Information.

QUESTIONS?

THANK YOU FOR YOUR TIME

AI & Partners

Sean Musch
s.musch@ai-and-partners.com
+31(6) 57285579

Michael Charles Borrelli
m.borrelli@ai-and-partners.com
+44(0)7535 994 132

https://www.ai-and-partners.com/