

IEEE 29148-STYLE DOCUMENT

Software Requirements Specification

Apex Ledger — Expense Management Platform
Prepared for Meridian Logistics Group

Document ID: SRS-APEX-2026-v2.1
Version: 2.1 (Baselined)
Issue Date: March 9, 2026
Prepared by: Priya Chandrasekaran, Senior Business Analyst
Reviewed by: Daniel Osei, Lead Systems Architect
Approved by: Fatima Al-Rashid, VP Engineering, Vertex Software Inc.
Standard: ISO/IEC/IEEE 29148:2018

Revision History

Ver.	Date	Description	Author
1.0	2025-11-04	Initial draft circulated for stakeholder review	P. Chandrasekaran
1.5	2025-12-18	Added payroll integration & audit export requirements	P. Chandrasekaran
2.0	2026-02-02	Incorporated UAT feedback; baselined for Sprint 14	D. Osei
2.1	2026-03-09	Clarified NFR-4 latency targets; traceability matrix refresh	P. Chandrasekaran

Contents

1	Introduction	2
1.1	Purpose	2
1.2	Scope	2
1.3	Intended Audience and Reading Guide	2
1.4	Definitions, Acronyms, and Abbreviations	2
1.5	References	2
1.6	Document Overview	2
2	Overall Description	3
2.1	Product Perspective	3
2.2	Product Functions	3
2.3	User Classes and Characteristics	3
2.4	Operating Environment	3
2.5	Design and Implementation Constraints	3
2.6	Assumptions and Dependencies	4
3	Functional Requirements	4
3.1	User Account and Access Management	4
3.2	Expense Report Submission	4
3.3	Approval Workflow	5
3.4	Reimbursement Processing	5
3.5	Reporting and Audit	6
4	External Interface Requirements	6
4.1	User Interfaces	6
4.2	Hardware Interfaces	6
4.3	Software Interfaces	6
4.4	Communications Interfaces	6
5	Non-Functional Requirements	7
6	Use-Case Model	7
6.1	Actors	7
6.2	Use-Case Diagram	7
7	Requirements Traceability Matrix	7
8	Glossary	9

1 Introduction

1.1 Purpose

This Software Requirements Specification (SRS) defines the functional and non-functional requirements for **Apex Ledger**, a cloud-hosted expense management platform being developed by Vertex Software Inc. for Meridian Logistics Group. The document is written to the structure recommended by ISO/IEC/IEEE 29148:2018 [2] and is intended for use by the product management, engineering, quality assurance, and client stakeholder teams responsible for building, verifying, and accepting Release 3.0 of the platform.

1.2 Scope

Apex Ledger replaces Meridian’s spreadsheet-based expense process with a single system that lets employees submit expense reports, routes them through configurable approval chains, reconciles reimbursements against the corporate card feed, and pushes settled batches to the Meridian Payroll Connect interface. The scope of this document covers the web application, its REST API, the approval workflow engine, and the payroll/ERP integration layer. It excludes the mobile companion application and the travel-booking module, both of which are governed by separate SRS documents (SRS-APEX-MOBILE, SRS-APEX-TRAVEL).

1.3 Intended Audience and Reading Guide

- **Product & Business Analysts** should read Sections 2–3 for scope and feature intent.
- **Engineering** should treat Sections 3–5 as the binding contract for implementation.
- **QA** should derive test cases directly from the requirement IDs in Section 3 and cross-check coverage against the traceability matrix in Section 6.
- **Client stakeholders (Meridian)** should focus on Sections 2, 3, and 7 for acceptance sign-off.

1.4 Definitions, Acronyms, and Abbreviations

Full definitions appear in the Glossary (Section 8). Frequently used acronyms: **SRS** (Software Requirements Specification), **FR** (Functional Requirement), **NFR** (Non-Functional Requirement), **RBAC** (Role-Based Access Control), **SSO** (Single Sign-On), **SLA** (Service Level Agreement).

1.5 References

- ISO/IEC/IEEE 29148:2018, *Systems and software engineering — Life cycle processes — Requirements engineering* [2]
- IEEE Std 830-1998, *Recommended Practice for Software Requirements Specifications* [1]
- Wiegers, K. & Beatty, J., *Software Requirements*, 3rd ed. [4]
- OWASP Application Security Verification Standard 4.0 [3]
- Meridian Logistics Group – Vendor Data Handling Policy, rev. 2025-09

1.6 Document Overview

Section 2 describes the product context, user classes, and constraints. Section 3 enumerates functional requirements grouped by subsystem. Section 4 covers external interfaces. Section 5 specifies non-functional requirements. Section 6 presents the use-case model. Section 7 gives the requirement-to-test traceability matrix, and Section 8 closes with the glossary.

2 Overall Description

2.1 Product Perspective

Apex Ledger is a new, self-contained system that replaces Meridian’s legacy spreadsheet-and-email expense process. It exposes a browser-based front end, a versioned REST API, and two outbound integrations: a nightly settlement feed to *Meridian Payroll Connect* and an on-demand export to the Nimbus ERP general ledger. Figure 1 (Section 6) shows the system boundary and the actors that interact with it.

System Context

Apex Ledger sits between the corporate card issuer feed, the identity provider (SSO), and the downstream payroll/ERP systems. It is the single source of truth for expense report status from submission through reimbursement.

Trust Boundary

All traffic crosses the boundary over TLS 1.2+. Card-feed and payroll integrations are server-to-server; no browser client ever holds payroll credentials.

2.2 Product Functions

At a high level, Apex Ledger provides: (1) expense report authoring with receipt capture, (2) configurable multi-step approval workflows, (3) automated reimbursement batching, (4) audit and export reporting, and (5) payroll/ERP synchronization. Each function is decomposed into numbered functional requirements in Section 3.

2.3 User Classes and Characteristics

User Class	Description	Frequency
Employee	Submits expense reports and attaches receipts; the largest user population (approx. 4,200 seats).	Daily
Approver	Line manager who reviews and approves/rejects reports within their cost center.	Daily
Finance Administrator	Configures policies, runs reimbursement batches, manages exception queues.	Daily
External Auditor	Read-only access to closed reports and export logs during audit windows.	Quarterly
System Integrator	Vertex/Meridian technical staff maintaining the payroll and ERP connectors.	As needed

2.4 Operating Environment

Server components run as containerized services on Meridian’s contracted AWS ap-south-1 region. The web client targets evergreen Chrome, Edge, Firefox, and Safari (last two major versions). No client-side plugin or applet is required.

2.5 Design and Implementation Constraints

- Must integrate with Meridian’s existing Okta tenant for SSO (SAML 2.0).
- Payroll batch format is fixed by *Meridian Payroll Connect* v3 API and cannot be renegotiated within this release.
- Data residency: all personally identifiable expense data must remain within the ap-south-1 region per the Vendor Data Handling Policy.
- Release cadence is fixed to Meridian’s quarterly change-freeze calendar; no production deploys in the two weeks surrounding fiscal quarter close.

2.6 Assumptions and Dependencies

- Meridian will provide a sandbox card-feed file for integration testing no later than four weeks before UAT.
- Okta group membership accurately reflects the approval hierarchy at go-live; Apex Ledger does not independently validate organizational structure.
- Currency conversion rates are supplied by the existing Nimbus ERP rate table and are treated as authoritative.

3 Functional Requirements

Each requirement below carries a unique identifier of the form FR-*n.m*, used verbatim by QA when writing test cases and referenced in the traceability matrix (Section 7). Priority reflects Release 3.0 commitments only.

3.1 User Account and Access Management

FR-1.1 — SSO Authentication

The system shall authenticate all users exclusively via Meridian's Okta SAML 2.0 identity provider; local username/password accounts shall not be offered to Employee, Approver, or Finance Administrator roles. **HIGH**

FR-1.2 — Role-Based Access Control

The system shall enforce RBAC with, at minimum, the roles Employee, Approver, Finance Administrator, External Auditor, and System Integrator, mapping each Okta group to exactly one Apex Ledger role at provisioning time. **HIGH**

FR-1.3 — Session Expiry

The system shall terminate an idle browser session after 30 minutes and require re-authentication before any state-changing action. **MEDIUM**

3.2 Expense Report Submission

FR-2.1 — Line-Item Entry

The system shall allow an Employee to add one or more expense line items to a report, each capturing date, category (from a controlled vocabulary), amount, currency, merchant, and an optional note not exceeding 500 characters. **HIGH**

FR-2.2 — Receipt Attachment

The system shall allow an Employee to attach a receipt image or PDF (max 10 MB) to any line item and shall block submission of line items over \$25 that lack an attached receipt, per Meridian expense policy. **HIGH**

FR-2.3 — Draft Autosave

The system shall autosave a report in Draft status at intervals of no more than 60 seconds while the Employee is actively editing. **MEDIUM**

FR-2.4 — Policy Validation

Upon submission, the system shall validate each line item against the active expense policy (per-category caps, disallowed categories) and shall present all violations to the Employee in a single pass rather than one at a time. **HIGH**

3.3 Approval Workflow**FR-3.1 — Configurable Approval Chain**

The system shall route a submitted report through a Finance-Administrator-configured approval chain of one to three sequential approvers, determined by the Employee's cost center and the report total. **HIGH**

FR-3.2 — Approve, Reject, or Return

The system shall allow an Approver to Approve, Reject (with mandatory reason code), or Return for correction (with mandatory free-text comment) a report awaiting their decision. **HIGH**

FR-3.3 — Delegation

The system shall allow an Approver to delegate their pending queue to a named backup Approver for a bounded date range, and shall record the original and delegated approver on every resulting decision. **MEDIUM**

FR-3.4 — Escalation

The system shall escalate a report to the next approver in the chain if the current approver takes no action within 5 business days, and shall notify the Finance Administrator of the escalation. **MEDIUM**

3.4 Reimbursement Processing**FR-4.1 — Batch Assembly**

The system shall allow a Finance Administrator to assemble all fully approved reports into a reimbursement batch, grouped by pay period, and shall prevent a report from appearing in more than one open batch. **HIGH**

FR-4.2 — Card-Feed Reconciliation

The system shall automatically match corporate-card-fed transactions to submitted line items on merchant, date (± 2 days), and amount, and shall flag unmatched card transactions for manual review. **MEDIUM**

FR-4.3 — Payroll Export

The system shall export an approved reimbursement batch to *Meridian Payroll Connect* in its documented v3 file format within one business day of batch closure. **HIGH**

3.5 Reporting and Audit

FR-5.1 — Audit Log

The system shall record an immutable audit entry for every state transition of a report (submit, approve, reject, return, escalate, batch, export), capturing actor, timestamp, and prior/next state.

HIGH

FR-5.2 — Auditor Export

The system shall allow an External Auditor to export closed reports and their audit trails for a selected date range as a signed CSV bundle, without exposing reports outside that range.

MEDIUM

FR-5.3 — Spend Dashboards

The system shall provide a Finance Administrator dashboard summarizing spend by category, cost center, and pay period, refreshed at least once every 15 minutes.

LOW

4 External Interface Requirements

4.1 User Interfaces

The primary interface is a responsive single-page web application. Key screens: Report Editor, Approval Inbox, Batch Console, and Audit Export. All interactive controls must meet WCAG 2.1 Level AA contrast and keyboard-navigation requirements (see NFR-5, Section 5).

4.2 Hardware Interfaces

None. Apex Ledger requires no dedicated client hardware beyond a standard workstation or laptop capable of running an evergreen browser; receipt capture on mobile devices is handled by the companion mobile application, out of scope for this document.

4.3 Software Interfaces

Interface	Purpose	Protocol
Okta SAML IdP	Authentication and role provisioning (FR-1.1, FR-1.2)	SAML 2.0 / HTTPS
Meridian Payroll Connect v3	Reimbursement batch export (FR-4.3)	SFTP, fixed-width file
Nimbus ERP General Ledger	Spend export for GL posting (FR-5.3)	REST/JSON over HTTPS
Corporate Card Issuer Feed	Nightly transaction feed for reconciliation (FR-4.2)	SFTP, CSV

4.4 Communications Interfaces

All client-server and server-to-server traffic uses TLS 1.2 or higher. The public REST API is versioned at `/api/v3` and returns JSON; webhook callbacks to Meridian's internal systems are signed with an HMAC-SHA256 header (`X-Apex-Signature`) so recipients can verify authenticity without a shared secret over the wire.

5 Non-Functional Requirements

ID	Category	Requirement
NFR-1	Performance	95th-percentile API response time shall not exceed 800 ms under 500 concurrent users; report submission end-to-end shall complete in under 2 s.
NFR-2	Availability	The production service shall meet a 99.9% monthly uptime SLA, excluding pre-announced maintenance windows.
NFR-3	Security	All data at rest shall be encrypted with AES-256; all data in transit shall use TLS 1.2+; the platform shall pass an annual penetration test against OWASP ASVS 4.0 Level 2 [3].
NFR-4	Scalability	The system shall support linear scale-out to 10,000 registered users and 50,000 reports/month without architectural change.
NFR-5	Usability	The web client shall conform to WCAG 2.1 Level AA; a first-time Employee shall be able to submit a compliant report within 5 minutes without training.
NFR-6	Maintainability	Each microservice shall maintain at least 80% unit-test line coverage and expose a <code>/healthz</code> endpoint for orchestration probes.
NFR-7	Auditability	Audit log entries (FR-5.1) shall be retained for a minimum of 7 years and shall be write-once (no update or delete API shall exist for the audit table).
NFR-8	Recoverability	Recovery Point Objective (RPO) of 15 minutes and Recovery Time Objective (RTO) of 4 hours for the production database.

Rationale — Why NFR-4 Exists

Meridian's headcount is contracted to grow from 1,900 to 3,500 seats over the two years following go-live, driven by the pending acquisition of two regional carriers. NFR-4 exists so the platform does not require a re-architecture mid-rollout.

6 Use-Case Model

6.1 Actors

Actor	Description
Employee	Primary/human actor; authors and submits expense reports.
Approver	Human actor; reviews reports within their approval authority.
Finance Administrator	Human actor; configures policy and operates reimbursement batches.
External Auditor	Human actor; read-only access during audit windows.
Meridian Payroll Connect	External system actor; receives settled reimbursement batches.

6.2 Use-Case Diagram

Figure 1 shows the primary use cases for Release 3.0 and the actors that initiate them. The dashed arrow denotes an `<include>` relationship: submitting a report always triggers the receipt-attachment check (FR-2.2).

7 Requirements Traceability Matrix

The matrix below links each functional requirement to the use case that exercises it and the QA test case that verifies it. QA must not mark a release candidate green until every row has a passing test-case execution logged in the test-management system.

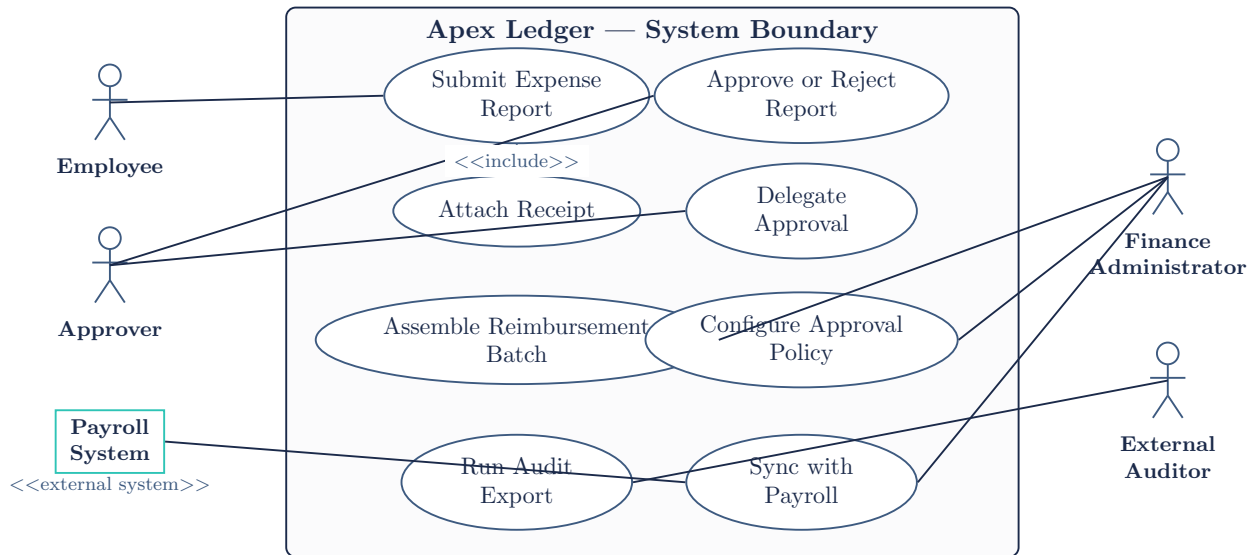


Figure 1: Use-case diagram for Apex Ledger, Release 3.0.

Req. ID	Requirement	Use Case	Test Case	Pri.
FR-1.1	SSO authentication via Okta	Submit Expense Report	TC-AUTH-001	HIGH
FR-1.2	Role-based access control	(all use cases)	TC-AUTH-014	HIGH
FR-1.3	30-minute idle session expiry	Submit Expense Report	TC-AUTH-022	MEDIUM
FR-2.1	Line-item entry on a report	Submit Expense Report	TC-RPT-003	HIGH
FR-2.2	Receipt attachment enforcement	Attach Receipt	TC-RPT-011	HIGH
FR-2.3	Draft autosave every 60s	Submit Expense Report	TC-RPT-018	MEDIUM
FR-2.4	Single-pass policy validation	Submit Expense Report	TC-RPT-025	HIGH
FR-3.1	Configurable approval chain	Configure Approval Policy	TC-WFL-002	HIGH
FR-3.2	Approve / reject / return decisions	Approve or Reject Report	TC-WFL-009	HIGH
FR-3.3	Approver delegation	Delegate Approval	TC-WFL-016	MEDIUM
FR-3.4	5-day escalation	Approve or Reject Report	TC-WFL-021	MEDIUM
FR-4.1	Reimbursement batch assembly	Assemble Reimbursement Batch	TC-BAT-004	HIGH
FR-4.2	Card-feed reconciliation	Assemble Reimbursement Batch	TC-BAT-010	MEDIUM
FR-4.3	Payroll export within 1 business day	Sync with Payroll	TC-BAT-017	HIGH
FR-5.1	Immutable audit log	(all use cases)	TC-AUD-001	HIGH
FR-5.2	Auditor CSV export	Run Audit Export	TC-AUD-007	MEDIUM
FR-5.3	Finance spend dashboard	Configure Approval Policy	TC-AUD-013	LOW

Open Item at Baseline

FR-4.2 (card-feed reconciliation) is Medium priority for Release 3.0 pending confirmation of the sandbox feed file from Meridian (see Assumptions, Section 2.7). If the file is not available by the UAT entry date, FR-4.2 will slip to Release 3.1 and manual reconciliation will continue as an interim process.

8 Glossary

Term	Definition
Approval Chain	The ordered sequence of Approvers a report must pass through before it is eligible for reimbursement.
Batch	A group of fully approved expense reports assembled for a single reimbursement run and payroll export.
Cost Center	An organizational unit code used to route reports to the correct approval chain and to attribute spend in reporting.
Escalation	Automatic forwarding of a pending report to the next approver after 5 business days of inactivity (FR-3.4).
FR	Functional Requirement — a numbered, testable statement of required system behavior.
NFR	Non-Functional Requirement — a quality attribute constraint (performance, security, availability, etc.).
RBAC	Role-Based Access Control — authorization model in which permissions are granted to roles rather than individual users.
Reconciliation	The process of matching corporate-card-fed transactions to submitted expense line items.
SLA	Service Level Agreement — a contracted commitment on a measurable service quality, such as uptime.
SSO	Single Sign-On — authentication scheme allowing one login to grant access across multiple systems, here via Okta SAML.

References

- [1] IEEE std 830-1998: Recommended practice for software requirements specifications, 1998.
- [2] ISO/IEC/IEEE 29148:2018 — systems and software engineering — life cycle processes — requirements engineering, 2018.
- [3] OWASP Foundation. OWASP application security verification standard 4.0. Technical report, OWASP Foundation, 2019.
- [4] Karl Wieggers and Joy Beatty. *Software Requirements*. Microsoft Press, 3rd edition, 2013.