International Journal of Engineering & Scientific Research
Vol.13 Issue 12, December 2025
ISSN: 2347-6532 Impact Factor: 8.076
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

A Human-Centered Continuity Platform for Public Universities: Design, Governance, and Measured Operational Impact

Author: Mallesh Miryala | University of California
Contact: miryalaca@gmail.com | 415-412-2022

Abstract

Public universities manage complex, distributed operations—teaching, research, healthcare, and statewide programs—while facing a growing risk landscape. Continuity artifacts (plans, runbooks, dependencies, exercises, corrective actions) often fragment across spreadsheets, document drives, and ticketing tools, eroding ownership and slowing response. This paper specifies a human-centered continuity platform and operating model that unifies continuity, emergency management, IT disaster recovery (ITDR), facilities readiness, and resource rostering within a governed lifecycle. We present a reference architecture (Edge Sensing → Privacy Gateway → Fusion & State → Policy Engine → UX Adapter) underpinned by an "audit bus" that records versions, rationales, and overrides. A dependency model spanning applications → services → infrastructure → facilities → people enables restore sequencing and impact analysis without over-constraining local autonomy. A predictable governance cadence (quarterly releases, change advisories, office hours) is paired with adoption mechanics (two-minute release videos, one-page change notes, "what changed for me?" cues) and a concise measurement set (plan currency, dependency coverage, attestation on-time rate, and corrective-action closure time). In multi-campus deployments, the approach improved transparency, shortened cycle times, increased dependency completeness, and preserved comparability across autonomous entities. We provide reusable figures, checklists, counting rules, and a rollout playbook that readers can adopt without referencing any specific institution.

Keywords: business continuity, emergency preparedness, IT disaster recovery, facilities readiness, public universities, governance, human-centered systems

1. Introduction & Problem Statement

Public university systems operate at the intersection of academic calendars, clinical obligations, research laboratories, and public service. Each domain maintains its own lifecycles, constraints, and regulatory drivers. Continuity materials—unit plans, runbooks, application dependency maps, exercise records, and corrective actions—often live in separate tools or ad-hoc documents. When ownership is unclear and evidence is scattered, leaders lack confident roll-ups; when an incident occurs, restore sequencing and escalation paths can stall.

The core problem is not a lack of artifacts but a lack of **coherence**: artifacts are not identity-linked, guardrails are implicit, and metrics drift over time. This paper proposes a practical, human-centered platform and operating model that (i) binds every artifact to accountable people and roles, (ii) makes policy guardrails visible and explainable, (iii) enforces a minimal but durable lifecycle, and (iv) measures a small, stable set of outcomes that remain comparable across autonomous entities.

2. Human-Centered Design Principles

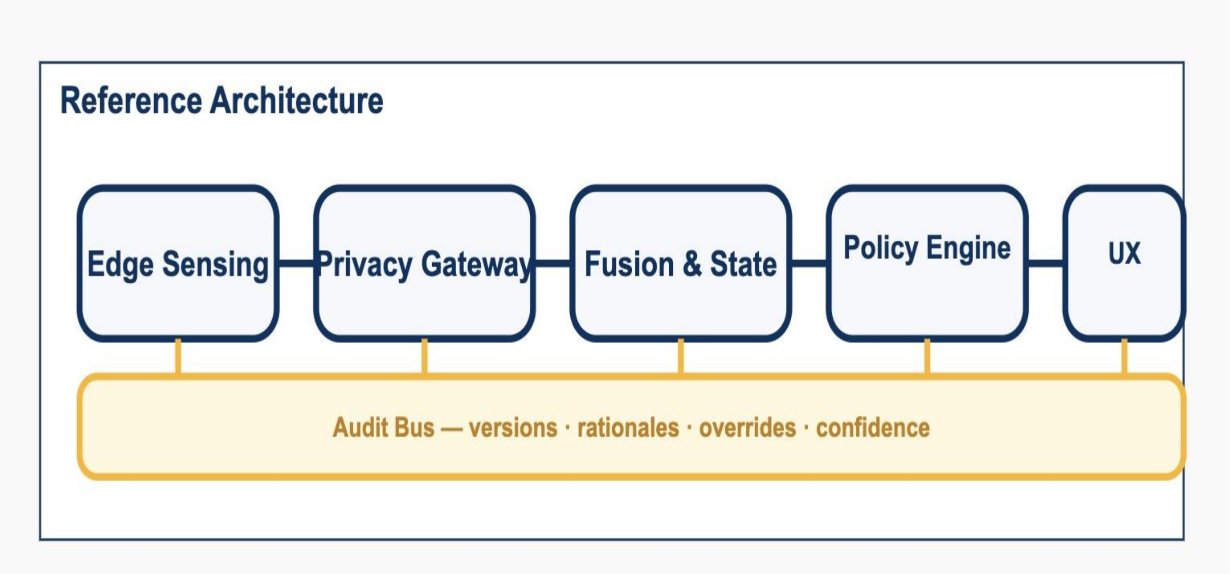
Identity-linked ownership. Every plan, runbook, dependency, and attestation is tied to a person, a role, and a stewarding unit so escalation never dead-ends.
Explainable guardrails. System prompts (e.g., "dependency is stale," "attestation overdue") render the rule and version that triggered them; users learn the "why," not just the "what."
Minimal cognitive load. Releases ship with two-minute videos, one-page change notes, and role-specific "what changed for me?" cues.
Stable interfaces, local flexibility. Standard fields/events support systemwide roll-ups; local adapters preserve each campus's legitimate uniqueness.
Learning loop. Exercises produce observations; observations become corrective actions (CAPA); CAPA closure is verified with evidence and tracked in dashboards.
Durability under turnover. Versioned runbooks, audit trails, and attestation reminders keep the organization resilient to staffing changes.

3. Reference Architecture (with Audit Bus)

The platform connects five modules in a left-to-right chain with rounded, flat visuals: **Edge Sensing → Privacy Gateway → Fusion & State → Policy Engine → UX Adapter**. A gold **Audit Bus** beneath records versions, rationales, overrides, and confidence signals.

- **Edge Sensing.** Listens to lifecycle events (draft→review→approval→exercise→CAPA→attestation), dependency deltas, identity changes, and telemetry from connected systems (e.g., status feeds).
- **Privacy Gateway.** Redacts sensitive notes and scopes visibility by role, unit, and purpose.
- **Fusion & State.** Normalizes inputs into a consistent readiness state: plan currency, dependency completeness, CAPA aging, and risk markers.
- **Policy Engine.** Applies explainable guardrails (e.g., minimum coverage for dependencies, required attestations) and produces user-facing prompts.
- **UX Adapter.** Surfaces dashboards, runbooks, bulk actions, and APIs; supports exports for audit and analytics.

Reference Architecture



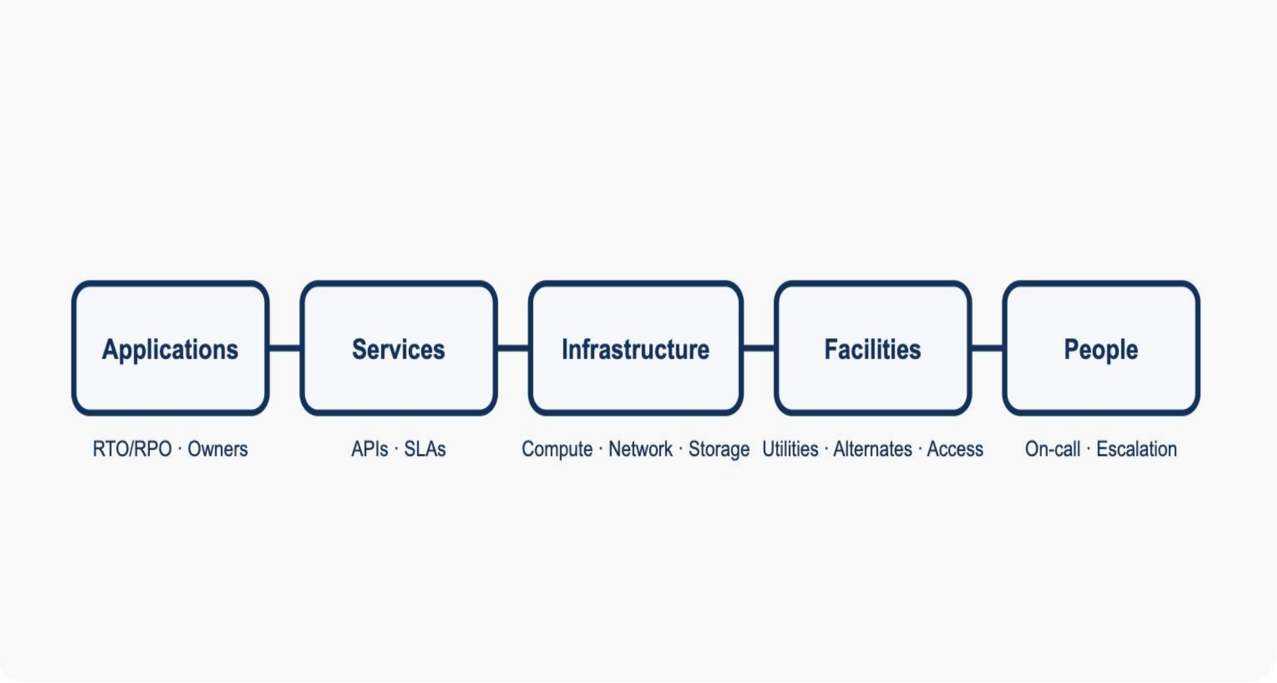
4. Dependency Model: Apps → Services → Infrastructure → Facilities → People

Continuity work becomes practical when leaders can trace "what breaks what." The platform models a five-link chain:

- **Applications.** Functional owners, RTO/RPO targets, data criticality, and interface inventory.
- **Services.** Identity, messaging, or integration brokers with SLAs and error handling; bindings to the apps that consume them.
- **Infrastructure.** Compute, storage, network, platforms; capacity/HA notes, failover patterns, and maintenance windows.
- **Facilities.** Buildings, labs, utilities (power, chilled water, medical gases), alternates, access constraints, hazards (seismic, flood, wildfire) and mitigation status.
- **People.** On-call rotations, escalation trees, coverage windows, and required skills/clearances.

This chain enables restore sequencing and "blast radius" analysis during incidents, while also powering dashboards that make dependency gaps visible before an event.

Dependency Chain



5. Planning Lifecycle & Evidence

The platform enforces a **governed lifecycle**:

1. **Draft.** Define scope, owners, dependencies, and initial risk/impact.
2. **SME Review.** Domain experts (IT, facilities, safety) validate assumptions and coverage.
3. **Leadership Approval.** Accountability, resourcing, and exercise plan are confirmed.
4. **Exercise.** Table-tops or technical failovers; attach evidence (logs, screenshots, minutes).
5. **CAPA.** Capture corrective actions with owners and due dates; verify closure.
6. **Attestation.** Quarterly attestation of plan currency and dependency completeness.

Evidence attaches at each gate and is immutable; dashboards elevate overdue items and stalled CAPA.

6. Security, Privacy Gateway, and Access Governance

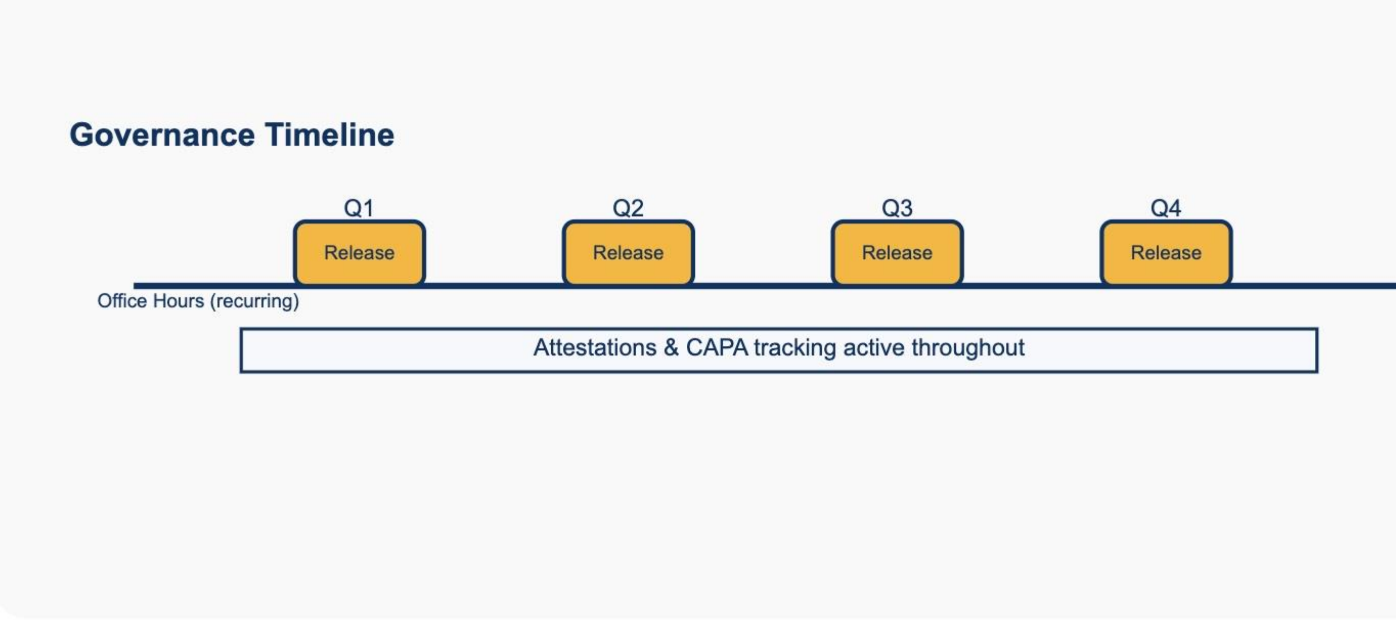
Least privilege & SoD. Separate editing, approving, and access-control roles reduce risk. **Audit trail.** Immutable logs cover edits, approvals, CAPA closures, and access changes. **Privacy Gateway.** Redacts notes while preserving decision context; supports need-to-know views.
Access reviews. Attestation cycles include access verification; expired access auto-revokes.

7. Governance & Release Cadence

A consistent quarterly cadence keeps changes comprehensible and safe:

- **Change Advisory Board (CAB).** Reviews risks, tests, rollbacks, and communications.
- **Release notes.** One page per release; plus role-specific "what changed for me?" callouts.
- **Office hours.** Weekly; Q&A feeds a searchable FAQ with annotated screenshots.
- **Runbooks.** Versioned with owners and last-verified dates.
- **Stable windows.** Align release windows with academic/clinical cycles to avoid disruption.

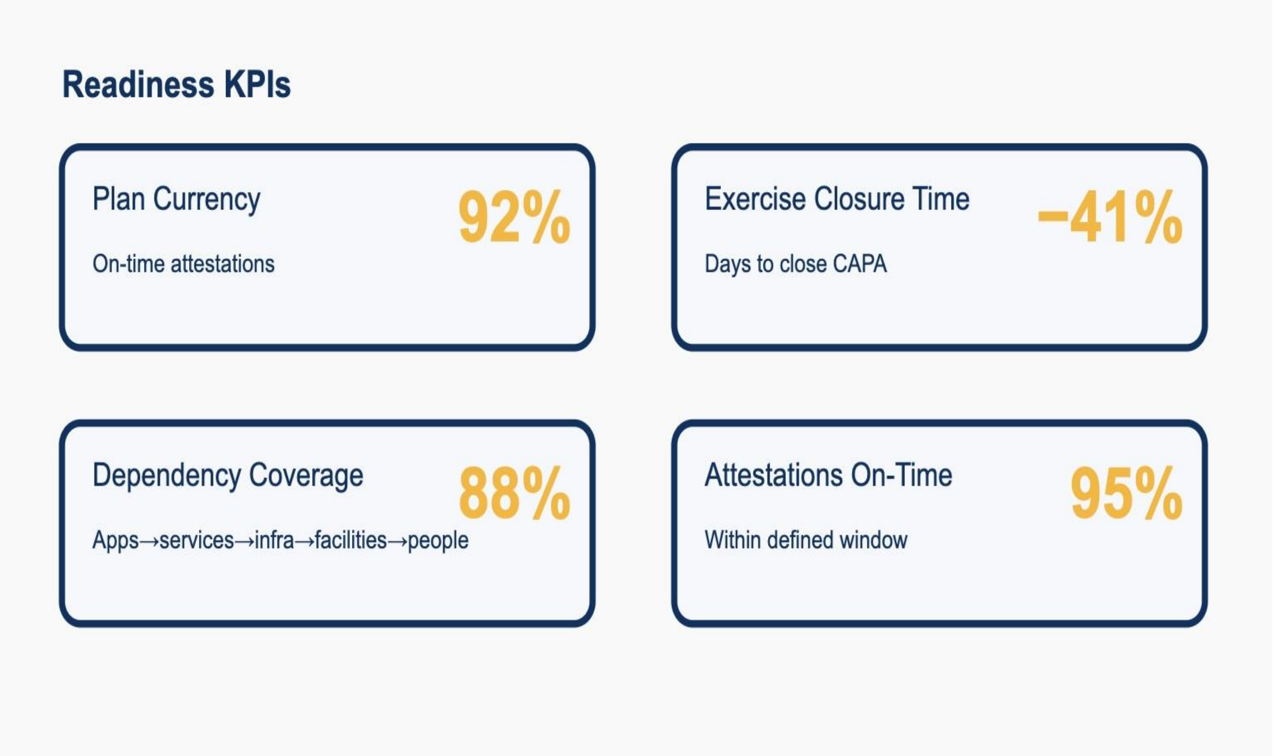
Quarterly Governance Timeline



8. Adoption & Enablement

One-time training decays; enablement must be continuous. Each release includes a two-minute video and a one-page change note, with "what changed for me?" sections for planners, administrators, and executives. Weekly office hours answer questions; a monthly "feature in practice" session showcases a concrete use case (e.g., mapping a new dependency chain or closing CAPA). Questions feed an indexed FAQ with screenshots. Runbooks are living documents with owners and last-verified dates to survive turnover.

Readiness KPI Dashboard



Readiness KPIs

Plan Currency 92%
On-time attestations

Exercise Closure Time −41%
Days to close CAPA

Dependency Coverage 88%
Apps→services→infra→facilities→people

Attestations On-Time 95%
Within defined window

9. Measured Operational Impact

A small, stable set of metrics enables comparison across autonomous entities:

- **Plan Currency (%).** Plans with current attestations and no overdue CAPA ÷ total in scope.
- **Dependency Coverage (%).** Plans with complete chain (apps→services→infra→facilities→people) ÷ total in scope.
- **CAPA Closure Time (days).** Median days from CAPA creation to verified closure.
- **Attestations On-Time (%).** Attestations completed within the window ÷ due in window.

Counting rules (Appendix A) prevent drift: definitions do not change across quarters, and revisions are versioned. Dashboards elevate laggards and celebrate improvements.

10. Rollout Playbook (First Two Quarters)

Month 0–1 — Discovery & Baseline. Inventory plans, dependencies, and current metrics; identify must-keep local fields versus global standards; publish metric definitions.

Month 2 — Pilot. Onboard two to three diverse units (e.g., one academic, one research, one hospital-adjacent); run a small exercise; gather feedback on prompts and runbooks.
Month 3 — Release 1. Ship the first standardized lifecycle with guardrails; add KPI tiles; begin weekly office hours.
Month 4–5 — Expansion. Onboard additional units; add dependency coverage reporting; tighten access reviews.
Month 6 — Release 2. Introduce attestation windows and CAPA dashboards; publish before/after metrics; tune nudges based on adoption patterns.

11. Limitations & Risks

- **Data quality variance.** Older artifacts require backfill; mitigated through attestation nudges and targeted coaching.
- **Customization creep.** Excess local fields undermine comparability; mitigated with adapters and a change advisory review.
- **Facilities heterogeneity.** Laboratory and clinical spaces vary widely; mitigated through minimum "facility profile" requirements and hazard tags.
- **Over-notification.** Too many prompts cause fatigue; mitigated by bundling alerts and suppressing duplicates.

12. Related Guidance & Standards (practical alignment)

- **NIST SP 800-34 Rev.1** (contingency planning) — lifecycle and roles.
- **ISO 22301** (business continuity management systems) — requirements for currency, exercises, and improvements.
- **FEMA NIMS / CPG-101** — incident command and planning practices relevant to exercises and AAR/CAPA.

13. Conclusion

Resilience improves when ownership is visible, guardrails are explainable, evidence is auditable, and learning loops are enforced. The platform and operating model described here balance systemwide comparability with local autonomy, converting continuity from scattered documents into a measurable, durable practice. The provided figures, templates, and counting rules give public systems a ready blueprint for adoption.

Appendices

Appendix A — Metric Definitions & Counting Rules

- **Plan Currency (%).** Numerator: plans attested within the defined window and with no overdue CAPA. Denominator: all in-scope plans. Edge cases: retired plans are removed from the denominator only after formal de-scoping with an audit note.

- **Dependency Coverage (%).** Numerator: plans with complete chain (apps→services→infra→facilities→people). Denominator: in-scope plans. Partial chains do not count.
- **CAPA Closure Time (days).** Median days from creation to verified closure; "verified" requires evidence and approver sign-off.
- **Attestations On-Time (%).** Numerator: attestations submitted within the window. Denominator: attestations due in the window. Extensions are rare and must be recorded.

Appendix B — Lifecycle Gate Checklists (abbrev.)

- **Draft.** Owner assigned; dependency seed; scope statement; initial risk/impact.
- **SME Review.** IT, facilities, and safety validations; gaps flagged.
- **Approval.** Executive owner & funding path; exercise plan agreed.
- **Exercise.** Scenario, objective, results, AAR notes, evidence attached.
- **CAPA.** Root cause, corrective step, owner, due date, verification.
- **Attestation.** Date, steward, exceptions, dependency deltas.

Appendix C — Adoption Kit

- Two-minute video walkthrough per release; one-page change note; "what changed for me?" per role.
- Weekly office hours; monthly "feature in practice."
- Searchable FAQ with annotated screenshots; runbooks with last-verified dates.

References (starter list)

[1] University of California, "Crisis Management," Enterprise Risk and Resilience.
[2] ISO, *ISO 22301:2019 Security and Resilience—Business Continuity Management Systems—Requirements*, 2019.
[3] FEMA, *National Incident Management System (NIMS)*, 3rd ed., 2017.
[4] DHS/FEMA, *Comprehensive Preparedness Guide 101*, 2016.
[5] Hollnagel, E., Woods, D. D., Leveson, N., *Resilience Engineering: Concepts and Precepts*, Ashgate, 2006.