Lifecycle Overview & Control Matrix

Document ID: MPG-002-LIFECYCLE-SUMMARY · **Version:** 1.0 · **Effective Date:** 2025-11-07
Owner: Project Management Office (PMO)

Purpose

This document summarizes the MPG-002 lifecycle phases, key deliverables, and control coverage across common industry frameworks (SOC/SOC 2, ISO 27001, NIST CSF, PCI DSS, HIPAA, ITIL/ISO 20000, WCAG 2.1). Use it as an executive reference, audit aide, and onboarding guide.

Phase Snapshot

Phase	Focus	Primary Deliverables	Gate Decision
Phase 1 – Initiation & Governance	Chartering, governance setup, team enablement	Charter, governance plan, communications plan, risk register, RACI	Phase 1 exit / move to Planning
Phase 2 – Planning & Requirements	Requirements elaboration, architecture design, schedule/cost baselines	Requirements baseline, RTM, architecture package, WBS, schedule/cost baselines	Phase 2 gate to Design/Build
Phase 3 – Design & Build	Detailed design, development, CI/CD, QA	Technical design updates, code baseline, test results, defect/debt register, security evidence	Sprint reviews / readiness for formal testing
Phase 4 – Testing, Release & Transition	Formal testing, release execution, hypercare	TRR/ RR packets, UAT results, performance/security reports, runbook, gate packet	Go-live / Phase 4 gate
Phase 5 – Operations & Continuous Improvement	Service operations, monitoring, benefits realization	Operational dashboard, incident/problem logs, CI backlog, benefits reports, compliance evidence	Quarterly SRB / annual lifecycle review
Phase 6 – Retirement & Decommissioning	Retirement planning, data disposition, shutdown	Retirement plan, data disposition plan, decommission logs, compliance/financial closure, lessons learned	Closure decision

---

Control Coverage Matrix

Control Area	Frameworks	Phase 1	Phase 2	Phase 3	Pl

Governance & Leadership	SOC/SOC 2 CC1, ISO 27001 A.5, NIST ID.GV	Charter, RACI, escalation SLAs	Requirements governance reviews	Sprint reviews, ADR approvals	Go/N sign
Risk Management	ISO 31000, SOC/SOC 2 CC2, NIST ID.RM	Risk register kickoff	Risk register refinement, mitigation plans	Sprint risk reviews	Test risk
Change & Release Management	ITIL/ISO 20000, SOC/SOC 2 CC8, PCI DSS 6	Change policy in governance plan	Impact assessments, change log	Branching, code reviews, SDLC controls	Rele cale eme char poli
Secure Development	SOC/SOC 2 CC7, ISO 27034, OWASP	N/A	Privacy/accessibility requirements	DRY/SOLID, secure coding, SAST/DAST evidence	Pen secu appl
Data Protection & Privacy	GDPR, HIPAA, SOC/SOC 2 P, PCI DSS 3	Data classification, consent plan	Privacy-by-design traceability	Encryption, minimization in design	Data mas UAT test
Monitoring & Incident Response	SOC/SOC 2 A, NIST DE/RS, ITIL Ops, SRE	Escalation paths	Monitoring requirements in design	CI logging, telemetry	Post mon hyp
Documentation & Naming	ISO 9001, internal policy	Naming rubric, onboarding	Documentation style guide	Code/document naming adherence	Rele artif nam
Accessibility & Inclusion	WCAG 2.1, Section 508	Charter accessibility goals	Accessibility acceptance criteria	Accessible component design, testing	Acc regr resu
Compliance & Audit Readiness	SOC/SOC 2, ISO 27001 Annex A, HIPAA, PCI DSS	Audit-ready approvals stored	Control matrix references	Security control evidence stored	Com pacl dep
Financial & Contract Governance	SOX 404, ISO 55001	Funding approvals, budget baseline	Cost baseline, estimation logs	Sprint burn-down, budget variance	Go- sum

Usage: Update control status quarterly or after major releases; highlight gaps in SRB meetings and assign corrective actions.

Master Artifact Inventory

Artifact	Phase	Storage Path (relative)	Control Areas
Charter	Phase 1	`/docs/phase-1/...`	Governance, Risk
Governance Plan	Phase 1	`/docs/governance/...`	Governance, Change
Stakeholder Register	Phase 1	`/docs/phase-1/...`	Governance
Communications Plan	Phase 1	`/docs/communications/...`	Governance
Requirements Baseline	Phase 2	`/docs/phase-2/requirements/`	Governance, Privacy
RTM	Phase 2	`/docs/phase-2/rtm/`	Traceability, Risk
Architecture Package	Phase 2	`/docs/phase-2/architecture/`	Secure Development
WBS & Schedule Baseline	Phase 2	`/docs/phase-2/planning/`	Governance
Sprint Plans & Reports	Phase 3	`/docs/phase-3/planning/`	Change, Secure Development
Test Results & Coverage	Phase 3 & 4	`/docs/phase-3/quality/`, `/docs/phase-4/testing/`	Secure Development, Quality
Security Evidence Packs	Phases 3–6	`/docs/phase-#/security/`	Security, Compliance
Runbooks & Release Notes	Phase 4	`/docs/phase-4/release/`	Change, Operations
Operational Dashboard	Phase 5	`/docs/phase-5/operations/`	Operations, Compliance
Incident/Problem Logs	Phase 5	`/docs/phase-5/operations/`	Operations
Benefits Report	Phase 5	`/docs/phase-5/governance/`	Value Realization
Retirement Plan & Logs	Phase 6	`/docs/phase-6/...`	Governance, Compliance
Lessons Learned	All	`/docs/phase-#/closure/`	Knowledge

Audit Evidence Checklist

- Control matrix (above) updated with links to artifacts and last review date.
- SOC/SOC 2 / ISO 27001 crosswalk stored in `/docs/phase-5/governance/control_crosswalk.xlsx`.

- For each release, maintain a “Release Evidence Pack” (Phase 4) referencing requirements, tests, approvals, deployment logs, and monitoring snapshots.
- For each retirement, archive “Retirement Evidence Pack” (Phase 6) containing data disposition, access revocations, financial closure, and lessons learned.
- Ensure all approvals (electronic signatures, emails) are exported to `/docs/approvals/phase-#/` with version-aligned filenames.

Quick Reference: Industry Standards Mapping

Standard / Guidance	Primary Phases Impacted	Notes
SOC/SOC 2 Trust Services Criteria	All	Control mapping per matrix; maintain evidence packs.
ISO 27001 / Annex A	1–6	Align governance, access control, operations, supplier management.
NIST CSF	1–6	ID/PR/DE/RS/RC activities distributed across phases.
ITIL 4 / ISO 20000	1, 4, 5, 6	Change, release, incident, problem, service management workflows.
PCI DSS	2–6	Secure development, testing, operations, retirement evidence.
HIPAA	2–6	Privacy impact assessments, access controls, data retention/destruction.
WCAG 2.1 / Section 508	2–5	Accessibility baked into requirements, design, testing, operations.
SOX 404	1–6	Financial approvals, change management, segregation of duties, logs.

Acronyms and Abbreviations

- **ADR:** Architecture Decision Record - Document capturing design choices and rationale
- **BA:** Business Analyst - Role responsible for requirements gathering and analysis
- **CAB:** Change Advisory Board - Governance body approving significant changes
- **CI/CD:** Continuous Integration/Continuous Delivery - Automated pipeline for build, test, and deployment
- **CMDB:** Configuration Management Database - Repository of IT assets and their relationships
- **DRY:** Don't Repeat Yourself - Software development principle emphasizing code reuse
- **GDPR:** General Data Protection Regulation - European Union data protection and privacy regulation
- **HIPAA:** Health Insurance Portability and Accountability Act - U.S. healthcare data protection regulation
- **ISO 20000:** International standard for IT service management
- **ISO 27001:** International standard for information security management systems
- **ISO 27034:** International standard for application security
- **ISO 31000:** International standard for risk management

- **ISO 55001:** International standard for asset management
- **ISO 9001:** International standard for quality management systems
- **ITIL:** Information Technology Infrastructure Library - Framework for IT service management
- **NIST CSF:** National Institute of Standards and Technology Cybersecurity Framework - U.S. cybersecurity framework
- **OWASP:** Open Web Application Security Project - Non-profit organization focused on web application security
- **PCI DSS:** Payment Card Industry Data Security Standard - Security standard for payment card data
- **PM:** Project Manager - Role responsible for project coordination and delivery
- **PMO:** Project Management Office - Organizational unit ensuring adherence to standards and methodologies
- **RACI:** Responsible, Accountable, Consulted, Informed - Matrix defining roles and responsibilities
- **RTM:** Requirements Traceability Matrix - Document linking requirements to design, tests, and deployment
- **SAST/DAST:** Static Application Security Testing / Dynamic Application Security Testing - Security testing methodologies
- **SDLC:** Software Development Life Cycle - Process for planning, creating, testing, and deploying software
- **SLA:** Service Level Agreement - Contractual commitment to service performance levels
- **SLO:** Service Level Objective - Target metric for service performance
- **SME:** Subject Matter Expert - Individual with specialized knowledge in a particular domain
- **SOC/SOC 2:** System and Organization Controls - Framework for security, availability, and confidentiality controls
- **SOLID:** Software design principles (Single Responsibility, Open/Closed, Liskov Substitution, Interface Segregation, Dependency Inversion)
- **SOX 404:** Sarbanes-Oxley Act Section 404 - U.S. financial reporting and internal controls regulation
- **SRB:** Service Review Board - Quarterly governance meeting overseeing operations
- **SRE:** Site Reliability Engineering - Discipline combining software engineering and operations
- **TRR:** Test Readiness Review - Meeting confirming prerequisites for formal testing
- **UAT:** User Acceptance Testing - Testing performed by end users to validate business requirements
- **WBS:** Work Breakdown Structure - Hierarchical decomposition of project scope into manageable components
- **WCAG 2.1:** Web Content Accessibility Guidelines 2.1 - International standard for web accessibility

---

Maintenance

- PMO updates this document quarterly or after significant methodology / compliance changes.
- Control owners must review entries for accuracy prior to audits or executive reviews.
- Suggested storage path for crosswalk artifacts: `/docs/phase-5/governance/` .