D3 — Regulatory Alignment: PDPL and NCA-ECC

D3 · Regulatory alignment · content of 2026-09-18 · source ffeb2779

Companion document to the MURAQIB Security Whitepaper. Section references prefixed with §11 refer to the limitations register in that document.

Part 1 — Scope, Position and Method

1.1 Purpose

This document maps MURAQIB against two Saudi regulatory frameworks: the Personal Data Protection Law (Royal Decree M/19, as amended by M/148) with its Implementing Regulation, and the National Cybersecurity Authority's Essential Cybersecurity Controls, ECC-2:2024.

It is written for a technical reviewer assessing MURAQIB for deployment and for a regulatory reviewer assessing whether that deployment can be defended. It states what MURAQIB provides toward each obligation, and states with equal plainness where it provides nothing. Every gap identified here is recorded in the limitations register in Section 11 of the MURAQIB security whitepaper. Several were identified by this mapping exercise rather than by the whitepaper's own review, and were added to that register before this document was issued; none is stated here without a corresponding register entry.

1.2 A note on the ECC control count

ECC-2:2024 contains 108 controls across 28 subdomains in four domains. This figure was established by reading every control table in the published document. It differs from the count of 110 that appears in widely-circulated secondary commentary.

The discrepancy arises from subdomain 1-7. Appendix C of ECC-2:2024 records that ECC-1's control 1-7-1 was deleted and its 1-7-2 was modified and renumbered, becoming ECC-2's 1-7-1. Appendix C refers to the controls by their former numbering, so an identifier 1-7-2 appears in the appendix but exists nowhere in the control section. Because 1-7-1 is the last control in its subdomain, no numbering gap results, and no automated check relying on sequence detection can find the error.

Automated extraction of the document does not settle the question either. Extraction yields 109 if the appendix reference is counted as a control, and 108 if it is not — but a naive extraction also yields 108 for an unrelated reason, silently dropping control 1-9-3, which is joined to a preceding word in the document's text layer. Two independent artifacts happen to differ by one. Only reading the pages resolves it.

The distinction is stated here because the method matters more than the number: a control count taken from secondary sources is not a verified fact, and this document does not restate figures it has not established.

1.3 What MURAQIB is, for the purposes of this mapping

MURAQIB is a pre-execution decision point for AI agent actions. An agent submits a proposed action and receives a verdict — approved, blocked, or escalated to human authorisation — before acting. Each verdict is sealed into an append-only evidence chain.

Two properties bear directly on regulatory assessment and are stated here rather than left for a reader to discover:

MURAQIB is not an enforcement point. It issues decisions; it does not execute or block. An agent that receives a refusal and proceeds is not stopped, and an agent that does not submit an action is not observed. Any control mapped in this document to MURAQIB is a control over the record of a decision, not over the performance of an action.

MURAQIB's assurances are evidentiary. Where this document states that MURAQIB supports a control, the support consists of a tamper-evident record of a decision, independently verifiable, and not of a technical measure preventing an outcome.

1.4 Personal data processed

MURAQIB processes personal data within the meaning of Article 1(4) of the PDPL, in three distinct stores with different protection properties. A deploying entity's assessment must account for all three.

Sealed evidence records. Of 433 governed decisions in the production chain, 269 carry an actor identity and 269 an actor name, with 264 carrying both; the remainder do not. Where an action is subject to a four-eyes control and the calling system produces a signed assertion, the assertion body additionally carries the authoriser's identifier and role, a flag recording whether that party is a section head, and the identifiers of the makers; an email address is present on seventeen records. Twenty-nine of 433 records carry a valued assertion. Email addresses appear nowhere else in any sealed record, and there is no authoriser name field.

Personal data is also carried in the action summary — free text describing the proposed action, which may contain personal data of third parties depending on the submitting agent.

Unsealed record fields. The evidence log holds approval provenance — the approving individual, the time of approval and an approval note — and generated explanations in English and Arabic. The explanations are populated across all 1,073 rows. `approved_by` is populated on **three** rows, against 469 marked as requiring approval; `approval_note` is populated on none. Of those three, one is a genuine resolution performed through an authenticated session on 30 August 2026; the other two date to 15 May 2026, name individuals in free text who hold no account in the deployment, and were written by a code path that has no caller and writes to a database this system no longer uses.

These columns are not covered by the evidence seal, and that is a statement about the columns rather than about the information. They sit in a table with no append-only trigger on which the application role holds update permission, so their values can be altered in place without breaking any seal. The resolution they describe is nevertheless sealed, in its own later event (`DECISION_RESOLVED`), carrying the outcome, the resolver's session-derived identity and role, and the time — so the resolution state of every sealed escalation is recoverable from the chain alone and agrees with the columns exactly. The columns are a cache; the sealed event is the record. The cache is lossy in one specific way an institution must know: it is written identically for an approval and a rejection, and only the sealed event records which occurred, so a populated `approved_by` is not by itself evidence of approval. The reasoning behind a decision seals from 16 September 2026 as a trace and a digest; the rendered prose explanations are deliberately not sealed, being generated from fields the record already seals. Section 11.2.18 of the whitepaper records this.

Operational stores. The deployment additionally holds personal data outside the evidence chain: user accounts with names, email addresses and telephone numbers; an agent registry recording each agent's owner and human sponsor; an agent memory store carrying owner identities, free-text content in both languages, an explicit data-subjects field and a personal-data flag; API key ownership records; tenant grant and access records; and policy change approvals.

Constraints on submitted content. MURAQIB does not constrain the content of an action summary, and does not inspect it for personal data beyond the declared-summary scan described in Section 4.6 of the whitepaper. That scan reads three declared fields — the summary, the actor's name and the actor's identifier — and does not read an outbound message, an attachment, an exported file, a database payload, or the signed authorisation body. It has no "could not classify" state: content whose form it does not recognise returns clean, indistinguishable from genuinely clean. A controller relying on the scan as a personal-data control should understand that limit.

MURAQIB does constrain summary size. A summary exceeding 16,384 characters is refused rather than truncated, and a request body exceeding one mebibyte is rejected before processing. The refusal is deliberate: a silently shortened summary would make the sealed record differ from what the caller declared.

Retention. No mechanism deletes or ages out evidence records: no scheduled purge exists, the application role holds no delete permission on the evidence tables, and the chain is append-only by construction, so a record cannot be deleted or altered without breaking the chain and rendering every subsequent record unverifiable. Retention of sealed evidence is therefore unbounded. Section 11.6.4 of the whitepaper records this.

Three qualifications. The unsealed fields described above are not protected by that property. The scan log — which records the findings of the declared-summary scan, and therefore the personal data those findings identify — is one evidence-adjacent table on which the application role does hold delete and truncate permission. And the immutability of the chain resists deletion by the application, not by a privileged database operator: Section 11.2.10 of the whitepaper records that an operator with schema privileges can remove the append-only triggers and delete rows freely.

Historical exposure, now closed. Until 19 August 2026 each scan finding also stored a six-character prefix of the matched value verbatim, labelled with the detected type and the PDPL article engaged — so a record of a detected Saudi National ID carried the first six digits of that identifier alongside its classification. The field was removed from the scanner, and the three affected historical rows were stripped of it as a recorded operator action; the before-state was captured and hashed before any row was altered, and a copy was taken off the host manually; no automated path replicates it. That capture retains the removed values. The specimen never entered the sealed evidence chain: no sealed payload carries the field, which was verified rather than assumed. Section 11.5.4b of the whitepaper records this limitation; Section 11.5.4 records the broader position that evidence is stored in plaintext.

The implications of unbounded retention for data-subject rights are addressed in Part 4.

1.5 Position under the PDPL: assessment, not conclusion

Article 1(18) of the PDPL defines a Controller as an entity that specifies the purpose and manner of processing. Article 1(19) defines a Processor as an entity that processes personal data for the benefit and on behalf of a Controller.

In a hosted deployment serving a tenant organisation, OQIRON assesses its position as that of a Processor. The tenant determines which agents submit actions, which policies apply, and what personal data those actions carry; OQIRON processes that data to render and record a governance decision on the tenant's behalf. OQIRON does not determine the purpose of the underlying processing.

This assessment has not been confirmed by external legal opinion as of this document's date. It is stated as OQIRON's own reading of Articles 1(18) and 1(19) and should be treated as such by any party relying on it.

Two consequences of the assessment are material and are stated here because they bear on how the rest of this document should be read.

First, the PDPL's principal security obligations — Article 19 (security measures), Article 20 (breach notification) and Article 31 (records of processing activities) — are imposed on the Controller, not the Processor. This document therefore does not claim that MURAQIB complies with those articles. It states what MURAQIB provides to a Controller seeking to discharge them.

Second, Article 17(4) of the Implementing Regulation provides that a Processor which violates the Controller's instructions or the processing agreement shall be considered a Controller and held directly accountable. A processor's position is therefore conditional on its conduct, not fixed by its contract. This is addressed in Part 2.

1.6 Method

For each obligation or control in scope, this document states one of:

- **Supports** — MURAQIB provides something a deploying entity can use as evidence toward the control, described specifically
- **Partially supports** — MURAQIB provides something toward the control, with a stated limitation
- **Does not support** — MURAQIB provides nothing toward the control
- **Deploying entity's responsibility** — the control is organisational or environmental and falls outside what any governance rail can provide

Where a limitation is stated, it cross-references the corresponding item in Section 11 of the whitepaper. No limitation appears here that is not recorded there.

ECC subdomains addressed in Part 3 are those where a governance rail is either the subject of a control or a source of evidence toward one. Subdomains concerning cybersecurity strategy, physical security, project management and awareness and training are the deploying entity's responsibility in full, and are listed as such in Part 3 rather than mapped control by control. Human resources controls are addressed selectively rather than excluded: control 1-9-5, requiring that personnel powers be reviewed and revoked immediately on termination of employment, is one to which MURAQIB's user store and revocation path are directly relevant.

Part 2 — PDPL Alignment

2.1 How to read this Part

Every principal security obligation in the PDPL — Article 8 (selection and monitoring of processors), Article 19 (security measures), Article 20 (breach notification) and Article 31 (records of processing activities) — is imposed on the Controller. The Law imposes no direct security, breach-notification or record-keeping obligation on a Processor; those duties reach a processing system contractually, through Article 8 and Article 17 of the Implementing Regulation.

This Part therefore makes no claim that MURAQIB complies with those Articles. On OQIRON's assessment of its own position (Part 1.5), MURAQIB does not owe them. What this Part states is what MURAQIB provides to a Controller seeking to discharge them, and where it provides nothing.

2.2 Article 8 — Selection and monitoring of Processors

Article 8 requires a Controller to select only Processors providing the necessary guarantees, and to monitor their compliance. Implementing Regulation Article 17(3) adds that the Controller shall periodically assess the Processor's compliance, and may appoint an independent third party to assess and monitor that compliance on its behalf.

Supports. MURAQIB's evidence chain is verifiable by a party other than OQIRON. The verification tool is published under an open licence, the canonical form is specified in Appendix B of the whitepaper, and the anchor public key is published. A Controller, or an independent third party appointed under Article 17(3), holding an evidence bundle can confirm that the records are internally consistent and that the signed checkpoints were produced by the published key, without OQIRON's cooperation or consent.

This answers part of what Article 17(3) contemplates: the assessment can be performed against MURAQIB's records rather than against OQIRON's assurances. It does not answer all of it. The Article contemplates an assessor acting on the Controller's behalf, and the bundle that assessor examines is produced by OQIRON on request. The analysis is independent; the supply of material for it is not.

One dependency should be stated. The verification tool and the anchor public key are published and obtainable independently. This document set, which contains the canonical form specification in Appendix B, is not published; a Controller or its appointed assessor holds it because OQIRON provided it. The whitepaper states that the canonical form is also published with the verification tool, so an assessor holding only the tool should be able to proceed — but an assessor relying on Appendix B is relying on a document supplied by the party being assessed.

Limitation. Independent verification establishes that a chain is self-consistent and that its checkpoints carry a valid signature. It does not establish that the chain presented is the current one. A Controller who retains nothing of its own is trusting OQIRON's presentation. Meaningful independent assessment requires the Controller to retain checkpoint digests as they are issued, and to compare them against the chain later presented. Whitepaper §11.2.1 and Appendix B.6(e) state this; ADVISORY-2026-001 states it publicly, published alongside the verification tool at `github.com/oqiron/muraqib-verify` and readable

without an account. The advisory concerns a defect in verifier version 1.0.0, corrected in version 1.1.0, and puts the underlying point in the same terms: a chain of fingerprints proves consistency relative to a signature, and cannot establish that the signature is the most recent one issued.

Three further limitations bound what an assessor can establish, and each is recorded in the whitepaper. A chain cannot prove it has been shown in full, and withholding records permits concealment without falsification (§11.2.2, §11.2.3). The signing ceremony authenticates the database's claim about itself rather than an independent account of what occurred (§11.2.6). And the verifier's own provenance must be established independently: an assessor obtaining the verification tool must satisfy itself that the tool it holds is the published one (§11.2.12).

A fourth limitation bounds availability rather than analysis. There is no self-service path by which a Controller or its assessor can obtain an evidence bundle. Bundle generation is an operator action; no route emits one. An assessor therefore examines material supplied by the party being assessed, on a schedule that party controls. Whitepaper §11.2.19 records this.

Does not support. MURAQIB provides no attestation of its own operational compliance — no certification, no audited control report, no third-party assurance engagement. A Controller's Article 8 diligence on OQIRON as an organisation rests on this document set and on whatever contractual guarantees are agreed, not on external attestation.

2.3 Implementing Regulation Article 17 — the processing agreement

Article 17(1) requires the agreement between Controller and Processor to specify the purpose of processing, the categories of personal data, the duration, the Processor's commitment to notify the Controller of a personal data breach without undue delay, the position on foreign regulation and mandatory disclosure, and the identification of any subcontractors.

These are contractual terms, not technical controls, and MURAQIB provides nothing toward most of them. Three are informed by facts stated in this document set.

Categories of personal data. Part 1.4 states what MURAQIB processes across its three stores. A Controller drafting an Article 17(1) agreement can take the categories from that section rather than from a general description.

Duration. Retention of sealed evidence is unbounded, for the reasons given in Part 1.4 and addressed as a structural limitation in Part 4.2.3. A Controller must state this in the agreement rather than assume a defined retention period.

Sub-processors. A hosted deployment currently involves the following third parties. Article 17(5) requires prior Controller acceptance of sub-processors and advance notice with an opportunity to object; a Controller must treat each of these accordingly.

- **Amazon Web Services** — hosting of the production rail, `eu-central-1` (Frankfurt)
- **DigitalOcean, LLC** — recipient of encrypted backup archives, Frankfurt
- **Anthropic, PBC** — Arabic explanation generation
- **Resend** — operator alerting

- **Twilio** — SMS and messaging notification. Configured with live credentials; no dispatch observed in the retained logs.
- **Google (SMTP)** — email dispatch. Configured with live credentials and exercised ninety-nine times without a successful dispatch; the position is stated below.

None of these is disclosed to a customer today. Section 11.6.6 of the whitepaper records that no customer-facing list, processing agreement or privacy notice names any of them, and that MURAQIB's own policy catalogue contains controls requiring precisely this disclosure of the entities it governs. Section 11.6.6b records that no cybersecurity risk assessment of any of them exists.

The Anthropic path requires particular attention, and is stated as a historical fact rather than a latent capability. The Arabic explanation generator transmits the declared action summary, truncated to 200 characters, to that provider's API. It has executed 439 times between 16 February and 8 August 2026, evidenced by non-zero token costs recorded against the legacy evidence store across that period. The path is not reachable from the production clearance endpoint — that endpoint builds explanations locally — and the executions arose through the legacy endpoint, seeding and direct invocation. That bounds its future use, not its history.

This is a completed cross-border transfer of personal data, not a risk of one, wherever a transmitted action summary contained personal data. A Controller must assess it against Article 29 of the PDPL and the Data Transfer Regulation and state the position in the Article 17(1) agreement.

The Google SMTP path requires the same distinction and resolves differently. The journal records ninety-nine failed send attempts between 24 May and 4 August 2026, in three bursts, and no successful dispatch at any point. Every failure is a Gmail `421 4.3.0` transient server condition rather than a rejection of the message or its recipients, and no error carries a sender or recipient address, so neither the envelope sender nor any recipient was refused. The message is serialised and handed to the transport only after authentication succeeds, and the log does not record which stage of the SMTP session returned the 421. A connection to Google's mail service was therefore opened and credentials presented ninety-nine times; whether any message content or recipient address reached Google is not established from the record, and is recorded here as unestablished rather than as absent, on the same basis as the facts in Part 4.3.3.

2.4 Implementing Regulation Article 17(4) — the reclassification provision

Article 17(4) provides that a Processor which violates the Controller's instructions, or the processing agreement, shall be considered a Controller and held directly accountable for any violation of the Law.

This provision is stated here separately because it bears on why a Controller might deploy MURAQIB at all, and not merely on how MURAQIB is assessed.

A Controller deploying autonomous agents faces the risk that an agent processes personal data outside the Controller's instructions. Where the processing is performed by a Processor's system, Article 17(4) converts that deviation into direct Processor liability. Where it is performed by the Controller's own agents, it is a straightforward breach of the Controller's own obligations.

Supports. MURAQIB records the instruction and the decision before the action. A governed action carries a sealed record stating which policy applied and what verdict was returned. Where an agent proceeds against a refusal, the refusal is sealed and the record is outside the agent's control. A Controller can therefore establish, for governed actions, what its instructions were and whether a decision consistent with them was issued.

Where a four-eyes control applies and the calling system produces a signed assertion, the sealed record also carries the identities asserted as maker and authoriser. This applies to a minority of records: 29 of 433 sealed events carry a valued assertion, and six of eight active production agents are capable of producing one. A Controller should not read the assertion as a general property of governed actions.

Four limitations bound what the four-eyes record establishes, beyond the distinctness point stated elsewhere in this document. The rail does not independently verify the human behind an asserted identity (§11.3.1). The signature binds the assertion but does not bind the parameters of the action it authorises (§11.3.4). The absence of a signature does not distinguish a record that was not signed from one where a signature was not required (§11.3.7). And possession of a signing key does not establish that the intended process holds it, no workload attestation being built (§11.3.10).

Limitation, and it is material. MURAQIB is not an enforcement point. It does not prevent an agent from acting against a refusal, and an action never submitted to MURAQIB leaves no record at all. The evidentiary position it creates is strong for actions that were submitted and weak to absent for actions that were not. A Controller relying on MURAQIB for Article 17(4) purposes is relying on the completeness of its agents' submission behaviour, which MURAQIB does not enforce and cannot verify. Whitepaper §11.1.1 records this.

2.5 Article 19 — Security measures

Article 19 requires the Controller to implement organisational, administrative and technical measures to protect personal data.

Supports. Personal data in MURAQIB's evidence chain is protected against undetected alteration. A sealed record cannot be modified without breaking the chain, and the break is detectable by any party performing the verification described in Appendix B. Checkpoints are signed with a key held offline by a custodian and present on no OQIRON production host.

Access to the rail requires authentication. Agent credentials are per-agent and revocable. Nightly backups of the database, configuration and secrets are encrypted to a 4096-bit key before leaving the origin host, and the host holding those archives possesses no key capable of decrypting them.

Partially supports. Several measures a Controller would expect are absent, incomplete, or of unestablished status. Each is recorded in the whitepaper's limitations register:

- Confidentiality of evidence at rest depends on whether the underlying cloud volume is encrypted — a control-plane setting outside the application, which the whitepaper does not establish either way (§11.5.4). There is no application-layer or filesystem encryption beneath it. A Controller should establish the volume's encryption status directly rather than rely on either party's assumption.
- Tenant read isolation is not enforced. The machinery is proven and six routes are wired; twelve remain (§11.1.2). In a shared deployment, tenant separation is presently a property of the record rather than of

access control.

- Sixty-two percent of the sealed chain carries no tenant attribution, since attribution began part-way through the chain's life and cannot be applied retroactively without breaking seals (§11.5.9).
- Approval provenance is unsealed and alterable in place by the application role, without breaking any seal and without database superuser access (§11.2.18).
- A decision cannot be independently replayed: the record states what was decided, not that the verdict was the correct result of applying the recorded catalogue to the recorded inputs (§11.1.5).
- Nothing attests the deployed code. The policy catalogue, the application code and the service account are not separated: the service runs as the account that owns the application directory, and that account can write both the catalogue it enforces and the code that enforces it. A file written to the application directory becomes running code within roughly an hour, with no deployment gate. The signed catalogue pin does not cover the programs that compute and verify it, nor the evaluator that executes the catalogue (§11.4.3). Read with the preceding item, this is the mechanism by which a catalogue or evaluator could differ from what a record states.
- Credentials are present in historical plaintext backup archives and no rotation procedure exists for them (§11.1.6, §11.5.5, §11.5.6).
- API key storage uses unsalted SHA-256; the argument for its adequacy rests entirely on generation entropy (§11.5.7).
- There is no second authentication factor anywhere in the application, including for the most privileged human role (§11.5.7c).

A Controller assessing MURAQIB under Article 19 should read Section 11 of the whitepaper in full rather than this summary.

2.6 Article 20 — Breach notification

Article 20 requires the Controller to notify the Competent Authority upon knowing of a breach, and to notify affected Data Subjects where the breach would cause damage or prejudice their rights. Implementing Regulation Article 17(1) requires the Processor to commit to notifying the Controller without undue delay.

Supports. The evidence chain makes certain classes of interference detectable. An alteration to a sealed record breaks the chain; a wholesale re-sealing produces a tip that does not match the last signed checkpoint. The interval between signed checkpoints bounds the window in which an undetected rewrite could occur.

Detection is also partly automated. A monitoring timer runs at five-minute intervals and dispatches alerts on failure conditions, and a daily watcher raises an alert when the evidence chain's most recent anchor becomes stale.

Partially supports. These alerts are directed to OQIRON's operator. There is no notification path to a Controller, no alert a Controller receives, and no mechanism by which a Controller learns of a detected condition other than by asking or by performing verification itself (§11.5.19b).

Three behavioural detectors are implemented but have never produced a result (§11.5.8). Anchoring is operator-driven and checkpoint intervals have run to nearly four days and 135 events (§11.2.5), so the automated staleness alert bounds that interval rather than eliminating it.

Does not support. There is no defined notification timeline, no documented incident response plan, no escalation procedure, no severity model and no incident record type anywhere in the system (§11.5.19). A Processor's Article 17(1) commitment to notify the Controller without undue delay would rest on OQIRON's operational undertaking. The technical capability to detect exists and is running; the capability to notify a Controller does not.

2.7 Article 31 — Records of processing activities

Article 31 requires the Controller to maintain records of processing activities containing, at minimum: the Controller's contact details, the purpose of processing, a description of the categories of Data Subjects, any entity to which personal data has been or will be disclosed, whether data has been or will be transferred outside the Kingdom, and the expected retention period.

Supports. For governed actions, MURAQIB produces a durable, tamper-evident record of each processing decision: what was proposed, which policy applied, what was decided, when, and on whose asserted authority. This is a stronger artefact than Article 31 requires — the Article contemplates a register of processing activities, not a per-decision log — and a Controller can draw on it as evidence that its stated processing practices were in fact followed.

Does not support. MURAQIB does not maintain an Article 31 register. Individual evidence records carry facts bearing on two of the six required elements — a request reference identifying a recipient, and a flag indicating whether an action is external — but the register's six elements are Controller-level facts about the Controller's own processing, not per-decision facts. Contact details, stated purposes, Data Subject categories, disclosure recipients, transfer positions and retention periods are the Controller's to compile. MURAQIB records decisions about actions; it does not record the Controller's processing inventory. A Controller must maintain its Article 31 register separately.

Part 3 — NCA-ECC Alignment

3.0 Scope of this Part

ECC-2:2024 contains 108 controls. This Part maps 44 of them: those in subdomains where a governance rail is either the subject of a control or a source of evidence toward one.

The remaining 64 controls are the deploying entity's responsibility in full. They concern cybersecurity strategy, governance structures, risk management, project management, personnel security, awareness and training, physical security, and operational domains — asset management, email, network, mobile devices, vulnerability management, penetration testing, and business continuity — to which no governance rail contributes evidence.

One subdomain is excluded on a different basis and is named here rather than passed over. Subdomain 1-3, Cybersecurity Policies and Procedures, requires that policies be identified, documented, implemented, and reviewed at planned intervals with changes documented and approved. MURAQIB seals a policy catalogue digest into its records, maintains a policy change log, and has recorded one policy change event in the chain — so the rail does hold material bearing on this subdomain. It is not mapped because the subdomain concerns the entity's own cybersecurity policies, not the policy catalogue MURAQIB evaluates agent actions against; these are different artefacts that share a word. An entity should not read MURAQIB's policy provenance as evidence toward 1-3.

Subdomain 1-9 (Human Resources) is addressed selectively rather than excluded: control 1-9-5 concerns revocation of powers, to which MURAQIB's user store and credential revocation path are directly relevant.

Each control receives one of six verdicts. Four are the primary set: Supports, Partially supports, Does not support, and Deploying entity's responsibility. Two are used where none of those would be accurate. Not established is used where a control turns on a fact this assessment could not verify, and asserting either a positive or a negative would overstate what is known. Split is used where a control applies to more than one component of the deployment and those components reach different positions.

3.1 Subdomain 1-7 — Compliance with Standards, Laws and Regulations

1-7-1 — Identification of and compliance with nationally approved international agreements containing cybersecurity requirements

Does not support.

MURAQIB contains a jurisdiction registry enumerating twenty jurisdictions with their regulators and policy families, including a Saudi entry naming SAMA, CMA, NDMO, SDAIA, NCA, ZATCA and MHRSD. This registry is a mechanism for evaluating agent actions against jurisdictional rules. It is not a register of the operating entity's own commitments, and this control concerns the latter.

The distinction is stated rather than elided because the registry could be mistaken for support of this control. A deploying entity's identification of international agreements binding upon it is an obligation MURAQIB does not address.

Two limitations of the registry itself are recorded in the whitepaper and bear on any reliance placed on it elsewhere: the jurisdiction setting that gates two controls is a deployment-level environment value, not covered by the signed policy pin, not sealed into any record, and not logged when changed; and only one jurisdiction is defined in force, so changing the value has no present effect (§11.4.8).

3.2 Subdomain 1-8 — Periodical Review and Audit

1-8-1 — Periodic review by the entity's cybersecurity department of its own control implementation

Does not support.

MURAQIB evaluates agent actions against a policy catalogue at request time. It contains no review-cycle scheduler, no control-implementation register, and no attestation workflow. A deploying entity's periodic self-review is outside what the rail provides.

The absence is not confined to the deploying entity. Section 11.6.1c of the whitepaper records that no periodic review of any kind is scheduled or recorded in the deployment itself — not of access rights, agent credentials, policy content, configuration, or the controls set out in the whitepaper.

1-8-2 — Review and audit by parties other than the cybersecurity department, conducted independently

Partially supports.

This control turns on independence. MURAQIB produces records that a party outside the entity can verify without that entity's cooperation: the verification tool is published under an open licence, the anchor public key is published, and chain data is retrievable through dedicated routes. An external auditor can therefore check the evidence rather than accept an assertion about it — which is the property the control's independence requirement exists to secure.

MURAQIB does not conduct an audit, does not apply Generally Accepted Auditing Standards, and does not address conflict of interest. It supplies verifiable material to an audit; it is not one.

The limitations stated in Part 2.2 apply here identically. Verification establishes that a chain is self-consistent and that its checkpoints carry a valid signature; it does not establish that the chain presented is the current one, that it has been shown in full, or that the verification tool an auditor holds is the published one (§11.2.1, §11.2.2, §11.2.3, §11.2.12, Appendix B.6(e)).

1-8-3 — Documentation of audit results and presentation to the cybersecurity supervisory committee and Authorized Official

Does not support.

MURAQIB provides two kinds of export. The offline evidence bundle is generated from the sealed evidence chain and refuses to emit a file whose seals it cannot re-verify. The spreadsheet and PDF export routes are generated from the unsealed operational store and carry no seal. Both are exports of decision records. They carry no scope statement, no observations, no recommendations, no corrective actions and no remediation plans, and there is no committee-presentation workflow or addressee model. An entity may draw on exported evidence when preparing a report under this control; the report itself is the entity's work.

3.3 Subdomain 1-9 — Human Resources (control 1-9-5)

1-9-5 — Personnel powers reviewed and revoked immediately upon end or termination of employment

Partially supports.

Two revocation mechanisms exist and are in live use. Human user accounts carry a status enforced at authentication: an account not in active status is refused. Of eight accounts in the production deployment, seven are suspended and one active, so the mechanism is exercised rather than nominal. Agent credentials are revoked individually by setting a key inactive; of thirty registered keys, fourteen are active and sixteen revoked. Revocation propagates within a fifteen-second registry cache interval.

Two qualifications bound this.

Suspension is applied by exclusion. The mechanism sets to suspended every account not present in a supplied list of accounts to remain active, rather than acting on an individual termination. This is an effective control over who holds access; it is not a per-person termination workflow, and an entity describing it as one would be describing something else.

Revocation is manual. There is no integration with a human resources system, no joiner-mover-leaver feed, and nothing that triggers on a termination event. The control requires revocation immediately upon termination. MURAQIB provides the mechanism; the trigger is the deploying entity's, and the interval between a termination and a revocation is a function of the entity's process rather than of the rail.

3.4 Subdomain 2-2 — Identity and Access Management

2-2-1 — IAM requirements identified, documented and approved

Does not support. MURAQIB implements an access model; it does not hold a deploying entity's IAM requirements document or a record of its approval. Section 11.6.1b records that no requirements document exists for this or any other control domain in the deployment itself.

2-2-2 — IAM requirements implemented

Partially supports. MURAQIB implements identity and access management for its own surface: password authentication for human users, API-key and bearer-token authentication for agents, and a role model. This is evidence toward the control only insofar as MURAQIB is itself a system within the entity's scope. It implements nothing for the entity's wider estate.

2-2-3 — Minimum IAM requirements

2.2.3.1, single-factor authentication. Supports. Passwords are stored using bcrypt at cost 12 over a SHA-256 pre-hash. The whitepaper records the pre-hash arrangement and the argument for its adequacy (§11.5.10b).

2.2.3.2, multi-factor authentication. Does not support. No multi-factor mechanism is implemented anywhere in the application, and no code path exists into which one could be dropped (§11.5.7c). This is a verified absence, not an assumption. The most privileged human role — the account that creates users, issues and revokes agent credentials, and reads across tenants — authenticates by password alone, and this control specifically requires multi-factor for privileged accounts.

The host's remote access is separately configured: SSH accepts public keys only, with password and keyboard-interactive authentication disabled and intrusion-prevention jails active. A single valid key is sufficient, so this is single-factor by key rather than multi-factor. A deploying entity should not read host key-only access as satisfying the multi-factor requirement for privileged application accounts.

2.2.3.3, authorisation principles. Partially supports. A role model is in live use across seven roles, with per-role permission sets. API keys carry scopes, though only four distinct scope values are in use across thirty keys. At the database layer the application role is not a superuser and per-table grants are materially narrower than the aggregate: the evidence and checkpoint tables permit insert and select only.

Segregation of duties is enforced by the four-eyes distinctness test, which rejects an authoriser appearing in the maker set by either identifier or email. The limitation stated throughout this document set applies: the test operates over identities the calling system asserts, and cannot establish that two identifiers denote two people (§11.3.2).

Tenant attribution, distinct from tenant read isolation, is incomplete across the historical chain: sixty-two percent of sealed decisions carry no tenant identifier (§11.5.9). An entity assessing segregation across tenants should treat the historical record as unattributed rather than attributed to a default.

2.2.3.4, privileged access management. Partially supports. Role-level separation distinguishes privileged from ordinary administrative capability. There is no privileged access management system, no credential vaulting, no session recording and no just-in-time elevation (§11.5.10f).

2.2.3.5, periodic review of identities and access rights. Does not support. No review mechanism exists (§11.6.1c). Last-use timestamps are recorded on twenty-nine of thirty API keys, which is an input a reviewer could use rather than a review. The whitepaper records four of five legacy identities holding active credentials with no entry in the agent registry (§11.5.6) — precisely the condition a periodic review would surface, and evidence that none has been performed.

2-2-4 — IAM implementation periodically reviewed

Does not support (§11.6.1c).

3.5 Subdomain 2-3 — Information Systems and Processing Facilities Protection

2-3-1 — Protection requirements identified, documented and approved

Does not support (§11.6.1b).

2-3-2 — Protection requirements implemented

Partially supports, for MURAQIB's own surface only: TLS termination, request rate limiting, and fail-closed sealing. Nothing for the entity's workstations or wider infrastructure.

2-3-3 — Minimum protection requirements

2.3.3.1, protection from malware. Does not support within the guest. No anti-malware scanner, host intrusion detection system or file integrity monitor is installed on the instance, and nothing would report a modified binary, an added service or a new file in the application tree (§11.5.18). Whether the cloud provider operates malware detection outside the guest is not observable from within it, and is recorded here as unestablished rather than absent.

2.3.3.2, restriction on external storage media. Does not support. No kernel module for USB, FireWire or Thunderbolt storage is blacklisted or denied, no device-control software is installed, and no rule refuses a block device (§11.5.18b). No removable device is attached and the physical attack surface this control addresses is largely absent on a cloud instance, but the position rests on the environment rather than on anything configured.

2.3.3.3, patch management. Partially supports. Unattended upgrades are installed, enabled and running daily, so packages are applied without intervention. What is absent is a patch currency posture: automatic reboot is not enabled, so upgrades requiring one accumulate until an operator acts; no maximum age is defined for a pending upgrade; no reboot window is scheduled; and no threshold exists at which a pending upgrade or outstanding reboot becomes a finding (§11.5.22). As at the date of this assessment the host carries twenty-seven pending upgrades, none flagged as security updates, and a reboot is outstanding.

2.3.3.4, centralised clock synchronisation. Supports. The system clock is synchronised and the time service active, selecting the cloud provider's time synchronisation service as its source with public NTS servers as candidates. The control names SASO as an example rather than a requirement, and a provider time service is an accurate and trusted source within its terms.

One qualification with consequences elsewhere: the whitepaper records that rejection of stale authorisation assertions depends on a server clock that nothing independently attests (§11.3.6). The clock is synchronised; its trustworthiness is not attested to the rail.

2-3-4 — Implementation periodically reviewed

Does not support (§11.6.1c).

3.6 Subdomain 2-7 — Data and Information Protection

2-7-1 — Data handling requirements identified, documented and approved

Does not support. MURAQIB holds a policy catalogue with regulatory bindings, evaluated against agent actions at request time. This governs actions; it is not the entity's documented and approved data-handling requirements, and none exists for the deployment itself (§11.6.1b). The distinction is the same one drawn at control 1-7-1 and at subdomain 1-3, and is stated again because the catalogue invites the same misreading.

2-7-2 — Protection requirements implemented based on classification level

Partially supports, and the qualification is material.

A data sensitivity classification is captured on every governed action and sealed into the evidence record. Across 433 sealed decisions the distribution is 333 low, 87 medium, 11 confidential and 2 high. The classification is read by the risk scorer and weighted.

It does not affect what is permitted. The whitepaper records that the risk score has no authority — no control reads it, established by exhaustive sweep (§11.4.6) — and that data sensitivity sits among fifteen declared attributes that are recorded without affecting the verdict (§11.4.5). The classification is also declared by the calling agent rather than derived or verified.

So MURAQIB records classification and makes it auditable; it does not implement protection differentiated by classification. An entity relying on this control should not read the presence of a sealed classification field as evidence that handling differs by level.

2-7-3 — Implementation periodically reviewed

Does not support (§11.6.1c).

Two facts bear on this subdomain and are stated here rather than left to be rediscovered: evidence payloads are stored in plaintext, with no application-, column- or host-level encryption (§11.5.4), and whether the underlying storage volume is encrypted is not observable from within the instance.

3.7 Subdomain 2-8 — Cryptography

2-8-1 — Cryptographic requirements identified, documented and approved

Does not support. No cryptographic requirements standard or approval record exists (§11.6.1b). The anchor ceremony is documented as a runbook, and Appendix B of the whitepaper specifies the chain construction, but a specification of what was built is not an approved requirement stating what shall be built.

2-8-2 — Cryptographic requirements implemented

Supports, for MURAQIB's own surface. Cryptography is implemented across five purposes: SHA-256 for evidence chain hashing; Ed25519 in minisign prehashed mode over BLAKE2b-512 for anchor checkpoint signatures; Ed25519 for agent authorisation assertions; bcrypt at cost 12 over a SHA-256 pre-hash for

human passwords; and RSA-4096 under OpenPGP for backup archives. API keys are stored as unsalted SHA-256, and session tokens use HS256.

2-8-3 — Minimum cryptographic requirements

2.8.3.1, approved standards. Not established. Whether these primitives, their key lengths and their handling satisfy the NCA National Cryptographic Standards at the level this deployment would be assigned has never been checked against that standard's text, and no assessment record exists (§11.5.21). The statement here is neither conformance nor non-conformance: the question has not been asked.

The primitives in use are mainstream. Two would attract a reviewer's attention: API keys are stored as unsalted SHA-256, where the argument for adequacy rests entirely on generation entropy (§11.5.7), and session tokens use a symmetric algorithm, so any holder of the verifying secret can also mint tokens.

A deploying entity requiring NCS conformance should treat this as an open assessment item rather than a satisfied control.

2.8.3.2, secure key management across the lifecycle. Does not support. This is the weakest position in the mapping and the whitepaper records it in four places. No documented rotation procedure exists for any credential (§11.5.5). The anchor key — the key on which independent verification depends — has no rotation, revocation or compromise-response design, and the whitepaper lists this among the items that would stop a deployment (§11.1.4). Agent signing keys have an unwritten manual procedure with no revocation distinct from deregistration (§11.3.8). One key signs two different protocols without domain separation (§11.2.9).

Keys are generated and used correctly. They are not managed across a lifecycle.

2.8.3.3, encryption in transit and at rest. Partially supports. In transit is implemented: TLS 1.2 and 1.3 with an authenticated-encryption-only cipher list, with live negotiation confirmed at TLS 1.3. Backup archives are encrypted to a 4096-bit key before leaving the origin host.

At rest, evidence is stored in plaintext with no application-, column- or host-level encryption (§11.5.4). Whether the underlying storage volume is encrypted is not observable from within the instance and is not established here. The control requires encryption according to classification; as recorded at control 2-7-2, classification is captured but drives no protection decision, so no encryption differs by classification level.

2-8-4 — Implementation periodically reviewed

Does not support (§11.6.1c).

3.8 Subdomain 2-9 — Backup and Recovery

2-9-1 — Backup and recovery requirements identified, documented and approved

Does not support (§11.6.1b). The backup scripts carry extensive design rationale in comments; that is not a requirements document.

2-9-2 — Requirements implemented

Supports. A nightly backup timer is enabled and running, producing four artefact families: a database dump, cluster globals, a code and configuration archive, and a secrets archive encrypted at creation. A second timer pushes encrypted copies to a separate provider's host. Retention is by generation count rather than by elapsed time: the policy keeps thirty generations, and the dump, globals and configuration families each currently hold twenty-five, while the secrets archive holds two because code and secrets were separated only on 10 August 2026. Because more than one run has occurred on some days, twenty-five generations presently span nine days rather than twenty-five; under steady one-run-per-day operation thirty generations would approximate thirty days, but the window is a consequence of run frequency and not a configured period. Source-side presence checks abort a run if any member artefact is missing.

2-9-3 — Minimum requirements

2.9.3.1, scope covering critical assets. Partially supports. The database, cluster globals, application code and configuration, and secrets are covered. The host operating system is not. The manifest that describes a backup set does not travel off-box with it.

2.9.3.2, ability to perform quick recovery after an incident. Does not support. No recovery time objective or recovery point objective exists anywhere in the deployment. The whitepaper records the absence of both, together with the absence of tested disaster recovery, and lists this among the items that would stop a deployment (§11.1.3). Restoration of a database dump into a scratch instance is exercised weekly; recovery of the service is not exercised at all, and no target for it has been set.

2.9.3.3, periodic testing of recovery effectiveness. Supports, and this is the strongest position in the subdomain. An automated restore drill runs weekly. It restores a dump into a scratch database and verifies seventeen conditions: row counts against a manifest, chain integrity, anchor signatures, append-only trigger behaviour, database grants and credential behaviour. The most recent run passed all seventeen.

Its bound is recorded in Appendix A.2 and §11.5.13. The drill exercises only the locally retained plaintext artefacts. It performs no decryption, because the originating host holds no private key and cannot decrypt what it produces — the property that makes the off-box channel safe is the same property that leaves it untested. End-to-end recovery from the encrypted off-box channel has never been demonstrated.

2-9-4 — Implementation periodically reviewed

Partially supports. The weekly drill is a recurring test of recovery, which satisfies part of what this control seeks. No review of the backup arrangement itself — its scope, retention window, or objectives — is scheduled or recorded (§11.6.1c).

3.9 Subdomain 2-12 — Event Logs and Monitoring

This subdomain requires the log classes in the deployment to be assessed separately. They have materially different retention properties, and a single position would misdescribe all of them.

2-12-1 — Logging requirements identified, documented and approved

Does not support (§11.6.1b).

2-12-2 — Requirements implemented

Partially supports. Three log classes are implemented: the evidence chain, recording governance decisions; the system journal, recording service, authentication and application audit events; and web server access and error logs.

2-12-3 — Minimum requirements

2.12.3.1 and 2.12.3.2, activation for critical assets, privileged accounts and remote access. Partially supports. Event logging is active. The system journal captures service and authentication events including remote access, the web tier captures request events, and the application emits to a dedicated audit channel.

One gap is established rather than asserted: no mode-change record exists anywhere in the journal's retained window, despite that being the logged event for a privileged configuration change.

2.12.3.3, SIEM techniques for log collection. Does not support. Application, proxy, database and system logs stay on the machine that produced them. Nothing forwards them, nothing aggregates them across the two hosts, and kernel-level auditing is not installed, so privileged command execution, file access and configuration change leave no record independent of the operator performing them (§11.5.16). There is no collection point at which correlation across sources could occur.

2.12.3.4, continuous monitoring of event logs. Partially supports, and the qualification is where the substance lies. Two monitoring timers run: one at five-minute intervals with an alerting path, and one daily raising an alert when the evidence chain's most recent anchor becomes stale. Both are live and credentialled.

What they monitor is service health, chain anchoring staleness, and a fixed list of failure markers the deployment emits about itself. No rule set operates over the security event log as a class, and no correlation across sources occurs, which is what this control concerns. Separately, three behavioural detectors are implemented and have never produced a result (§11.5.8).

2.12.3.5, retention of at least twelve months. Split.

For the evidence chain: satisfied by construction. No purge job, scheduled deletion, or time-to-live exists, and the application role holds no delete permission on the evidence tables. Retention is unbounded. The chain's PostgreSQL lineage is approximately two months old and has therefore not yet accumulated twelve months of history, but nothing will remove records as it does.

For the system journal: not satisfied. The retained window is approximately 101 days against a 365-day requirement, bounded by disk consumption rather than by a configured period, and it shortens as log volume grows (§11.5.17). It is this class that carries the authentication, privileged access and remote access events the control names, and it is the only such record.

For web server logs: not satisfied. A fourteen-day rotation window.

A deploying entity should read this control as unsatisfied. The class that meets the requirement is not the class the requirement is about.

2-12-4 — Implementation periodically reviewed

Does not support (§11.6.1c).

3.10 Subdomain 2-13 — Incident and Threat Management

2-13-1 — Incident and threat management requirements identified, documented and approved

Does not support (§11.6.1b).

2-13-2 — Requirements implemented

Partially supports. Detection and operator alerting are implemented. No incident management process, case tracking, or classification exists; the deployment holds no incident, threat or indicator records of any kind.

2-13-3 — Minimum requirements

2.13.3.1, incident response plans and escalation procedures. Partially supports. Automated detection and alerting run continuously: a five-minute monitoring cycle with an alerting path, a daily anchor staleness check that raises an alert, and critical-level logging when a seal fails closed. These reach an operator mailbox.

No documented procedure states who is notified when the rail is compromised, degraded, or found to have decided wrongly. There is no severity model, no escalation path, no stated response time, and no record type for an incident anywhere in the system (§11.5.19). Alerting is detection, and detection is not response; nothing has been rehearsed.

2.13.3.2, incident classification. Does not support.

2.13.3.3 and 2.13.3.4, reporting incidents and sharing threat intelligence with the NCA. Does not support. This was checked specifically. There is no integration with the national reporting platform, no NCA endpoint, no reporting client and no submission format, and nothing receives, evaluates or acts on threat intelligence (§11.5.20). Every outbound destination configured anywhere in the deployment is enumerable and none is a regulatory one.

MURAQIB's policy catalogue contains rules citing NCA advisories, and can require an agent to evidence compliance with these very controls. That is content the rail evaluates. It is not a reporting path the entity operates, and the distinction should not be blurred.

2.13.3.5, threat intelligence feeds. Does not support (§11.5.20). No feed ingestion, indicator store or enrichment.

2-13-4 — Implementation periodically reviewed

Does not support (§11.6.1c).

3.11 Subdomain 2-15 — Web Application Security

2-15-1 — Requirements identified, documented and approved

Does not support (§11.6.1b).

2-15-2 — Requirements implemented

Partially supports. TLS termination, per-credential rate and concurrency limiting, a deny rule for sensitive file extensions, and four security response headers: frame options, content-type options, referrer policy and cross-site scripting protection.

2-15-3 — Minimum requirements

2.15.3.1, web application firewall. Does not support within the deployment. Requests reach the application through a reverse proxy that terminates TLS and applies rate limits and performs no request inspection: no module, no managed rule set, no signature matching, no anomaly scoring (§11.5.14). The application's own input handling is the entire defence. Whether a provider-side firewall sits in front of the origin is not observable from within the instance and is not claimed either way.

2.15.3.2, multi-tier architecture. Supports. Three tiers with the inner two bound to loopback: the web tier is publicly bound, the application tier and the database are reachable only from the host itself. Neither the application nor the database is directly addressable from the network.

2.15.3.3, secure protocols. Partially supports. TLS 1.2 and 1.3 with authenticated-encryption ciphers only; live negotiation confirmed at TLS 1.3.

Two gaps, both verified. There is no redirect from HTTP to HTTPS: the plaintext port returns a not-found response rather than upgrading the request. This is arguably safer than a redirect, but a client following a documented base URL over plaintext receives an error rather than the service. And no strict transport security header is present, so a browser that has once reached the service over TLS is never instructed to refuse plaintext on a later visit — which is precisely what defends the first request of a session, before any redirect can act (§11.5.15). Content security policy is also not set.

2.15.3.4, secure usage policy for users. Does not support. No acceptable use, terms of use, or usage policy page exists (§11.6.1d).

2.15.3.5, user authentication and authentication factors. Partially supports. Password authentication is implemented with bcrypt at cost 12 over a SHA-256 pre-hash. No multi-factor mechanism exists (§11.5.7c).

The sub-item requires factors to be defined on the basis of an impact assessment of authentication failure and bypass. No such assessment exists (§11.5.7d). The whitepaper records that cross-site protection on the clearance endpoint rests on the session cookie's same-site policy alone, with no token and no origin check (§11.5.7).

2-15-4 — Implementation periodically reviewed

Does not support (§11.6.1c).

3.12 Subdomain 4-1 — Third-Party Cybersecurity

4-1-1 — Third-party contract requirements identified, documented and approved

Deploying entity's responsibility. Contracts and their cybersecurity requirements are contractual instruments MURAQIB neither holds nor records.

4-1-2 — Minimum clauses in third-party contracts and agreements

Deploying entity's responsibility as to the drafting. One factual position bears directly on sub-item 4.1.2.1 and is stated here because a drafter must know it before agreeing a clause:

Secure removal of the entity's data upon end of service is not implementable against MURAQIB's evidence chain. The chain is append-only by construction, the application role holds no delete permission on the evidence tables, and retention is unbounded. A record cannot be removed without breaking the chain and rendering every subsequent record unverifiable. Any clause requiring secure deletion of processed data on service termination would conflict with the design of the product, not merely with its current configuration.

An entity requiring such a clause and OQIRON as a counterparty must resolve this before contracting, not after.

4-1-3 — Requirements for outsourcing and managed service providers

Sub-item 4.1.3.1, risk assessment before contracting. Does not support. No cybersecurity risk assessment of any third party in the delivery path is recorded anywhere in the deployment — no assessment document, no register, no table, no contractual artefact (§11.6.6b). The six providers named in Part 2.3 have been relied upon without any recorded evaluation.

Sub-item 4.1.3.2, managed monitoring and operations centres using remote access to be fully located in the Kingdom. Does not support, and this is a structural finding rather than a gap.

The monitoring and operations function — the periodic monitoring timers, the anchor staleness watcher, and administrative access to the host — operates on infrastructure located in Frankfurt, Germany, and administrative access is exercised from outside the region (§11.6.2).

This control is not satisfiable by documentation or configuration. For a Saudi entity subject to it, a hosted deployment on the current infrastructure does not meet the requirement, and an in-Kingdom deployment topology would be required. Part 4.2.2 states why that topology is not presently available.

4-1-4 — Third-party requirements periodically reviewed

Does not support (§11.6.1c). The agent registry records each agent's owner and human sponsor but implements no review cycle, expiry enforcement, or attestation.

3.13 Subdomain 4-2 — Cloud Computing and Hosting Cybersecurity

4-2-1 — Cloud and hosting requirements identified, documented and approved

Does not support (§11.6.1b).

4-2-2 — Requirements implemented

Partially supports. The deployment runs on two cloud providers, both in Frankfurt: the production rail on one, the encrypted backup destination on the other. Guest-side controls are implemented — transport encryption, key-only administrative access, intrusion prevention, and encrypted transfer off the host. Provider-side controls are not observable from within the instance and are not claimed.

4-2-3 — Minimum cloud requirements

Sub-item 4.2.3.1, protection according to classification and return of data in usable format. Partially supports. Data return is implemented: evidence is exportable in spreadsheet and document formats. OQIRON can produce a verifiable evidence bundle on request; there is no self-service path to one (whitepaper §11.2.19). Protection differentiated by classification is not implemented, for the reasons stated at control 2-7-2: classification is captured and scored but drives no protection decision, and evidence is stored in plaintext.

Sub-item 4.2.3.2, separation of the entity's environment from other entities' environments. Does not support, and the failure occurs before the question this control is usually asked about.

Nine virtual hosts are served from the production machine, six application listeners and one database instance share it, and one of those applications belongs to a separate system entirely (§11.5.10, §11.6.2). Separation therefore fails at the host level, which is within OQIRON's control, before any question arises about separation between cloud tenants at the provider level — a matter not observable from within the instance and not claimed here.

Combined with the tenant read isolation position recorded at control 2-2-3 and in Part 2.5, an entity requiring environment separation should treat the current hosted topology as not meeting this control.

4-2-4 — Implementation periodically reviewed

Does not support (§11.6.1c).

Part 4 — Gaps, Structural Limitations and Open Positions

4.1 How to read this Part

Parts 2 and 3 state, control by control, what MURAQIB provides and does not. This Part collects the findings a deploying entity should consider before rather than during an assessment, and separates them by kind, because they are not equally remediable.

Section 4.2 states three structural limitations. These are properties of the current architecture and deployment topology, not configuration gaps, and no documentation closes them.

Section 4.3 states positions OQIRON has taken which have not been externally confirmed.

Section 4.4 collects the remediable gaps identified in Parts 2 and 3.

Every limitation in this Part is recorded in Section 11 of the MURAQIB security whitepaper. Several were identified by this mapping exercise and added to that register before this document was issued.

4.2 Structural limitations

4.2.1 There is no enforcement point

MURAQIB issues decisions. It does not execute or block an action. An agent that receives a refusal and proceeds is not stopped, and an agent that does not submit an action is not observed (§11.1.1).

Every control mapped in Parts 2 and 3 as supported is a control over the record of a decision. None is a control over the performance of an action. An entity assessing MURAQIB as a preventive technical measure — under PDPL Article 19, or under any ECC control requiring that something be prevented — is assessing it for a property it does not have.

The evidentiary position this creates is set out in Part 2.4 and is substantial. It is not the same thing.

4.2.2 The hosted topology does not satisfy Saudi localisation requirements

Two findings combine, and neither is remediable by configuration.

ECC sub-item 4.1.3.2, within control 4-1-3, requires that managed monitoring and operations centres using remote access be fully located in the Kingdom. MURAQIB's monitoring and operations function runs on infrastructure in Frankfurt, Germany.

ECC sub-item 4.2.3.2, within control 4-2-3, requires separation of an entity's environment from other entities' environments. Nine virtual hosts share the production machine, including an application belonging to a separate system (§11.5.10). Separation fails at a layer within OQIRON's control, before any question about separation between cloud tenants arises.

Section 11.6.2 of the whitepaper records the position: production runs on a commercial cloud instance in Frankfurt, the secondary machine holding the encrypted off-box backups belongs to a second provider also in Frankfurt, and administrative access is exercised from outside the region. Nothing is deployed in

the Kingdom.

For a Saudi entity subject to these controls, the current hosted topology does not meet them. Meeting them would require an in-Kingdom deployment on dedicated infrastructure.

That alternative is not currently available and should not be read as one. Section 11.6.3 records that on-premise deployment does not exist, and that the claim of an identical clearance contract on-premise is architectural rather than observed. No such deployment has been built, and the equivalence between hosted and on-premise behaviour is asserted by design intent rather than demonstrated. An entity requiring in-Kingdom deployment is requiring something that would have to be built and proven, not selected.

4.2.3 Retention is unbounded and neither destruction nor legal hold is designed

MURAQIB's evidence chain is append-only by construction. No purge mechanism exists, the application role holds no delete permission on the evidence tables, and a record cannot be removed without breaking the chain and rendering every subsequent record unverifiable.

This is the intended position. Governance evidence is retained for the life of the accountability it supports, and immutability is the property the product exists to provide.

Article 18 of the PDPL bears on this in two directions, and MURAQIB has designed for neither.

Article 18(1) requires the Controller, without undue delay, to destroy personal data when it is no longer necessary for the purpose for which it was collected. This is a standing duty, not triggered by a data subject's request and not dependent on one being made. The Article permits retention beyond that point where the retained data contains nothing that could specifically identify the data subject — so de-identified retention is available in principle, though not as MURAQIB is built, since identities are sealed into records that cannot be rewritten. Data subject rights over personal data arise separately under Article 4, whose erasure right at 4(5) is itself expressed without prejudice to Article 18.

Article 18(2)(b) requires the opposite where data is closely related to a case before a judicial authority: the Controller shall retain it until proceedings conclude, and shall destroy it once those procedures are concluded. Governance evidence about a disputed action is exactly the material this contemplates. The provision is a deferral of the destruction duty, not an exemption from it — so it does not resolve the collision, it postpones the point at which MURAQIB cannot comply.

MURAQIB satisfies neither obligation by design. It cannot destroy on the expiry of purpose, and it cannot demonstrate a legal hold either — it retains everything unconditionally, which meets a hold's outcome by default rather than by any controlled or evidenced mechanism. A Controller cannot show that particular records were held because proceedings required it, only that nothing was ever removed.

Section 11.6.4 of the whitepaper records the position directly: sealed payloads contain human identities and business content, the chain is immutable by design, and no retention period, minimisation policy, legal-hold behaviour or approach to erasure is defined — compatible with evidentiary integrity, but requiring design that has not been done.

ECC sub-item 4.1.2.1, within control 4-1-2, requires third-party contracts to provide for secure removal of the entity's data on end of service. That clause is not implementable against the evidence chain.

Three facts bound the collision without resolving it.

First, the personal data in sealed records is narrow and enumerable. Every record carries the identifier and name of the calling agent and of the actor on whose behalf it acted, a request reference, and a free-text action summary; across the whole chain these resolve to eighteen distinct actor identifiers and fourteen distinct agent identifiers. Where a four-eyes assertion carries a value — twenty-nine of four hundred and thirty-three records — the assertion body additionally holds the authorising party's identifier and role, a flag recording whether that party is a section head, and the identifiers of the makers; an email address is present on seventeen of those records. Email addresses appear nowhere else in any sealed record. No field in any sealed record falls within the sensitive categories defined at Article 1(11) of the PDPL.

Second, the unsealed record fields, including approval provenance and generated explanations, are alterable and are not protected by the chain's immutability.

Third, a Controller retains discretion over what its agents place in an action summary, which is the field most likely to carry third-party personal data.

One further qualification bears on the immutability claim itself. Section 11.2.10 records that a database operator with schema privileges can remove the append-only triggers and delete rows freely, and that a superuser can delete evidence with nothing to recover it. The chain resists deletion by the application; it does not resist deletion by a privileged operator. This weakens the technical obstacle to destruction without making destruction a controlled or auditable operation.

OQIRON has not obtained a legal opinion on how an immutable evidence chain sits against Article 18's paired obligations. That assessment is outstanding and is the sharpest open question in this document.

4.3 Positions not externally confirmed

4.3.1 Processor status

OQIRON assesses its position in a hosted deployment as that of a Processor under Article 1(19) of the PDPL, for the reasons given in Part 1.5. This has not been confirmed by external legal opinion.

The assessment is material because Implementing Regulation Article 17(4) provides that a Processor which violates the Controller's instructions or the processing agreement shall be considered a Controller and held directly accountable. A Processor's position is conditional on its conduct.

4.3.2 Conformance with National Cryptographic Standards

Whether the cryptographic primitives in use satisfy the NCA's National Cryptographic Standards has never been checked against that standard's text, and no assessment record exists (§11.5.21). Part 3.7 states the primitives; it does not claim conformance. An entity requiring NCS conformance should treat this as an open assessment item.

4.3.3 Facts not observable from within the deployment

Five facts bear on controls in Part 3 and cannot be established from within the instance. They are recorded as unestablished rather than as present or absent: whether the underlying storage volume is encrypted at rest; whether the cloud provider operates host-level malware detection outside the guest; whether a

provider-side web application firewall sits in front of the origin; whether the provider separates virtual servers between tenants at the hypervisor; and the geographic location from which human operators connect.

The first is the most consequential and the most easily settled. An entity assessing MURAQIB under ECC sub-item 2.8.3.3 or PDPL Article 19 should establish the volume's encryption status directly from the cloud provider's console rather than rely on either party's assumption.

4.4 Remediable gaps

The following are gaps in implementation rather than architecture. Each is recorded in the whitepaper's limitations register.

Requirements documentation. No document states the cybersecurity requirement, and none has been approved, for any control domain the deployment touches — identity and access, systems protection, data protection, cryptography, backup and recovery, logging, incident management, web application security, or cloud (§11.6.1b). This is the parallel of the periodic review finding below: every subdomain mapped in Part 3 fails its requirements-documentation control as systematically as it fails its review control.

Access and identity. No second authentication factor anywhere in the application, including for the most privileged human role (§11.5.7c). No periodic review of identities or access rights; four of five legacy identities hold active credentials with no registry entry (§11.5.6). No privileged access management, credential vaulting, session recording or just-in-time elevation (§11.5.10f).

Key management. No documented rotation procedure for any credential (§11.5.5). The anchor key, on which independent verification depends, has no rotation, revocation or compromise-response design, and the whitepaper lists this among the items that would stop a deployment (§11.1.4). Agent signing keys have an unwritten manual procedure (§11.3.8). One key signs two protocols without domain separation (§11.2.9). Credentials are present in historical plaintext backup archives with no rotation procedure (§11.1.6).

Tenancy. Tenant read isolation is not enforced; six routes are wired and twelve remain (§11.1.2). Sixty-two percent of the sealed chain carries no tenant attribution and cannot acquire it retroactively (§11.5.9). In a shared deployment, tenant separation is a property of the record rather than of access control.

Evidence integrity. Approval provenance is unsealed and alterable in place by the application role without breaking any seal (§11.2.18). A decision cannot be independently replayed (§11.1.5), and nothing attests the deployed code (§11.4.3).

Logging and monitoring. No log collection, forwarding or correlation, and no kernel-level auditing, so privileged command execution leaves no record independent of the operator performing it (§11.5.16). System journal retention is approximately 101 days against a twelve-month requirement, bounded by disk consumption rather than policy, and it is this class that carries authentication and remote access events (§11.5.17). Content matching is confined to six named failure conditions the deployment emits about itself and one rate-limit pattern driving the login ban jail; nothing evaluates the security event log as a class (§11.5.16). Three behavioural detectors have never produced a result (§11.5.8).

Incident management. No documented response plan, escalation procedure, severity model or incident record type (§11.5.19). No reporting path to the national authority and no threat intelligence handling (§11.5.20). No notification path to a Controller, and no defined notification timeline (§11.5.19b).

Recovery. No recovery time or recovery point objective and no tested disaster recovery, which the whitepaper lists among the items that would stop a deployment (§11.1.3). End-to-end recovery from the encrypted off-box channel has never been demonstrated (§11.5.13).

Endpoint protection. No anti-malware scanner, host intrusion detection system or file integrity monitor is installed within the guest (§11.5.18). Whether the cloud provider operates detection outside the guest is not established (Part 4.3.3).

Removable media. External storage media are not restricted by any configured control (§11.5.18b). The physical attack surface is largely absent on a cloud instance and no removable device is attached, but the position rests on the environment rather than on anything configured.

Patch currency. Automatic patching is configured, enabled and running daily. What is absent is a patch currency posture: automatic reboot is not enabled, so upgrades requiring one accumulate until an operator acts; no maximum age is defined for a pending upgrade; and no threshold exists at which a pending upgrade or outstanding reboot becomes a finding (§11.5.22). As at the date of this assessment the host carries twenty-seven pending upgrades, none flagged as security updates, and a reboot is outstanding.

Web tier. No web application firewall within the deployment (§11.5.14). No strict transport security header and no content security policy (§11.5.15). No acceptable use policy (§11.6.1d). No documented impact assessment of authentication failure or bypass (§11.5.7d).

Sub-processors. Six third-party providers are involved in or configured for the hosted deployment, and none is disclosed to a customer (§11.6.6). None has been risk-assessed (§11.6.6b). One has received declared action summary text at a cross-border destination on 439 occasions; Part 2.3 states the position.

Periodic review. No periodic review of any kind is scheduled or recorded anywhere in the deployment — not of access rights, agent credentials, policy content, configuration, or the controls set out in the whitepaper (§11.6.1c). Every subdomain mapped in Part 3 contains a control requiring periodic review of its own implementation, and none is satisfied.

4.5 What this document does not do

It does not certify MURAQIB against either framework. Neither the PDPL nor the ECC provides for self-certification, and this is not one.

It does not assess OQIRON as an operating entity. The ECC's governance, personnel, physical security and business continuity domains are not mapped, and OQIRON's own conformance with them is not stated.

It does not substitute for a deploying entity's own assessment. It states what MURAQIB provides toward each control so that an entity's assessors have a starting position, and states plainly where it provides nothing.