MICKAI™

MICKAI EBOOK SERIES · PLAYBOOK No. 7

The UK Procurement Checklist for Sovereign AI.

A twelve-dimension rubric for evaluating any AI vendor against a UK regulated buyer's egress posture, audit chain expectation, and operational resilience plan.

AUTHOR

Micky Irons

Founder and named inventor, Mickai LTD.
Crunchbase · LinkedIn · GitHub · mickai.co.uk

DATE · 16 May 2026 · v1

Mickai LTD · Companies House 17166618 · press@mickai.co.uk · mickai.co.uk
UK IPO register GB2607309.8 to GB2611702.8 and GB2611885.1 onwards · Trade mark UK00004373277

TABLE OF CONTENTS

Contents

Foreword

A note from the author

Part I · The Rubric

1. Twelve dimensions
2. Scoring methodology
3. Pass thresholds for defence, finance, pharma, CNI

Part II · Per-dimension walkthrough

4. Architecture posture, key custody, cryptographic algorithm
5. Inference location, audit format, verifier model
6. Trust domain, air-gap, UK IPO position
7. UK regulated fit, latency, threat intelligence

Part III · Worked examples

8. A defence-nuclear procurement
9. A PRA-regulated bank procurement
10. A pharma pre-clinical procurement

Part IV · Closing

11. Template procurement clauses
12. Closing

Appendix

About the author
References and further reading

FOREWORD

A note from the author

The UK regulated buyer cannot ask 'is this AI safe?' as a yes-or-no procurement question. The answer depends on twelve structural dimensions that the vendor either satisfies or does not. This ebook is the procurement officer's rubric, written so that defence, finance, pharma, and CNI buyers can score any AI vendor's response against a common standard.

The rubric is the engineering-led counterpart to the procurement-led question. It does not replace the legal review, the commercial review, or the security questionnaire; it sits underneath all three.

The Mickai substrate primitives are filed at the UK IPO across the GB2607309.8 to GB2611702.8 and GB2611885.1 onwards families. The trade mark Mickai is registered at UK00004373277.

Micky Irons

Founder and named inventor, Mickai LTD · 16 May 2026

PART I · THE RUBRIC

Twelve dimensions, scored against pass thresholds

1. Twelve dimensions

The twelve dimensions are: (1) Architecture posture, (2) Key custody, (3) Cryptographic algorithm, (4) Inference location, (5) Audit format, (6) Verifier model, (7) Trust domain, (8) Air-gap suitability, (9) UK IPO position, (10) Sector fit, (11) Latency surface, (12) Threat intelligence model. Each dimension is scored 0 to 3 against the buyer's data class.

2. Scoring methodology

Each dimension carries a score 0 (fails) to 3 (operator-controlled, post-quantum, hash-linked baseline). The buyer sets the pass threshold per dimension based on the data class. A defence-nuclear buyer typically requires 3 on dimensions 2, 3, 4, 5, 7, and 8; a PRA-regulated bank requires 3 on 2, 4, 5, 7, and 11; a pharma buyer requires 3 on 2, 4, 5, and 9. The aggregate score is informational; the per-dimension threshold is binding.

3. Pass thresholds for defence, finance, pharma, CNI

Defence-nuclear and defence-prime buyers should treat scores of 0 or 1 on dimensions 2, 4, 5, 7, or 8 as automatic disqualification. PRA-regulated banks should treat 0 or 1 on 2, 4, 5, or 7 as disqualification. Pharma buyers under MHRA chain-of-custody should treat 0 or 1 on 2, 4, or 5 as disqualification. CNI operators under sector-regulator expectation should treat 0 or 1 on 2, 4, 5, 7, or 11 as disqualification.

PART II · PER-DIMENSION WALKTHROUGH

How to score each dimension in detail

4. Architecture posture, key custody, cryptographic algorithm

(1) Architecture posture

0: cloud-only platform. 1: cloud with edge cache. 2: edge with cloud fallback. 3: substrate on operator iron, no cloud dependency.

(2) Key custody

0: vendor-held key. 1: shared HSM with vendor escrow. 2: operator HSM with vendor backup. 3: operator TPM/HSM, no vendor copy.

(3) Cryptographic algorithm

0: classical-only, no PQC roadmap. 1: classical with documented PQC plan. 2: hybrid classical and PQC. 3: pure PQC from inception (ML-KEM, ML-DSA, SHA-3).

5. Inference location, audit format, verifier model

(4) Inference location

0: vendor cloud only. 1: vendor edge with cloud sync. 2: operator edge with vendor relay. 3: operator workstation, no off-perimeter inference.

(5) Audit format

0: vendor JSON, vendor-stored. 1: vendor JSON, operator-exportable. 2: open schema, operator-stored. 3: open schema, hash-linked, post-quantum-signed, operator-controlled.

(6) Verifier model

0: vendor-portal only. 1: vendor SDK with vendor server. 2: operator-side verifier, vendor library dependency. 3: browser-resident verifier, offline, deterministic verdicts.

6. Trust domain, air-gap, UK IPO position

(7) Trust domain

0: vendor-only. 1: vendor-and-operator. 2: vendor-operator-regulator. 3: operator-regulator-worker-third-party (full trust-domain externalisation).

(8) Air-gap suitability

0: cloud-required. 1: cloud-recommended. 2: edge with periodic cloud sync. 3: air-gap-suitable, no network dependency for inference or audit.

(9) UK IPO position

0: no UK patent filings, foreign-only IP. 1: UK patent applications pending under foreign inventor. 2: granted UK patents under foreign assignee. 3: UK IPO-recorded patent family under a UK inventor.

7. UK regulated fit, latency, threat intelligence

(10) Sector fit

0: no UK regulated reference customers. 1: one UK reference. 2: multiple UK references in adjacent sector. 3: multiple UK references in the buyer's exact sector.

(11) Latency surface

0: cloud round-trip. 1: vendor edge round-trip. 2: operator edge with vendor relay. 3: workstation-local, sub-100ms response.

(12) Threat intelligence model

0: feed-bundled vendor lock. 1: vendor feed with operator override. 2: open feed with vendor enrichment. 3: substrate-neutral (any feed welcome above).

PART III · WORKED EXAMPLES

Three procurements scored against the rubric

8. A defence-nuclear procurement

A defence-nuclear engineering workstation procurement starts with the rubric's hard floor on dimensions 2, 4, 5, 7, and 8. Cloud-only platforms score 0 on most of these and are eliminated at the gate. Hybrid platforms (edge with cloud relay) score 1 to 2 and rarely clear the threshold. Substrate platforms (operator-iron inference, operator key custody, hash-linked signed audit, browser-resident verifier, air-gap suitable) score 3 across the binding dimensions and pass the rubric.

The procurement officer's job is to apply the rubric, not to debate the architecture. The architecture is what the rubric measures.

9. A PRA-regulated bank procurement

A PRA-regulated bank's AI procurement under SS1/23 expectations starts with the rubric's hard floor on dimensions 2, 4, 5, 7, and 11. Cloud-AI platforms score 0 to 1 on most of these. The bank's operational resilience plan requires that AI vendor failure does not propagate into the bank's customer-facing service or audit chain; substrate platforms satisfy that property by construction, while cloud platforms cannot.

10. A pharma pre-clinical procurement

A pharma pre-clinical informatics procurement under MHRA chain-of-custody expectation starts with the rubric's hard floor on dimensions 2, 4, and 5. The compound library and the trial dataset are structural IP assets; the inference cannot happen on a vendor cloud, the key custody cannot rest with the vendor, the audit chain cannot be vendor-formatted. The substrate platform passes; the cloud platform does not.

PART IV · CLOSING

Template procurement clauses, closing

11. Template procurement clauses

The recommended procurement clause set for any UK regulated AI procurement is:

· The supplier shall demonstrate that inference happens on operator-controlled hardware. (Dimension 4.)
· The supplier shall demonstrate that signing keys are held under operator TPM or HSM custody, with no vendor escrow. (Dimension 2.)
· The supplier shall produce a hash-linked, post-quantum-signed audit chain in an open canonical format. (Dimensions 3, 5.)
· The supplier shall provide a browser-resident, offline, deterministic verifier under terms that survive contract termination. (Dimension 6.)
· The supplier shall demonstrate UK IPO position on cryptographic substrate primitives. (Dimension 9.)
· The supplier shall provide reference deployments in the buyer's exact regulated sector. (Dimension 10.)

12. Closing

The rubric is the procurement officer's instrument. Used consistently across UK regulated AI procurements, it raises the structural standard of the AI vendor ecosystem and gives the engineering function inside the buyer organisation a defensible counterpart to the legal and commercial reviews.

Engineering and procurement leadership at any UK regulated buyer is open to a thirty-minute substrate 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 GB2611702.8 and GB2611885.1 onwards. 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. © 2026 Mickai LTD. Reproduction permitted for internal procurement and engineering use within UK regulated organisations. External redistribution by written permission of the author.

References and further reading

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

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

· NCSC, Timelines for migration to post-quantum cryptography.

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

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