**MCPX‑KendoBridge — RACI & Decision‑Rights Matrix**

**Document:** docs/14\_raci.docx  
**Project Code:** MCPX‑KendoBridge  
**Version:** 1.0.0 (Draft)  
**Last Updated:** 2025‑09‑24  
**Document Owner:** DoSE (Accountable) — DocFactory (Responsible)

**Purpose.** Define **who does what**—roles, decision rights, approvals, and communication cadence—for MCPX‑KendoBridge across the Technijian SDLC (**GitHub‑first**, four environments **Alpha → Beta → RTM → Prod**), with embedded guardrails (**No‑Hard‑Coding**, **Stored‑procedure‑only** DB access, **add‑only** migrations, secrets **only** in GitHub Environments/vendor portals). This RACI governs all documents, code, CI/CD, and runbooks and is referenced by the Evidence Pack and compliance audits.

**Compliance banner (applies to all roles/activities):** **Add‑only** schema; **SP‑only** DAL; **No‑Hard‑Coding**; **RTM validates on Prod DB (read‑only)**; secrets never in code/docs/DB. Approvals and Evidence Pack retention **≥ 1 year**.

**Document Control**

**Revision History**

| **Version** | **Date** | **Author/Role** | **Summary of Changes** |
| --- | --- | --- | --- |
| 1.0.0‑D | 2025‑09‑24 | DocFactory (R) | Initial comprehensive RACI, decision rights, approvals, comms |

**Approvals**

| **Name / Role** | **Responsibility** | **Signature / Date** |
| --- | --- | --- |
| Director of Software Engineering (DoSE) | Accountable (A) | \_\_\_\_ / \_\_\_\_ |
| Systems Architect (T‑Arch) | Consulted (C) | \_\_\_\_ / \_\_\_\_ |
| Security Lead | Consulted (C) | \_\_\_\_ / \_\_\_\_ |
| QA Lead | Consulted (C) | \_\_\_\_ / \_\_\_\_ |
| DevOps/SRE Lead | Consulted (C) | \_\_\_\_ / \_\_\_\_ |

**Table of Contents**

1. Roles & Definitions
2. Decision‑Rights & RACI Legend
3. Master RACI — Deliverables & Activities
4. Environment Promotions & Approvals (Alpha → Beta → RTM → Prod)
5. CI/CD Gates & Merge‑Queue Governance
6. Communication Cadence & Working Agreements
7. Escalation & Incident Roles
8. Access & Separation of Duties
9. Traceability to Controls (FR/NFR/Compliance)
10. Assumptions
11. Next Steps
12. Appendices (Sign‑off Templates & Checklists)

**1) Roles & Definitions**

| **Role** | **Abbrev** | **Description / Scope** |
| --- | --- | --- |
| **Director of Software Engineering** | **DoSE** | **Accountable** owner of quality gates, approvals, risk acceptance, and final release sign‑off. Oversees merge queue policies and Evidence Pack completeness. |
| **DocFactory** (Technijian SDLC Document‑Factory) | **DocFactory** | **Responsible** for generating/updating all SDLC docs, scaffolding CI/CD, OpenAPI, DB contracts, and runbooks; ensures GitHub‑first alignment and guardrails appear in every artifact. |
| **Systems Architect** | **T‑Arch** | **Consulted** on architecture, C4/DFD/STRIDE, session model, transport/legacy flag ADRs; reviews RTM parity strategy (Prod DB read‑only). |
| **Security Lead** | **SecLead** | **Consulted** on ASVS mapping, threat mitigations, CodeQL/Dependency Review/Secret Scanning policies; signs off on security exceptions. |
| **Dev Lead** | **DevLead** | **Responsible** for API/controllers, STDIO bridge, session registry, content negotiation, and error envelope implementation; supports perf tuning. |
| **QA Lead** | **QALead** | **Responsible** for test strategy, coverage targets, E2E/Gherkin, k6, axe, and release acceptance evidence. |
| **DevOps/SRE Lead** | **SRELead** | **Responsible** for workflows, deployments, environment protections, ingress/SSE config, monitoring, and 24‑hour post‑release checks. |
| **DBA / Data Architect** | **DBA** | **Consulted** and **Approver** for DB migrations and SPs; enforces **SP‑only** and **add‑only** rules; sets EXECUTE‑only grants. |
| **Ops Admin** | **OpsAdmin** | **Responsible** for read‑only ops UI usage, health/readiness checks, and promotion execution post‑approval. |
| **Product Owner** | **PO** | **Consulted** on scope/priorities and acceptance; input to backlog & release notes. |
| **Compliance Officer** (as required) | **CO** | **Consulted** on evidence retention, HIPAA mapping (if PHI‑adjacent), and audit playbook. |

**2) Decision‑Rights & RACI Legend**

**Legend**

* **R** = Responsible (does the work)
* **A** = Accountable (final decision/approval; one per row)
* **C** = Consulted (two‑way input)
* **I** = Informed (one‑way notification)

**Decision‑Right examples**

* **Security exceptions & compensating controls:** **A = DoSE**, **C = SecLead, T‑Arch**, **R = DevLead/SRELead**.
* **Schema/SP changes:** **A = DoSE**, **R = DBA**, **C = T‑Arch, DevLead**, **I = QA/SRE**.
* **Transport/Session ADRs:** **A = DoSE**, **R = T‑Arch/DocFactory**, **C = DevLead/SecLead**, **I = QA/SRE/PO**.

**3) Master RACI — Deliverables & Activities**

**Scope includes**: all default DocFactory outputs, gates, and runbooks. All activities must respect **GitHub‑first** processes, **No‑Hard‑Coding**, **SP‑only**, and **RTM on Prod DB** validation.

**3.1 Documents & Specs**

| **Deliverable / Activity** | **DoSE** | **DocFactory** | **T‑Arch** | **SecLead** | **DevLead** | **QALead** | **SRELead** | **DBA** | **OpsAdmin** | **PO** | **CO** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 01\_vision.docx | **A** | **R** | C | I | I | C | I | I | I | C | I |
| 02\_glossary.docx | A | **R** | C | I | I | I | I | I | I | C | I |
| 03\_actors\_usecases.docx | A | **R** | C | C | C | **C** | I | I | I | C | I |
| 04\_context.docx (C4/DFD/STRIDE) | A | **R** | **C** | **C** | C | I | I | C | I | I | I |
| 05\_fr.docx (Functional) | A | **R** | C | C | **C** | C | I | C | I | C | I |
| 06\_nfr.docx (Non‑Functional) | A | **R** | C | **C** | C | **C** | **C** | C | I | I | I |
| 07\_data\_contracts.docx (+ SQL/SPs) | A | **R** | C | C | C | I | I | **C/R (DB)** | I | I | I |
| 08\_ui\_ux.docx (UI SOP) | A | **R** | C | C | C | **C** | I | I | I | C | I |
| 09\_test\_strategy.docx | A | **R** | C | C | C | **R** | C | I | I | I | I |
| 10\_ci\_cd.docx | A | **R** | C | C | I | I | **R** | I | I | I | I |
| 11\_monitoring.docx | A | **R** | C | C | I | C | **R** | I | C | I | I |
| 12\_evidence\_pack.docx | A | **R** | I | **C** | I | **C** | **C** | I | I | I | **C** |
| 13\_compliance.docx | **A** | **R** | C | **C** | I | C | C | I | I | I | **C** |
| 14\_raci.docx (this doc) | **A** | **R** | C | C | I | I | I | I | I | I | I |
| ADRs (Transport/Legacy/Session/SP‑only/RTM) | **A** | **R** | **C** | **C** | C | I | I | C | I | I | I |

**3.2 API, Runtime & Security**

| **Activity** | **DoSE** | **DocFactory** | **T‑Arch** | **SecLead** | **DevLead** | **QALead** | **SRELead** | **DBA** | **OpsAdmin** | **PO** | **CO** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| OpenAPI 3.1 (servers Alpha/Beta/RTM/Prod; bearer; error envelope; lint/diff) | A | **R** | **C** | **C** | **C** | C | I | I | I | I | I |
| Error envelope governance | A | **R** | C | **C** | **R** | C | I | I | I | I | I |
| CORS/Origin allow‑list policy (from DB) | A | R | C | **C** | **R** | I | I | **C** | I | I | I |
| Secrets governance (license, SQL conn) | **A** | R | I | **C** | I | I | **C** | I | I | I | **C** |
| Security scanning (CodeQL/Deps/Secrets) | **A** | R | I | **C** | C | I | **R** | I | I | I | I |
| Evidence Pack completeness & audit | **A** | **R** | I | **C** | I | **C** | **C** | I | I | I | **C** |

**3.3 CI/CD, Deploy & Operate**

| **Activity** | **DoSE** | **DocFactory** | **T‑Arch** | **SecLead** | **DevLead** | **QALead** | **SRELead** | **DBA** | **OpsAdmin** | **PO** | **CO** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Branch protection & merge queue | **A** | R | I | I | I | I | **R** | I | I | I | I |
| Build & Test pipelines | A | **R** | I | I | **R** | **R** | **C** | I | I | I | I |
| Deploy Alpha → Beta → RTM → Prod | **A** | R | I | I | I | **C** | **R** | I | **R** | I | I |
| RTM parity on **Prod DB (RO)** | **A** | R | **C** | I | I | **C** | **R** | **C** | I | I | I |
| Monitoring & 24‑h post‑release checks | **A** | R | I | I | I | **C** | **R** | I | **R** | I | I |
| Runbooks (deploy/rollback/incident/license rotation/scale‑out) | A | **R** | **C** | C | C | C | **C/R (ops)** | C | **R** | I | I |

**Note:** In every activity, **No‑Hard‑Coding** and **SP‑only** rules apply; secrets are configured **only** through GitHub Environments or vendor portals—never in DB or source.

**4) Environment Promotions & Approvals (Alpha → Beta → RTM → Prod)**

**Approval map (per environment):**

| **Stage** | **Approver(s) (A)** | **Responsible (R)** | **Consulted (C)** | **Evidence Required** |
| --- | --- | --- | --- | --- |
| **Alpha** | DoSE | SRELead (deploy), DocFactory (docs) | QALead, DevLead | CI green; coverage targets; OpenAPI lint; SBOM; scans |
| **Beta** | DoSE | SRELead | QALead, DevLead | E2E pass; perf smoke; monitoring snapshot |
| **RTM** *(validates on* ***Prod DB (read‑only)****)* | **DoSE** | SRELead | DBA, T‑Arch | Parity report; /ready green; config snapshot; OpenAPI diff re‑run |
| **Prod** | **DoSE** + change window approver | SRELead (canary→rollout) | QALead, SecLead, T‑Arch | All gates green; Evidence Pack assembled; 24‑h post‑release plan queued |

**Promotion rules**

* No direct jumps; each promotion requires sign‑off and artifact checks.
* RTM must point to **Prod DB (read‑only)** for config parity prior to Prod approval.

**5) CI/CD Gates & Merge‑Queue Governance**

* **Required checks** on PR and merge‑queue batch: Build/Tests, **CodeQL**, **Dependency Review**, **Secret Scanning**, **SBOM**, **OpenAPI lint/diff**.
* **Blocking criteria:** any high‑severity dependency issue, secret leak detection, OpenAPI breaking change without ADR, or Evidence Pack deficiency.
* **DoSE** is **Accountable** for gate policy; **SRELead** implements and enforces; **DocFactory** ensures docs reflect gates and Evidence Pack schema.

**6) Communication Cadence & Working Agreements**

| **Rhythm** | **Participants** | **Purpose** |
| --- | --- | --- |
| **Daily** (15 min) | DevLead, QALead, SRELead, DocFactory | Coordination, blockers, deployment status |
| **Twice weekly** | DoSE, T‑Arch, SecLead, Leads | Risk review, ADRs, exception handling |
| **Pre‑promotion** | DoSE, SRELead, QALead, DBA | Gate checklist, evidence review |
| **Post‑release (24 h)** | DoSE, SRELead, QALead | SLO review (latency p50/p95, TTFB ≤ 200 ms, availability ≥ 99.9%), incident recap; attach snapshot to Evidence Pack |

**Working agreements**

* Changes touching API/DB/security **must** tag CODEOWNERS.
* All dynamic values via DB SPs; **no literals** in code, docs, or tests.
* Logs exclude secrets/PII; /config/effective returns **non‑secret** keys only.

**7) Escalation & Incident Roles**

| **Scenario** | **Primary** | **Secondary** | **Notes** |
| --- | --- | --- | --- |
| **P1 outage or SLO breach** | **SRELead** | DoSE | Page immediately; follow runbooks/incident.md; consider rollback; attach post‑mortem to release |
| Security finding (critical) | **SecLead** | DoSE | Open incident; evaluate compensating controls; update CI gates |
| DB change issue | **DBA** | SRELead | Enforce **add‑only**; revert migration via forward‑fix; verify SP signatures |
| SSE ingress breakage | **SRELead** | DevLead | Verify text/event-stream passthrough; TTFB/heartbeat checks |

**8) Access & Separation of Duties**

* **GitHub**: PRs require CODEOWNERS (API/DB/security paths). Merge queue enforces required checks before landing on main.
* **DB**: App principal has **EXECUTE on SPs only**; DBA controls migrations.
* **Secrets**: Maintained **only** in environment vaults; rotation requires DoSE approval and Ops execution; never exported to docs or logs.

**9) Traceability to Controls (FR/NFR/Compliance)**

| **Control** | **Accountability** | **Where Proven** |
| --- | --- | --- |
| **FR‑001** (Transport /mcp, streaming) | DoSE | OpenAPI 3.1, Test Strategy, Monitoring snapshot |
| **FR‑006** (Session model) | DoSE | Context & sequences, E2E Gherkin |
| **FR‑007** (Origin allow‑list) | DoSE | Data contracts (config key), tests, logs |
| **NFR‑Performance** (P50 ≤ 300 ms; P95 ≤ 800 ms) | DoSE | k6 reports, Monitoring snapshot |
| **NFR‑TTFB ≤ 200 ms** | DoSE | Streaming harness results, dashboards |
| **DB COMPLIANCE** (add‑only/SP‑only/No‑Hard‑Coding) | DoSE | Data contracts, grants scripts, Evidence Pack DB section |
| **Evidence retention ≥ 1 year** | DoSE | Evidence Pack, Release assets |
| (See docs 05/06/11/12/13 for full definitions.) |  |  |

**10) Assumptions**

1. GitHub Environments exist with required secrets and protection rules.
2. Ingress supports text/event-stream without buffering; keep‑alive and timeouts come from DB via SPs.
3. RTM uses **Prod DB (read‑only)** for parity validation; no writes in RTM.

**11) Next Steps**

1. Record named individuals to each role and publish CODEOWNERS coverage for /api/\*\*, /db/\*\*, /.github/\*\*, /runbooks/\*\*.
2. Add the RACI link to PR template and release checklist; require **DoSE** sign‑off before **RTM** and **Prod**.
3. Pilot a full Alpha→Prod cycle; verify approvals and Evidence Pack align with this RACI.

**12) Appendices**

**A) Sign‑off Template (Environment Promotion)**

Release: MCPX‑KendoBridge vX.Y.Z

Environment: [Alpha | Beta | RTM | Prod]

Checks:

- Build/Tests ✓ CodeQL ✓ Dependency Review ✓ Secret Scanning ✓ SBOM ✓

- OpenAPI lint/diff ✓

- RTM parity on Prod DB (RO) ✓ (RTM only)

- Monitoring snapshot attached ✓

Approvals:

- DoSE (A): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_

- SRELead (R): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_

- QALead (C): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_

- DBA (C): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_

Notes / Risks / Exceptions:

- [ ] None [ ] See attached exception with compensating controls

**B) PR Checklist (RACI hook)**

* **No‑Hard‑Coding**—all dynamic values from DB SPs (sp\_Config\_\*, sp\_Feature\_IsEnabled).
* OpenAPI updated; lint/diff passes; error envelope intact.
* Tests pass; coverage targets met; CodeQL/Dependency Review/Secret Scanning green.
* If DB touched: migration is **add‑only**; SP signatures stable; DBA consulted.

**C) Evidence Pack Linking**

* Ensure this RACI is included in **docs/14\_raci.docx** and referenced by **docs/12\_evidence\_pack.docx** so auditors can map **Accountability** to artifacts and approvals.

**Footer (optional for Word header/footer):**  
*MCPX‑KendoBridge • RACI & Decision‑Rights • Version 1.0.0 (Draft) • 2025‑09‑24 • Confidential — Technijian Internal*