IMPLEMENTATION UPDATE • TASK 49 COMPLETE

Unified Ticketing, Agile & Documentation Platform

Project plan for a Jira-inspired service, work, knowledge, and calendar system

North star: one calm, trustworthy place where staff and customers can request work, move it through a visible workflow, find controlled documentation, and act on deadlines.

PLAN STATUS	TARGET KICKOFF	DELIVERY MODEL
v1.4 — Tasks 1–49 complete; controlled pilot remains	Implementation underway	One task at a time; tested at every gate

Prepared 1 August 2026 • Implementation update 12 August 2026

Research snapshot: official sources current on the preparation date

IMPLEMENTATION STATUS • 12 AUGUST 2026

Tasks 1–49 are complete and verified

The roadmap is now an active commercial-release record. Task 49 adds accountable pilot ownership, an evidence-backed Launch Center, role-specific first-day guidance, and printable administrator/customer handoff material.

DELIVERED TASKS	CURRENT BUILD	API TESTS	WEB TESTS
49	0.49.0	152 passed	29 passed

Verified delivery ledger

Tasks 1–49 are implemented or published in the working baseline. Build 0.49.0 has 152 passing API/domain/model tests, 29 passing web tests, clean production builds, an applied migration, no database-model drift, and live browser evidence for launch-plan and checklist persistence.

TASK	BUILD	DELIVERED INCREMENT	STATUS
1	0.1.0	Solution and API/web foundation	Complete
2	0.2.0	PostgreSQL data foundation and first migration	Complete
3	0.3.0	Issue creation and retrieval API	Complete
4	0.4.0	First issue workspace UI	Complete
5	0.5.0	Configurable drag-and-drop workflow board	Complete
6	0.6.0	Ticket timers and worklogs	Complete
7	0.7.0	Microsoft Entra identity foundation	Complete
8	0.8.0	People and permission administration	Complete
9	0.9.0	Customer accounts and contacts	Complete
10	0.10.0	Secure attachments and protected downloads	Complete
11	0.11.0	Ticket comments and unified activity history	Complete
12	0.12.0	Notification inbox and email delivery foundation	Complete
13	0.13.0	Permission-aware ticket search and saved views	Complete
14	0.14.0	Ticket editing, references, and linked work	Complete
15	0.15.0	Backlog and sprint planning	Complete
16	0.16.0	Project calendar and milestone scheduling	Complete
17	0.17.0	Wiki spaces and application documentation	Complete
18	0.18.0	Teams and manager administration	Complete
19	0.19.0	Team-owned tickets and server-enforced visibility	Complete

TASK	BUILD	DELIVERED INCREMENT	STATUS
20	0.20.0	My Tickets, My Teams, and All Teams views	**Complete**
21	0.21.0	Controlled documents and review workflows	**Complete**
22	0.22.0	Acknowledgments, controlled exports, and compliance	**Complete**
23	0.24.1	Governed Microsoft 365 directory, email, and calendar	**Complete**
24	0.24.0	Permission-aware unified workspace search	**Complete**
25	0.25.0	Safe automation rules and execution history	**Complete**
26	0.26.0	Operational reporting and workload insights	**Complete**
27	0.27.0	Reusable saved reports and governed CSV export evidence	**Complete**
28	0.28.0	Safe scheduled report delivery and delivery evidence	**Complete**
29	0.29.0	Business-calendar SLA policies and live monitoring	**Complete**
30	0.30.0	Immutable ticket SLA snapshots, pauses, milestones, and attainment	**Complete**
31	0.31.0	Deduplicated SLA breach alerting and delivery evidence	**Complete**
32	0.32.0	SLA breach acknowledgments and named accountability evidence	**Complete**
33	0.33.0	Owned SLA recovery commitments and immutable outcomes	**Complete**
34	0.34.0	Frozen Version 1.0 commercial scope and measurable release gates	**Complete**
35	0.35.0	Commercial organization provisioning and authenticated tenant isolation	**Complete**
36	0.36.0	External customer identities and reporter-scoped self-service portal	**Complete**
37	0.37.0	Customer-visible replies, private internal notes, and request participants	**Complete**
38	0.38.0	Governed Outlook email-to-ticket routing, deduplication, rejection, and recovery	**Complete**
39	0.39.0	Production Microsoft 365 consent, callbacks, subscriptions, recovery, and health	**Complete**
40	0.40.0	Customer SLA contracts, holiday calendars, immutable cycles, and governed reopen	**Complete**
41	0.41.0	On-call schedules, substitutes, proactive reminders, and multi-level escalation	**Complete**

TASK	BUILD	DELIVERED INCREMENT	STATUS
42	0.42.0	Production attachment storage, ClamAV quarantine, and Outlook attachment scanning	**Complete**
43	0.43.0	Manual trials, subscriptions, customer-managed licensing, and internal seat limits	**Complete**
44	0.44.0	Production containers, file-mounted secrets, migration-gated deployment, and rollback	**Complete**
45	0.45.0	Monitoring, durable-queue alerting, complete backup, guarded restore, and recovery proof	**Complete**
46	0.46.0	Retention/privacy governance, abuse protection, key ownership, and security evidence	**Complete**
47	0.47.0	Performance timing, lazy routes, accessibility automation, and compatibility evidence	**Complete**
48	0.48.0	Safe diagnostics, product-support cases, service notices, and expiring support access	**Complete**
49	0.49.0	Commercial launch plans, readiness evidence, role guidance, and handoff material	**Complete**

TASK 49 LIVE CHECK 152 backend and 29 web tests pass; API and production web builds are clean; the Task 49 migration is applied with no model drift. G2, G8, and G9 remain Partial pending named human, hosted, legal/privacy, customer, and pilot evidence.

Next implementation gate. Task 50 runs the controlled customer pilot, closes or explicitly accepts remaining release evidence, and produces the final Version 1.0 go/no-go record.

EXECUTIVE ORIENTATION

1. Executive recommendation

RECOMMENDATION Build a focused, tenant-ready modular platform—not a feature-for-feature Jira clone. Start with one complete workflow from request to resolution, then add Agile boards, controlled documentation, and Microsoft 365 calendar/email capabilities behind the same permission and audit model.

The product should combine the internal depth of a work-management tool with the simplicity of a customer service portal. Jira is the benchmark for configurable work items, backlogs, boards, queues, and workflows [S1–S4]; Microsoft Entra ID and Microsoft Graph are the integration foundation for workforce identities, directory data, Outlook mail, and calendars [S5–S11].

The documentation module should support useful knowledge articles and formal controlled documents. It can be designed to support ISO-aligned quality and information-security processes, but software alone does not confer ISO certification. Formal conformance mapping must use licensed copies of the applicable standards and be validated by the organization's quality/security owners [S12–S15].

The words you were looking for

You described	Working term for this plan
"Jury / something beginning with J"	Jira — the reference model for issues, projects, backlogs, and boards
"Where all the people are in Outlook"	Microsoft Entra ID (formerly Azure Active Directory), accessed through Microsoft Graph
"Attaching stuff"	File attachments, stored securely with malware scanning, retention, and access controls
"ISO documentation"	Controlled documented information: versions, approvals, effective dates, review, evidence, and audit history
"A calendar we create"	An application calendar for work dates, with optional Outlook calendar integration

2. What this plan commits to—and what it does not

Committed direction

- One coherent application with separate staff, manager, administrator, auditor, and customer experiences.
- Projects, issues/tickets, accountable owners, customer organizations/accounts, contacts, comments, links, attachments, notifications, and audit history.
- Configurable Kanban and Scrum-style views with drag-and-drop plus a complete keyboard-accessible alternative.

- A documentation/knowledge system that supports both everyday articles and controlled records.
- A first-class calendar plus deliberate Microsoft 365/Outlook integration.
- Sequential delivery with a demonstration and written approval before each next phase.

Task 34 decisions and remaining commercial choices

- Task 49 result: the Launch Center, accountable pilot plan, eight evidence-backed readiness gates, role guidance, and administrator/customer handoff material are implemented. Task 50 remains the controlled pilot and final Version 1.0 go/no-go.
- Final cloud/hosting provider, data residency, backup objectives, and operating budget.
- Exact ISO scope, certification intent, retention periods, legal hold needs, and regulatory obligations.
- Final technology versions and commercial component licenses; these require proof-of-concept and architecture decisions.
- AI assistants, asset/CMDB management, marketplace extensions, native mobile apps, and advanced portfolio planning.

CONTROL POINT No production feature development should begin until Phase 0 decisions and the Phase 1 product charter are approved. Prototypes and technical spikes are permitted only to reduce uncertainty.

3. Product vision and design principles

One work record, many views. A ticket can appear in a queue, board, project, customer portal, calendar, dashboard, and linked document without duplicating its source data.

Configuration over code. Administrators should configure types, fields, workflows, forms, SLAs, boards, templates, and automation within safe guardrails.

Least privilege by default. A user sees only the organizations, projects, tickets, documents, and fields they are authorized to see.

Auditability is a feature. Changes to important records, permissions, workflows, documents, integrations, exports, and attachments are attributable and reviewable.

Fast for common work. Creation, assignment, status changes, commenting, linking, and search should be efficient with mouse, touch, and keyboard.

Accessible, not merely attractive. Target WCAG 2.2 AA, including visible focus, meaningful structure, adequate contrast, target sizes, and alternatives to dragging [S17].

Progressive complexity. A new team can begin with a simple template; advanced teams can add fields, SLAs, automations, and controlled-document workflows.

Open integration boundaries. Use documented APIs, webhooks/events, stable IDs, idempotency, and an outbox so external systems do not corrupt core transactions.

4. Users, organizations, and permissions

Use precise language from the beginning: an Account is a customer organization; a Contact is a person at that account; a User Identity is a login; a Team is an internal working group; and a Role grants capabilities within a scope. This avoids the common ambiguity of using “account” for both a customer and a login.

Role	Primary responsibilities	Typical scope
Platform administrator	Identity, global settings, integrations, security, retention, audit export	Whole deployment
Project administrator	Project workflow, forms, fields, board, membership, queue and SLA setup	Assigned projects
Agent / contributor	Triage, own, update, comment, attach, link, resolve, document work	Permitted projects/accounts
Manager / product owner	Prioritize backlog, plan sprints, manage capacity, approve workflow changes, review metrics	Portfolio/team
Document owner / approver	Author, review, approve, publish, schedule review, supersede, acknowledge	Document spaces/types
Customer contact	Submit and track requests, add public comments/attachments, view allowed knowledge	Own account/request sharing
Auditor / read-only reviewer	Inspect records, document versions, approvals, access and audit trails	Explicitly granted scope
Integration service principal	Perform narrowly defined machine actions with monitored credentials	Configured API permissions

Permission model

- Role-based access control (RBAC) for standard capabilities, with scope at deployment, project, account, document space, and record level.
- Relationship rules for customers: reporter, request participant, customer organization, and explicitly shared request.
- Field-level protection for sensitive data where business need justifies the complexity.
- Separation of duties for controlled documents and high-risk administration; the same person should not silently author and approve when policy forbids it.
- Microsoft Entra groups can map to internal roles, but the application remains the authority for project/account-specific permissions.

5. Platform capability blueprint

The platform has four purpose-built product experiences on one governed foundation. This keeps ticketing, Agile planning, application knowledge, and calendar communication connected without forcing every user into the same screen or workflow.

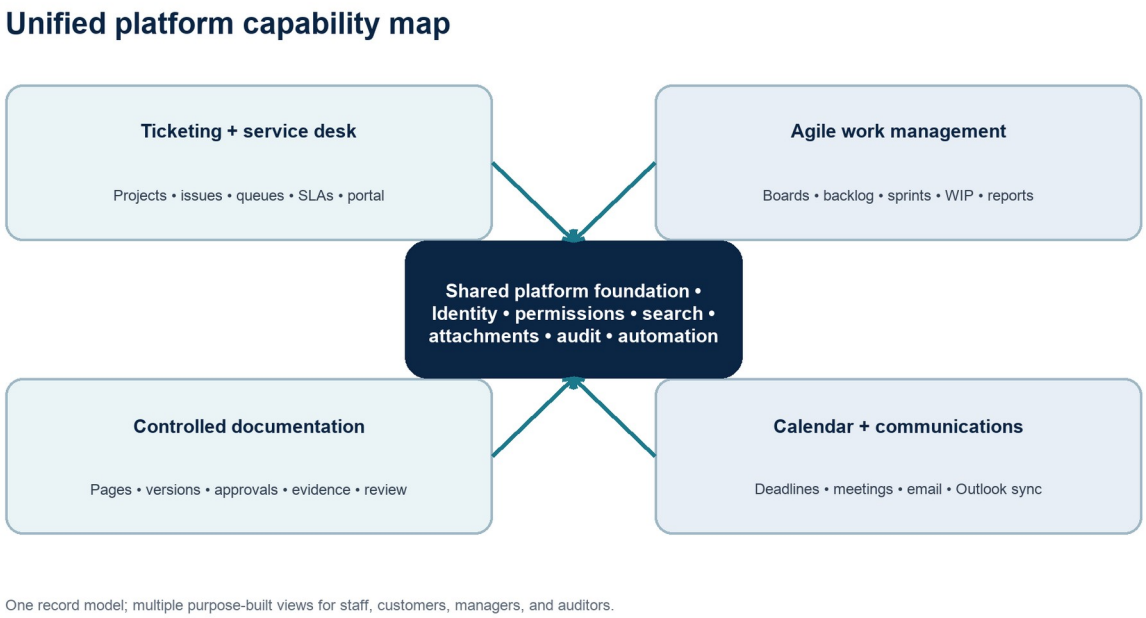

Figure 1. Four purpose-built experiences on one governed platform foundation.

Release boundaries

Release horizon	Outcome	Included capability
Pilot / MVP	A small internal team can manage real work end to end.	SSO, projects, tickets, workflow, comments, secure attachments, basic search, audit, Kanban view, simple documents, outbound notifications
Version 1	Internal teams and selected customers can operate the full service.	Customer accounts/portal, queues, SLAs, inbound email, Scrum planning, controlled documents, application calendar, Outlook integration, automation, dashboards
Version 1.x	Scale, governance, and usability mature.	Advanced reporting, document acknowledgment, richer retention, service catalog, portfolio views, localization, public API/webhooks
Separate future applications	Whiteboard and live engagement proceed only as independent products.	Optional future integrations may link tickets, wiki records, meetings, or decisions without joining the Version 1.0 scope.
Future options	Expand only after measured demand.	AI assistance, CMDB/assets, marketplace, native mobile, advanced resource planning, multi-region SaaS

6. Ticketing and service-management requirements

Core record anatomy

- Stable human key and immutable internal ID; project; type; summary; rich description; status; priority; resolution.
- Reporter, owner/assignee, accountable team, watchers, approvers, customer account, contacts, and request participants.
- Created/updated/resolved dates, due date, SLA clocks, estimates, work logs, sprint/release, and calendar visibility.
- Public and internal comments, mentions, reactions if needed, attachment metadata, linked issues, linked documents, and related calendar events.
- Components/services, labels, custom fields, forms, checklist/subtasks, parent/child hierarchy, and complete activity history.

Workflow engine

- Configurable statuses and guarded transitions with conditions, validators, required fields, approval steps, and post-actions.
- Status categories—To do, In progress, Done—remain stable for reporting even when teams rename detailed statuses.
- Published workflow versions: existing work keeps a traceable migration path when administrators change the design.
- A simple default flow: New → Triage → In Progress → Waiting for Customer / Blocked → Resolved → Closed, with reopen controls.

Service-desk experience

- Customer-friendly request types and forms map to internal work types; external and internal terminology can differ [S3].
- Queues use saved filters, ordering, SLA urgency, ownership, customer, and service; agents can claim or assign work.
- SLA policies support business calendars, pause conditions, response and resolution goals, breach warnings, and history.
- Portal users see allowed requests, public comments, status wording, attachments, approvals, knowledge suggestions, and notifications.

- Email-to-ticket preserves message identity, threading, participants, attachments, and an inbound processing log; failed messages enter a recoverable queue [S4].

MVP VERTICAL SLICE Create a request → triage it → assign an owner → move it through workflow → exchange public/internal comments → attach a safe file → resolve it → verify notifications and audit history. This must work before broad feature expansion.

7. Agile planning and drag-and-drop boards

Jira-style boards are views over work, not separate copies. Columns map to workflow statuses; filters decide which tickets appear; swimlanes group by assignee, account, epic, service, or priority. Scrum and Kanban are supported as operating modes, not forced onto every team [S1, S16].

Kanban mode

- Backlog optional; continuous flow; column WIP limits; blocked-state visibility; aging indicators; cumulative-flow and cycle-time reporting.
- Drag cards between allowed statuses with optimistic UI, server validation, conflict handling, and undo when safe.
- Quick filters, saved views, card density options, swimlanes, collapsed columns, and board-level permissions.

Scrum mode

- Ordered product backlog, epics, estimates, sprint creation, sprint goal, planning, start/complete controls, and carryover decisions.
- Sprint board, velocity/trend reports, burn chart, scope-change visibility, and a Definition of Done field/template.
- Do not assume every service team needs Scrum; enable it per project.

Accessible interaction requirements

- Every drag action also has a keyboard and menu action such as “Move to status…”, satisfying the WCAG 2.2 requirement to provide a non-dragging method [S17].
- Cards and drop targets have visible focus, programmatic names, status announcements, error recovery, and logical reading order.
- Color never carries status alone; combine labels, icons, and text. Honor reduced motion and zoom/reflow.

- Test with keyboard-only navigation and representative screen readers; automated tests are necessary but insufficient.

8. Customers, accounts, and contact management

The platform is not a full CRM. It stores the customer context required to deliver and report service without turning the first release into a sales system.

Entity	Minimum fields	Important behavior
Customer account	Name, domains, status, tier, owner, service entitlements, locale/time zone, notes	Controls portal visibility, SLA/service eligibility, reporting, and sharing
Contact	Name, email, phone optional, role/title, locale, account memberships	May belong to multiple accounts; duplicate and merge workflow required
User identity	Provider ID, sign-in name, status, MFA/claims metadata, linked contact	Login record is separate from business/contact profile
Contract/service entitlement	Service, effective dates, support hours, SLA policy, limits	Used for routing and SLA goals; optional in the pilot
Account activity	Tickets, documents shared, calendar items, notes, satisfaction	Permission-filtered timeline; no leakage between customer accounts

Customer onboarding paths

- Internal workforce: Microsoft Entra sign-in, directory profile sync, group-to-role mapping, and application-scoped access.
- External customers: invitation or verified email portal account; optional customer SSO/federation later.
- Email-only requester: configurable creation policy, verification and anti-abuse controls; portal access is not assumed automatically.
- Deactivation: revoke login while preserving historical authorship and ownership; provide reassignment and legal-retention behavior.

9. Documentation and ISO-aligned control system

IMPORTANT DISTINCTION A knowledge article is optimized for quick help and collaborative improvement. A controlled document is governed evidence: it has an owner, revision, approval, effective state, scheduled review, and defensible history. The product should support both without forcing every note through formal approval.

Confluence-style application wiki

Each team, product, project, or application can have a permissioned wiki space with a home page, nested page tree, breadcrumbs, labels, templates, drafts, publishing, comments, watchers, attachments,

version history, comparison, restore, archive, backlinks, and permission-aware search. These are proven collaboration patterns in Confluence and its technical-documentation guidance [S21–S22].

- Application home: purpose, business owner, technical owner, support team, lifecycle status, criticality, repository, service links, and primary contacts.
- Architecture: context/container diagrams, components, data flows, dependencies, integration contracts, technology stack, environments, and security/data classification.
- Build and operations: local setup, configuration, deployment, release process, monitoring, alerts, backup/recovery, troubleshooting, runbooks, and escalation.
- Change knowledge: roadmap, requirements, architecture decision records (ADRs), release notes, known issues, postmortems, migrations, and deprecation plans.
- Reusable application-space template and completeness dashboard so every application documents the same essential facts without forcing identical prose.
- Smart relationships: embed or list related tickets, incidents, changes, releases, documents, customers, calendar events, and dashboards without copying their data.
- Portable content: readable exports, stable links, redirects after page moves, API access, and an exit path so knowledge is not trapped in one editor.

WIKI GOVERNANCE Collaborative wiki pages can publish quickly and improve continuously. A page becomes a controlled document only when its type or policy activates formal owner, review, approval, effective-date, retention, and evidence requirements.

Document types

- Knowledge article, FAQ, troubleshooting guide, how-to, decision record, meeting note, runbook, policy, procedure, work instruction, form/template, standard/evidence record, and release note.
- Administrators choose which types are controlled, require approval, require acknowledgment, have review intervals, or may be customer-visible.

Controlled-document lifecycle

State	Required behavior
Draft	Author edits; version not effective; collaboration and comments allowed.
In review	Named reviewers assess content; changes are traceable; rejection returns to draft.
Approved	Authorized approver signs off; approval identity, date, and decision are retained.
Effective / published	The approved version is the current controlled copy; audience and effective date apply.
Review due	Owner receives reminders; review outcome is confirm, revise, or retire.
Superseded / archived	Old revision remains findable to authorized users but is visibly non-current and cannot be mistaken for the effective copy.

Required metadata and controls

- Document ID, title, type, space, owner, author, reviewers, approver, revision, status, effective date, review date, classification, retention category, audience, and related records.
- Side-by-side version comparison, change summary, approval record, full history, superseded banner, canonical link, export/print watermark options, and controlled-copy labeling.
- Review and acknowledgment tasks with reminders and evidence; acknowledgment is not a substitute for training where training is required.
- Links from tickets, projects, services, customer accounts, risks, controls, audits, incidents, and corrective actions.
- Templates and reusable sections with governance over template versions; bulk review and owner reassignment.

ISO posture as of 1 August 2026

ISO 10013:2021 provides guidance for developing and maintaining documented information that supports an effective quality management system [S13]. ISO/IEC 27001:2022 remains the information-security management reference [S15]. ISO's site shows ISO 9001:2026 under publication with an expected September 2026 publication, replacing ISO 9001:2015 after a transition period [S14]. Therefore, the product should store configurable control mappings and avoid hard-coding one edition's clause structure.

COMPLIANCE LIMIT Do not copy copyrighted ISO clause text into the product without permission. Store organization-authored procedures and licensed control references. A qualified quality/security lead should approve the final mapping and certification scope.

10. Calendar, email, and Microsoft 365 integration

Application calendar is the work calendar of record

- Month, week, agenda, and timeline views for ticket due dates, SLA breaches, sprint boundaries, releases, document reviews, approvals, audits, maintenance, and customer appointments.
- Personal, team, project, account, and shared calendars with permission-filtered overlays and saved views.
- Time zones, all-day events, recurrence, reminders, dependencies, conflict indicators, and links back to the source record.

- The source record owns its date. Editing a ticket due date updates the calendar projection instead of creating a disconnected copy.

Microsoft Entra ID and Graph

- Sign-in uses OpenID Connect/OAuth through the Microsoft identity platform; the application never handles a workforce user's Microsoft password [S7].
- Request only least-privileged Graph scopes and separate delegated user actions from background application permissions [S8].
- Directory synchronization uses Microsoft Graph user delta queries for incremental changes instead of repeatedly reading the full directory [S5–S6].
- Outbound email uses Graph sendMail or a governed shared mailbox; Mail.Send is the documented least-privileged permission for that action, and accepted requests still require delivery monitoring [S9].
- Calendar integration can create/read/update permitted calendars and events and use availability functions when needed [S10].
- Graph operations use idempotency, durable queues, correlation IDs, retry-after handling, exponential backoff, and dead-letter recovery; avoid polling when delta/change patterns exist [S11].

Integration behavior decisions

Decision	Recommended default	Reason
Directory ownership	Entra owns workforce identity; app owns business roles/scopes	Avoid duplicating credentials while preserving project-level authorization
Ticket notifications	Shared service mailbox with durable delivery log	Continuity, traceability, easier support than personal mailboxes
Inbound email	Thread by immutable message IDs plus guarded token fallback	Reduces duplicate or mis-threaded tickets
Calendar sync	One-way source dates first; selective two-way meetings later	Prevents early conflict loops and unclear ownership
Customer identity	Separate external portal identities from workforce directory	Customers may not exist in the organization's Entra tenant

11. Search, automation, notifications, and reporting

Unified search

- Permission-aware search across tickets, comments, attachment metadata/text when allowed, customers, projects, and documents.

- Filters, facets, saved searches, recent items, highlighted matches, synonyms, typo tolerance, and stable links.
- Start with PostgreSQL search if it meets measured needs; add a dedicated search service only when scale/relevance requirements justify the operational cost.

Automation engine

- Trigger → conditions → actions model with templates, dry-run/test mode, versioning, owner, scope, audit log, rate limits, recursion protection, and failure queue.
- Triggers include record creation/change, status transition, SLA threshold, date reached, inbound email, document review due, schedule, and webhook.
- Actions include assign, transition, set field, comment, notify, create/link ticket, request approval, create calendar item, call webhook, and escalate.

Notification center

Support in-app and email channels first, with per-event preferences, digesting, quiet hours, deduplication, unsubscribe rules where appropriate, delivery status, retries, and separate internal/public templates. Never include restricted ticket or document content in a notification to a recipient who cannot open the source record.

Dashboards and measures

- Operational: new/open/aged tickets, backlog by status/owner/account, SLA at risk/breached, response and resolution time, reopen rate, blocked work, throughput, and work-in-progress.
- Agile: sprint commitment/completion, velocity trend, cycle/lead time, cumulative flow, scope change, and aging work.
- Knowledge: searches with no result, article usefulness, ticket deflection proxy, stale/review-due documents, approval cycle time, acknowledgment completion.
- Customer: volume by account/service, satisfaction, escalation, repeated issues, entitlement usage, and notification delivery failures.
- Governance: access changes, privileged actions, exports, attachment scan results, integration failures, backup/restore tests, and document-control exceptions.

12. Information model and records

The logical model should be reviewed before schemas are frozen. Every business record receives a stable UUID, human-readable key where useful, organization/scope identifiers, created/updated metadata, soft-deletion or archival policy, and audit linkage.

Domain	Core entities	Key relationships
Identity/access	User identity, profile, group, role, permission, membership, service principal	Users gain scoped capabilities through roles and relationships
Customer	Account, contact, entitlement, service, satisfaction	Accounts own contacts and may access shared requests/documents
Work	Project, ticket, type, field, workflow, transition, comment, attachment, link, SLA	Ticket belongs to project and may reference account, sprint, docs, events
Agile	Board, filter, column, swimlane, backlog rank, sprint, epic, release	Views select and organize work records; do not duplicate them
Documentation	Space, page/document, version, review, approval, acknowledgment, template	A version is immutable after approval; links connect evidence to work
Calendar/comms	Calendar, event projection, notification, message, delivery attempt	Events/messages retain source and external correlation IDs
Platform	Automation rule/run, webhook, audit event, saved query, dashboard, integration	All privileged/configuration activity is attributable

Data rules that prevent expensive rework

- Do not use email address as a permanent person ID; emails change and one person may have multiple identities.
- Do not store file bytes in the main relational database by default; store protected object references and integrity metadata.
- Make comments explicitly public or internal; never infer visibility from author type alone.
- Version configuration that changes historical meaning—workflows, SLAs, forms, document templates, and automation.
- Use immutable event/audit records for security-relevant history; business history and technical logs have different retention/access needs.
- Design export, retention, deletion, anonymization, and legal-hold behaviors before production data arrives.

13. Recommended technical architecture

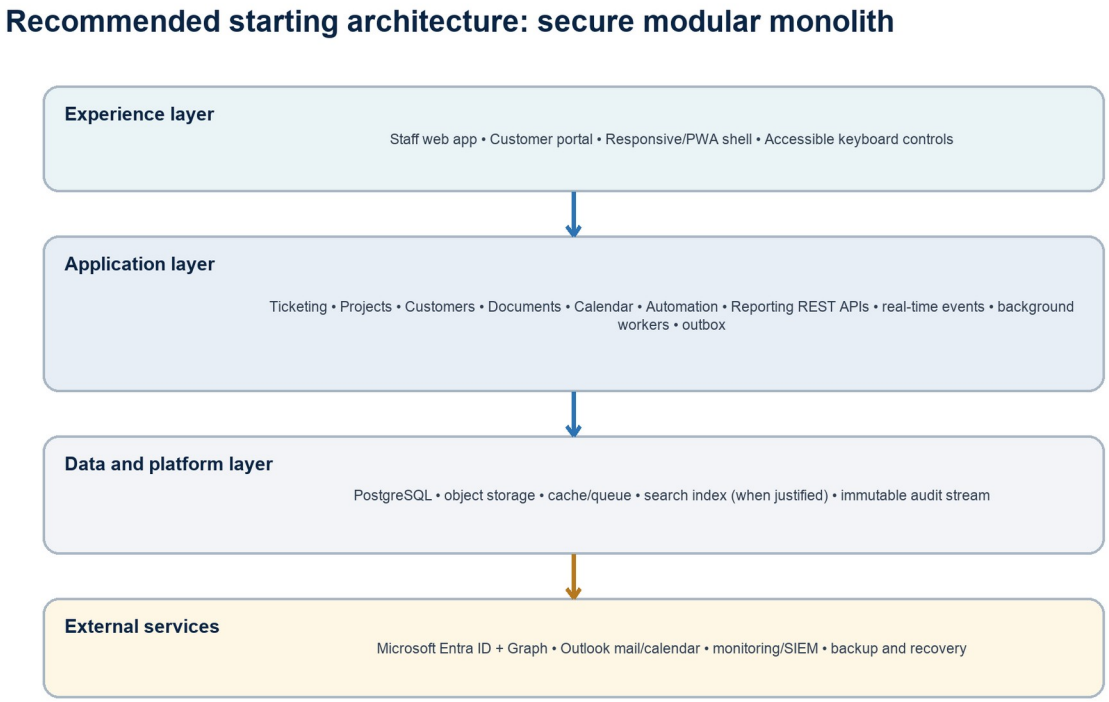

Figure 2. Begin with a secure modular monolith and split services only where evidence requires it.

Recommended baseline—subject to Phase 1 architecture decision records

- Web: React and TypeScript, server-backed routing, a documented component library, semantic HTML, design tokens/CSS custom properties, and automated accessibility checks.
- API/application: ASP.NET Core on the current organization-approved .NET LTS release, organized into strict domain modules; Microsoft Graph SDK used behind an integration adapter.
- Data: PostgreSQL with migration discipline; tenant/scope filters enforced centrally; Redis-compatible cache/queue only for measured needs.
- Files: Azure Blob or S3-compatible object storage, private by default, short-lived signed access, checksums, quarantine, malware scanning, and lifecycle policies.
- Asynchronous work: durable background worker, transactional outbox, idempotent handlers, retry/dead-letter queues, and observable correlation IDs.
- Delivery: containerized environments, infrastructure as code, automated build/test/security gates, separate development/test/staging/production, and controlled database migrations.

- Hosting: Azure is the leading option because of Microsoft identity/Graph and enterprise controls, but cost, residency, skills, and portability must be decided in Phase 1.

Why a modular monolith first

Ticket, workflow, permission, document, and notification operations are highly transactional. A modular monolith reduces distributed failure modes and deployment overhead while the domain is still changing. Clear module boundaries, outbox events, and integration adapters preserve a path to extract high-scale services later. Microservices are a scaling option, not a starting requirement.

14. UX, visual design, and CSS system

Experience map

- Global shell: organization/project switcher, create action, permission-aware search, notifications, help, profile, and admin entry.
- Work views: list, board, backlog, timeline/calendar, queue, dashboard, and record detail with a consistent side panel or full-page editor.
- Customer portal: catalog/request creation, own/shared requests, approvals, knowledge, account members, and profile/preferences.
- Documentation: space tree, search, editor, version/approval panel, related work, review queue, and read-optimized published page.
- Administration: templates, types, fields, workflows, forms, SLAs, permissions, automation, integrations, retention, and audit.

CSS and component discipline

- Use a small design-token system for color, typography, spacing, radius, elevation, motion, and density; expose light/dark/high-contrast themes only after the base theme is stable.
- Build reusable components for status, priority, person, account, date/SLA, attachment, comment, editable field, card, empty/error/loading state, dialog, table, and form control.
- Keep board cards compact but never hide ownership, priority, status, SLA risk, and accessibility names behind color or hover alone.
- Define responsive behavior deliberately: boards may scroll by lane; record pages reflow; dense tables offer column selection; portals prioritize mobile request creation and status.
- Create Storybook-style component documentation and visual regression tests so “pretty” remains consistent rather than becoming scattered one-off CSS.

Prototype before polish

Prototype and test five critical journeys first: create a request, triage/assign, move work on a board without a mouse, approve/publish a controlled document, and find a deadline on the calendar. Visual polish follows validated structure, labels, permissions, and error handling.

15. Security, privacy, and compliance engineering

Security baseline

- Threat-model cross-account access, customer sharing, privileged administration, workflow/automation abuse, inbound email, rich text, file uploads, exports, and Graph permissions before implementation.
- Use Entra SSO/MFA/Conditional Access for workforce users; support secure external identity flows; no shared accounts; tightly controlled break-glass access.
- Enforce authorization server-side on every object and action; test horizontal and vertical privilege escalation, including search and exports.
- Encrypt data in transit and at rest; place secrets/keys in managed secret storage; rotate credentials; use managed identities where supported.
- Protect rich text against stored cross-site scripting; validate all inputs; apply CSRF/session/cookie controls; rate-limit risky endpoints.
- Follow NIST SSDF practices throughout the lifecycle and use a defined web-application verification baseline such as OWASP ASVS [S20].

Attachment controls

- Allowlist business-required extensions; validate file signature/type instead of trusting the browser Content-Type header; limit size and count.
- Generate storage names; retain the user-facing original name as metadata; store outside the web root/private container.
- Quarantine, malware scan, optionally apply content disarm/reconstruction, and block download until the result is safe or an authorized exception exists.
- Use short-lived authorized download links, anti-enumeration IDs, checksums, content disposition, retention rules, and scan/delete audit events [S18].

Logging and audit

Maintain application audit events for business accountability and separate operational/security logs for detection and diagnosis. Log authentication and authorization failures, privileged actions,

permission/configuration changes, exports, file-upload scan results, integration failures, and automation outcomes without placing secrets or unnecessary personal content in logs [S19].

Privacy and records governance

- Inventory personal/sensitive data and purpose; minimize collection; define retention by record type; document deletion/anonymization and legal-hold exceptions.
- Provide account-scoped export and data-subject workflows where jurisdiction/policy requires them; protect exports with the same authorization as the source.
- Define data residency, subprocessors, telemetry content, backup retention, recovery, breach response, and customer contract requirements before launch.

16. Quality strategy and definition of done

Test layers

Layer	What must be proven	Automation expectation
Unit/domain	Workflow, permissions, SLA clocks, ranking, document state, recurrence, automation conditions	High coverage of business invariants
API/integration	Database, object store, queue/outbox, Entra/Graph adapters, email/calendar failure behavior	Repeatable isolated tests plus contract tests
End-to-end	Critical staff/customer journeys and cross-module links	Small stable suite on every release candidate
Security	Threat cases, authorization, dependency/container scans, secrets, file/rich-text handling	CI gates plus expert manual testing
Accessibility	Keyboard, screen reader, zoom/reflow, contrast, dragging alternative, error recovery	Automated checks plus manual assistive-tech testing
Performance/ resilience	Search, board load/move, queues, large accounts, attachments, background jobs, Graph throttling	Defined load profiles and fault injection
Recovery/ operations	Backup restore, rollback, migrations, monitoring, alerts, runbooks, audit export	Scheduled drills with evidence

Feature-level definition of done

- Acceptance criteria met; error and empty states designed; server-side authorization verified; audit requirements implemented.
- Unit/integration tests pass; required end-to-end test added; accessibility and responsive checks pass.
- Telemetry, alerting, retry/dead-letter behavior, runbook, configuration and migration/rollback are ready.
- User documentation and admin documentation updated; release note and security/privacy review complete.
- Product owner accepts the demonstrated behavior in the staging environment.

17. Delivery model, governance, and team

Working model

Use two-week delivery increments inside sequential phases. “One phase at a time” means the next phase does not become the primary commitment until the current exit gate is met. Small discovery spikes may run ahead only when explicitly approved and time-boxed.

Core team for the baseline schedule

- Product owner (decisions and backlog), project/delivery lead, UX/product designer, technical lead/architect, two to four full-stack engineers, QA/automation engineer, and part-time security/platform support.
- Named business partners: service/support owner, quality/document-control owner, Microsoft 365/Entra administrator, privacy/legal contact, and pilot customer/internal users.
- If the team is materially smaller, preserve the phase order and reduce scope; do not hide schedule risk by skipping security, accessibility, testing, migration, or adoption work.

Decision governance

- Product decisions: product owner, informed by users and sponsor.
- Architecture decisions: technical lead with security/platform review, recorded as Architecture Decision Records (ADRs).
- Quality/ISO control decisions: designated quality/security owners using licensed standards and organization policy.
- Go/no-go: sponsor and product owner, with explicit security, operations, data migration, and pilot evidence.

MEETING CADENCE Weekly product/technical review; end-of-increment demonstration; phase-gate review; monthly risk/security review; short decision log kept continuously. Avoid status meetings that do not produce decisions or remove blockers.

18. Step-by-step implementation roadmap

Baseline assumes a focused 4–6 person delivery team and mostly sequential phases. Estimated elapsed time is approximately 29–36 weeks for Version 1; an internal pilot can begin earlier after the core vertical slice is safe and usable. Dates become commitments only after Phase 1 sizing.

Phase	Indicative time	Primary gate
0. Confirm direction	1 week	Sponsor approves charter inputs and decision owners
1. Discovery and architecture	2 weeks	Product charter, process maps, risks, ADRs approved
2. Secure foundation	2–3 weeks	SSO, CI/CD, environments, audit skeleton demonstrated
3. Core ticketing vertical slice	4–5 weeks	Request-to-resolution journey accepted
4. Customers and service desk	3–4 weeks	Portal/queues/SLA pilot accepted
5. Agile boards and planning	3–4 weeks	Accessible Kanban/Scrum workflows accepted
6. Wiki and documentation	4–5 weeks	Application wiki and controlled-document flows accepted
7. Calendar and Microsoft 365	3–4 weeks	Graph permissions, reliability, and user journeys accepted
8. Automation/search/reporting	3–4 weeks	Operational dashboards and rule safety accepted
9. Hardening and pilot	3–4 weeks	Go-live readiness and pilot exit criteria met
10. Launch and optimize	2 weeks + ongoing	Stable rollout, support handoff, measured backlog

Phase 0 — Confirm direction and constraints

- Name sponsor, product owner, quality owner, technical lead, Microsoft 365 administrator, and pilot group.
- Decide initial deployment model, target users, data sensitivity, budget range, and whether ISO certification is an objective or only alignment.
- Confirm that this plan is the governing outline and open a decision/risk log.

Exit gate: Approved kickoff brief; known decision owners; no unresolved blocker to discovery.

Phase 1 — Discovery, process design, and architecture

- Interview staff, administrators, document owners, and representative customers; map current request/document/calendar journeys.
- Inventory data, integrations, migration sources, identity domains, workflows, SLAs, reports, and compliance obligations.
- Prototype five critical journeys; define MVP/V1 backlog, non-functional requirements, data model, threat model, and architecture decisions.
- Set measurable acceptance criteria and re-estimate the roadmap.

Exit gate: Signed product charter, service blueprint, prioritized backlog, initial UX, threat model, data/integration plan, ADRs, and release plan.

Phase 2 — Secure platform foundation

- Create repositories, environments, infrastructure as code, CI/CD, coding standards, dependency/security scanning, observability, and feature flags.
- Implement Entra sign-in spike, user/profile model, RBAC scopes, audit event framework, database migrations, API conventions, and design-system foundations.
- Prove deployment, rollback, backup/restore path, secrets management, and a first monitored background job.

Exit gate: A thin authenticated application deploys safely to staging; authorization/audit patterns are testable and reviewed.

Phase 3 — Core ticketing vertical slice

- Implement projects, ticket types/fields, create/edit/view, workflow transitions, assignment, comments, activity, links, notifications, basic search, and secure attachments.
- Add list/queue view, filters, bulk-safe operations, audit history, and admin templates for one pilot project.
- Test the complete request-to-resolution journey including failures and recovery.

Exit gate: Pilot team accepts real internal tickets through the complete workflow; security/accessibility/performance baseline passes.

Phase 4 — Customers and service desk

- Add customer accounts, contacts, external identities/invitations, portal, request types/forms, public/internal comments, sharing rules, queues, and SLA engine.
- Add governed inbound email, threading, attachment handling, message logs, failure recovery, and customer notification templates.
- Pilot with selected internal service customers before external exposure.

Exit gate: No cross-account leakage; portal and email journeys succeed; SLA clocks and notification evidence are accepted.

Phase 5 — Agile boards and planning

- Add rank/backlog, board filters, columns/status mapping, cards, swimlanes, WIP, quick filters, keyboard move, and optimistic conflict handling.

- Add optional sprints, sprint goal, estimates, start/complete controls, epics/releases, and initial flow/sprint reporting.
- Load-test representative boards and manually test keyboard/screen-reader interaction.

Exit gate: Teams can plan and move real work quickly with and without dragging; board data remains consistent with ticket workflow.

Phase 6 — Wiki, documentation, and knowledge

- Implement spaces, nested page tree, editor, application-space templates, permissions, search, attachments, backlinks, watchers/comments, ticket links, versions, comparison, restore, archive, and publishing.
- Add application documentation patterns for ownership, architecture, setup, environments, dependencies, ADRs, release notes, runbooks, known issues, and postmortems.
- Add controlled types, review/approval, effective/superseded states, review schedule, acknowledgment/evidence as prioritized, export labeling, and audit.
- Validate collaborative-wiki behavior with application teams and controlled lifecycle/metadata with the quality/document-control owner using licensed requirements.

Exit gate: Application teams and quality owners accept the wiki, ordinary-article, and controlled-document workflows; historical versions are defensible.

Phase 7 — Calendar, notifications, and Microsoft 365

- Build application calendar projections and views, reminders, recurrence/time zones, record links, and permissions.
- Complete directory delta sync, shared-mailbox delivery, calendar integration, consent/admin setup, retry/throttling, dead-letter recovery, and monitoring.
- Begin with one-way source-of-truth rules; enable selective two-way meeting behavior only after conflict tests.

Exit gate: Microsoft 365 administrator approves permissions; integration reliability and calendar ownership rules pass user acceptance.

Phase 8 — Automation, search, dashboards, and APIs

- Deliver safe trigger/condition/action rules, test mode, versioning, limits, audit, and failure recovery.
- Improve permission-aware search and add saved queries, dashboards, scheduled reports/exports, API/webhook documentation, and admin health views.
- Tune against measured relevance/performance and operational workflows.

Exit gate: Managers and operators can see service health; automation failures are visible/recoverable; export/API access is secure.

Phase 9 — Hardening, migration, training, and pilot

- Run security review/penetration testing, accessibility audit, load/resilience tests, backup restore, disaster-recovery exercise, privacy review, and operational rehearsal.
- Clean/migrate pilot data with dry runs and reconciliation; prepare training, support model, runbooks, admin guides, release notes, and rollback plan.
- Operate a time-boxed pilot, measure adoption/quality, triage defects, and hold a formal go/no-go.

Exit gate: Critical defects closed; pilot metrics and user sign-off meet thresholds; operations, security, data, and sponsor approve launch.

Phase 10 — Staged launch and optimization

- Roll out by team/customer cohort, monitor service and delivery logs, hold daily launch triage, and keep rollback available.
- Measure goals, fix usability/reliability issues, archive launch decisions, and prioritize Version 1.x from evidence.
- Establish quarterly access, retention, document-review, dependency, recovery, and roadmap reviews.

Exit gate: Stable adoption and support handoff; documented post-launch review; funded, evidence-based next backlog.

18A. Commercial Version 1.0 release baseline

Task 34 converts the remaining commercial work into a controlled Version 1.0 baseline. The intended first product is a hosted business-to-business service for Microsoft 365-oriented organizations. The current application remains suitable for demonstrations, but unrestricted production sale requires the evidence gates below and final pilot approval.

TASK 34 SCOPE DECISION Internal workforce members are licensed seats; external customer contacts and email-only requesters are treated separately. Exact prices and plan limits are decided in Task 43 after hosting and support costs are measured. Only Gate G0 passes in Task 34.

Commercial sequence: Tasks 34–50

These seventeen increments lead to the sale-ready milestone. Each advances one or more mandatory gates; none may silently weaken organization isolation, auditability, privacy, or recoverability.

TASK	COMMERCIAL INCREMENT	GATES
34	Version 1.0 requirements and release gates	G0
35	Organization provisioning and tenant isolation	G1, G2
36	Customer identities and self-service portal	G1, G2, G5
37	Customer-visible replies and private internal notes	G2, G5, G8
38	Outlook email-to-ticket processing	G2, G3, G5, G6
39	Production Microsoft 365 integration	G3, G6
40	Customer SLA contracts, holidays, and reopen handling	G2, G5
41	SLA reminders, on-call ownership, and escalation	G2, G6
42	Production attachment storage and malware protection	G4, G5, G6
43	Plans, subscriptions, licensing, and billing boundary	G1, G5, G9
44	Production hosting and deployment pipeline	G5, G6
45	Monitoring, backup, restore, and disaster recovery	G6
46	Security, privacy, and compliance hardening	G1, G3–G5
47	Performance, accessibility, and compatibility certification	G7, G8
48	Product administration and customer-support operations	G6, G9
49	Commercial onboarding, guidance, and product polish	G2, G8, G9
50	Controlled pilot, release certification, and Version 1.0	G1–G10

Mandatory evidence gates

A partial foundation is not a commercial approval. A gate passes only when its required result is demonstrated and its minimum evidence is retained for the go/no-go review.

GATE	SALE-READY RESULT	TASK 49 STATE
G0 — Scope and change control	Published boundary, environments, assumptions, owners, evidence rules, and controlled change process.	**Partial — governed tenant/privacy boundary**
G1 — Tenant isolation	No interactive or background path can expose one organization's records to another.	**Partial — customer path**
G2 — Product journeys	Workforce, customer, manager, documentation, calendar, reporting, and administration journeys pass.	**Partial — guided acceptance and pilot evidence path**
G3 — Microsoft 365	Entra, directory, Outlook mail, inbound email, and approved calendar behavior are safe and recoverable.	**Partial — production Graph controls**
G4 — Attachments	Files use protected storage, malware scanning, quarantine, retention, backup, and reconciliation.	**Partial — key and provider evidence open**
G5 — Security and privacy	Threat, vulnerability, abuse, encryption, logging, retention, export, and deletion controls pass review.	**Partial — external assurance required**
G6 — Reliability and recovery	Deployment, rollback, monitoring, queues, backup, restore, disaster recovery, and runbooks are proven.	**Partial — support diagnostics and communication**
G7 — Performance and scale	Representative data and job volumes meet approved response and processing objectives.	**Partial — local engineering baseline**
G8 — Accessibility and compatibility	Required journeys meet the WCAG 2.2 AA target across the supported browser matrix.	**Partial — role guidance; human review remains**
G9 — Commercial and support	Plans, subscriptions, legal documents, onboarding, support, and customer communications are ready.	**Partial — onboarding and handoff implemented**
G10 — Pilot and go/no-go	A controlled pilot passes and authorized product, security, operations, and commercial owners approve launch.	**Not started**

Sale-ready acceptance boundary

- A new customer organization can be provisioned, authenticated, administered, suspended, and isolated from every other organization.
- An external requester can safely submit and follow a request through the portal or approved Outlook email without seeing internal notes or another customer's work.
- Agents and managers can complete ticketing, workflow, timing, team, Agile, SLA, documentation, calendar, reporting, and audit journeys under server-enforced permissions.
- Microsoft 365, notifications, background processing, storage, and reports succeed or fail visibly, retry safely, and preserve attributable evidence.
- Operators can deploy, roll back, monitor, restore, and recover the service, while support and commercial owners can onboard and support a paying customer.

- The pilot closes critical defects and obtains explicit product, security, operations, commercial, Microsoft 365, and sponsor approval before Version 1.0 is offered for sale.

Deferred beyond Version 1.0

Separate future companion applications

The Miro-style whiteboard and Slido-style live-engagement ideas are now separate future applications, not modules or Tasks 51–60 inside this ticketing product. Their planning remains available independently and does not expand or delay Tasks 49–50.

Post-launch options remain: native/offline apps, AI, CMDB, marketplace extensions, advanced portfolios, sales CRM, and multi-region hosting.

18B. Task 35 — organization provisioning and tenant isolation

Task 35 delivers the first commercial multi-organization boundary. A protected control plane can create an isolated organization, bind one Microsoft tenant, establish its owner, create its initial project and default workflow, and later suspend or reactivate access without changing tenant identity.

SECURITY RESULT Microsoft Entra requests now reject browser-supplied organization or acting-person identifiers that do not match the authenticated membership. Workspace discovery also resolves only that organization.

What changed

- Provisioning is disabled by default and requires a separate operator key of at least 32 characters supplied outside source control.
- Provisioning is atomic and creates the organization, unique Microsoft tenant binding, owner, initial project, nine default workflow lanes, audit evidence, and outbox event.
- Active organizations resolve Microsoft memberships; suspension blocks interactive membership resolution. Status changes use optimistic revisions and are auditable.
- A shared API guard checks route, query, JSON, and form inputs before endpoint execution, then rewinds request bodies for normal model binding.
- The original workspace lookup no longer returns the first active organization to a signed-in user; it uses the authenticated organization identifier.

Evidence and gate position

The API baseline is now 109 passing tests, including negative tenant and actor substitution tests and a complete provision/read/suspend/stale-revision/reactivate journey. The web baseline remains 20 passing tests.

CONTROL	RETAINED EVIDENCE	TASK 35 RESULT
Provisioning boundary	Separate 32+ character control-plane key; surface disabled by default	**Implemented**
Organization lifecycle	Unique key and Microsoft tenant; audited provision, suspend, and reactivate	**Implemented**
Interactive isolation	Negative query/body tests for substituted organization and acting person	**Implemented**
Complete G1 gate	Storage, integrations, jobs, exports, recovery, and controlled-pilot isolation	**Still partial**

Task 36 entry point

Task 36 adds external customer identities and a self-service portal on top of this organization boundary. It must never reuse workforce permissions and must retain negative evidence for customer-to-customer, account-to-account, and organization-to-organization access attempts.

18C. Task 36 — customer identities and self-service portal

Task 36 gives external contacts a separate identity and product experience. Authorized staff link an exact identity-provider issuer and subject to one active customer contact; the customer can then create requests and follow only the work reported through that verified contact.

SECURITY RESULT Portal requests do not accept organization, customer-account, reporter, or acting-person identifiers. The server derives those values from the authenticated customer identity and returns not found for every record outside the exact organization, account, and reporter scope.

What changed

- A dedicated customer authentication policy supports explicit local development identities or a separately configured HTTPS external identity authority and audience.
- One persisted portal identity binds issuer and subject to one customer contact; enable, suspend, and reactivate actions require customer-administration permission and optimistic revisions.
- The new customer portal has its own sign-in, personal request summary, request form, and request history instead of exposing or filtering the staff workspace.
- Allowed destinations are active shared-service projects or active projects assigned to the authenticated customer account; request numbering and the starting lane are selected transactionally.
- Portal creation and identity lifecycle changes produce attributable audit and outbox evidence while the last successful customer sign-in is retained.

Evidence and gate position

The API baseline is now 116 passing tests, including seven focused customer-portal authentication, lifecycle, create/read, cross-account, cross-organization, foreign-ID, and suspension tests. The web baseline is 21 passing tests, including the customer sign-in and personal-request journey.

CONTROL	RETAINED EVIDENCE	TASK 36 RESULT
Identity separation	Dedicated external scheme and issuer/subject record; no workforce role reuse	**Implemented**
Portal request scope	Exact organization, customer account, and reporter predicates on every read	**Implemented**
Access lifecycle	Permission-checked enable, suspend, reactivate, revision, audit, and outbox evidence	**Implemented**
Complete G1/G2/G5	Replies, abuse controls, privacy, production identity, storage, operations, and pilot	**Still partial**

Task 37 entry point

Task 37 adds customer-visible replies, request participants, and private internal notes. The implementation must preserve the Task 36 identity scope while proving that an external customer can never read an internal note.

18D. Task 37 — customer conversations and request participants

Task 37 separates private service-team context from the customer conversation. Staff explicitly choose an internal note or public reply; verified contacts see public messages only when they reported the request or were named as a participant from the same customer account.

PRIVACY RESULT Internal is the required safe default for new and historical comments. Customer portal queries filter by active CustomerVisible messages before serialization, so a private note is never sent to the browser.

What changed

- Every ticket message stores immutable visibility: Internal or CustomerVisible. Editing text cannot change its audience.
- Staff activity labels each message, explains the audience, and defaults the composer to an internal note.
- Portal request detail shows public replies, accepts customer public replies, and states that private notes never appear.
- Reporter access is permanent; authorized staff can add or remove active contacts from the exact customer account as participants.
- Public replies and participant changes retain content hashes, audit records, subject-issue links, and transactional outbox evidence.
- SLA first response now requires an active, customer-visible team-member reply; an internal note cannot satisfy the promise.

Evidence and gate position

The verified baseline is 120 passing API tests and 21 passing web tests. New evidence covers the safe internal default, explicit public replies, internal-note non-disclosure, same-account participant access, unshared-contact denial, removal revocation, cross-account rejection, and accessible staff/customer conversation controls.

CONTROL	RETAINED EVIDENCE	TASK 37 RESULT
Safe message default	Required visibility field; historical and omitted values migrate as Internal	**Implemented**
Portal non-disclosure	Persistence query returns active CustomerVisible replies only	**Implemented**
Participant scope	Reporter plus explicit same-account contacts; add/remove audit and negative tests	**Implemented**
Complete G2/G5/G8	E2E, privacy/retention, abuse, accessibility certification, and pilot evidence	**Still partial**

Task 38 entry point

Task 38 adds governed Outlook email-to-ticket processing. It must resolve the correct organization, customer, request, and public/private behavior; deduplicate Graph deliveries; reject unsafe senders and attachments; and make retry or dead-letter failures visible to operators.

18E. Task 38 — governed Outlook email-to-ticket processing

Task 38 turns approved customer email into governed work. Each workspace binds one normalized Outlook mailbox to one non-archived project; exact customer identities can create account-scoped service requests or add public replies, while duplicates and unsafe mail stop before they can change a ticket.

INBOX SAFETY RESULT Email can never create an internal note. Unknown senders, unauthorized ticket references, automatic messages, and attachments are rejected with operator-visible evidence. Attachments remain blocked until Task 42 supplies protected storage, malware scanning, and quarantine.

What changed

- A persisted mailbox route has unique organization and normalized-mailbox boundaries, a non-archived project destination, delta continuation, health, errors, and optimistic concurrency.
- Microsoft Graph requests Mail.Read, plain-text bodies, immutable message IDs, and bounded Inbox delta pages; mailbox plus Graph message ID is a database-level idempotency key.
- New mail resolves an exact active customer contact and account before creating a service request in an allowed shared or account-scoped project.
- Replies resolve through a strict [PROJECT-NUMBER] token or an already accepted conversation in the same mailbox, then require reporter or explicit-participant access.
- Accepted replies are always CustomerVisible and carry issue-linked audit, content-hash, and transactional outbox evidence.
- Failures use exponential retry and dead-letter after three attempts; the administration view exposes route state, intake decisions, ticket links, reasons, and revision-safe retry.
- Development simulation demonstrates a new ticket, public reply, unknown sender, unsafe attachment, and duplicate no-op without reading or changing Microsoft 365.

Evidence and gate position

The verified baseline is 123 passing API tests and 22 passing web tests. Evidence covers mailbox-route validation, processed and rejected outcomes, immutable-ID duplicate no-op behavior, retry backoff, dead-letter transition, persistence constraints, the operator intake view, and a clean production web build.

CONTROL	RETAINED EVIDENCE	TASK 38 RESULT
Mailbox route	Unique workspace and normalized mailbox; non-archived destination project; integrations.manage	**Implemented**
Safe resolution	Exact active contact/account plus strict ticket token or accepted mailbox conversation	**Implemented**
Duplicate protection	Unique mailbox + immutable Graph message ID; stored delta continuation	**Implemented**
Unsafe mail	Automatic, unknown, unauthorized, malformed, and attachment messages stop with a safe reason	**Implemented**
Recovery	Exponential retry, three-attempt dead letter, revision-safe operator retry, health view	**Implemented**
Complete G2/G3/G5/G6	Production consent, callbacks, background work, privacy, storage, recovery, E2E, and pilot	**Still partial**

Microsoft design references retained in the architecture record: Outlook immutable identifiers, message delta queries, the Graph message resource, Outlook change notifications, and the Microsoft Graph permissions reference.

Task 39 entry point

Task 39 activates the production Microsoft 365 connection: customer-specific Entra consent, restricted mailbox access, webhook or scheduled-delta execution, callback validation, subscription renewal and missed-event recovery, durable background processing, monitoring, alerting, and operator runbooks.

18F. Tasks 39–45 — production operations and recovery

Tasks 39 through 45 convert the product foundation into an operable release package. Production Microsoft 365, customer SLA contracts, escalation routing, protected attachments, licensing, deployment, and disaster recovery now share explicit fail-safe configuration and retained operating evidence.

TASK 45 RECOVERY RESULT The disposable production stack completed a matched database-and-attachment backup, destructive restore, marker removal proof, migrations, and readiness recovery in 11 seconds against the 7,200-second target. Hosted off-site replication and pilot evidence remain mandatory before sale.

Completed production increments

TASK	PRODUCTION INCREMENT	RESULT
39	Production Microsoft 365 consent, callbacks, subscriptions, recovery, and health	Complete
40	Customer SLA contracts, holiday calendars, immutable cycles, and governed reopen	Complete
41	On-call schedules, substitutes, proactive reminders, and multi-level escalation	Complete
42	Production attachment storage, ClamAV quarantine, and Outlook attachment scanning	Complete
43	Manual trials, subscriptions, customer-managed licensing, and internal seat limits	Complete
44	Production containers, file-mounted secrets, migration-gated deployment, and rollback	Complete
45	Monitoring, durable-queue alerting, complete backup, guarded restore, and recovery proof	Complete

Reliability controls now available

- Readiness checks PostgreSQL, private attachment read/write access, and a live malware-scanner probe.
- A separately keyed operations endpoint reports stale or exhausted outbox, failed email, and Microsoft 365 dead-letter evidence without exposing tenant records.
- The one-minute monitor records health locally and can notify an approved HTTPS webhook only when state changes.
- Six-hour application-consistent backups bind the database, attachments, deployment evidence, release, region, UTC time, and SHA-256 integrity manifest.
- Guarded restore requires an exact destructive-action confirmation, verifies every payload, makes a safety backup by default, restores both data stores, migrates, and waits for readiness.
- A controlled drill proves post-backup database and file markers disappear and records actual recovery time against the two-hour RTO.

Verification and remaining gates

Build 0.45.0 has 145 passing API/domain/model tests, 24 passing web tests, clean TypeScript and production builds, verified deployment/recovery assets, no pending Entity Framework model changes, healthy protected operational checks, and the timed recovery drill. Gates G4 and G6 remain Partial until the real host proves encrypted off-host replication, approved retention, paging ownership, incident communications, and pilot recovery.

Task 46 entry point

Task 46 performs security, privacy, and compliance hardening: threat and abuse review, vulnerability evidence, encryption/key ownership, retention and deletion approval, privacy operations, and final attachment/security controls.

18G. Task 46 — security, privacy, and compliance hardening

Task 46 gives every organization an actionable Trust & privacy workspace while strengthening the public and production boundaries. The application records approvals, requests, decisions, audit history, and open evidence without making unsupported claims of legal certification or independent penetration testing.

TASK 46 SECURITY RESULT Build 0.46.0 adds governed retention and privacy operations, abuse throttling, persistent production key protection, stricter response controls, repeatable vulnerability checks, and retained incident/remediation evidence. External penetration, legal/privacy, hosting-provider, accessibility, and pilot approvals remain sale gates.

Control posture

CONTROL	TASK 46 RESULT	STATE
Retention governance	Revision-safe policy with named approval, legal-hold reference, and deletion method	**Implemented**
Privacy operations	Access, correction, deletion, and restriction register with verification and decisions	**Implemented**
Abuse protection	Partitioned limits for customer portal and Microsoft Graph webhook entry points	**Implemented**
Encryption ownership	Production-required key owner, evidence references, and persistent data-protection keys	**Evidence open**
Security review	Secret signatures, transitive .NET vulnerabilities, npm audit, and deployment assets	**Passed**
External assurance	Independent penetration test plus privacy/legal and hosting-provider review	**Required**

What administrators can do

- Set and revise retention periods for work items, attachments, audit evidence, exports, integration logs, and backups.
- Record a legal-hold process and secure-deletion method, then explicitly approve the complete policy with a named note.
- Register privacy requests with a due date and accountable assignee while keeping intake notes intentionally minimal.
- Require identity verification before approval or completion and retain the final decision without silently reopening terminal requests.
- Review implemented, configuration-required, externally evidenced, and open security controls from one visible workspace.

Verification and remaining gates

Build 0.46.0 has 147 passing API/domain/model tests, 25 passing web tests, clean TypeScript and production web builds, no reported vulnerable .NET or npm dependencies, verified production-security assets, and no pending Entity Framework model changes. Gates G1, G3, G4, and G5 remain Partial until independent and hosted evidence is approved.

Task 47 entry point

Task 47 validates performance, scale, and resilience with representative data, concurrent-user targets, background-job pressure, recovery behavior, measurable thresholds, and a retained remediation record.

18H. Task 47 — performance, accessibility, and compatibility

Task 47 turns quality expectations into measurable engineering controls. It records response targets, recent application timing, route-level web delivery, automated accessibility results, and the human/hosted evidence that must still be completed before the commercial gates can pass.

TASK 47 ENGINEERING RESULT All 900 bounded local requests succeeded; the slowest route p95 was 146.332 ms against 500 ms. Initial JavaScript fell to 126.87 kB gzip, the largest route is 22.52 kB gzip, and 148 API plus 27 web tests pass. G7 and G8 remain Partial pending production-sized load and named browser/assistive-technology review.

Measured evidence

EVIDENCE	TASK 47 RESULT	STATE
API timing	Bounded route patterns, status classes, percentiles, Server-Timing	**Implemented**
Local profile	900/900 successful; worst route p95 146.332 ms vs 500 ms	**Passed**
Web delivery	126.87 kB initial gzip; largest route 22.52 kB gzip	**Passed**
Accessibility	27 web tests including axe-core representative journeys	**Passed**
Compatibility	Current/previous Edge, Chrome, Firefox, Safari matrix	**Human review**
Hosted scale	Representative dataset, workers, files, reports, Graph traffic	**Required**

Controls now available

- The Quality workspace shows approved p95 objectives, a bounded live request window, slow-route summaries, and honest gate status.
- Route patterns are measured without query strings, tenant identifiers, or request/response payloads.
- Major workspaces load as separate JavaScript chunks, and the production budget fails when initial or route assets exceed the approved limits.
- Representative Overview and Quality journeys run through axe-core; source checks protect language, skip links, navigation labels, tab order, and image alternatives.
- The published hosted profile defines organizations, users, tickets, comments, documents, reports, integrations, background work, and named capacity assumptions.

Certification boundary and ongoing evidence

A local laptop result and automated accessibility tool are engineering evidence, not commercial capacity or WCAG certification. The named Task 47 hosted and human evidence remains open through the commercial pilot.

18I. Task 48 — product administration and support operations

Task 48 gives workspace Owners and Administrators a safe product-support operating surface. It separates platform cases from customer tickets, presents non-sensitive tenant diagnostics, controls service communications, and makes temporary support authorization explicit, narrow, expiring, revocable, and attributable.

TASK 49 ENGINEERING RESULT Build 0.49.0 passes 152 backend and 29 web tests with clean builds, an applied migration, and no database-model drift. The Launch Center and handoff guides are ready for review; the controlled pilot, hosted evidence, contracts, named coverage, customer acceptance, and final approval remain Task 50.

CONTROL	TASK 48 RESULT	BOUNDARY
Diagnostics	Subscription/seats, support queue, durable jobs, delivery failures, diagnostic reference	No secrets, payloads, ticket text, or attachments
Product cases	Severity targets, lifecycle, owner, required update notes, append-only history	Separate from customer work tickets
Service notices	Draft, publish, resolve/cancel transitions with evidence	No accidental publication
Support access	Named operator, narrow scope, reason, 15-minute to 7-day expiry, revocation	Authorization record—not a credential or impersonation
Security	Tenant scope, support.manage permission, optimistic concurrency, audit and outbox	Owners and Administrators only

Release boundary and next task

G9 advances with an implemented onboarding and handoff mechanism. Task 49 is complete; Task 50 remains the controlled pilot and final Version 1.0 go/no-go. Named support coverage, approved contracts, hosted operational evidence, customer acceptance, and final authorization are still required.

18J. Task 49 — commercial onboarding, guidance, and product polish

Task 49 gives every internal user a guided first-day path and gives Owners and Administrators an accountable launch record. The workspace stores the pilot name, implementation owner, customer-safe support contact, and target date. Eight fixed readiness areas cover ownership, people and teams, customer experience, workflow and service promises, knowledge and controlled documents, Microsoft 365, security and operations, and training/handoff.

Evidence, guidance, and release boundary

Completed items require evidence, blocked items require a reason, and every change is tenant-scoped, revision-protected, audited, and emitted through the transactional outbox. Role guides and printable administrator/customer handoff material are included. Build 0.49.0 passes 152 backend and 29 web tests; migration, model-drift, build, and live-browser checks pass. G2, G8, and G9 remain Partial pending Task 50 pilot evidence.

19. MVP acceptance criteria

The MVP is acceptable only when a real pilot team can safely complete the following outcomes in staging and then production-like pilot conditions.

- A workforce user signs in through Entra; roles/scopes block unauthorized projects and customer accounts.
- An authorized user creates a project and ticket using an approved type/form; required fields and workflow rules behave correctly.
- An agent triages, assigns, comments internally/publicly, attaches a safely scanned file, links related work, and resolves the ticket.
- A customer or restricted pilot user sees only permitted requests and knowledge and receives correct, non-leaking notifications.
- A board shows the same ticket state as the record page; moving it by drag, keyboard, or menu applies the same validated transition.
- Search never returns unauthorized content; audit history identifies material changes and privileged actions.
- A knowledge page can be authored, versioned, linked to a ticket, searched, published, and clearly distinguished from a controlled document.
- A controlled document can be reviewed, approved, made effective, scheduled for review, and superseded without erasing prior evidence.
- An application team can create a wiki space from a standard template, build a nested page tree, document architecture/setup/runbooks/decisions, restore an earlier version, and link pages to live work records.
- A work due date appears in the application calendar; outbound email and the selected Microsoft 365 integration complete or fail visibly and recoverably.
- Automated tests, manual accessibility/security checks, monitoring, backup/restore evidence, runbooks, and rollback are present.

20. Migration, launch, and operating model

Migration approach

- Inventory source systems/files; classify authoritative data; define field, identity, account, status, attachment, comment, and document mappings.

- Clean duplicates and inactive records before import; preserve legacy IDs and source links; quarantine unsupported or unsafe attachments.
- Use repeatable scripts, dry runs, counts/checksums, sampled business verification, exception reports, cutover freeze, and rollback criteria.
- Do not migrate everything merely because it exists. Set retention and archive boundaries with record owners.

Production operations

- Service objectives for availability, response time, job latency, notification delivery, search freshness, recovery point (RPO), and recovery time (RTO).
- Dashboards/alerts for API errors, queue depth, dead letters, Graph throttling, failed mail/calendar sync, attachment scans, storage, database health, backup and certificate/secret expiry.
- Runbooks for access incident, customer data exposure, stuck workflow/SLA, integration outage, failed migration, malicious attachment, restore, and rollback.
- Regular access review, dependency patching, vulnerability response, restore test, audit-log export, retention execution, and document review.

21. Success measures

Goal	Example measure	Initial target-setting method
Fast intake and ownership	Median time to triage/first assignment; unassigned aging	Baseline current process, then set pilot improvement target
Predictable delivery	Cycle/lead time, WIP aging, sprint goal outcome, reopened work	Set per work type/team; avoid one global target
Reliable service	SLA attainment, response/resolution time, escalations, delivery failures	Segment by priority, service, and customer tier
Useful knowledge	Successful search, no-result queries, article usefulness, linked resolutions	Instrument from pilot; combine analytics with user feedback
Controlled documentation	Overdue reviews, approval time, superseded-use incidents, acknowledgment completion	Quality owner defines thresholds by document type
Adoption and usability	Active teams, task completion, support questions, satisfaction, accessibility defects	Pilot cohort baseline and journey testing
Security and resilience	Access violations, high-risk findings, patch time, restore success, integration recovery	Security/operations policy and tested objectives

MEASUREMENT RULE Do not reward ticket closure volume alone. Pair speed with quality, reopen rate, customer outcome, blocked work, and team health so metrics do not create bad behavior.

22. Principal risks and mitigations

Risk	Severity	Primary mitigation
Scope becomes “all of Jira + Confluence + Outlook”	High	Enforce MVP/V1 horizons, phase gates, and one vertical slice before breadth.
Permission or customer-sharing leak	Critical	Central authorization, deny-by-default, relationship tests, tenant/account isolation tests, security review.
ISO claims exceed evidence	High	Use “ISO-aligned”; licensed standards; named quality/security owners; external certification remains separate.
Email/calendar sync duplicates or conflicts	High	Source ownership rules, immutable external IDs, idempotency, outbox, retry/dead-letter, one-way first.
Attachments introduce malware/data exposure	Critical	Allowlist/type validation, private storage, quarantine/scan, signed access, retention and audit.
Configuration becomes impossible to support	High	Opinionated templates, guardrails, versioning, validation, preview/test mode, admin audit and health checks.
Board UI is pretty but inaccessible/slow	High	Keyboard alternative, semantic cards, virtualization only with a11y testing, representative load/performance budgets.
Migration corrupts history or identity	High	Dry runs, stable source IDs, reconciliation, exception queue, record-owner sign-off, rollback.
Microservices increase cost before value	Medium	Modular monolith; extract only measured bottlenecks or isolation needs.
Small team skips non-feature work	High	Definition of done includes security, tests, observability, runbooks, migration, docs, and accessibility.

23. Decisions required for the commercial pilot

1. Who is the sponsor and who is the day-to-day product owner with authority to choose scope?
2. Task 34 decision: the commercial release supports external customer service in isolated hosted organizations; the production isolation model must pass Gate G1.
3. Which two internal teams and which customer group (if any) will pilot the system?
4. What existing data/system must be migrated, and what can remain archived?
5. Which Microsoft 365 tenant, shared mailbox, Entra groups, and calendar scenarios are in scope?
6. Is ISO 9001, ISO/IEC 27001, or another standard a certification objective, contractual need, or general design guidance?
7. What data classifications, jurisdictions, retention periods, residency, RPO/RTO, and availability objectives apply?
8. What is the approved team, budget range, hosting preference, and target pilot date?
9. Which features are explicitly out of MVP even if they remain in the long-term vision?

24. Proposed first-week agenda

If work begins in the week of 3 August 2026, the first week should produce decisions and evidence—not production code.

Session	Participants	Output
1. Vision and boundaries (90 min)	Sponsor, product owner, service/quality leads, technical lead	North star, users, deployment model, MVP boundary, decision rights
2. Current-work mapping (2 × 90 min)	Agents, managers, customers/representatives, document owners	Request-to-resolution and document lifecycle maps; pain points
3. Identity/data/security workshop (90 min)	Technical lead, Entra admin, security/privacy, data owners	Identity flows, permissions, classifications, integrations, risks
4. Critical journey prototype review (90 min)	Product/UX, pilot users, accessibility/QA	Validated labels, navigation, board interaction, portal and document concepts
5. Charter and gate review (60 min)	Sponsor and named decision owners	Approved Phase 1 charter, backlog, risks, proof-of-concept list, schedule

FIRST APPROVAL Approve the discovery charter and the named decision owners. Do not approve the entire multi-month roadmap as fixed scope before discovery has tested the assumptions.

Appendix A — Research basis and source register

Sources below are authoritative or first-party and were accessed for this plan on 1 August 2026. They inform product patterns and engineering controls; they are not a substitute for licensed standards, legal advice, or organization-specific policy.

[S1] A Brief Introduction to Jira Boards — Atlassian. *Board columns, backlogs, Scrum/Kanban, WIP limits and swimlanes.*

[S2] Introduction to Jira Work Items — Atlassian. *Work item anatomy and hierarchy.*

[S3] About requests and work items — Atlassian Support. *Customer requests versus internal work items, portals and queues.*

[S4] Use an existing email address to receive requests — Atlassian Support. *Email-to-ticket channel behavior and constraints.*

[S5] Microsoft Graph user resource type — Microsoft Learn. *Microsoft Entra user representation and supported operations.*

[S6] Get incremental changes for users — Microsoft Learn. *Efficient directory synchronization through delta queries.*

[S7] Microsoft identity platform documentation — Microsoft Learn. *OIDC/OAuth sign-in and protected API access.*

[S8] Scopes and permissions in the Microsoft identity platform — Microsoft Learn. *Least-privilege permission guidance.*

[S9] user: sendMail — Microsoft Learn. *Graph mail sending, permissions, attachments and accepted/delivery distinction.*

[S10] Working with calendars and events using Microsoft Graph — Microsoft Learn. *Calendar/event operations, availability and calendar permissions.*

[S11] Microsoft Graph throttling guidance — Microsoft Learn. *Retry-After, backoff, avoiding polling and using change tracking.*

[S12] Guidance on the requirements for documented information of ISO 9001:2015 — ISO. *Examples of maintained documents and retained records subject to control.*

[S13] ISO 10013:2021 — Guidance for documented information — ISO. *Development and maintenance of documented information for management systems.*

[S14] ISO 9001 — Quality management systems (2026 edition status) — ISO. *Current publication status and expected 2026 transition.*

[S15] ISO/IEC 27001:2022 — Information security management systems — ISO. *Risk-based information security management principles.*

[S16] The 2020 Scrum Guide — ScrumGuides.org. *Scrum accountabilities, events, backlog, sprint goal and Definition of Done.*

[S17] Web Content Accessibility Guidelines (WCAG) 2.2 — W3C. *Accessibility target including focus, target size, authentication and dragging alternatives.*

[S18] File Upload Cheat Sheet — OWASP. *Allowlisting, type validation, storage, size limits, scanning and authorization.*

[S19] Logging Cheat Sheet — OWASP. *Security/application logging coverage and handling guidance.*

[S20] Secure Software Development Framework (SSDF) Version 1.1 — NIST. *Secure development practices integrated through the lifecycle.*

[S21] Confluence Features — Atlassian. *Collaborative pages, spaces, structured content trees, templates, page versioning, permissions, search and notifications.*

[S22] Use Confluence for technical documentation — Atlassian Support. *Technical-documentation spaces, page trees, reusable content, watching, version history, comparison and contributors.*

[S23] Miro for workshops & meetings — Miro Help Center. Infinite canvas, freehand drawing, sticky notes and meeting collaboration patterns.

[S24] Sticky notes; Templates; Voting — Miro Help Center. Visual objects, reusable facilitation structures and anonymous timed voting patterns.

[S25] Board access rights; Who has access to my board? — Miro Help Center. Owner/editor/commenter/viewer and scoped sharing patterns.

[S26] Board history: activity — Miro Help Center. Attributable board changes, recent-change visibility and recovery patterns.

[S27] How to make your Miro boards more accessible — Miro Help Center. Accessible preparation, navigation and access-level guidance.

[S28] Slido features — Slido. Q&A, voting, polls, word clouds, timed quizzes, leaderboards and engagement analytics.

Appendix B — Glossary

Term	Meaning in this plan
Account	A customer organization; not a login.
Agent	An internal user who triages and resolves requests.
Audit event	An attributable record of a security-, configuration-, or business-significant action.
Board	A filtered visual view of work items grouped into workflow columns.
Contact	A person associated with one or more customer accounts.
Controlled document	Documented information governed by ownership, version, approval, effective status, review, and history.
Customer request	The external/customer view of a unit of work; internally represented as a ticket/work item.
Documented information	Information an organization maintains or retains and controls as part of its management system.
Entra ID	Microsoft's cloud identity and access service, formerly Azure Active Directory.
Issue / ticket / work item	The core record used to track a request, problem, task, change, story, bug, or other work.
Kanban	A flow-based method that visualizes work and often limits work in progress.
Microsoft Graph	Microsoft API surface for authorized access to identity, mail, calendar, and other Microsoft 365 data.
Project	A governed container for work types, workflow, permissions, board/queue views, and configuration.
SLA	A timed service goal such as time to first response or resolution, with defined calendars and pause conditions.
Sprint	A fixed-length Scrum event containing a sprint goal and selected backlog work.
Tenant-ready	Designed to enforce organization boundaries even if the first deployment serves one organization.