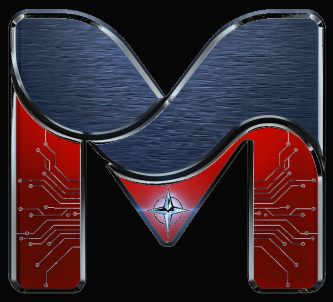

MICKAI EBOOK SERIES · PLAYBOOK No. 9

What is Governance, for an AI Agent?.

Governance for AI is not a policy document. It is a cryptographic position. This ebook is the engineering walk-through of what governance actually means when the system being governed is an autonomous agent.

AUTHOR

Micky Irons

Founder and named inventor, Mickai LTD.

Crunchbase · LinkedIn · GitHub · mickai.co.uk

DATE · 17 May 2026 · v1

EBOOK · No. 9 IN A SERIES OF 14

Mickai LTD · Companies House 17166618 · press@mickai.co.uk · mickai.co.uk

UK IPO patent family GB2607309.8 to GB2610422.4 · Trade mark UK00004373277

TABLE OF CONTENTS

Contents

FOREWORD

A note from the author

Every UK board is asked to sign off on AI governance. Most boards do not have the engineering vocabulary to know what they are signing. This ebook is the engineering definition: governance is the cryptographic position the operator holds over the actions of an autonomous agent, plus the policy layer that decides what those actions are allowed to be.

The cryptographic position is the substrate. The policy layer rides above it. Without the substrate, the policy is unenforceable; without the policy, the substrate is unused.

The Mickai substrate primitives are filed at the UK IPO across the GB2607309.8 to GB2610422.4 patent family. The trade mark Mickai is registered at UK00004373277.

Micky Irons

Founder and named inventor, Mickai LTD · 17 May 2026

PART I · GOVERNANCE, DEFINED

Three layers, in plain language

1. Policy, technical, and cryptographic layers

AI governance has three layers. The policy layer is the document the board approves. The technical layer is the code that enforces the policy. The cryptographic layer is the audit chain that proves the enforcement happened.

Most UK boards in 2026 have the policy layer in place. Many have a technical layer in some form. Very few have the cryptographic layer. The substrate question is whether the third layer exists; without it, the first two are unverifiable.

2. What the regulator actually requires

The regulator's chain-of-custody expectation cuts across all three layers. The ICO, the FCA, the PRA, the MHRA, the ONR, the OFCOM/OFGEM/OFWAT cluster each ask, at hour zero of an incident review: show us the AI's decision, the input it acted on, the authority it acted under, the policy it satisfied, and the cryptographic evidence that the chain is canonical. The substrate produces the evidence; the policy provides the context.

3. The governance gap in commercial AI

Most commercial AI offerings in 2026 ship a policy layer (terms of service, acceptable use, vendor-side controls) and a partial technical layer (rate limiting, content filters, audit dashboards). Almost none ship the cryptographic layer in a form the operator owns. The governance gap is structural; the operator cannot govern what the operator cannot verify.

PART II · THE ENGINEERING OF GOVERNANCE

The brains in the Mickai Governance Layer

4. Policy Brain in the Mickai SIOS

The Policy Brain holds the operator's policy graph as a versioned, signed artefact. Every AI action in the SIOS resolves against the Policy Brain before commit; the resolution outcome (permit, deny, escalate, defer) is recorded in the OAR chain. The Policy Brain is updateable, but every update is itself a signed governance event.

5. Audit Ledger Brain

The Audit Ledger Brain holds the OAR chain. Every brain action emits a record to the Audit Ledger Brain, which serialises, hash-links, signs, and appends. The Audit Ledger Brain is the trust root of the SIOS; the chain identifier is the SIOS instance identifier as far as the regulator is concerned.

6. Permissions Brain and Revocation Brain

The Permissions Brain enforces capability access for every brain in the SIOS. The Revocation Brain handles the inverse: capability revocation, key revocation, brain decommission. Both are signed-event surfaces that produce audit records.

7. Quorum Brain

The Quorum Brain handles multi-party authorisation. For high-stakes actions (large transactions, irreversible operations, security-relevant changes), the Quorum Brain requires multiple operator signatures before commit. The quorum requirement is itself a policy decision held in the Policy Brain.

PART III · GOVERNANCE IN PRACTICE

Three governance moments in the operating year

8. Sign-off chain for the board

The board's annual AI governance sign-off becomes a substrate event. The Policy Brain produces the current policy graph, signed and chained. The board reviews, approves, and the approval itself is a governance event recorded in the OAR chain. The auditor walks the chain and sees the sign-off as a cryptographic record, not as a meeting minute.

9. Incident review by the regulator

On a regulator incident review, the operator produces the relevant chain segment and the verifier. The regulator walks the chain, sees every AI action recorded, every policy resolution recorded, every authority context recorded, and produces a deterministic verdict per record. The incident review is data-driven, not negotiation-driven.

10. Annual governance recital

Each year, the operator produces a governance recital: a summary of the AI actions across the year, the policy resolutions, the quorum events, the revocations, and the verifier verdicts. The recital is itself a governance artefact, signed, chained, and shipped to the board and the regulator.

PART IV · THE SUBSTRATE

Why governance without cryptography is unenforceable

11. Why governance without cryptography is unenforceable

A governance policy that cannot be cryptographically verified is a policy that depends on the AI vendor's good behaviour. Vendors are not adversarial in normal operation, but vendors fail, vendors are acquired, vendors are sued, vendors exit markets. The governance policy that survives these events is the policy backed by the substrate; the operator's chain verifies under the operator's key regardless of downstream vendor events.

> **Governance without cryptography is governance under vendor goodwill.**

12. The OAR primitive

The OAR primitive is the substrate that makes governance enforceable. Hash-linked CBOR records, FIPS 204 ML-DSA-65 signatures, browser-resident verifier, four-verdict output. The governance layer above the OAR is the operator's organisational answer; the OAR underneath is the cryptographic answer.

13. Closing

AI governance is not a policy document. It is a cryptographic position plus a policy layer. The board's job is to set the policy; the substrate's job is to make the policy enforceable. The substrate exists, is filed at the UK IPO, and is in operation at Mickai today.

Engineering and board leadership at any UK regulated buyer is open to a thirty-minute governance briefing at any time. press@mickai.co.uk.

APPENDIX · ABOUT THE AUTHOR

Micky Irons

Founder of Mickai LTD (Companies House 17166618, England and Wales, registered office 20 Wenlock Road, London, N1 7GU). Named inventor on the Mickai SIOS patent corpus, recorded on the UK Intellectual Property Office public register at numbers GB2607309.8 to GB2610422.4. Trade mark Mickai registered at UK00004373277 (classes 9 and 42, filed 15 April 2026).

Before founding Mickai, Micky was a Sellafield site worker. The egress constraint observed from inside the regulated workstation is the engineering origin of the substrate described across the Mickai ebook series.

Profiles and links

mickai.co.uk · the canonical Mickai site.

crunchbase.com/person/micky-irons · founder profile.

linkedin.com/in/mickyirons · personal LinkedIn.

github.com/Micky-CMO · open-source position.

linkedin.com/company/mickai · Mickai LTD company page.

crunchbase.com/organization/mickyirons · Mickai LTD Crunchbase entry.

Email: press@mickai.co.uk

Colophon

Set in Inter Tight (Variable) and Inter Black. Brand voice audited under the Mickai AMT preflight gate; zero violations at publish.

References and further reading

· Information Commissioner's Office, AI and data protection guidance.

· PRA Supervisory Statement SS1/23, model risk management for banks.

· NCSC, AI Cyber Security Code of Practice (DSIT consultation 2024 to 2025).

· Mickai brain taxonomy: mickai.co.uk/brains.

· Mickai trade mark UK00004373277, classes 9 and 42, filed 15 April 2026.