

MAINE

Public-service software and automation

A role-by-role engineering map for the people and the government that serves them.

100 role archetypes / 52 workflows / 24 reusable components
85 playbook steps / 44 institutional groups / 28 acceptance specifications

The architecture connects responsibility, evidence, lawful decisions and actual delivery. It does not place every record or power in one system.

Design and evidence status

September 20, 2026. Proposed reference design, not enacted policy, an approved procurement, a certified employee census or a deployed government service. Public interfaces and technical standards do not establish permission to connect them.

The accompanying explorer, workbook and registry hold the complete role/workflow map. The implementation pack contains a synthetic offline demonstration and its 18 passing unit tests, not production software.

Contents

1. What this adds	3
2. The architecture in one view	3
3. Begin with Maine's existing technology, not a blank procurement	4
4. The resident workspace	5
5. The software available at each seat	6
6. Automate the administrative work before adding agents	7
7. A durable obligation ledger, not a chain of emails	7
8. Evidence, rules and the official decision manifest	8
9. Protect the boundaries that make shared tools acceptable	9
10. Accessibility is an end-to-end operating requirement	9
11. Implementation choices without a premature vendor selection	10
12. Staffing, delivery and measurable cost	10
13. Delivery sequence and release gates	11
14. What the included prototype actually demonstrates	11
15. The completion criterion	12
Appendix A. Component specifications	13
Appendix B. Detailed automation playbooks	20
Appendix C. Institutional coverage and workspace index	30
Appendix D. Source and evidence ledger	36

Research cutoff: September 20, 2026. Reference architecture, not an enacted policy, procurement selection, verified position census, authorized integration or deployed government service.

1. What this adds

The previous design asked who remains responsible until a person receives a lawful, usable result. This expansion specifies the software that supports that responsibility: the resident workspace, the employee workspace, the authoritative records, the permitted automated actions, the human decisions, the integrations, the failure recovery and the tests.

The structured map preserves all 44 institutional-group identifiers and all 52 workflow identifiers from the prior ledger. It adds 100 role archetypes, 24 reusable software components, 85 detailed steps across 12 playbooks, 12 integration-discovery records, 28 deployment acceptance tests, 12 implementation epics and 10 data contracts. Ninety-eight role entries describe government or public-service work; two describe the resident and authorized representative. These are archetypes, not a claim that Maine has precisely this many jobs or that additional positions must be created. [B01, B02]

The accompanying offline explorer searches the map by role, workflow, component or institution. The workbook exposes the same records as editable tables. The implementation folder supplies a synthetic Python reference kernel with 18 passing unit tests and an illustrative API/schema pack. Those tests establish only the behaviors tested in that small offline demonstration, not production security, legal compliance, system interoperability or statewide effectiveness.

Evidence boundaries

Three evidence classes remain separate. First, inherited design and current-state summaries remain preserved in the baseline object; they were not silently reclassified as freshly verified facts. Second, current primary research describes existing Maine governance and public system interfaces, along with relevant technical standards. Third, the proposed role tools, commands, data contracts and acceptance tests are engineering designs for evaluation.

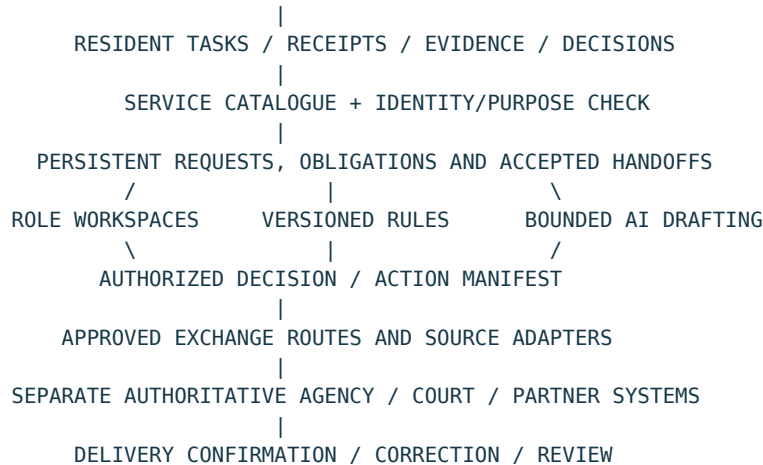
No Gmail, personal litigation corpus, private SharePoint, payroll system, internal API or production database was accessed. A public web portal establishes a public interface, not permission to connect a bot or the existence of a supported API. Each integration record names what must still be verified.

2. The architecture in one view

The architecture shares service components while keeping powers and protected records separate. It is not one statewide all-access agent, one global caseworker or one consolidated database of every resident.

PEOPLE AND AUTHORIZED HELPERS

Conversation | accessible forms | telephone | mail | assisted visits



Across all layers: accessibility, privacy, independent audit, retention, incident response, human assistance and rollback.

The main unit is an obligation: somebody owes a next action toward a public result. An obligation is smaller than an entire court case or benefit history. A matter may contain several obligations owned by different authorities. Software can coordinate their administrative dependencies without giving any one coordinator power to decide every issue.

A benefits determination, an available medical appointment, an authorized invoice, a settled payment, a filed motion and a judicial decision are separate events. The data model keeps them separate. This prevents a convenient technical milestone from becoming an inaccurate claim of completed public service.

3. Begin with Maine's existing technology, not a blank procurement

Maine already publishes enterprise IT governance, including policies covering data exchanges, classification, identity integration, low-code development, accessibility and generative AI. Their scope and applicable exceptions must be checked; an executive-branch policy is not automatically the rule governing every independent branch, municipality or Tribal government. [T01, T05-T07]

The April 17, 2026 Data Exchange Policy assigns agencies responsibility for lawful authority, requires agreements for covered new standing exchanges subject to its exception, and describes documented exchange routes. It identifies the Maine Service Bus as the default proxy for covered new nonbulk standing exchanges, with stated exceptions; bulk transfer has a different route. Therefore a new integration layer must assess reuse of that existing infrastructure or obtain the applicable exception, rather than assume Maine needs an entirely new bus. Production topology and the status of any migration were not verified. [T02]

Maine's Microsoft low-code governance already contemplates Power Automate, Power Apps and Dynamics in the state environment. Existing entitlements, supported connectors, capacity, licensing and operational staffing were not audited. Low-code is a possible implementation tool, not proof that a given service can be delivered without additional engineering. [T04]

The MyMaine page describes an integrated gateway initiative; live service coverage remains unverified in this review. My Maine Connection, the Tax Portal, BMV services, procurement services and eCourts supply documented existing interfaces. The map describes proposed contracts around them, not replacement contracts or granted credentials. [T08-T14]

A material source-control issue

The GenAI policy URL produced a nine-page text extraction but a seven-page rendered first page during this review. Both the discrepancy and its operational consequence are recorded in source T03. This report does not certify particular models, products or autonomous actions as currently approved. Before implementation, obtain a signed/versioned governing copy, record its hash and applicability, and resolve conflicting versions. The appropriate automation response to uncertain governing material is an explicit review task, not a confident guess. [T03]

4. The resident workspace

The resident's interface is organized around tasks: what they are trying to accomplish, what has been received, what government still owes, what genuinely remains theirs to supply and what can be corrected or reviewed. Conversation is optional. A person can use a conventional accessible form, assisted phone call or in-person help instead.

A task view shows its original receipt, current official status, responsible team, next action, applicable deadline source, evidence received, missing facts with reasons, safe communication preference and available correction/review routes. It distinguishes an estimated processing time from a binding legal deadline. It does not label an upload as legally filed unless the competent source confirms that status.

The evidence view preserves originals and supports a controlled reuse request. It explains which agency needs a fact, why, the applicable date range and the permitted recipient. It does not turn 'tell us once' into permission for every office to receive everything. Different programs may legitimately need different facts, freshness or authority.

The decision view presents the actual authorized decision, understandable reasons, a calculation receipt where applicable, the evidence relied on and actual review instructions. An optional explanation assistant can clarify the approved material but cannot rewrite the decision or create a deadline extension. Unsupported questions become an identified human question.

Authorized help without password sharing

A representative receives a specific grant: who they may assist, which services, which actions, which records, when the grant expires, and how it can be revoked. Authority must be verified through the applicable process; a shared surname, household, device or claimed relationship is not enough. Revocation must affect search results, cached links and downloads, not merely hide a button. Identity federation and assurance can use established technical patterns, but identity verification remains distinct from permission to see a record. [T05, T15, T16]

For anonymous general information, do not impose identification merely because sign-in is technically available. For transactions that legally require identity or representation, provide proportionate assurance and a functioning assisted recovery route. Neither a failed identity service nor a requirement for an account may be used to obstruct appropriate emergency human contact.

5. The software available at each seat

Every role receives a task list linked to its actual public obligation, not a generic chatbot. The workspace shows source-supported context, the current approved instructions, missing evidence, remaining dependencies, legitimate approval controls and the action history. It also shows the limits of the role's authority.

A clerk's workspace emphasizes received documents, form/version issues, notices and accurate status. A caseworker's emphasizes evidence, program-specific rules, explanation and delivery gaps. A field inspector's emphasizes offline observations, qualified measurements, conditions and corrective work. An auditor's emphasizes reproducible populations, read-only source access and independently verified corrections.

A judge or hearing officer receives only the permitted record and approved research tools. A prosecutor and defender have separate workspaces, indexes and AI retrieval boundaries. A governor, director or legislator can inspect appropriately aggregated operational dependencies without acquiring universal access to private cases. Constituent assistance is kept separate from political profiling and campaign activity.

The role charter must specify permitted commands. 'Summarize permitted documents' is different from 'issue a notice,' and 'issue a notice' is different from 'decide entitlement.' No prompt can expand these permissions. The command gateway obtains authority from verified server-side grants, policy and official action records, never from an AI-generated assertion that a user is authorized.

The four automation modes

Explain: retrieve and explain approved sources. Show dates, citations and uncertainty. No state-changing command.

Prepare: extract candidate fields, assemble packets, compare text, calculate approved scenarios and draft notices. Material output remains a draft until the required verification.

Execute bounded operations: send an approved reminder, schedule an accepted appointment, transmit an authorized invoice, perform an explicitly authorized deterministic renewal or reconcile a known payment. Permission, idempotency, auditing and recovery apply.

Reserved decision: credibility, contested legal findings, policy choices, clinical decisions, discipline, judicial relief and other legally consequential judgments remain with the authorized person or lawful predefined process. A language model is not substituted for that authority.

These are technical action categories, not rankings of political actors or policies. Some lawful deterministic transactions can be automated without a person clicking every time; the pathway must be explicitly authorized, versioned, tested, explainable and reviewable. 'Human review' is not a universal excuse to create another unnecessary approval layer.

Human review has to be real

A reviewer must see relevant sources and contrary evidence, have time and training, understand the proposed action, be able to change it, and have genuine authority to decline. A quota or interface that rewards agreeing with generated output creates a rubber stamp, not an effective safeguard. Review workload is included in the capacity model.

6. Automate the administrative work before adding agents

Many high-value improvements do not need generative AI. Deterministic checks can detect a missing required field, a duplicate invoice, an expired form version or a task without an owner. A scheduler can find permitted dates. A payment adapter can reconcile settlement. An approved rules engine can reproduce a calculation. These actions have explicit inputs and expected outputs.

Use AI where language variability is the actual difficulty: interpreting a person's description of a need, finding relevant approved instructions, extracting candidate evidence, drafting an accessible explanation, assembling a balanced record index or identifying textual dependencies in an amendment. The model should return structured candidates with source spans rather than unsupported fluent conclusions.

If the user writes that a document is missing, the model may identify the request and route it. It cannot infer why the document is absent, label someone dishonest or determine the legal consequence. A retrieved page can be superseded; a filed allegation can be disputed; a copied summary can be inaccurate. Store the evidence type and source status explicitly.

A bounded assistant specification

Each assistant has a service owner, permitted input classes, approved model/environment, task-specific instructions, source scope, allowed tools, maximum actions/cost, required approvals, failure route, retention schedule, evaluation dataset and change policy. It may not create credentials, amend its own rules or bypass limits because a document asks it to.

A document-reading assistant has no direct payment tool. A routing assistant cannot reject a case. A legislative drafting assistant cannot publish an official version. A records assistant can suggest redactions but cannot authorize disclosure. A care-administration assistant cannot become a therapeutic clinician.

Maine's enacted chapter 687 text, approved April 13, 2026, distinguishes administrative or supplementary assistance from restricted independent therapeutic functions. The exact use and applicable legal requirements need qualified review; this report does not treat the enactment as a general ban on all government chatbots or assert an independently verified effective date. [T27]

7. A durable obligation ledger, not a chain of emails

A persistent request record owns the original receipt and source references. Each obligation has a responsible team, authorized role, next action, dependencies, state and completion evidence. A receiving team explicitly accepts a handoff or explains why it cannot. The sending team retains routing responsibility until then.

Elapsed public time stays visible through transfers and corrections. Legal clocks are separately calculated from approved rules, actual triggering facts, calendar versions and relevant time zones. Where the necessary legal fact is unresolved, the clock is marked unresolved for human determination. A language model does not calculate jurisdictional dates from prose.

Long-running cases must survive short-running jobs

Microsoft's Power Automate documentation sets a 30-day duration for an individual cloud-flow run, including pending approvals. A months-long case therefore cannot depend on one sleeping cloud-flow instance. Persist its state in an approved durable store and use short-running event-triggered jobs, or a durable workflow system with tested recovery. Licensing, retention and ownership limits need separate verification. [T24]

The distinction is architectural: the legal matter and its obligations continue to exist when a job finishes, a worker leaves, a connector changes or a process restarts. A case is not an email thread or a run-history screen.

Retry safely

Every external command has a stable business key and payload hash. If the same key is submitted with changed contents, reject the ambiguity. If a connector times out after a payment may have been accepted, query the authoritative transaction reference before trying again. Record uncertainty honestly.

Durable workflow tools help resume work; they do not magically make every external effect happen exactly once. Activity documentation explicitly makes idempotency relevant to retries. The design combines command/outbox persistence, source receipts and reconciliation. A standardized event envelope supports interoperability but is not itself authorization or a delivery guarantee. [T21, T25]

A failed connector enters an owned exception queue with an incident trigger. It does not silently drop work, deny an application, close a complaint or create a second payment. A technical response of 'success' is interpreted according to the source contract: it may mean received, queued, accepted, posted or settled. The adapter cannot collapse those meanings.

8. Evidence, rules and the official decision manifest

The evidence service preserves the original, content hash, source, receipt time, source-created time, classification, permitted purpose, retention and derived-text locations. Extraction candidates refer to the page/section they came from. An original claim, observed fact, verified program fact and adjudicated finding are distinct labels; the system does not convert one into another by repetition.

A rules package has a legal/program owner, version, effective period, date recorded, required inputs, deterministic calculations, tests and authorized action scope. Historical replay uses the relevant rule and source facts, not whichever instruction is currently online. Unresolved interpretation goes to a qualified person.

The official decision/action manifest joins the accountable actor, delegation, evidence references, rule version, calculation, draft/model version when relevant, material human changes, reasons, permitted downstream actions, applicable notice process and authentic approval. A model answer is not the manifest. An authorization-policy log is useful supporting evidence, not the complete official decision. [T22, T23]

Correction is a first-class transaction

An authorized correction preserves what was wrong, what changed, who approved it and its effective meaning. A dependency index identifies known lawful downstream uses. The system opens remediation tasks for affected payment, coverage, notice, scheduling or access consequences and verifies their resolution.

This does not mean broadcasting corrected private information to every agency. Each recipient still requires authority. It also does not mean every complaint proves an error. Pending disputes, actual corrections and requested remedies remain distinguishable.

A person need not understand which internal replicas or systems were affected. Once the competent body determines a correction, its administrative consequences have named owners. Closing the first correction ticket does not by itself restore the service.

9. Protect the boundaries that make shared tools acceptable

Authorization is evaluated on every protected action: authenticated identity, role, purpose, case/subject relationship, valid delegation, record classification, source restrictions and current revocation state. Apply enforcement to APIs, search indexes, database rows, exports and temporary links. Hiding interface controls is insufficient. PostgreSQL row-level security is one possible defense-in-depth tool, not a substitute for application authorization or testing of privileged-user behavior. [T28]

Separate judicial, prosecution, defense, child-welfare, education, clinical, fiscal and other restricted contexts as their laws and functions require. Shared platform operations may need limited technical access under controlled procedures; that is not permission to use record content for general AI assistance.

Untrusted documents can contain instructions aimed at the model or tool system. Treat retrieved text as data, use action allowlists and validate tool parameters outside the model. Prompt injection testing includes malicious PDFs, email threads, web pages and hidden text. Retrieval with citations alone does not remove this risk. [T29]

Do not collect a universal credibility score, infer political preferences, reduce service because a person complains frequently or use profanity/sentiment as an automatic adverse factor. Where staff safety or actual threats require response, use the competent evidence-based human process, not a general annoyance score.

Retention and transparency

Record enough to explain decisions and investigate failures while respecting purpose limits, retention schedules and verified legal holds. Derived text, embeddings, AI conversation logs, caches and exports need lifecycle controls too. Auditability does not mean preserving every personal record forever.

Public reporting uses defined populations, data minimization and appropriate small-cell suppression. Independent reviewers receive authorized evidence, not merely management-selected summaries. Publication itself has an accountable privacy and records review.

10. Accessibility is an end-to-end operating requirement

The reference design targets WCAG 2.2 AA as an engineering standard, while distinguishing it from the WCAG 2.1 AA standard described in the federal Title II rule. DOJ's current factsheet reflects an April 2026 extension to April 26, 2027 for the larger public-entity category and April 26, 2028 for smaller entities and special districts. Applicability and existing duties require separate review; delayed compliance dates do not justify an unusable service. [T18, T19]

Test keyboard navigation, screen-reader semantics, zoom, low bandwidth, phone-only completion, language assistance, disability accommodations, shared-device safety and assisted recovery. A successful automated accessibility scan does not establish actual task completion.

A voice transcript can help a person review a conversation, but needs consent and appropriate retention. Machine translation is a draft when meaning materially affects rights, benefits or safety; provide qualified review and assistance. Do not force people to use AI to reach a human.

Offline field work needs its own design. Keep encrypted minimal caches, local provenance, clear synchronization state and conflict resolution. A device clock is not automatically authoritative. Two inspectors' conflicting observations remain visible until a qualified person resolves the difference.

11. Implementation choices without a premature vendor selection

An existing-suite implementation can use approved low-code forms, role applications and short-running flows around a persistent obligation store. This may fit organizations already equipped to operate that suite. Its actual connector availability, licensing, retention, service ownership and environment isolation require verification. Critical state must not depend on an individual employee's account. [T04, T24]

A composable implementation can use accessible web applications, a durable workflow engine, a relational obligation ledger, encrypted evidence storage, a rules service, policy enforcement and approved adapters. Temporal, Open Policy Agent and PostgreSQL are technical examples, not procurement winners or claims about Maine's installed estate. Each adds operations, security and workforce responsibilities. [T21-T23, T28]

A federated adapter implementation can preserve major systems and add only shared navigation, task coordination, status and necessary boundary exchanges. It avoids a statewide replacement cutover but must accurately represent lag, unavailable APIs and incomplete source coverage.

These approaches can coexist. The architecture contract matters more than product branding: state ownership, authenticated authority, source receipts, rules/versioning, accessible interaction, independent audit, recovery and an exit path. A government-cloud label alone does not establish permission for every data class or purpose.

Screen automation is a last-resort, temporary permitted bridge where supported interfaces are unavailable. It needs system-owner permission, service credentials, bounded actions, version monitoring, validation and a retirement plan. The absence of an API is not authorization for credential sharing, uncontrolled scraping or concealed writes.

12. Staffing, delivery and measurable cost

A pilot needs product/service ownership, program expertise, legal/rules review, integration and application engineering, identity/security/privacy, records management, accessibility testing, quality assurance, operations and frontline participation. Some duties can be shared, but listing them does not prove spare capacity exists. Human review, coordination and incident response are real work that must be scheduled and costed.

The accompanying workbook exposes illustrative inputs rather than promising savings. Its example uses 60,000 transactions per year, 28 existing staff minutes, 7 remaining handling minutes, 5 review minutes and a 20 percent exception rate adding 15 minutes. The new expected handling is 15 minutes per transaction. Gross capacity released is 13,000 hours; after 1,200 annual operations/support hours, net modeled capacity is 11,800 hours.

At an assumed loaded rate of \$55 per hour, that is \$649,000 of capacity value, not automatically cash saved. The default cash-realization rate is zero. With illustrative recurring nonlabor cost of \$240,000 and one-time implementation cost of \$450,000, first-year cash effect under that default is negative \$690,000. A different rate is a user-supplied scenario, not an observed fiscal result. Separate operations labor is already subtracted in net capacity; do not subtract it again as the same recurring labor cost.

The public-time scenario assumes a reduction from 45 to 28 minutes per transaction, or 17,000 public hours. It excludes wait-time and consequential-harm claims that were not measured. No monetary value is assigned to those public hours by default.

Measure total elapsed time separately from touch time. A system can reduce data entry while waiting remains constrained by staff or providers. Track approval-to-delivery gaps, source-data errors, repeated evidence requests, abandoned intake, reversal/correction rates, user effort and operating costs. Do not reward a particular judicial outcome, denial rate, enforcement count or low complaint volume.

13. Delivery sequence and release gates

The backlog is a dependency sequence, not a political priority ranking or an approved calendar. Establish the signed authority/source map, observe baseline work and repair current instructions. Build a synthetic persistent request kernel and bounded authorization before connecting personal records. Develop one approved adapter, worker/resident views, delivery reconciliation and correction handling. Add AI drafts only after the source and permissions boundaries work.

A limited pilot must have a defined cohort, staffed fallback, approved data, incident response, rollback, records treatment and independent acceptance. Do not turn the pilot into a mandatory exclusive route before its failures are understood. New services repeat their own authority, access and quality checks; the first pilot's permission is not transferable to every domain.

Release gates test concrete failures. What happens when a worker leaves? A payment succeeds but times out? A person revokes a helper? An uploaded PDF orders the AI to disclose records? A form version conflicts? A clinic has no appointment? A court requires a different source receipt? The 28 control specifications make these conditions testable rather than burying them in a general security paragraph.

Go-live requires measured performance at representative peak load, recovery from backup, tested restoration of in-flight transactions, qualified human availability and acceptable accessibility results. Retire old systems only after source records, dependencies, retention and operational continuity are reconciled. A procurement acceptance event does not by itself justify decommissioning.

14. What the included prototype actually demonstrates

The Python kernel is an offline SQLite demonstration with no external network connections. It persists requests, accepted handoffs, authorized synthetic commands, unconfirmed/confirmed source results and an audit chain. It rejects changed payloads under the same idempotency key, denies cross-domain access in its simple trusted-context model, blocks a drafting assistant from authorizing commands, preserves original receipt time and prevents completion while a commanded effect remains unresolved.

Eighteen standard-library unit tests passed when the package was built. They include restart persistence, duplicate receipt/command handling, missing evidence, unconfirmed settlement, privilege boundaries and detection of a modified audit event. The demo does not implement production authentication, cryptographic receipt validation, full relationship/purpose permissions, actual legal calendars, encryption/key management, distributed consensus, retention, disaster recovery or real integrations. Its hash chain is illustrative and does not protect against a privileged actor rewriting the entire database and chain.

The API and JSON schemas are contracts for review, not running servers or official Maine endpoints. The demo deliberately does not connect to Gmail, government systems, courts, a bank or a model provider. Trusted context and assigned-team parameters must be derived from verified server-side authorization in production; the test fixtures are not a deployable identity system.

Run the local example with `python service_kernel.py` and the tests with `python -m unittest -v` from its implementation directory. Read the implementation README before adapting it.

15. The completion criterion

For every proposed automation, the service owner must be able to answer: whose burden changes, which authorized action occurs, which evidence supports it, how a person challenges it, what happens when it fails, and who remains responsible afterward.

The software is doing its job when it reduces repeated work and makes the remaining government obligation easier to perform and inspect. It is not doing its job merely because it generates fluent text, closes tickets quickly, centralizes records or replaces a staffed channel with a login screen.

Appendix A. Component specifications

M01 - Service and authority catalogue

Public purpose: Find the right service without knowing the department.

Software: Versioned requirements, jurisdiction, effective dates, forms, change-impact graph and named content owners.

Authority: Program/legal editor approves publication; conflicting rules go to review.

Output and test: Current checklist and cited source snapshot. Expired guidance is flagged; conflicting effective dates cannot silently overwrite each other.

Sources: B01, T01. Proposed component; no live integration.

M02 - Identity and delegated authority

Public purpose: Use help safely without surrendering a password.

Software: Federated sign-in, risk-proportionate proofing, safe recovery, per-service representative grants and revocation.

Authority: Custodian verifies the legal representative and limits; emergency exceptions use an approved process.

Output and test: Scoped identity assertion and active grant. Revoked agent loses access immediately, including cached search and download links.

Sources: T05, T15, T16. Proposed component; no live integration.

M03 - Multichannel intake

Public purpose: Begin by conversation, form, phone, paper or assisted visit.

Software: Capture minimum facts, offer optional AI parsing, durable draft, resume token and accessible review before submission.

Authority: Resident or authorized helper confirms facts and intended transaction.

Output and test: Receipt with channel, content hash and legal-status disclaimer. Switching channel preserves work; disabling AI does not block the service.

Sources: B02, T18, T19. Proposed component; no live integration.

M04 - Evidence and provenance

Public purpose: Submit necessary evidence without repeated untracked copying.

Software: Encrypted original objects; derived text linked to page/section; deduplication; field-level provenance and correction links.

Authority: Human validates material extracted facts; allegations remain labeled.

Output and test: Evidence manifest and supported fact candidates. Bad extraction cannot become an authoritative field without validation.

Sources: T02, T06, T29. Proposed component; no live integration.

M05 - Persistent workflow and obligation ledger

Public purpose: Keep government-owned tasks visible until actually finished.

Software: Durable states, dependency graph, inbox/outbox, receipts, responsible team, next action and separate public/legal clocks.

Authority: Authorized official approves legally consequential transitions.

Output and test: Task, obligation, handoff and completion records. Restart during delivery yields one business effect and preserved elapsed time.

Sources: T21, T24, T25. Proposed component; no live integration.

M06 - Versioned rules and calculations

Public purpose: Apply reproducible requirements rather than model guesses.

Software: Tested decision tables/calculators; effective-from and recorded-at dates; input validation; change-impact simulation.

Authority: Program/legal owner signs each rule version; ambiguous cases route to a person.

Output and test: Calculation receipt, rule version, reasons and unresolved inputs. Old cases replay against the correct historical rule, not today's rule.

Sources: T01, T22. Proposed component; no live integration.

M07 - Appointments and capacity

Public purpose: Coordinate real availability, travel and accommodations.

Software: Constraint-based candidate slots, waitlist offers, interpreter/equipment needs, provider acceptance and no-show follow-up.

Authority: Person chooses from permissible options; staff resolve urgency and exceptions.

Output and test: Confirmed service slot plus preparation list. No booking claims delivery; failed provider acceptance remains open.

Sources: B01, T18. Proposed component; no live integration.

M08 - Notices and safe communication

Public purpose: Know the next step without unsafe or excessive messages.

Software: Approved templates, translation workflow, minimal-content alerts, preference checks, delivery states and fallback channels.

Authority: Official approves decision notices; language professional reviews material language where needed.

Output and test: Reasoned notice, delivery proof where applicable and review instructions. SMS failure is not treated as legal service; protected details never enter notification previews.

Sources: T06, T18, T19. Proposed component; no live integration.

M09 - Payments and reconciliation

Public purpose: Know whether money was actually received.

Software: Deterministic invoice checks, authorized release, idempotency keys, settlement lookup and ledger reconciliation.

Authority: Fiscal officer retains approval and segregation of duties; disputed charges go to review.

Output and test: Payment status from instruction through settlement. Timeout after acceptance does not create duplicate payment.

Sources: T13, T21. Proposed component; no live integration.

M10 - Bounded AI assistance

Public purpose: Reduce reading and clerical burden without opaque decisions.

Software: Permission-filtered retrieval, source anchors, draft summaries, extraction candidates, tool allowlist and output validation.

Authority: Role-specific reviewer verifies material output; authority cannot come from a prompt.

Output and test: Cited draft or explicit unsupported/uncertain response. Malicious text in an attachment cannot invoke tools or expose another case.

Sources: T03, T17, T29. Proposed component; no live integration.

M11 - Role workspace

Public purpose: Give each seat the information and tools for its actual duties.

Software: Role-scoped tasks, cited brief, missing facts, calculators, approval controls, staffing coverage and current operating instructions.

Authority: Role holder decides within delegation and can reject automation.

Output and test: Versioned work product and signed action. Leaving a role revokes permissions without orphaning its tasks.

Sources: B01, T05. Proposed component; no live integration.

M12 - Corrections, review and restoration

Public purpose: Repair the error and its downstream effects.

Software: Register contested fields; preserve original; assign independent route; propagate lawful corrections; verify restored access or payment.

Authority: Competent reviewer decides correction/relief; complaints do not silently toll deadlines.

Output and test: Correction lineage, reason and unresolved effects. One source correction identifies known downstream copies and incomplete remediation.

Sources: B02, T02. Proposed component; no live integration.

M13 - Integration gateway and adapters

Public purpose: Connect existing systems without pretending access exists.

Software: Approved APIs first; managed file exchange second; bounded attended automation only as a temporary permitted bridge.

Authority: Data owners approve exchange and permissions; system owner validates endpoint semantics.

Output and test: Typed request/response, source receipt and freshness. Adapter failure shows unconfirmed status, not success.

Sources: T02, T05, T20. Proposed component; no live integration.

M14 - Audit, retention and disclosure

Public purpose: Explain what happened without building a permanent shadow dossier.

Software: Tamper-evident purpose-scoped logs, retention schedules, legal holds, deletion of derived caches and independent audit export.

Authority: Records/privacy officer decides retention and lawful disclosure.

Output and test: Decision manifest and authorized audit view. Expired content is deleted as required while permitted audit metadata remains sufficient.

Sources: T06, T23. Proposed component; no live integration.

M15 - Service observability and operations

Public purpose: Catch stopped work before the resident has to report it.

Software: Queue age, acknowledgments, connector health, dead-letter ownership, recovery probes and outage receipt preservation.

Authority: Duty team owns incident handling; branch/service leaders address capacity.

Output and test: Incident, recovery task and affected-transaction list. Disabled workflow or absent worker produces an assigned alarm, not just an email.

Sources: T01, T21, T24. Proposed component; no live integration.

M16 - Delivery and unmet-capacity register

Public purpose: Separate approval from an actually available service.

Software: Track authorized service, provider acceptance, first delivery, cancellations, capacity gaps and lawful alternatives.

Authority: Provider and program officer confirm reality and clinical/professional decisions.

Output and test: Delivery confirmation or explicit unmet-need record. Waiting for a provider cannot be reported as service delivered.

Sources: B01, T11. Proposed component; no live integration.

M17 - Public evidence and aggregate reporting

Public purpose: Make performance inspectable without exposing private cases.

Software: Define denominator including abandonment, age distribution, subgroup minimums, change log and independently sampled quality.

Authority: Analyst/privacy reviewer approves releases; no merits quotas.

Output and test: Accessible dashboard and reproducible methods. Closed-ticket counts do not omit failed intake or incorrectly closed cases.

Sources: B02, T06. Proposed component; no live integration.

M18 - Workforce and knowledge continuity

Public purpose: Keep expertise and responsibility available when someone leaves.

Software: Role mapping, delegated backup, training sandbox, task handover, workload/capacity models and access recertification.

Authority: Supervisor and HR retain hiring, discipline and workload decisions.

Output and test: Coverage plan, learning aids and unowned-task alert. A departure cannot disable a service-owned automation.

Sources: T04, T05, T24. Proposed component; no live integration.

M19 - Procurement, grants and assets

Public purpose: Connect authorizations to functioning delivery and maintained assets.

Software: Requirement traceability, tender versions, contract milestones, field acceptance evidence, reimbursement and maintenance schedules.

Authority: Procurement/engineering/grant officials make authorized selections and accept work.

Output and test: Acceptance record and obligation register. Vendor invoice cannot self-certify the service acceptance that releases its payment.

Sources: T13. Proposed component; no live integration.

M20 - Legislation and rule-change engineering

Public purpose: Keep guidance, systems and training aligned with authoritative changes.

Software: Document comparison, cross-reference linting, dependency impact, implementation checklist and public text versions.

Authority: Drafters and lawmakers decide meaning and policy; courts retain interpretation.

Output and test: Change-impact report with unresolved legal questions. A model summary cannot replace the adopted text or change a rule automatically.

Sources: B01, T01. Proposed component; no live integration.

M21 - Field and infrastructure workspace

Public purpose: Assist people who work away from a desk.

Software: Offline work orders, equipment checklists, geospatial tasks, provenance-preserving photos and controlled synchronization.

Authority: Qualified staff inspect, certify conditions and direct safety actions.

Output and test: Observed condition and completed maintenance record. Conflicting offline edits cannot silently overwrite safety-critical observations.

Sources: B01, T06. Proposed component; no live integration.

M22 - Independent research and hearing workspace

Public purpose: Support balanced review of the permitted record.

Software: Search authorized materials; label allegations/findings; separate parties; anchor citations and display unresolved conflicts.

Authority: Judge, reviewer, investigator or counsel forms their own judgment.

Output and test: Record index and separately approved reasons. No hidden off-record document enters an adjudicative summary.

Sources: T10, T17. Proposed component; no live integration.

M23 - Developer delivery and automated assurance

Public purpose: Keep software changes testable and reversible.

Software: Versioned configurations, contract tests, synthetic cases, dependency scans, signed releases, canaries and rollback manifests.

Authority: Release owner signs; data/clinical/legal reviewers approve affected material changes.

Output and test: Test evidence, deployment record and rollback plan. Model/provider update reruns the same reference tests before release.

Sources: T01, T17, T20. Proposed component; no live integration.

M24 - Privacy and safety enforcement

Public purpose: Prevent convenience from becoming unauthorized access.

Software: Purpose/role/relationship checks on every action; data minimization; segregated domains; per-tool budgets and emergency-access logs.

Authority: Custodian authorizes lawful use; privacy/security teams review exceptions.

Output and test: Allow/deny with auditable basis; safe human fallback. Same name, shared device or shared login never proves a legal relationship.

Sources: T02, T05, T06, T22, T28. Proposed component; no live integration.

Appendix B. Detailed automation playbooks

These 85 steps expand 12 of the 52 mapped workflows. The explorer and workbook contain the complete 52-workflow map. Every step below is proposed, not a claim of current functionality.

W01 - General request and wrong-office routing

1. Capture need

Software: Accessible intake saves minimal facts and original receipt. **Human:** Person confirms intended outcome; helper has explicit scope. **Failure/boundary:** No account needed for general guidance; an interrupted session can resume.

2. Resolve routing

Software: Versioned catalogue proposes competent service and names unresolved jurisdiction. **Human:** Navigator checks ambiguous routing. **Failure/boundary:** Model cannot invent a department or authority.

3. Request handoff

Software: Persistent task is sent through approved adapter with correlation ID. **Human:** Originating team remains responsible until accepted. **Failure/boundary:** No transport receipt is treated as human acceptance.

4. Accept or explain

Software: Receiving team records accepted scope or specific reason for return. **Human:** Receiver identifies next responsible role. **Failure/boundary:** Repeated wrong-door routing creates a coordinator task.

5. Show next action

Software: Resident sees responsible team, required facts, applicable clock and update. **Human:** Official validates legal deadline language. **Failure/boundary:** Missing legal deadline remains unknown, not guessed.

6. Resolve obligation

Software: Assigned staff complete delivery or issue the proper reasoned decision. **Human:** Competent official owns substantive action. **Failure/boundary:** Service remains open if a promised downstream action is incomplete.

7. Close and review

Software: Record completion evidence; send explanation and correction/review route. **Human:** Closure follows objective evidence or authorized disposition, not mandatory customer click. **Failure/boundary:** Reopening preserves first receipt and previous work.

W06 - Food, cash and health coverage application

1. Choose programs

Software: Intake builds candidate program requests from person-confirmed needs. **Human:** Person selects intended applications; worker helps when needed. **Failure/boundary:** Optional navigation is not an eligibility prediction.

2. Identify evidence

Software: Rules catalogue lists legally necessary facts and acceptable current sources. **Human:** Custodian approves reuse and date coverage. **Failure/boundary:** Old income or household facts are not silently treated as current.

3. Extract candidates

Software: File parser stores original and source-linked candidate fields. **Human:** Worker/person validates material disputed fields. **Failure/boundary:** Wrong date, missing page and conflicting evidence remain explicit.

4. Run rules

Software: Approved deterministic tables calculate outputs with rule/input versions. **Human:** Program authority defines lawful straight-through and exception actions. **Failure/boundary:** Unreachable data source is not evidence of ineligibility.

5. Review exception

Software: Workspace displays evidence, contrary facts, proposed reasons and actions. **Human:** Reviewer has time, access and authority to change or reject draft. **Failure/boundary:** No approval button is preselected; override is recorded without penalty.

6. Issue decision

Software: Signed manifest authorizes the appropriate source-system change and notice. **Human:** Official checks reasons, service rules and review instructions. **Failure/boundary:** Language-model output cannot call an adverse-action endpoint directly.

7. Verify usability

Software: Read back active coverage or payment status from authority and delivery channel. **Human:** Delivery coordinator handles absent provider or settlement. **Failure/boundary:** A successful HTTP response is not evidence that support is usable.

8. Correct downstream

Software: Authorized corrections create linked remediation tasks and preserve history. **Human:** Competent reviewer determines remedy and any interim action. **Failure/boundary:** Fixing source income does not automatically prove payment/coverage restoration.

W07 - Benefit renewal and change reporting

1. Open renewal obligation

Software: Source rule creates dated renewal task with applicable calendar. **Human:** Program owner validates rules and clock triggers. **Failure/boundary:** Internal task creation cannot alter statutory dates.

2. Refresh authorized facts

Software: Adapters request only approved current assertions. **Human:** Data custodian limits purpose and retention. **Failure/boundary:** No blanket household-data sweep.

3. Test sufficiency

Software: Versioned rules distinguish sufficient evidence from genuine unknowns. **Human:** Worker handles contradictions and changes. **Failure/boundary:** Timeout or absent source cannot become a negative fact.

4. Complete lawful renewal

Software: Approved deterministic renewal runs only within signed authority. **Human:** Authorized official owns and audits the rule pathway. **Failure/boundary:** Not every action needs individual review, but lawful automation must be explicit.

5. Ask focused question

Software: Only unresolved required items become a clear accessible request. **Human:** Worker validates necessity, language and actual response period. **Failure/boundary:** Person receives assisted alternatives, not a resubmit-everything demand.

6. Review adverse exception

Software: Evidence and proposed action route to responsible reviewer. **Human:** Applicable safeguards and notices control. **Failure/boundary:** Model cannot terminate assistance based on a confidence score.

7. Reconcile result

Software: Confirm status/notice and create correction or delivery tasks as necessary. **Human:** Owner examines interruption cases and failed notices. **Failure/boundary:** Renewal success excludes neither abandoned requests nor incorrect closures.

W12 - Child-care provider payment

1. Receive invoice

Software: Issue invoice ID, content hash, provider scope and idempotency key. **Human:** Provider confirms invoice and account. **Failure/boundary:** Repeated identical upload returns the original receipt.

2. Validate authority

Software: Match service period, authorization and deterministic invoice requirements. **Human:** Program reviewer resolves disputed attendance/service. **Failure/boundary:** Duplicate pattern is a question, not a fraud finding.

3. Consolidate defect

Software: Generate one specific request for defects presently identifiable. **Human:** Payment specialist checks exception and backup ownership. **Failure/boundary:** Later new evidence may require questions; no false promise of one request ever.

4. Authorize release

Software: Separate service acceptance from fiscal release. **Human:** Required approvers sign within delegation. **Failure/boundary:** Submitting vendor cannot certify its own payment acceptance.

5. Submit payment

Software: Adapter passes signed instruction with unique business key. **Human:** Fiscal system remains authoritative. **Failure/boundary:** Retry reuses key; a changed amount requires a new authorized instruction.

6. Resolve uncertainty

Software: Query provider transaction reference after timeout before another submission. **Human:** Exception owner handles irreconcilable state. **Failure/boundary:** No claim of exactly-once delivery without sink reconciliation.

7. Confirm settlement

Software: Reconcile instructed, settled, reversed and disputed amounts. **Human:** Officer investigates residual balance. **Failure/boundary:** Authorized is not paid; ticket cannot close on authorization alone.

W14 - Preschool special-education transition

1. Establish responsibility

Software: Identify locality/phase-specific sending and receiving authorities. **Human:** Both authorities verify their duties. **Failure/boundary:** No statewide assumption that every transition occurred on the same day.

2. List required support

Software: Authorized current plan yields reviewed service and transport obligations. **Human:** Qualified education professional validates the list. **Failure/boundary:** AI cannot infer eligibility or replace the approved plan.

3. Transfer minimum record

Software: Approved exchange sends necessary records with manifest and access restrictions. **Human:** Custodians approve scope and recipients. **Failure/boundary:** Technical receipt is separate from accepted responsibility.

4. Accept and provision

Software: Receiver assigns professional, provider and transport tasks. **Human:** Receiving official confirms resources or records gap. **Failure/boundary:** No provider availability is invented.

5. Confirm first service

Software: Appointment and actual first delivery recorded separately. **Human:** Provider/authorized professional verifies reality. **Failure/boundary:** File transfer cannot mark the whole transition complete.

6. Escalate gap

Software: Predefined continuity task addresses missing provider, transport or record. **Human:** Competent officials decide remedy with applicable safeguards. **Failure/boundary:** System cannot reduce a service plan to make a queue appear complete.

7. Verify transition

Software: Record completed and unresolved obligations with named ongoing owner. **Human:** Sending/receiving authorities reconcile closure. **Failure/boundary:** Family does not have to discover orphaned tasks after the transfer.

W21 - Motor vehicle credential or title

1. Choose transaction

Software: Catalogue asks activity-specific questions and current requirements. **Human:** Person confirms transaction and preferred assistance. **Failure/boundary:** Chat is optional; shared-device privacy is preserved.

2. Check readiness

Software: Document preflight identifies determinable missing items. **Human:** Staff handles identity/evidence exceptions. **Failure/boundary:** Preflight never guarantees credential approval.

3. Reserve capacity

Software: Scheduling considers service duration, equipment and accommodations. **Human:** Person accepts a slot or assisted alternative. **Failure/boundary:** Appointment availability does not imply total service capacity.

4. Preserve encounter

Software: Check-in shows queue status and prior submitted material where authorized. **Human:** Counter worker verifies actual originals/identity as required. **Failure/boundary:** A prior scan does not waive an in-person legal requirement.

5. Decide and execute

Software: Authorized examiner records action; source system performs credential/title update. **Human:** Officer resolves ownership or eligibility disputes. **Failure/boundary:** No LLM decides identity or title ownership.

6. Confirm result

Software: Explain actual outcome, next delivery or precise defect and review route. **Human:** Responsible team owns incomplete downstream issuance. **Failure/boundary:** Print/payment failure remains an open task; repeat trip reason is measured.

W22 - Environmental or land-use permit

1. Map authority

Software: Activity/site catalogue names separate local/state/federal requirements. **Human:** Coordinator validates ambiguous jurisdiction. **Failure/boundary:** A universal approval endpoint is not proposed.

2. Freeze checklist version

Software: Requirement snapshot includes authority, effective date and conflict flag. **Human:** Content/legal owner resolves contradictory guidance. **Failure/boundary:** Latest web retrieval is not necessarily controlling law.

3. Receive evidence

Software: Store technical originals, calculations, maps and public-participation record. **Human:** Applicant and qualified reviewer validate material data. **Failure/boundary:** Extraction confidence does not certify a measurement.

4. Run parallel tasks

Software: Compatible reviews receive shared authorized evidence and dependencies. **Human:** Each reviewer keeps decision authority. **Failure/boundary:** Public comment and statutory sequence cannot be optimized away.

5. Consolidate questions

Software: Coordinator reconciles repeated factual requests. **Human:** Technical reviewers sign specific requests. **Failure/boundary:** A receiving authority may need different evidence for a different legal test.

6. Approve findings

Software: Reviewer inspects evidence, approved calculations and contrary submissions. **Human:** Qualified official decides findings/conditions. **Failure/boundary:** No AI permit approval or automatic override of unfavorable evidence.

7. Issue separate decisions

Software: Publish authorized decisions, conditions and review routes. **Human:** Each authority signs its own act. **Failure/boundary:** One permit issuance cannot mark every authority approved.

8. Verify conditions

Software: Inspections and maintenance obligations enter delivery ledger. **Human:** Qualified inspector certifies required work. **Failure/boundary:** Project closure excludes no unresolved mandatory condition.

W33 - Court filing and technical correction

1. Select current form

Software: Catalogue returns current requirement and case/court scope. **Human:** Assistance staff resolve procedural questions within authority. **Failure/boundary:** Superseded form warning is not a ruling against the claim.

2. Preflight technical fields

Software: Check file readability, form version and determinable required fields. **Human:** Filer confirms submission; staff reviews ambiguous requirements. **Failure/boundary:** No machine-only rejection based on writing style or merits.

3. Preserve attempt

Software: Save immutable original reference, timestamp and content hash. **Human:** Court rules determine legal consequences. **Failure/boundary:** Receipt explicitly says whether it is only submission/attempt evidence.

4. Submit through approved route

Software: Adapter uses court-authorized interface or accountable manual transfer. **Human:** No integration runs without branch approval. **Failure/boundary:** API absence is not permission to scrape or automate credentials.

5. Record clerk result

Software: Authoritative receipt sets accepted/returned status and stated defects. **Human:** Clerk acts within governing authority. **Failure/boundary:** Draft AI explanation cannot alter the official rejection reason.

6. Correct with lineage

Software: Resubmission links prior attempts and supporting outage/defect evidence. **Human:** Filer and court apply actual cure/timeliness rules. **Failure/boundary:** System does not invent relation-back or extend deadline.

7. Expose next state

Software: Distinct docket/service/scheduling/presentment states visible as permitted. **Human:** Responsible clerk/official owns each step. **Failure/boundary:** Submission success cannot be labeled judicial consideration.

8. Recover outages

Software: Reconcile all in-flight attempts with court receipts before closure. **Human:** Duty owner and court determine permitted fallback. **Failure/boundary:** No automatic denial, destruction or duplicate charge on restart.

W36 - Hearing record, transcript and appeal assembly

1. Identify hearing and scope

Software: Request references actual docket/hearing and requested format. **Human:** Requester authority verified by authorized staff. **Failure/boundary:** Similar party names or linked family cases do not grant access.

2. Record governing posture

Software: Track applicable access order, fees, waiver request and alternatives. **Human:** Court/authorized official decides each issue. **Failure/boundary:** Policy text or vendor estimate is not an order.

3. Inventory existing record

Software: Manifest identifies recordings, exhibits, orders and absent components. **Human:** Custodian validates completeness of inventory. **Failure/boundary:** Generated transcript is labeled unofficial until authorized process approves it.

4. Assign production

Software: Production task names source holder, vendor/office and required follow-up. **Human:** Coordinator confirms receiving responsibility. **Failure/boundary:** Vendor cancellation creates unresolved-record task rather than complete status.

5. Deliver securely

Software: Authorized recipient receives approved file and source receipt. **Human:** Custodian approves disclosure and retention. **Failure/boundary:** Public summary never exposes sealed/private audio.

6. Confirm official state

Software: Record delivery separately from official appellate record-completion determination. **Human:** Court controls sufficiency and deadlines. **Failure/boundary:** No software inference that payment failure equals legal completeness.

7. Resolve remaining gaps

Software: Missing items and corrections keep their original dates and owner. **Human:** Competent official determines remedy. **Failure/boundary:** Complaint/help ticket does not imply an appellate deadline was tolled.

W41 - Public records request

1. Accept without extra gate

Software: Capture usable scope/contact under applicable access process. **Human:** Access officer identifies proper regime and custodians. **Failure/boundary:** No compulsory account, AI chat or extra form unless legally required.

2. Acknowledge accurately

Software: Track acknowledgment, estimate and applicable deadlines separately. **Human:** Officer approves estimates and necessary clarification. **Failure/boundary:** Acknowledgment does not count as production.

3. Search reproducibly

Software: Assign bounded searches across approved custodians; log terms and returned sources. **Human:** Custodians explain limitations and missing repositories. **Failure/boundary:** Search-result absence is not a universal no-record conclusion.

4. Review candidates

Software: Draft deduplication and redaction suggestions preserve inspectable originals. **Human:** Authorized reviewer decides exemptions and release. **Failure/boundary:** Model cannot independently withhold or disclose.

5. Test redaction

Software: Check pixels, text layer, attachments and metadata for prohibited residual data. **Human:** Reviewer inspects output and log. **Failure/boundary:** Black rectangle overlay without actual removal fails acceptance.

6. Produce and explain

Software: Send accessible production or specific withholding reasons and review route. **Human:** Custodian authorizes release. **Failure/boundary:** Partial batches do not silently close outstanding scope.

7. Retain lawfully

Software: Apply approved retention/hold schedule and delete expired derived caches. **Human:** Records officer approves lifecycle. **Failure/boundary:** Auditability does not mean perpetual retention of private contents.

W42 - Legislation from problem to implementation

1. Ingest authoritative version

Software: Store official source, hash, stage and text comparison. **Human:** Legislative professional validates status. **Failure/boundary:** Bill text cannot be treated as enacted law.

2. Map impacts

Software: Dependency graph links definitions, forms, rules, systems, data and training. **Human:** Agencies validate affected responsibilities. **Failure/boundary:** Machine-detected effect is a candidate, not a legal conclusion.

3. Produce questions

Software: AI prepares sourced implementation questions and unresolved alternatives. **Human:** Nonpartisan experts check facts and assumptions. **Failure/boundary:** No political ranking or recommendation is produced.

4. Estimate transparently

Software: Scenario model exposes volumes, labor, capacity and uncertainty. **Human:** Fiscal professionals sign official estimates. **Failure/boundary:** Capacity value cannot silently become cash savings.

5. Record actual action

Software: Authorized action/version/effective date recorded from official source. **Human:** Legislators/officials make policy and procedural choices. **Failure/boundary:** The workflow cannot vote, sponsor or adopt a rule.

6. Prepare controlled release

Software: Approved rule/form/config versions and test cases built in advance. **Human:** Legal, service and release owners sign relevant components. **Failure/boundary:** Deployment requires effective-date/authority checks, not a web-page change trigger alone.

7. Verify public implementation

Software: Check guidance, staff instructions, notices and software agree. **Human:** Named content/service owners correct divergence. **Failure/boundary:** Old rule retained for historical cases and source lineage.

W47 - Hiring, onboarding and workforce back-up

1. Validate authorized change

Software: Position/delegation and effective date verified before tasks start. **Human:** HR/supervisor approves hire/role change. **Failure/boundary:** AI does not rank applicants or infer fitness.

2. Provision least privilege

Software: Create approved access, equipment, payroll and training tasks. **Human:** Owners approve specific grants. **Failure/boundary:** Same department is not permission to all its case records.

3. Confirm readiness

Software: Verify working device, necessary training and actual account access. **Human:** Worker/supervisor validate task readiness. **Failure/boundary:** Account-created event alone is not ready-to-work.

4. Maintain coverage

Software: Every service task has role owner and approved backup. **Human:** Supervisor allocates realistic workload. **Failure/boundary:** No hidden unpaid coordination burden added without capacity.

5. Transfer or revoke

Software: Role departure revokes access and transfers pending tasks. **Human:** Custodians revalidate new responsibilities. **Failure/boundary:** Service automation is not owned solely by a departing personal account.

6. Reconcile pay and cases

Software: Check effective pay/benefits and unowned tasks after change. **Human:** HR/payroll/service owner resolves exception. **Failure/boundary:** Security revocation is distinct from lawful records retention.

Appendix C. Institutional coverage and workspace index

All entries are proposed role archetypes, not certified position titles. The explorer and workbook supply their detailed actions and boundaries.

U01 - Governor and executive coordination

R001 Executive service coordinator (Cross-department obligations desk); R002 Executive policy and legal adviser (Authority and implementation workspace).

U02 - House, Senate and legislative committees

R003 Representative or senator (Constituent and legislative workspace); R004 Committee clerk and legislative drafter (Hearing and drafting workbench); R096 Legislative fiscal and nonpartisan research analyst (Bill-to-system impact workspace).

U03 - Secretary of State and official records

R005 Official records and business-registration clerk (Versioned filing workspace); R006 Records archivist and custodian (Lifecycle and authenticity workspace).

U04 - Treasurer, cash and debt functions

R007 Treasury cash and settlement officer (Settlement and liquidity workspace); R008 Debt and obligation analyst (Public commitments ledger).

U05 - Attorney General and public legal functions

R009 Government counsel (Protected legal research workspace); R010 Consumer response and legal-intake specialist (Complaint triage workspace).

U06 - State Audit and OPEGA

R011 Financial auditor (Read-only audit workbench); R012 Program evaluator (Outcome and burden analysis workspace).

U07 - DAFS budget, controller and financial service centres

R013 Budget analyst (Authority-to-delivery financial map); R014 Controller and accounts-payable specialist (Exception and reconciliation desk); R097 Administrative service-centre coordinator (Cross-function invoice and HR desk).

U08 - Procurement, grants and contract administration

R015 Procurement officer (Requirement-to-acceptance workspace); R016 Grant and contract administrator (Delivery and reimbursement workspace).

U09 - Human resources, payroll and employee development

R017 HR recruitment and onboarding specialist (Position and readiness workspace); R018 Payroll and benefits specialist (Employee-change reconciliation desk).

U10 - MaineIT, cyber, data and digital service teams

R019 Service/product owner (Public-task delivery workspace); R020 Platform and integration engineer (Connector and durable-workflow workbench); R089 Cybersecurity analyst (Permission and incident workbench); R090 Privacy and data-protection steward (Purpose and data-rights workspace); R091 Accessibility engineer and tester (Inclusive service test workspace); R092 Quality and release engineer (Synthetic case and regression workspace).

U11 - Tax administration and collections

R021 Taxpayer service specialist (Obligation and account-explanation workspace); R022 Tax processing and compliance examiner (Rules and evidence workbench).

U12 - DHHS benefit eligibility and OFI

R023 Eligibility worker (Household assistance workspace); R024 Benefits navigator (Multichannel completion workspace).

U13 - MaineCare administration and provider interfaces

R025 MaineCare member and provider liaison (Coverage-to-care workspace); R026 Claims and payment-integrity specialist (Claims exception workbench).

U14 - Public health, laboratories and vital records

R027 Public-health analyst and laboratory coordinator (Surveillance and sample-tracking workspace); R028 Vital-records specialist (Identity-event records workspace).

U15 - Aging, disability and long-term supports

R029 Disability/aging support coordinator (Authorized-support and delivery workspace); R030 Facility and support-program inspector (Evidence and correction workspace).

U16 - Behavioral health and state treatment facilities

R031 Behavioral-health care coordinator (Administrative continuity workspace); R032 Facility operations and discharge planner (Bed/capacity and onward-service workspace).

U17 - Child protection and family-support services

R033 Child-protection intake professional (Protected report and evidence workspace); R034 Family-support case professional (Service implementation workspace).

U18 - Child care and early-family support

R035 Child-care subsidy and provider-payment specialist (Attendance-to-settlement workspace); R036 Early-family service navigator (Family service continuity workspace).

U19 - Education, schools and early special education

R037 School registrar and student-support coordinator (Education access and continuity workspace); R038 Special-education transition professional (Sending/receiving responsibility workspace).

U20 - Public higher education, training and education finance

R039 College/adult-learning adviser (Learning-to-work pathway workspace); R040 Education finance administrator (Award and payment obligation workspace).

U21 - Labor, unemployment, paid leave and rehabilitation

R041 Unemployment and paid-leave examiner (Claim and wage-evidence workspace); R042 Workforce and rehabilitation adviser (Employment-support delivery workspace).

U22 - Business development, tourism, innovation and FAME

R043 Business-development adviser (Business task and program-navigation workspace); R044 Economic and program analyst (Program delivery and evidence workspace).

U23 - Housing, MaineHousing and community assistance

R045 Housing navigator (Need-to-available-option workspace); R046 Housing development and compliance manager (Project and resident-service workspace).

U24 - Professional and occupational boards

R047 Licensing analyst (Requirement and credential workspace); R048 Board member and professional investigator (Independent discipline workspace).

U25 - Banking, insurance and consumer-credit regulation

R049 Insurance/banking consumer specialist (Financial complaint resolution workspace); R050 Financial regulator/examiner (Controlled examination workspace).

U26 - Transport, roads, bridges, ferries, rail, ports and aviation

R051 Transportation engineer and asset manager (Field condition and lifecycle workspace); R052 Ferry/transit operations and accessibility coordinator (Journey continuity workspace).

U27 - Motor vehicle licensing and registration

R053 BMV counter and mobile-service specialist (Transaction-readiness workspace); R054 BMV back-office examiner (Credential and title-evidence workspace).

U28 - DEP and environmental adjudication

R055 Permit project coordinator (Multi-authority review workspace); R056 Environmental technical reviewer/inspector (Scientific evidence and findings workspace).

U29 - Agriculture, forestry, parks, public lands and land-use administration

R057 Agriculture/forestry field professional (Seasonal assistance and observation workspace); R058 Land-use/public-lands and parks manager (Stewardship and access workspace).

U30 - Inland fisheries, wildlife and marine resources

R059 Fisheries/wildlife biologist (Observation and permit-data workbench); R060 Marine/wildlife licence and field-enforcement specialist (Seasonal compliance workspace).

U31 - Energy policy, utility regulation, consumer advocacy and efficiency delivery

R061 Energy program coordinator (Bill-to-project assistance workspace); R062 Utility regulator and consumer-advocacy analyst (Separated regulatory/advocacy workspaces).

U32 - Broadband and communications infrastructure

R063 Broadband project and grant officer (Coverage-to-connection workspace); R064 Digital access navigator (Assisted public-service workspace).

U33 - Public safety, emergency medical services and fire functions

R065 Emergency dispatcher and response coordinator (Human-led incident workspace); R066 Fire/EMS standards and support specialist (Readiness and corrective-action workspace).

U34 - Defence, veterans and emergency management

R067 Emergency manager and recovery administrator (Resource and recovery obligation workspace);
R068 Veterans service officer (Benefit navigation and authorized-representation workspace).

U35 - Corrections, youth custody and re-entry

R069 Corrections release coordinator (Release-readiness and onward-support workspace); R070
Facility/youth-services administrator (Care, education and operations workspace).

U36 - Judges, magistrates, clerks and court administration

R071 Court clerk and intake specialist (Filing-state and correction workspace); R072 Judge or magistrate
(Permitted-record judicial workbench); R093 Court scheduler and interpreter coordinator
(Hearing-readiness workspace); R094 Court records and transcript coordinator (Hearing-record fulfillment
workspace); R095 Self-represented-litigant assistance specialist (Neutral form and process workspace).

U37 - Prosecution and public defence

R073 Prosecutor (Prosecution-only case preparation workspace); R074 Public defender and investigator
(Defense-only privileged workbench).

U38 - Administrative hearings, civil-rights and professional-conduct review

R075 Administrative hearing officer (Independent review workspace); R076 Civil-rights/conduct intake
and investigator (Jurisdiction and remedy workspace).

U39 - County, municipal, school and special-purpose interfaces

R077 Municipal clerk and local service coordinator (Locally governed service workspace); R078
County/special-district operations manager (Shared obligation and asset workspace).

U40 - Tribal-state interfaces

R079 Tribal-state liaison (Government-to-government agreement workspace); R080 Intergovernmental
data steward (Agreement and exchange-control workspace).

U41 - Libraries, archives, arts, museums and historical resources

R081 Librarian and public access specialist (Assisted navigation and information workspace); R082
Museum/arts/archive program and collection manager (Collection and public-program workspace).

U42 - Public authorities, retirement and public financing entities

R083 Retirement/public-finance administrator (Member obligation and calculation workspace); R084 Authority board and asset/program manager (Independent commitments workspace).

U43 - Election administration and ethics disclosure

R085 Election operations records administrator (Restricted operations-readiness workspace); R086 Ethics disclosure intake and review specialist (Disclosure completeness workspace).

U44 - Public access, FOAA and constituent services

R087 FOAA/public-access officer (Custodian search and disclosure workspace); R088 Constituent-service and complaint recovery lead (Wrong-door and correction workspace); R098 Resident-facing service designer (Observed-journey and testing workspace); R099 Resident or business applicant (My tasks, evidence and decisions); R100 Authorized helper or representative (Scoped delegated assistance).

Appendix D. Source and evidence ledger

Access date: September 20, 2026. Prior-artifact entries B01/B02 are inherited design sources; T entries are primary web research. The scope note states important limits. Technical references do not authorize use of protected records or establish installed products.

T01 - MaineIT services and policy index

Primary web research. Existing executive IT governance; not evidence of production interoperability or branch-wide applicability.

<https://www.maine.gov/oit/policies-standards>

T02 - Maine Data Exchange Policy

Primary web research. Revision text dated April 17, 2026: authority, covered standing exchanges, signed agreements, logs and Maine Service Bus route. Exact application is custodian-specific.

<https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/DataExchangePolicy.pdf>

T03 - Maine GenAI Policy

Primary web research. Version discrepancy: search extraction returned nine pages including agentic provisions; screenshot returned a seven-page version at the same URL. No permission or approved-product claim is treated as settled. Obtain a signed, versioned copy before implementation.

<https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/GenAIPolicy.pdf>

T04 - Maine Microsoft Low-Code Governance

Primary web research. Existing executive governance for Power Automate, Power Apps and Dynamics; document describes Government Community Cloud. Present licenses and technical entitlements not audited.

<https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/MSLowCodeGovernance.pdf>

T05 - Maine Vendor Identity System Integration Policy

Primary web research. Vendor identity integrations require applicable OIT approval and assessment; an account federation is not general case-data permission.

<https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/VendorIdentitySystemIntegrationPolicy.pdf>

T06 - Maine Data Classification Policy

Primary web research. Existing classification framework; map each data element with its custodian. Do not substitute this report's design labels for Maine classifications.

<https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/DataClassificationPolicy.pdf>

T07 - Maine Digital Accessibility Policy

Primary web research. Existing state policy reference; complete applicability and signed version remain deployment checks.

<https://www.maine.gov/oit/sites/maine.gov/oit/files/inline-files/DigitalAccessibilityPolicy.pdf>

T08 - MyMaine gateway initiative

Primary web research. Public page describes a future shared identity and gateway; production service coverage, APIs and promised rollout are not independently verified.

<https://mymaine.gov/>

T09 - Maine eCourts

Primary web research. Existing electronic filing, payments and records; staged deployment. Does not prove a public write API or authorize integration.

<https://www.courts.maine.gov/ecourts/>

T10 - Maine electronic court-record access

Primary web research. Different public, party, attorney, courthouse-only and restricted access; do not treat a uniform interface as uniform entitlement.

<https://www.courts.maine.gov/ecourts/access.html>

T11 - OFI and My Maine Connection

Primary web research. Current page identifies applications, renewal and change reporting. Program rules and actual interfaces require a separate approved integration review.

<https://www.maine.gov/dhhs/ofi>

T12 - Maine Tax Portal

Primary web research. Existing tax filing, payment and account-management interface; APIs and internal product entitlements not established.

<https://www.maine.gov/revenue/portal>

T13 - Maine procurement services

Primary web research. Existing procurement, contracts, grants and vendor services; does not establish a single shared backend.

<https://www.maine.gov/dafs/bbm/procurementservices/>

T14 - Maine Bureau of Motor Vehicles

Primary web research. Service catalogue and municipal/agent interfaces; no credential-decision automation or write access inferred.

<https://www.maine.gov/sos/bmv>

T15 - NIST SP 800-63-4

Primary web research. Final July 2025 technical identity guidance; risk-appropriate assurance, not permission for any particular data disclosure.

<https://csrc.nist.gov/pubs/sp/800/63/4/final>

T16 - NIST SP 800-63C-4

Primary web research. Federation and assertions across separately administered relying parties; reference design foundation, not Maine implementation evidence.

<https://csrc.nist.gov/pubs/sp/800/63/c/4/final>

T17 - NIST AI Risk Management Framework

Primary web research. Voluntary risk framework and generative-AI profile; does not independently authorize a government use.

<https://www.nist.gov/itl/ai-risk-management-framework>

T18 - WCAG 2.2

Primary web research. Engineering target for this proposal; distinguish from the WCAG 2.1 AA technical standard in the DOJ rule.

<https://www.w3.org/TR/WCAG22/>

T19 - DOJ Title II web accessibility rule factsheet

Primary web research. Current factsheet reflects April 2026 deadline extension to April 26, 2027 for 50,000+ and April 26, 2028 for smaller entities/special districts. Existing obligations and applicability remain distinct.

<https://www.ada.gov/resources/2024-03-08-web-rule/>

T20 - OpenAPI specification 3.0.4

Primary web research. Stable compatibility example for the included illustrative contract; not a claim this is the latest version.

<https://spec.openapis.org/oas/v3.0.4.html>

T21 - Temporal Activities documentation

Primary web research. Durable activity execution and retry behavior; side effects need idempotency. Product example, not a procurement selection.

<https://docs.temporal.io/activities>

T22 - Open Policy Agent documentation

Primary web research. Externalized software authorization and policy evaluation example; legal interpretation is not delegated to the engine.

<https://www.openpolicyagent.org/docs>

T23 - OPA decision logs

Primary web research. Policy evaluation metadata and sensitive-field masking; evaluation logs are not a complete official decision record.

<https://www.openpolicyagent.org/docs/management-decision-logs>

T24 - Power Automate run and retention limits

Primary web research. Documentation gives a 30-day cloud-flow run duration including waiting approvals; durable case state must not depend on one such run.

<https://learn.microsoft.com/en-us/power-automate/limits-and-config>

T25 - CloudEvents

Primary web research. Interoperable event-envelope specification; not a guarantee of exactly-once business effects or authorization.

<https://cloudevents.io/>

T26 - HL7 FHIR security

Primary web research. Interchange/security reference; FHIR availability, version and disclosure authority must be verified at each endpoint.

<https://www.hl7.org/fhir/security.html>

T27 - Maine enacted LD 2082 / chapter 687

Primary web research. Approved April 13, 2026; enacted text distinguishes administrative/supplementary support from prohibited independent therapeutic functions. Not a general government-chatbot law.

<https://legislature.maine.gov/legis/bills/getPDF.asp?item=3&paper=HP1397&snum=132>

T28 - PostgreSQL row-level security

Primary web research. Technical defense-in-depth option. Owner/superuser behavior and application authorization require separate tests.

<https://www.postgresql.org/docs/current/ddl-rowsecurity.html>

T29 - OWASP prompt injection

Primary web research. Threat model for untrusted documents and instructions; retrieval alone does not neutralize injection.

<https://genai.owasp.org/llmrisk/llm01-prompt-injection/>

B01 - Prior public-service design ledger

Provided prior artifact. All 44 U IDs and 52 W IDs retained. Prior source summaries are inherited design context, not newly verified in this pass.

/mnt/data/maine_deliverables/Maine_Public_Service_Design_Ledger.json

B02 - Prior public-service operating model

Provided prior artifact. Framing retained: usable public results, four layers, distinct clocks, position accountability and joined service without a joined dossier.

/mnt/data/maine_deliverables/Maine_Public_Service_Operating_Model.md