Risk Assessment

1. Risk Register

ID	Risk Description	Category	Likelihood	Impact	Mitigation Strategy
R1	Real-time/asynchronous editing and edit locking (6.1.1, 6.1.3) cause data conflicts or inconsistent states under load.	Technical	Medium	High	Design optimistic/pessimistic locking and conflict resolution patterns in 3.1.2; add concurrency test cases in 3.1.8; execute performance/load tests in 9.1.3 and fix defects in 9.1.5 before UAT.
R2	Backup/retention/archival configurations (3.1.4, 5.1.7, 7.1.1, 7.1.5) fail under recovery scenarios leading to data loss.	Technical	Medium	High	Define RPO/RTO in 3.1.4; implement automated backup verification and periodic restore drills during 13.1.1 rehearsals; multi-region storage via IaC (4.1.2); monitor jobs (4.1.5, 7.1.4).
R3	Security controls (RBAC, MFA, IP restrictions, encryption) (3.1.2, 5.1.6, 5.1.7) introduce latency or compatibility issues impacting UX.	Technical	Low	Medium	Establish NFR performance targets in 2.1.2; perform design reviews (3.1.2); enable feature flags and staged rollouts in lower envs (4.1.1, 4.1.3); validate via 9.1.3.
R4	Requirements growth beyond baseline 20 FRs/14 NFRs (2.1.2) causes scope creep and schedule/cost overrun.	Project Management	High	High	Baseline scope in RTM (2.1.6); enforce change control per PMP (1.1.2); timebox workshops (2.1.1); defer out-of-scope items to post-Go-Live backlog.
R5	Underestimation of XL security architecture (3.1.2) drives rework across design and build, impacting critical path.	Project Management	Medium	High	Conduct architecture spikes and checkpoints (3.1.2); add schedule/budget contingency; early prototyping of RBAC/MFA; gate reviews between 3 and 4.
R6	Tight phase dependencies (3→4→5→6→7→8→9→10→12→13) compress SIT/UAT (9,12) if earlier phases slip.	Project Management	Medium	Medium	Track critical path; protect buffers before 9 and 12; overlap documentation/training (11) where possible; escalate via governance (1.1.1).
R7	Security Analyst single-point dependency across compliance and security tasks (1.1.4, 2.1.4, 3.1.2, 4.1.6, 8.1.5, 9.1.4, 10.1.x) creates bottlenecks.	Resource	High	High	Add backup Security Analyst; sequence high-impact tasks; prioritize workload in PMP (1.1.2); cross-train team; pre-book time for 10.1.x.
R8	DevOps Engineer over-allocation across envs, CI/CD, secrets, observability, and go-live (4.x, 13.x) delays readiness.	Resource	Medium	High	Allocate additional DevOps capacity/contractor; automate via IaC (4.1.2); parallelize non-blocking tasks; lock production change windows (13.1.x).
R9	QA capacity constraints for SIT, performance, and UAT support (9.1.2, 9.1.3, 12.1.x) reduce test coverage.	Resource	Medium	Medium	Shift-left testing via Test Strategy (3.1.8); prioritize risk-based test cases; add automation; augment QA for peak periods; schedule triage cadence (12.1.2).
R10	UX wireframes (3.1.7) do not align with user workflows, reducing adoption of templates/dashboards (5.1.5,	User Adoption	Medium	Medium	Run early usability sessions using prototypes; iterate wireframes before build; include key personas in reviews (2.1.1, 12.1.1).

ID	Risk Description	Category	Likelihood	Impact	Mitigation Strategy
	8.1.2).				
R11	Training sessions/materials (11.1.3, 11.1.4) are insufficient for complex features (6.x, 7.x, 8.x), leading to low adoption and support burden.	User Adoption	Medium	High	Provide role-based training, hands-on labs, and recordings; schedule refresher sessions during hypercare (13.1.5); include admin runbooks (11.1.5).
R12	UAT participants (12.1.1) are not representative of all user groups, leading to undiscovered usability gaps pre Go-Live.	User Adoption	Low	Medium	Ensure diverse personas in UAT plan; expand UAT scenarios; collect feedback KPIs during KPI monitoring (14.1.2) for rapid post-go-live fixes.
R13	Compliance mapping gaps (2.1.4) discovered late during validation (10.1.1) require design rework.	Compliance	Medium	High	Maintain compliance traceability to requirements (2.1.6); schedule interim reviews with DPO/compliance (10.1.4); address gaps before SIT exit (9.x).
R14	Audit logs (5.1.8) lack required detail/immutability for audits (10.1.3), risking non-compliance.	Compliance	Medium	High	Define log schema/retention in design (3.1.2); implement WORM/tamper-evident storage; restrict access (4.1.6); periodic log reviews and evidence collection (10.1.2).
R15	Retention/archival policies (5.1.9, 7.1.5) conflict with legal hold requirements, risking unlawful deletion.	Compliance	Medium	High	Align retention with legal counsel; implement configurable legal holds; validate scenarios in SIT (9.1.2) and include in runbooks (11.1.5).