Risk Management Module - Phase 1 Scope Definition

Executive Summary

Phase 1 focuses on establishing the **foundational risk management capabilities** that enable the organization to identify, assess, treat, and monitor risks systematically. This phase emphasizes integration with existing Asset Management and Governance modules while keeping complexity manageable and delivering immediate business value.

Duration: 4 months
Goal: Operational risk register with basic assessment, treatment tracking, and reporting capabilities
Target: Support 100-200 risks, 20-30 KRIs, and 50+ active users

---

1. Phase 1 Scope - MUST HAVE (P0)

1.1 Risk Governance and Appetite

✅ **Risk Appetite Framework (P0)**

What's Included:

- Risk appetite statement (text document)
- Risk tolerance levels by category (qualitative: High/Medium/Low)
- Risk appetite per risk category (e.g., Cybersecurity: Low tolerance, Operational: Medium tolerance)
- Annual review workflow with approval tracking
- Board/executive approval workflow
- Version control for appetite statements

What's NOT Included (Future Phases):

- Quantitative risk appetite metrics (e.g., "max $5M loss")
- Risk capacity calculations
- Risk appetite by business unit (cascading)
- Real-time appetite vs. exposure dashboards

Why P0: Foundation for all risk decisions; required to evaluate if risks are acceptable

---

✅ **Risk Taxonomy (Classification) (P0)**

What's Included:

- Pre-defined risk categories (10-12 categories):

    1. Strategic Risks
    2. Operational Risks
    3. Technology/Cybersecurity Risks
    4. Financial Risks
    5. Compliance & Legal Risks
    6. Reputational Risks
    7. Third-Party/Vendor Risks
    8. Human Resources Risks
    9. Environmental/Physical Risks
    10. Project Risks
    11. Data Privacy Risks
    12. Business Continuity Risks
- Two-level hierarchy: Category → Sub-category
- Ability to add custom sub-categories
- Risk type attributes per category
- Standard risk tags

What's NOT Included (Future Phases):

- Three+ level hierarchies
- Industry-specific pre-built taxonomies
- AI-assisted categorization
- Risk taxonomy mapping to external frameworks

Why P0: Essential for consistent risk identification and reporting

---

1.2 Risk Identification and Registration

✅ Risk Register (P0)

What's Included:

Core Fields:

- Risk ID (auto-generated)
- Risk Title
- Risk Description (rich text)
- Risk Statement (If [cause], then [event], resulting in [impact])
- Risk Category and Sub-category
- Risk Owner (user reference)
- Risk Analyst (user reference)
- Business Unit(s) affected
- Date Identified
- Risk Status (Active, Monitoring, Closed, Accepted)
- Current Status Notes
- Tags

Risk Scenario:

- Threat source (internal, external, natural)
- Vulnerabilities exploited
- Risk velocity (Slow, Medium, Fast, Immediate)
- Early warning signs (text description)

Affected Entities:

- Linked Assets (from Asset Management - multi-select)
- Asset types impacted
- Business processes affected

Existing Controls:

- Linked Controls (from Governance module - multi-select)
- Overall control effectiveness rating (1-5 scale or %)

Metadata:

- Created by, Created date
- Last updated by, Last updated date
- Version number
- Attachments (documents, links)
- Related risks (manual linking)

What's NOT Included (Future Phases):

- Automated risk relationships (parent/child, cascading)
- Contributing factors as structured data
- Bow-tie diagrams
- Attack tree modeling
- Risk correlation analysis
- Scenario libraries/templates

Why P0: Central repository is foundation of risk management

✅ Risk Assessment - Qualitative (P0)

What's Included:

Likelihood Scale (1-5):

1. Rare: <10% chance in next 12 months
2. Unlikely: 10-30% chance
3. Possible: 30-50% chance
4. Likely: 50-80% chance
5. Almost Certain: >80% chance

Impact Scale (1-5):

1. Negligible: Minimal impact, routine operations
2. Minor: Limited impact, minor disruption
3. Moderate: Notable impact, temporary disruption
4. Major: Significant impact, extended disruption
5. Catastrophic: Severe impact, long-term consequences

Impact Categories (assess each):

- Financial impact ($ ranges per level)
- Operational impact (downtime, productivity loss)
- Reputational impact (media exposure, customer loss)
- Compliance impact (fines, sanctions)
- Safety impact (injuries, health risks)

Risk Score Calculation:

- Risk Score = Likelihood × Impact
- Risk Level: Low (1-6), Medium (8-12), High (15-20), Critical (25)

Risk States (Track separately):

- **Inherent Risk** (before any controls)
  - Inherent Likelihood (1-5)
  - Inherent Impact (1-5)
  - Inherent Risk Score (1-25)
  - Inherent Risk Level (Low/Med/High/Critical)
- **Current Risk** (with existing controls)
  - Current Likelihood (1-5)
  - Current Impact (1-5)
  - Current Risk Score (1-25)
  - Current Risk Level (Low/Med/High/Critical)
- **Target Risk** (desired state aligned with appetite)
  - Target Likelihood (1-5)
  - Target Impact (1-5)
  - Target Risk Score (1-25)
  - Target Risk Level (Low/Med/High/Critical)

Assessment Metadata:

- Assessment date
- Assessor name
- Assessment method (qualitative - 5x5 matrix)
- Assessment notes and assumptions
- Confidence level (High/Medium/Low)
- Supporting evidence (attachments)

Customizable Matrix:

- Define risk level boundaries (which scores = Low/Med/High/Critical)
- Customize per risk category if needed
- Color coding for risk levels

What's NOT Included (Future Phases):

- Semi-quantitative assessment (financial ranges, percentages)
- Quantitative assessment (ALE, FAIR, Monte Carlo)
- Residual risk calculation (after treatment)
- Multiple concurrent assessment methods
- Historical trending of risk scores
- Benchmarking against industry data
- Control effectiveness calculation

Why P0: Must assess risks to prioritize and treat them; qualitative is simplest to start

---

✅ On-Demand Risk Assessments (P0)

What's Included:

Assessment Request Form:

- Request title and description
- Requested by (user)
- Business justification
- Risk assessment trigger (dropdown):
  - New product/service launch
  - Major change to existing product/service
  - New technology adoption
  - New project initiation
  - Regulatory change
  - Major organizational change
  - Security incident/near-miss
  - Audit finding
  - Third-party change
  - Business leader request
  - Other (specify)
- Scope description
- Affected assets (optional, can select from Asset Management)
- Affected business units
- Priority (High/Medium/Low)
- Requested due date
- Attachments (project charter, change request, etc.)

Request Workflow:

- Submit request
- Route to risk management team
- Risk manager reviews and approves/rejects
- If approved: Assign to risk analyst
- Risk analyst conducts assessment
- Create or update risk records
- Notify requester of completion
- Link assessment results to request

Request Tracking:

- Request status (Submitted, Under Review, Approved, In Progress, Completed, Rejected)
- Assignment tracking
- Due date tracking
- Request history and audit trail
- Dashboard showing all requests by status

What's NOT Included (Future Phases):

- Automated risk identification from data sources
- AI-assisted risk discovery
- Integration with project management tools
- Automated triggering based on system events
- Self-service assessment (users conduct own assessment)

Why P0: Critical for capturing risks from business changes; supports proactive risk management

---

1.3 Risk Evaluation and Prioritization

✅ Risk Evaluation (P0)

What's Included:

Evaluation Against Appetite:

- Compare current risk level to risk appetite (by category)
- Risk appetite status:
  - Within Appetite (Green): Risk level acceptable
  - Near Appetite (Amber): Risk approaching limits, watch closely
  - Exceeds Appetite (Red): Risk unacceptable, treatment required
- Automated status calculation based on rules
- Filter risks by appetite status
- Dashboard showing risks exceeding appetite

Risk Prioritization:

- Sort by risk score (primary)
- Filter by risk level (Critical/High/Medium/Low)

- Filter by category, business unit, owner
- Tag high-priority risks
- Create "watchlist" of priority risks

Risk Lists/Views:

- All risks
- My risks (as owner)
- High and critical risks
- Risks exceeding appetite
- Risks requiring treatment
- Risks due for review
- Recently identified risks
- Closed risks

What's NOT Included (Future Phases):

- Multi-criteria prioritization (weighted scoring)
- Risk concentration analysis
- Risk correlation and cascading analysis
- Portfolio risk aggregation
- Quantitative exposure calculations
- Risk ranking algorithms

Why P0: Need to prioritize which risks to treat first; simple comparison to appetite is sufficient

---

1.4 Risk Treatment

✅ Risk Treatment Plans (P0)

What's Included:

Treatment Strategy (Select one primary strategy):

- **Mitigate/Reduce**: Implement controls to lower likelihood or impact
- **Transfer**: Shift risk via insurance or contracts
- **Accept**: Acknowledge risk and take no action (requires approval)
- **Avoid**: Eliminate risk by not pursuing activity

Treatment Plan Fields:

- Treatment Plan ID
- Linked Risk (reference)
- Treatment Strategy (dropdown)
- Treatment Description (detailed plan)
- Responsible Person (treatment owner)
- Supporting Team Members (optional)
- Target Start Date

- Target Completion Date
- Actual Completion Date
- Status (Planned, In Progress, Completed, On Hold, Cancelled)
- Progress Percentage (0-100%)
- Budget (estimated and actual - optional)
- Milestones (text list or structured)
- Dependencies (text description)
- Success Criteria
- Notes

For Mitigation Strategy:

- New controls to implement (free text or link to Governance control library)
- Expected risk reduction (target likelihood and impact after treatment)

For Transfer Strategy:

- Transfer mechanism (Insurance, Contract, Outsourcing)
- Insurance details:
  - Policy number
  - Insurer name
  - Coverage amount
  - Premium amount
  - Deductible
  - Renewal date
  - Coverage description
  - Attachments (policy document)
- Contract details:
  - Contract reference
  - Counterparty name
  - Transfer terms (text)
  - Contract effective date
  - Contract expiry date

For Accept Strategy:

- Acceptance justification (required)
- Business reason
- Approved by (must be senior to risk owner)
- Approval date
- Acceptance review date
- Compensating controls (if any)
- Monitoring plan

For Avoid Strategy:

- Avoidance actions (what activity will be stopped/not pursued)

- Business impact of avoidance
- Approved by
- Implementation date

Treatment Tracking:

- Create treatment plan from risk detail page
- Update progress and status
- Upload evidence of completion
- Link evidence from evidence repository
- Treatment history log
- Notifications to treatment owner (due dates, overdue)

What's NOT Included (Future Phases):

- Automated workflow for treatment approval
- Treatment dependencies and sequencing
- Resource allocation and capacity planning
- Automated ROCI (Return on Control Investment) calculation
- Treatment portfolio view
- Treatment effectiveness analytics
- Integration with project management tools
- Treatment templates by risk type

Why P0: Must track how risks are being addressed; basic treatment tracking essential

---

✅ Treatment Monitoring (P0)

What's Included:

Dashboards and Lists:

- All treatment plans by status
- My treatment plans (as owner)
- Overdue treatment plans
- Treatments due in next 30/60/90 days
- Completed treatments pending verification
- Treatments on hold or cancelled

Progress Tracking:

- Manual progress updates by treatment owner
- Status changes logged
- Completion date captured
- Actual vs. planned dates tracking

Notifications:

- Treatment plan assigned notification

- Treatment due in 7/14/30 days reminders
- Treatment overdue alerts
- Treatment completion notification (to risk owner)

Escalation:

- Manual escalation by risk analyst
- Overdue treatments highlighted on dashboards
- Email notifications to management for critical risk treatments

What's NOT Included (Future Phases):

- Automated escalation workflows
- Treatment health scoring
- Budget variance tracking and alerts
- Resource utilization dashboards
- Treatment roadmap/Gantt view
- Integration with change management

Why P0: Need visibility into treatment execution; basic tracking prevents treatments from falling through cracks

---

1.5 Risk Monitoring

✅ Key Risk Indicators (KRIs) (P0)

What's Included:

KRI Core Fields:

- KRI ID (auto-generated)
- KRI Name
- KRI Description
- KRI Type (Leading indicator, Lagging indicator)
- Linked Risk(s) (one or multiple)
- Risk Category
- Measurement Frequency (Daily, Weekly, Monthly, Quarterly)
- Data Source (description of where data comes from)
- Calculation Method (formula or description)
- Unit of Measurement (%, count, currency, days, etc.)

Thresholds:

- Target (Green): Desired/acceptable level
- Warning (Amber): Requires attention
- Critical (Red): Requires immediate action
- Threshold direction (Lower is better / Higher is better)

Current State:

- Current Value
- Current Status (Green/Amber/Red based on thresholds)
- Last Measurement Date
- Last Updated By
- Trend (Improving, Stable, Deteriorating) - manual or calculated

Ownership:

- KRI Owner (responsible for monitoring)
- Notification recipients (who gets alerts)

Example KRI Library (Starter set of 20-30 KRIs):

Cybersecurity:

- Number of critical/high vulnerabilities unpatched >30 days
- Failed login attempts per week
- Percentage of users with MFA enabled
- Number of phishing simulation failures
- Mean time to detect security incidents
- Percentage of systems with updated antivirus

Operational:

- System availability/uptime percentage
- Number of unplanned outages per month
- Average incident resolution time
- Backup success rate
- Number of change failures

Compliance:

- Number of overdue compliance actions
- Open audit findings count
- Policy acknowledgment percentage
- Days since last compliance assessment
- Number of active policy exceptions

Financial:

- Days sales outstanding (DSO)
- Cash flow variance from forecast
- Number of fraud incidents
- Budget variance percentage

Third-Party:

- Vendor SLA compliance percentage
- Number of vendor incidents
- Vendor assessments overdue

- Critical vendor dependency count

KRI Management:

- Create/edit/delete KRIs
- Link KRIs to risks (many-to-many)
- Define thresholds
- Manual data entry for KRI values
- KRI measurement history (track values over time)
- KRI status dashboard
- Threshold breach alerts (email notifications)

What's NOT Included (Future Phases):

- Automated data collection from systems
- Integration with monitoring tools
- Advanced trending and forecasting
- Predictive analytics
- Composite KRI scores
- KRI benchmarking
- Mobile KRI entry
- KRI effectiveness scoring

Why P0: Early warning system for risk changes; manual entry acceptable initially

---

✅ Risk Review and Reassessment (P0)

What's Included:

Scheduled Review Requirements:

- Risk review frequency based on risk level:
  - Critical risks: Quarterly review required
  - High risks: Semi-annual review required
  - Medium risks: Annual review required
  - Low risks: Biennial review or as-needed
- Automatic calculation of next review date
- Review due date tracking

Review Process:

- Risk owner receives review reminder notification
- Risk owner or analyst performs review:
  - Review risk description (still accurate?)
  - Review affected assets (any changes?)
  - Review existing controls (still effective?)
  - Review assessment (likelihood/impact still valid?)

    - Re-score risk if needed (inherent, current, target)
    - Update treatment plan status
    - Review KRIs
    - Update risk status (Active, Monitoring, Closed, Accepted)
    - Document review notes
- Record review completion date
- Calculate next review date
- Notify stakeholders of significant changes

Review Tracking:

- Dashboard showing risks due for review
- Overdue reviews highlighted
- Review history per risk (who reviewed, when, what changed)
- Review completion rate metrics

Triggered Reviews:

- Manual trigger for ad-hoc review
- Treatment completion triggers review
- KRI threshold breach suggests review
- Major business change triggers review

What's NOT Included (Future Phases):

- Automated triggering based on external events
- Workflow-based review with approvals
- Bulk review capabilities
- Review assignment and delegation
- Control effectiveness integration (auto-update risk when control changes)
- Incident-triggered reviews (when incident module available)

Why P0: Risks change over time; periodic review keeps register current

---

1.6 Integration with Existing Modules

✅ Asset Management Integration (P0)

What's Included:

Link Risks to Assets:

- Multi-select assets when creating/editing risk
- Asset type and asset ID references stored in risk record
- View all risks affecting an asset (from Asset detail page)
- View all assets affected by a risk (from Risk detail page)
- Asset criticality visible in risk assessment
- Asset owner information accessible

Asset-Driven Risk Features:

- Filter risks by asset type
- Asset count per risk
- Critical assets with risks report
- Assets without identified risks report

Shared Data:

- Business units (same table)
- Asset owners (can be risk owners)
- Tags (shared tagging system)

What's NOT Included (Future Phases):

- Asset criticality automatically influencing risk impact
- Asset changes automatically triggering risk reviews
- Asset compliance status integration
- Automated risk identification based on asset attributes
- Asset risk heat map visualization

Why P0: Assets are what we're protecting; linking risks to assets provides context

---

✅ Governance Module Integration (P0)

What's Included:

Link Risks to Controls:

- Multi-select controls from Unified Control Library when creating/editing risk
- Control references stored in risk record
- View all controls mitigating a risk (from Risk detail page)
- View all risks addressed by a control (from Control detail page)
- Control implementation status visible in risk view
- Control effectiveness rating influences current risk

Control-Driven Risk Features:

- Filter risks by linked controls
- Risks without controls report (control gaps)
- Controls without risks report (unused controls)
- Risk-control coverage matrix

Treatment to Control Linking:

- When treatment strategy is "Mitigate", optionally link to:
  - Existing controls to enhance
  - New controls to implement (from control library or propose new)
- Treatment completion can trigger control implementation

Shared Data:

- Control effectiveness assessments inform risk scores
- Findings can be linked to risks (audit finding → risk)
- Policy exceptions linked to risk acceptance

What's NOT Included (Future Phases):

- Automated risk score update when control effectiveness changes
- Control test failure automatically increases risk
- ROI calculation (cost of control vs. risk reduction)
- Suggested controls based on risk type (AI/ML)
- Control coverage optimization
- Integrated control-risk-asset view

Why P0: Controls are how we mitigate risks; showing which controls protect against which risks is essential

---

1.7 Reporting and Analytics

✅ Risk Register Reports (P0)

What's Included:

Standard Reports:

1. **Complete Risk Register**
    - All active risks with key fields
    - Filterable by: Category, Business Unit, Owner, Risk Level, Status
    - Sortable by: Risk Score, Date Identified, Review Date
    - Export to Excel/PDF
2. **High and Critical Risks Report**
    - Risks scored High or Critical
    - Includes treatment plan status
    - KRI status for each risk
    - Review due dates
    - Export to Excel/PDF
3. **Risk Heat Map**
    - Visual matrix: Likelihood (Y-axis) vs. Impact (X-axis)
    - Color-coded by risk level
    - Risk count in each cell
    - Click cell to see risks
    - Separate heat maps for Inherent, Current, and Target risk
    - Export as image or PDF
4. **Risks by Category**

- Count and percentage of risks per category
- Average risk score per category
- Bar chart visualization
- Drill-down to risk list
- Export to Excel/PDF

5. **Risks by Business Unit**
    - Risk distribution across business units
    - Count, average score, high/critical count per BU
    - Bar chart visualization
    - Drill-down to risk list
    - Export to Excel/PDF
6. **Risks by Owner**
    - Risks assigned to each owner
    - Count, risk levels, overdue reviews
    - Treatment plan status
    - Useful for 1-on-1 discussions
    - Export to Excel
7. **Risks Exceeding Appetite**
    - All risks currently exceeding risk appetite
    - Treatment plan status
    - Justification for acceptance (if accepted)
    - Priority for executive attention
    - Export to Excel/PDF
8. **Risks Due for Review**
    - Risks with review date in next 30/60/90 days
    - Overdue reviews highlighted
    - Risk owner and last review date
    - Sorted by due date
    - Export to Excel
9. **Treatment Plan Status Report**
    - All active treatment plans
    - Status, progress %, due date
    - Overdue treatments highlighted
    - Treatment owner
    - Linked risk details
    - Export to Excel
10. **KRI Dashboard Report**
    - All KRIs with current values and status
    - Threshold breaches highlighted
    - Trend indicators

    - Last measurement date
    - Linked risks
    - Export to Excel

What's NOT Included (Future Phases):

- Risk trend reports (historical changes)
- Risk velocity reports
- Risk concentration analysis
- Comparative analysis (year-over-year)
- Scenario analysis reports
- Risk maturity assessment
- Quantitative exposure reports (no quantitative assessment in Phase 1)
- Predictive risk reports
- Custom report builder

Why P0: Reports enable decision-making and communication; standard set covers most needs

---

✅ Risk Dashboards (P0)

What's Included:

Primary Risk Dashboard (Landing page):

Summary Cards (Top row):

- Total Active Risks (count)
- High/Critical Risks (count)
- Risks Exceeding Appetite (count)
- Overdue Reviews (count)
- Active Treatment Plans (count)
- KRIs in Red Status (count)

Charts (Middle section):

- Risk Distribution by Level (pie chart: Critical/High/Med/Low)
- Risk Distribution by Category (bar chart: top 10 categories)
- Risk Heat Map (small version, clickable for full view)
- Risks by Business Unit (bar chart: top 5 BUs)

Activity Feed (Right sidebar):

- Recently identified risks (last 10)
- Recent risk updates
- Upcoming reviews (next 7 days)
- Treatment plans completed
- KRI threshold breaches

Quick Actions (Left sidebar or top):

- Add New Risk button
- Request Risk Assessment button
- View My Risks
- View All Risks
- Reports menu

Filters:

- Date range filter (for activity feed)
- Business unit filter (affects all widgets)

My Risks Dashboard (Personal view):

- Risks I own (as risk owner)
- Treatment plans I own (as treatment owner)
- Assessments assigned to me
- My overdue items (reviews, treatments)
- My KRIs

What's NOT Included (Future Phases):

- Customizable dashboards (drag-drop widgets)
- Role-based dashboards (exec, BU leader, analyst)
- Real-time data refresh
- Interactive drill-downs
- Comparative dashboards
- Predictive indicators
- Mobile dashboard app

Why P0: Dashboard provides at-a-glance view; essential for daily use

---

1.8 User Management and Permissions

✅ Roles and Permissions (P0)

What's Included:

Risk Management Roles (Reuse existing role table):

1. **Risk Administrator**
    - Full access to all risk management features
    - Configure risk categories, appetite, KRI library
    - Manage all risks across organization
    - Generate all reports
    - Manage users and permissions
2. **Risk Manager**
    - Create/edit/delete risks

- Conduct risk assessments
- Create/edit treatment plans
- Manage KRIs
- Generate reports
- Approve risk assessment requests
- Cannot modify system configuration

3. **Risk Analyst**
    - Create/edit risks
    - Conduct assessments (assigned)
    - Update treatment plans (assigned)
    - Record KRI measurements
    - Generate reports
    - Cannot approve or configure
4. **Risk Owner** (Business user)
    - View risks they own
    - Update risk status and notes
    - Review risks (periodic reviews)
    - Create treatment plans for their risks
    - Update treatment progress
    - View reports for their risks
    - Cannot create new risks (request assessment instead)
5. **Business Unit Manager**
    - View all risks in their business unit
    - View reports for their BU
    - Approve risk acceptance in their BU
    - Assign risk owners in their BU
    - Cannot edit risk details directly
6. **Executive/Viewer**
    - View-only access to dashboards and reports
    - Cannot create or edit risks
    - Focus on high-level summaries

Permission Matrix:

Action	Admin	Manager	Analyst	Owner	BU Mgr	Exec
View risks	All	All	All	Own	BU	All
Create risk	✓	✓	✓	✗	✗	✗
Edit risk	✓	✓	✓	Own	✗	✗
Delete risk	✓	✓	✗	✗	✗	✗

Action	Admin	Manager	Analyst	Owner	BU Mgr	Exec
Assess risk	✓	✓	✓	✗	✗	✗
Create treatment	✓	✓	✓	Own	✗	✗
Update treatment	✓	✓	✓	Own	✗	✗
Accept risk	✓	✓	✗	✗	BU	✗
Manage KRIs	✓	✓	✓	✗	✗	✗
Enter KRI data	✓	✓	✓	✓	✗	✗
View reports	✓	✓	✓	Own	BU	✓
Export data	✓	✓	✓	✗	✓	✓
Configure system	✓	✗	✗	✗	✗	✗

Row-Level Security:

- Business unit filtering (users see risks for their BU)
- Risk owner filtering (owners see their risks)
- Configurable cross-BU visibility for risk team

What's NOT Included (Future Phases):

- Granular field-level permissions
- Custom role creation
- Dynamic permission assignment
- Temporary elevated permissions
- Permission delegation workflows

Why P0: Access control essential for security and data privacy; basic RBAC sufficient

---

1.9 Notifications and Alerts

✅ Risk Notifications (P0)

What's Included:

Email Notifications:

1. **Risk Ownership Notifications**
    - Risk assigned to you (as owner)
    - Risk details changed for your risks
    - Risk score increased significantly for your risks
2. **Assessment Notifications**
    - Risk assessment requested

    - Assessment assigned to you
    - Assessment due in 7 days
    - Assessment overdue

3. **Review Notifications**
    - Risk review due in 30/14/7 days
    - Risk review overdue
4. **Treatment Notifications**
    - Treatment plan assigned to you
    - Treatment due in 30/14/7 days
    - Treatment overdue
    - Treatment completed (to risk owner)
5. **Risk Appetite Notifications**
    - Risk now exceeds appetite (to risk owner and manager)
    - Critical risk identified (to management)
6. **KRI Notifications**
    - KRI threshold breached (Amber or Red)
    - KRI measurement overdue
7. **Approval Notifications**
    - Risk acceptance requires your approval
    - Risk assessment request requires your approval

In-App Notifications:

- Notification bell icon with badge count
- Notification center showing all notifications
- Mark as read/unread
- Notification types same as email

Notification Preferences:

- Users can opt-out of non-critical notifications
- Cannot opt-out of assigned tasks or approvals
- Digest option (daily summary instead of immediate)

What's NOT Included (Future Phases):

- SMS/text notifications
- Mobile push notifications
- Slack/Teams integration
- Customizable notification rules
- Escalation chains
- Notification scheduling (business hours only)

Why P0: Notifications drive action; email + in-app covers most needs

1.10 Administration

✅ System Configuration (P0)

What's Included:

Risk Categories Management:

- Add/edit/delete risk categories
- Add/edit/delete sub-categories
- Reorder categories
- Define risk appetite per category
- Activate/deactivate categories

Risk Assessment Configuration:

- Define likelihood scale labels (1-5)
- Define impact scale labels (1-5)
- Define financial impact ranges per level (optional)
- Define risk level thresholds (e.g., score 1-6 = Low, 8-12 = Medium, etc.)
- Customize risk matrix colors

Risk Appetite Configuration:

- Define overall risk appetite statement (rich text)
- Define risk tolerance per category (Low/Medium/High)
- Set approval workflow for appetite changes
- Version control for appetite statements

KRI Library Management:

- Add/edit/delete KRI definitions
- KRI templates/library
- Default thresholds

User and Role Management (Reuse existing):

- Assign users to roles
- Business unit assignments

Notification Settings:

- Configure notification triggers
- Email templates (basic customization)
- Reminder intervals

System Settings:

- Date formats
- Currency

- Fiscal year definition
- Data retention policies
- Audit log retention

What's NOT Included (Future Phases):

- Workflow designer (drag-drop)
- Custom field creation
- Advanced calculation formulas
- Integration with external systems configuration
- Branding/theme customization
- Multi-language support

Why P0: Basic configuration needed to tailor system to organization; advanced features can wait

---

2. Phase 1 Scope - SHOULD HAVE (P1)

These features add significant value but not critical for initial launch:

🔶 Risk Relationships (P1)

- Link related risks (risk A related to risk B)
- Parent-child risk hierarchy
- Contributing risk identification
- Visual relationship diagram (basic)

Why P1: Useful for understanding risk connections but can be added post-launch

---

🔶 Bulk Operations (P1)

- Bulk risk update (category, owner, status)
- Bulk KRI data entry
- Bulk review completion
- Bulk export

Why P1: Improves efficiency but not essential for launch

🔶 Advanced Search (P1)

- Full-text search across all risk fields
- Search filters (category, owner, score range, date range)
- Saved searches
- Search across risks, treatments, KRIs

Why P1: Nice to have but basic filtering and lists cover most needs initially

---

🔶 Risk Comments/Discussion (P1)

- Comment thread on risk records
- @ mentions
- Activity stream showing all changes and comments
- Email notifications for comments

Why P1: Facilitates collaboration but not critical for core functionality

---

🔶 Treatment Templates (P1)

- Pre-defined treatment plan templates by risk type
- Template library
- Clone treatment from another risk

Why P1: Speeds up treatment planning but manual entry acceptable initially

---

🔶 Risk Trend Indicators (P1)

- Risk score trending (increasing/stable/decreasing) based on last 2-3 assessments
- Visual trend arrows on risk lists
- Risk movement report (risks that increased/decreased)

Why P1: Provides historical context but single assessment sufficient for start

---

🔶 Enhanced Risk Statement Builder (P1)

- Guided risk statement creation (If/Then/Therefore wizard)
- Threat library (common threats by category)
- Impact library (common impacts)
- Auto-suggest based on category

Why P1: Helps consistency but free-text sufficient initially

🔶 Treatment Effectiveness Tracking (P1)

- Compare actual risk reduction to expected
- Treatment ROI calculation (manual)
- Treatment success rate by strategy

Why P1: Valuable for measuring program effectiveness but post-implementation metric

---

3. Phase 1 Scope - WON'T HAVE (P2/Future)

These features deferred to Phase 2 or later:

❌ Semi-Quantitative Assessment

- Financial impact ranges
- Percentage-based likelihood
- Expected loss calculations

Why Future: Qualitative sufficient for Phase 1; quantitative adds complexity

---

❌ Quantitative Risk Assessment

- ALE (Annualized Loss Expectancy)
- FAIR methodology
- Monte Carlo simulations
- SLE, ARO calculations

Why Future: Advanced capability requiring significant training and data

---

❌ Residual Risk Calculation

- Automatic calculation of residual risk after treatment
- Risk treatment waterfall charts
- Before/after comparisons

Why Future: Requires treatment completion and reassessment; Phase 2 feature

---

❌ Scenario Analysis

- Stress testing
- "What-if" scenarios
- Cascading risk modeling
- Business impact scenarios

Why Future: Advanced analytics requiring mature risk program

❌ Risk Aggregation

- Portfolio risk view
- Risk correlation analysis
- Concentration analysis
- Enterprise risk exposure calculation

Why Future: Requires significant data and sophisticated analytics

---

❌ Automated Data Collection

- KRI data from monitoring tools
- API integrations with security tools
- Automated risk identification
- Real-time risk scoring

Why Future: Requires integrations and technical complexity

❌ Predictive Analytics

- Machine learning risk prediction
- Risk forecasting
- Anomaly detection in KRIs
- Risk scoring algorithms

Why Future: Requires data history and ML capabilities

❌ Advanced Workflows

- Multi-level approval workflows
- Conditional routing
- Escalation automation
- SLA tracking

Why Future: Basic notifications sufficient initially

❌ Incident Integration

- Link incidents to risks
- Risk realization tracking
- Post-incident risk updates
- Incident-driven risk identification

Why Future: Depends on Incident Management module (not yet built)

❌ Vendor Risk Integration

- Vendor risk assessments
- Third-party risk scoring
- Vendor risk dashboard
- Fourth-party risk

Why Future: Vendor module not yet built

❌ Advanced Reporting

- Custom report builder
- Scheduled reports
- Report subscriptions
- Comparative analysis
- Trend reports
- Risk maturity assessment

Why Future: Standard reports sufficient initially

❌ Mobile Application

- Mobile-responsive is included
- Native mobile app is future

Why Future: Desktop/tablet browser sufficient for risk management

---

❌ External Integrations

- Threat intelligence feeds
- Industry benchmarking data
- Regulatory change alerts
- GRC tool integrations (Archer, ServiceNow)

Why Future: Requires partnerships and integration effort

---

4. Phase 1 Success Criteria

4.1 Functional Completeness

✅ Risk register operational with 100+ risks

✅ All P0 features implemented and tested

✅ Integration with Asset Management and Governance modules working

✅ 10 standard reports available

✅ KRI library with 20-30 indicators

✅ Risk appetite framework approved by board

4.2 User Adoption

✅ 50+ active users (risk owners, analysts, managers)

✅ 90% of identified risks have owners assigned

✅ 80% of high/critical risks have treatment plans

✅ 90% of users trained

✅ User satisfaction score > 7/10

4.3 Process Maturity

✅ Quarterly risk reviews established

✅ On-demand assessment process operational

✅ Risk appetite communicated organization-wide

✅ Monthly risk reporting to management

✅ Quarterly risk reporting to board/risk committee

4.4 Technical Performance

✅ Page load time < 2 seconds

✅ System supports 100 concurrent users

✅ 99% uptime during business hours

✅ Data backup and recovery tested

✅ Security testing passed (no critical vulnerabilities)

4.5 Integration Success

✅ 80% of risks linked to assets

✅ 70% of risks linked to controls

✅ Asset compliance calculation includes risk data

✅ Control assessments reference risk register

✅ Shared data (users, BUs, tags) working correctly

---

5. Phase 1 Deliverables

5.1 Software

- Risk Management Module (web application)
- Database schema (PostgreSQL)
- API endpoints (RESTful)
- Integration with Asset Management module
- Integration with Governance module
- 10 standard reports
- 2 dashboards (main + personal)

5.2 Documentation

- User Guide (50+ pages with screenshots)
- Administrator Guide (30+ pages)
- API Documentation (OpenAPI/Swagger)
- Database Schema Documentation
- Integration Guide
- Training Presentation Deck
- Video Tutorials (10-15 short videos)

5.3 Configuration

- Risk taxonomy (12 categories, 50+ sub-categories)
- Risk appetite statement template
- Risk assessment matrix (5x5)
- KRI library (30 KRIs with definitions and thresholds)
- Email notification templates
- Report templates

5.4 Training

- Administrator training (4 hours)
- Risk analyst training (8 hours)
- Risk owner training (4 hours)
- Executive briefing (1 hour)
- Training completion certificates

5.5 Testing

- Unit tests (80% code coverage)
- Integration tests (key workflows)
- User acceptance testing (10+ users, 50+ test cases)
- Performance testing (100 concurrent users)
- Security testing (OWASP Top 10, penetration testing)

---

6. Phase 1 Timeline (16 Weeks)

Weeks 1-2: Foundation

- Database schema design and review
- API design
- UI/UX wireframes
- Development environment setup
- Initial data model implementation

Deliverables: Approved schema, API spec, wireframes

Weeks 3-6: Core Development (Sprint 1-2)

- Risk register (CRUD)
- Risk taxonomy and categories
- Risk appetite framework
- Basic risk assessment (qualitative)
- User roles and permissions
- Integration with shared tables (users, BUs, audit logs)

Deliverables: Basic risk register functional

Weeks 7-10: Assessment and Treatment (Sprint 3-4)

- On-demand assessment requests
- Risk evaluation (appetite comparison)
- Treatment plans (all strategies)
- Treatment monitoring
- Asset integration (risk-asset linking)
- Control integration (risk-control linking)

Deliverables: Assessment and treatment features complete

Weeks 11-13: Monitoring and Reporting (Sprint 5)

- KRI management
- Risk review workflows
- Standard reports (10 reports)
- Dashboards (main + personal)
- Notifications (email + in-app)

Deliverables: Full feature set complete

Weeks 14-15: Testing and Documentation

- User acceptance testing
- Bug fixes
- Performance testing
- Security testing
- User guide and admin guide
- Training materials

Deliverables: Production-ready system, documentation complete

---

Week 16: Deployment and Training

- Production deployment

- Data migration (if needed)
- User training sessions
- Go-live support
- Hypercare period begins

Deliverables: System live, users trained

---

7. Phase 1 Resource Requirements

7.1 Development Team

- **Product Owner**: 1 person, 50% time (8 hours/week)
- **Scrum Master/Project Manager**: 1 person, 50% time (20 hours/week)
- **Backend Developers**: 2 people, full-time (16 weeks)
- **Frontend Developers**: 2 people, full-time (16 weeks)
- **QA/Test Engineer**: 1 person, full-time (last 8 weeks)
- **DevOps Engineer**: 1 person, 25% time (support)
- **UX Designer**: 1 person, 50% time (first 8 weeks)

7.2 Business/SME Resources

- **Risk Management SME**: 1 person, 25% time (advisory)
- **Compliance SME**: 1 person, 10% time (risk taxonomy, appetite)
- **Security SME**: 1 person, 10% time (cybersecurity risks, KRIs)
- **Business Unit Representatives**: 3-5 people, 10% time (requirements, UAT)

7.3 Infrastructure

- Database server (PostgreSQL 14+)
- Application server (Node.js/Python runtime)
- Web server (Nginx)
- Development, staging, production environments
- CI/CD pipeline (GitHub Actions or similar)

7.4 Tools and Licenses

- Development tools (IDEs, version control)
- Project management (Jira or similar)
- Documentation (Confluence or similar)
- Design tools (Figma or similar)
- Testing tools

---

8. Phase 1 Risks and Mitigation

Risk	Probability	Impact	Mitigation
Scope creep	High	High	Strict adherence to P0 list; change control process; defer P1 features
User resistance	Medium	High	Early stakeholder engagement; training; champions program; phased rollout
Integration issues	Medium	High	Early integration testing; API contracts; dedicated integration sprint
Resource availability	Medium	Medium	Backup resources identified; cross-training; prioritized backlog
Data quality	Medium	Medium	Data validation; data cleansing during migration; ongoing data governance
Performance issues	Low	Medium	Performance testing early; database optimization; caching strategy
Security vulnerabilities	Low	High	Security code review; penetration testing; regular updates

---

9. Phase 1 vs. Future Phases

What Phase 1 Enables:

✅ Systematic risk identification and registration

✅ Consistent risk assessment methodology

✅ Risk prioritization based on appetite

✅ Treatment plan tracking

✅ Basic risk monitoring via KRIs

✅ Standard risk reporting

✅ Integration with existing modules

✅ Foundation for advanced features

What Phase 2 Will Add:

🔮 Semi-quantitative and quantitative assessment

🔮 Residual risk tracking

🔮 Treatment effectiveness analytics

🔮 Risk aggregation and portfolio view

🔮 Scenario analysis

🔮 Advanced workflows

🔮 Predictive analytics

🔮 Custom reporting

🔮 External integrations

---

10. Approval and Sign-Off

Stakeholder Approval Required:

Executive Sponsor: ____________________ Date: ____________
Risk Management Lead: ____________________ Date: ____________
IT/Development Lead: ____________________ Date: ____________
Compliance Lead: ____________________ Date: ____________
Product Owner: ____________________ Date: ____________

Summary

Phase 1 delivers a **fully functional, production-ready Risk Management Module** with essential features:

- ✅ Risk register with qualitative assessment
- ✅ Risk appetite framework
- ✅ Treatment planning and monitoring
- ✅ KRI monitoring
- ✅ Integration with Assets and Governance
- ✅ Standard reporting and dashboards
- ✅ Role-based access control

This scope balances **immediate business value** with **manageable complexity**, establishing a solid foundation for advanced capabilities in future phases.

Risk Management Module - User Stories (Agile Format)

Epic Structure

- **Epic 1**: Risk Governance and Appetite (8 stories)

- **Epic 2**: Risk Identification and Registration (12 stories)
- **Epic 3**: Risk Assessment (10 stories)
- **Epic 4**: Risk Evaluation and Prioritization (6 stories)
- **Epic 5**: Risk Treatment (14 stories)
- **Epic 6**: Risk Monitoring (KRIs) (10 stories)
- **Epic 7**: Risk Review and Reassessment (6 stories)
- **Epic 8**: Integration with Asset Management (6 stories)
- **Epic 9**: Integration with Governance Module (6 stories)
- **Epic 10**: Reporting and Dashboards (14 stories)
- **Epic 11**: Notifications and Alerts (8 stories)
- **Epic 12**: Administration and Configuration (10 stories)

Total User Stories: 110
Estimated Story Points: ~850 points

Epic 1: Risk Governance and Appetite

User Story 1.1: Define Risk Appetite Statement

As a Chief Risk Officer
I want to create and document the organization's risk appetite statement
So that there is a clear, board-approved guideline for acceptable risk levels

Acceptance Criteria:

- Create risk appetite document with rich text editor
- Include sections: Overall statement, Risk tolerance by category, Approval section
- Version control (track changes over time)
- Approval workflow (submit → review → board approval)
- Digital signature capture for approvers
- Set effective date and next review date
- Status tracking: Draft, Under Review, Approved, Archived
- View risk appetite history (previous versions)
- Export to PDF
- Link to risk appetite from risk records

Story Points: 8
Priority: P0

User Story 1.2: Define Risk Tolerance by Category

As a Chief Risk Officer
I want to set risk tolerance levels for each risk category
So that risks can be evaluated against category-specific thresholds

Acceptance Criteria:

- For each risk category, define tolerance level: High, Medium, Low
- High tolerance = willing to accept high risks
- Medium tolerance = accept medium risks, mitigate high
- Low tolerance = accept only low risks, mitigate medium and high
- Default tolerance level for new categories
- Link tolerance to risk assessment matrix
- Tolerance levels influence risk evaluation (within/exceeds appetite)
- Display tolerance level on risk category selection
- Bulk update tolerance levels
- Audit trail of tolerance changes

Story Points: 5
Priority: P0

User Story 1.3: Approve Risk Appetite

As a Board Member
I want to review and approve the risk appetite statement
So that the organization operates within board-sanctioned risk boundaries

Acceptance Criteria:

- Receive notification when appetite statement submitted for approval
- View appetite statement with full formatting
- View previous version for comparison (if update)
- Approve, Reject, or Request Changes
- Add approval comments
- Digital signature captured
- Date of approval recorded
- Approved appetite becomes active on effective date
- All users notified of new/updated appetite
- Rejected appetite returns to draft with rejection reason

Story Points: 5
Priority: P0

User Story 1.4: View Current Risk Appetite

As a Risk Owner
I want to view the current risk appetite statement and tolerances
So that I understand what level of risk is acceptable for my risks

Acceptance Criteria:

- Access risk appetite from navigation menu
- Display current (active) appetite statement

- Display risk tolerance by category in table format
- Show effective date and next review date
- Show approval date and approvers
- Link to related guidance documents
- Mobile-responsive view
- Print-friendly format
- No edit capability (view-only for non-administrators)

Story Points: 3
Priority: P0

User Story 1.5: Schedule Risk Appetite Review

As a Risk Administrator
I want to schedule periodic reviews of the risk appetite
So that the appetite remains aligned with business strategy

Acceptance Criteria:

- Set review frequency (annual, biennial)
- Set next review date when appetite approved
- Automated reminder sent to CRO 90, 60, 30 days before review date
- Create new draft from current appetite for review
- Track review completion
- Dashboard shows appetite review status
- Overdue reviews flagged and escalated

Story Points: 5
Priority: P1

User Story 1.6: Manage Risk Categories

As a Risk Administrator
I want to define and manage the risk taxonomy
So that risks are consistently classified across the organization

Acceptance Criteria:

- Create risk categories (name, description, color code)
- Create sub-categories within categories
- Activate/deactivate categories (cannot delete if risks exist)
- Reorder categories (drag-and-drop or up/down arrows)
- Set risk tolerance per category
- Define category-specific attributes (optional)
- Category usage count (number of risks in each)
- Warning before deactivating category with risks

- Audit trail of category changes
- Pre-populated with 12 default categories

Story Points: 8
Priority: P0

User Story 1.7: Import Risk Taxonomy

As a Risk Administrator
I want to import a pre-defined risk taxonomy from a template
So that I can quickly set up categories based on industry standards

Acceptance Criteria:

- Select from taxonomy templates (Financial Services, Healthcare, Technology, Manufacturing, General)
- Preview taxonomy before import (categories and sub-categories)
- Option to import all or selected categories
- Merge with existing categories or replace
- Map to existing categories if names match
- Import includes category descriptions and suggested tolerance levels
- Import validation and error handling
- Import activity logged
- Success/failure summary report

Story Points: 8
Priority: P1

User Story 1.8: View Risk Appetite Dashboard

As an Executive
I want to see how our current risk exposure compares to risk appetite
So that I can ensure we're operating within acceptable boundaries

Acceptance Criteria:

- Dashboard showing: Total risks, Risks within appetite, Risks exceeding appetite
- Percentage within appetite (target: 90%+)
- Risks by category vs. category tolerance
- Color-coded indicators (green/amber/red)
- Trend over time (last 6 months)
- List of risks exceeding appetite with justification
- Drill-down to risk details
- Export dashboard to PDF
- Refresh data button

Story Points: 13
Priority: P1

Epic 2: Risk Identification and Registration

User Story 2.1: Create New Risk

As a Risk Analyst
I want to create a new risk record in the risk register
So that identified risks are documented for assessment and management

Acceptance Criteria:

- Access "Add Risk" form from dashboard or risk list
- Required fields: Risk title, Risk description, Risk category, Risk owner
- Optional fields: Sub-category, Risk statement (If/Then/Therefore), Business unit(s), Threat source, Vulnerabilities, Risk velocity, Early warning signs, Affected assets, Existing controls, Tags
- Risk ID auto-generated (e.g., RISK-2025-001)
- Rich text editor for description
- Date identified automatically set to current date
- Risk status defaults to "Active"
- Save as draft or submit
- Form validation with inline error messages
- Cancel button with unsaved changes warning
- Success message with link to view created risk

Story Points: 8
Priority: P0

User Story 2.2: Edit Risk Details

As a Risk Owner
I want to update the details of risks I own
So that risk information remains current and accurate

Acceptance Criteria:

- Access edit form from risk detail page
- Pre-populated with existing data
- All fields editable except: Risk ID, Date identified, Created by
- Version number increments on save
- Change reason field (optional but recommended)
- Changes logged in audit trail
- Last updated date and user recorded
- Notification sent to stakeholders if significant changes (score change, status change)

- Concurrent edit detection (warn if someone else editing)
- Auto-save draft every 2 minutes

Story Points: 5
Priority: P0

User Story 2.3: Delete/Archive Risk

As a Risk Manager
I want to remove risks that are no longer relevant
So that the risk register contains only active/valid risks

Acceptance Criteria:

- Delete button on risk detail page (permission-based)
- Confirmation dialog: "Are you sure? This action cannot be undone."
- Deletion reason required (dropdown: Duplicate, No longer relevant, Merged with another risk, Other)
- Soft delete (deleted_at timestamp, not physical deletion)
- Deleted risks not shown in default lists
- View deleted risks option (for administrators)
- Restore deleted risk capability (within 30 days)
- Audit trail preserved
- Related data handling: Treatment plans archived, KRIs unlinked
- Notification to risk owner

Story Points: 5
Priority: P0

User Story 2.4: Link Risks to Assets

As a Risk Analyst
I want to associate risks with the assets they affect
So that I understand what's at risk and can prioritize based on asset criticality

Acceptance Criteria:

- Multi-select asset picker in risk form
- Browse assets by type (Physical, Information, Application, Software, Supplier)
- Search assets by name or identifier
- Display asset criticality and business unit in picker
- Filter assets by type, business unit, criticality
- Show selected assets count
- View linked assets in risk detail page (table with asset name, type, criticality)
- Click asset to view asset details (opens asset module)
- Remove asset link (unlink)

- View all risks affecting an asset (from asset detail page in Asset Management module)
- Minimum 1 asset required for risk (configurable)

Story Points: 8
Priority: P0

User Story 2.5: Link Risks to Existing Controls

As a Risk Analyst
I want to identify which controls are already in place to mitigate a risk
So that I can assess the current risk level considering existing defenses

Acceptance Criteria:

- Multi-select control picker in risk form
- Browse controls from Unified Control Library
- Search controls by identifier, title, or description
- Filter controls by domain, implementation status
- Display control implementation status in picker
- Show selected controls count
- View linked controls in risk detail page (table with control ID, title, effectiveness rating)
- Click control to view control details (opens Governance module)
- Remove control link
- Control effectiveness rating (1-5 scale) influences current risk assessment
- View all risks addressed by a control (from control detail page in Governance module)

Story Points: 8
Priority: P0

User Story 2.6: View Risk Detail

As a Risk Owner
I want to view complete information about a risk
So that I can understand the risk and determine appropriate actions

Acceptance Criteria:

- Risk detail page with organized sections:
    - **Header**: Risk ID, Title, Status badge, Risk level badge
    - **Overview**: Description, Risk statement, Category, Sub-category, Owner, Business unit(s), Date identified
    - **Risk Scenario**: Threat source, Vulnerabilities, Risk velocity, Early warning signs
    - **Assessment**: Inherent risk (L/I/Score), Current risk (L/I/Score), Target risk (L/I/Score), Assessment date, Assessor, Confidence level
    - **Affected Entities**: Linked assets (table), Linked controls (table)
    - **Treatment**: Active treatment plans (cards/table), Treatment status

    - **Monitoring**: KRIs (table with current values), Review history
    - **Related Risks**: Linked related risks (if any)
    - **Attachments**: Uploaded files, documents
    - **Activity Log**: Recent changes, comments, updates
- Action buttons: Edit, Assess, Add Treatment, Add KRI, Review, Delete (permission-based)
- Export to PDF button
- Print-friendly layout
- Breadcrumb navigation
- Share link functionality

Story Points: 13
Priority: P0

User Story 2.7: Clone Risk

As a Risk Analyst
I want to create a new risk by copying an existing one
So that I can save time when identifying similar risks

Acceptance Criteria:

- "Clone Risk" button on risk detail page
- Creates new risk with copied data:
    - Category, Sub-category, Description template, Risk statement template, Threat source, Vulnerabilities, Linked assets (optional), Linked controls (optional), Tags
- Does NOT copy: Risk ID, Owner, Assessment scores, Treatment plans, KRI values, Review history
- New risk ID auto-generated
- "Cloned from RISK-XXXX" note added to description
- User must edit and assign owner before saving
- Saves as draft initially
- Success message: "Risk cloned. Please review and update details."

Story Points: 5
Priority: P1

User Story 2.8: Search Risks

As a Risk Analyst
I want to search for risks by keywords
So that I can quickly find specific risks

Acceptance Criteria:

- Global search bar in navigation header
- Searches across: Risk title, Description, Risk ID, Tags

- Autocomplete suggestions as user types (top 10 matches)
- Search results page with risk cards/table
- Highlight search term in results
- Sort results by relevance, date, risk score
- Filter search results by category, status, owner
- "No results found" message with suggestions
- Recent searches saved (last 5)
- Clear search button

Story Points: 8
Priority: P1

User Story 2.9: Filter Risk List

As a Risk Owner
I want to filter the risk list by various criteria
So that I can focus on specific subsets of risks

Acceptance Criteria:

- Filter panel (collapsible sidebar or top bar)
- Filter options:
  - Risk Category (multi-select checkboxes)
  - Risk Level (Critical, High, Medium, Low - multi-select)
  - Risk Status (Active, Monitoring, Closed, Accepted - multi-select)
  - Business Unit (multi-select)
  - Risk Owner (multi-select user picker)
  - Date Identified (date range)
  - Assessment Date (date range)
  - Treatment Status (With Treatment, Without Treatment, Treatment Overdue)
  - Appetite Status (Within, Exceeds)
  - My Risks Only (toggle)
- Apply multiple filters simultaneously
- Filter count displayed (e.g., "Showing 23 of 156 risks")
- Clear all filters button
- Save filter configuration (name and save for reuse)
- URL updates with filter parameters (shareable link)

Story Points: 13
Priority: P0

User Story 2.10: Sort Risk List

As a Risk Analyst
I want to sort risks by different attributes
So that I can prioritize my review and actions

Acceptance Criteria:

- Sortable columns in risk list table
- Sort options:
  - Risk Score (Inherent, Current, Target) - descending/ascending
  - Risk Level - Critical → Low or Low → Critical
  - Date Identified - newest/oldest
  - Last Updated - newest/oldest
  - Risk Title - A-Z or Z-A
  - Owner Name - A-Z
  - Review Due Date - soonest/latest
- Click column header to sort
- Sort direction indicator (up/down arrow)
- Multi-column sort (secondary sort by holding Shift)
- Remember last sort preference per user
- Default sort: Current Risk Score (descending)

Story Points: 5
Priority: P0

User Story 2.11: Tag Risks

As a Risk Analyst
I want to add tags to risks
So that I can categorize and find risks using custom labels

Acceptance Criteria:

- Tag input field in risk form (add/edit)
- Tag autocomplete from existing tags
- Create new tags inline
- Multiple tags per risk (no limit)
- Tag displayed as colored badges/chips
- Remove tag with X button
- Click tag to filter risks by that tag
- Tag management (admin): View all tags, Rename tags, Merge tags, Delete unused tags
- Tag usage count (number of risks per tag)
- Suggested tags based on category or keywords

Story Points: 5
Priority: P1

User Story 2.12: Export Risk Data

As a Risk Manager
I want to export risk data to Excel
So that I can perform offline analysis or share with stakeholders

Acceptance Criteria:

- Export button on risk list page
- Export current view (respects filters and sorting)
- Export all risks option
- Export format: Excel (.xlsx)
- Exported columns (configurable):
  - Risk ID, Title, Description, Category, Sub-category
  - Risk Owner, Business Unit
  - Date Identified, Last Updated
  - Inherent Risk (L/I/Score/Level)
  - Current Risk (L/I/Score/Level)
  - Target Risk (L/I/Score/Level)
  - Risk Status, Appetite Status
  - Treatment Status, Review Due Date
  - Tags, Affected Assets (count), Linked Controls (count)
- File naming: "Risk_Register_[Date]_[Time].xlsx"
- Download initiated immediately
- Export activity logged
- Progress indicator for large exports

Story Points: 8
Priority: P0

Epic 3: Risk Assessment

User Story 3.1: Conduct Qualitative Risk Assessment

As a Risk Analyst
I want to assess a risk's likelihood and impact using qualitative scales
So that I can determine the risk level and prioritize treatment

Acceptance Criteria:

- Access assessment form from risk detail page ("Assess Risk" button)
- Select assessment type: Inherent, Current, or Target
- Likelihood scale (1-5) with descriptions:
  - 1 - Rare: <10% chance in 12 months
  - 2 - Unlikely: 10-30% chance

    - 3 - Possible: 30-50% chance
    - 4 - Likely: 50-80% chance
    - 5 - Almost Certain: >80% chance
- Impact scale (1-5) with descriptions:
    - 1 - Negligible: Minimal impact
    - 2 - Minor: Limited impact
    - 3 - Moderate: Notable impact
    - 4 - Major: Significant impact
    - 5 - Catastrophic: Severe impact
- Impact category assessments (optional but recommended):
    - Financial Impact: Select 1-5 (with $ ranges per level)
    - Operational Impact: Select 1-5 (with downtime descriptions)
    - Reputational Impact: Select 1-5
    - Compliance Impact: Select 1-5
    - Safety Impact: Select 1-5
    - Overall impact = highest category impact or average
- Risk score auto-calculated: Likelihood × Impact (1-25)
- Risk level auto-assigned: Low (1-6), Medium (8-12), High (15-20), Critical (25)
- Confidence level: High, Medium, Low
- Assessment notes (text area for assumptions, evidence)
- Assessment date (defaults to today)
- Assessor (defaults to current user)
- Supporting documents upload
- Save assessment
- View assessment on risk matrix (visual plot)
- Assessment history table (view previous assessments)

Story Points: 13
Priority: P0

User Story 3.2: View Risk Assessment Matrix

As a Risk Analyst
I want to visualize risks on a likelihood vs. impact matrix
So that I can see the risk landscape at a glance

Acceptance Criteria:

- 5x5 matrix (Likelihood Y-axis, Impact X-axis)
- Color-coded cells:
    - Green: Low risk (scores 1-6)
    - Yellow: Medium risk (scores 8-12)
    - Orange: High risk (scores 15-20)
    - Red: Critical risk (score 25)

- Plot risks as dots/circles on matrix
- Risk count displayed in each cell
- Click cell to see list of risks in that cell
- Hover over risk dot to see risk title and ID
- Click risk dot to view risk details
- Toggle between Inherent, Current, and Target risk views
- Filter by category, business unit
- Legend explaining colors and scores
- Export matrix as image (PNG/PDF)

Story Points: 13
Priority: P0

User Story 3.3: Assess Inherent Risk

As a Risk Analyst
I want to assess risk before any controls are considered
So that I understand the worst-case scenario

Acceptance Criteria:

- Inherent risk assessment form (separate from current risk)
- Guidance: "Assess risk assuming no controls exist"
- Likelihood and Impact scales same as current risk
- Risk score and level calculated
- Inherent risk displayed prominently on risk detail page
- Inherent risk used for control effectiveness calculation
- Cannot assess inherent risk lower than current risk (validation warning)
- Assessment notes specific to inherent assessment
- Inherent risk plotted on matrix (separate view)

Story Points: 5
Priority: P0

User Story 3.4: Assess Current Risk

As a Risk Analyst
I want to assess risk considering existing controls
So that I know the actual current risk exposure

Acceptance Criteria:

- Current risk assessment form
- Guidance: "Assess risk with existing controls in place"
- Display linked controls with effectiveness ratings
- Control effectiveness influences assessment (guidance only, not automatic)

- Likelihood and Impact scales
- Risk score and level calculated
- Current risk displayed prominently on risk detail page
- Current risk compared to risk appetite (within/exceeds)
- Current risk used for prioritization
- Cannot assess current risk higher than inherent (validation warning)
- Assessment notes specific to current assessment

Story Points: 5
Priority: P0

User Story 3.5: Define Target Risk

As a Risk Owner
I want to set the desired target risk level after treatment
So that I have a clear goal for risk reduction

Acceptance Criteria:

- Target risk form (similar to assessment)
- Guidance: "Define desired risk level after treatment"
- Likelihood and Impact scales
- Risk score and level calculated
- Target risk should be ≤ current risk (validation warning if not)
- Target risk should align with risk appetite (guidance message)
- Gap analysis: Current Risk - Target Risk = Risk Reduction Needed
- Target risk drives treatment planning
- Treatment plan success measured against target
- Target risk displayed on risk detail page

Story Points: 5
Priority: P0

User Story 3.6: Configure Risk Assessment Matrix

As a Risk Administrator
I want to customize the risk assessment scales and matrix
So that the assessment method aligns with organizational preferences

Acceptance Criteria:

- Configuration page for risk assessment settings
- Customize likelihood scale:
    - Edit labels for each level (1-5)
    - Edit descriptions
    - Edit percentage ranges (optional)

- Customize impact scale:
    - Edit labels for each level (1-5)
    - Edit descriptions
    - Edit financial ranges per level (optional)
- Define risk level boundaries:
    - Low risk: scores X to Y (default 1-6)
    - Medium risk: scores X to Y (default 8-12)
    - High risk: scores X to Y (default 15-20)
    - Critical risk: score X (default 25)
- Define risk matrix colors (hex codes)
- Preview matrix with changes
- Save configuration
- Version control for assessment methodology
- Apply configuration to new assessments only (don't retroactively change old assessments)
- Export configuration for audit

Story Points: 13
Priority: P1

User Story 3.7: Record Assessment Assumptions

As a Risk Analyst
I want to document assumptions made during risk assessment
So that others understand the basis for likelihood and impact ratings

Acceptance Criteria:

- Assessment assumptions field (rich text)
- Prompt: "What assumptions did you make? What evidence supports this assessment?"
- Examples/guidance provided
- Assumptions displayed on risk detail page
- Assumptions included in assessment history
- Assumptions searchable
- Assumptions included in exported reports

Story Points: 3
Priority: P1

User Story 3.8: Track Assessment Confidence Level

As a Risk Analyst
I want to indicate my confidence in the risk assessment
So that stakeholders know how certain the ratings are

Acceptance Criteria:

- Confidence level dropdown: High, Medium, Low
- Guidance for each level:
    - High: Strong evidence, experienced assessor, clear scenario
    - Medium: Some evidence, moderate uncertainty
    - Low: Limited evidence, high uncertainty, emerging risk
- Confidence level displayed on risk detail page
- Low confidence risks flagged for additional analysis
- Filter risks by confidence level
- Confidence level included in reports

Story Points: 3
Priority: P1

User Story 3.9: Compare Risk Assessments Over Time

As a Risk Owner
I want to see how a risk's assessment has changed
So that I can track if the risk is increasing or decreasing

Acceptance Criteria:

- Assessment history table on risk detail page
- Columns: Assessment Date, Assessor, Type (Inherent/Current/Target), Likelihood, Impact, Score, Level, Confidence
- Sort by date (newest first)
- Highlight changes from previous assessment
- Trend indicator: ↑ Increasing, → Stable, ↓ Decreasing
- Line chart showing risk score over time
- Filter history by assessment type
- Compare two assessments side-by-side (select two rows)
- Export assessment history

Story Points: 8
Priority: P1

User Story 3.10: Link Assessment to Supporting Evidence

As a Risk Analyst
I want to attach documents supporting my risk assessment
So that the assessment is backed by evidence

Acceptance Criteria:

- Upload documents during assessment (PDF, Word, Excel, images)
- Link to existing evidence from evidence repository (Governance module)
- Multiple documents per assessment

- Document types: Assessment report, Data analysis, Industry research, Incident report, Other
- View attached documents on risk detail page
- Download documents
- Document version control
- Access control (confidential documents restricted)

Story Points: 8
Priority: P1

Epic 4: Risk Evaluation and Prioritization

User Story 4.1: Compare Risk to Appetite

As a Risk Manager
I want to see if a risk exceeds the organization's risk appetite
So that I can prioritize risks requiring immediate treatment

Acceptance Criteria:

- Appetite status calculated for each risk:
    - **Within Appetite** (Green): Current risk level acceptable per category tolerance
    - **Near Appetite** (Amber): Current risk approaching limits (e.g., Medium risk in Low tolerance category)
    - **Exceeds Appetite** (Red): Current risk unacceptable per category tolerance
- Appetite status badge on risk list and detail page
- Calculation logic:
    - If category tolerance = Low: Only Low risks within appetite
    - If category tolerance = Medium: Low and Medium risks within appetite
    - If category tolerance = High: All risk levels within appetite
- Automatic recalculation when risk assessment or appetite changes
- Dashboard widget: Risks exceeding appetite count
- Filter risks by appetite status
- Report: All risks exceeding appetite

Story Points: 8
Priority: P0

User Story 4.2: View High and Critical Risks

As a Risk Manager
I want to quickly access a list of high and critical risks
So that I can focus on the most significant threats

Acceptance Criteria:

- "High & Critical Risks" view in navigation menu

- Automatically filters to risks with High or Critical level
- Sort by risk score (descending) by default
- Display: Risk ID, Title, Category, Owner, Current Risk Score, Level, Treatment Status, Review Due Date
- Color coding by level (orange for High, red for Critical)
- Count displayed: "X High Risks, Y Critical Risks"
- Treatment status column: With Treatment, Without Treatment, Overdue
- Click risk to view details
- Export list to Excel
- Email list to management (on-demand)
- Scheduled weekly email to risk management team

Story Points: 5
Priority: P0

User Story 4.3: Prioritize Risks by Score

As a Risk Analyst
I want to see risks ranked by risk score
So that I can work on the highest-priority items first

Acceptance Criteria:

- Default risk list sorted by Current Risk Score (descending)
- Ties broken by Inherent Risk Score
- Risk level color coding in list
- Filter options remain available
- Exportable priority list
- "My Top Risks" view (my risks sorted by score)
- Priority number displayed (#1, #2, #3, etc.)
- Visual indicator for top 10 risks

Story Points: 3
Priority: P0

User Story 4.4: Create Risk Watchlist

As a Risk Manager
I want to flag specific risks for close monitoring
So that I can track priority risks separately

Acceptance Criteria:

- "Add to Watchlist" button on risk detail page
- Star/flag icon on risk in list view
- "My Watchlist" view showing flagged risks

- Watchlist per user (personal list)
- Remove from watchlist option
- Watchlist count displayed in navigation
- Email digest of watchlist risks (weekly)
- Watchlist included in personal dashboard

Story Points: 5
Priority: P1

User Story 4.5: View Risks by Category

As a Risk Manager
I want to see risk distribution across categories
So that I understand where risks are concentrated

Acceptance Criteria:

- "Risks by Category" report/dashboard
- Bar chart showing risk count per category
- Table with columns: Category, Total Risks, Critical, High, Medium, Low, Average Score
- Sort by risk count or average score
- Click category to view risks in that category
- Color-coded bars by average risk level
- Comparison to risk appetite tolerance per category
- Export chart and table
- Filter by business unit

Story Points: 8
Priority: P0

User Story 4.6: View Risks by Business Unit

As a Business Unit Manager
I want to see risks affecting my business unit
So that I can understand and manage my unit's risk exposure

Acceptance Criteria:

- "Risks by Business Unit" report
- Table: Business Unit, Total Risks, Critical, High, Medium, Low, Avg Score, Risks Exceeding Appetite
- Bar chart showing risk distribution
- Filter to my business unit only
- Click BU to view detailed risk list
- Compare BUs side-by-side
- Drill-down to category breakdown per BU

- Export to Excel
- Email to BU managers (scheduled monthly)

Story Points: 8
Priority: P0

Epic 5: Risk Treatment

User Story 5.1: Create Treatment Plan

As a Risk Owner
I want to create a treatment plan for a risk
So that I can document how the risk will be addressed

Acceptance Criteria:

- "Add Treatment Plan" button on risk detail page
- Treatment plan form with fields:
  - Treatment Plan ID (auto-generated)
  - Linked Risk (pre-populated)
  - Treatment Strategy: Mitigate, Transfer, Accept, Avoid (required, dropdown)
  - Treatment Description (rich text, required)
  - Responsible Person (treatment owner, required, user picker)
  - Supporting Team Members (optional, multi-select users)
  - Target Start Date (optional)
  - Target Completion Date (required)
  - Status: Planned, In Progress, Completed, On Hold, Cancelled (default: Planned)
  - Progress Percentage (0-100%, default: 0)
  - Budget Estimated (optional, currency)
  - Budget Actual (optional, currency)
  - Milestones (text list or bullet points)
  - Dependencies (text)
  - Success Criteria (text)
  - Notes (text)
- Strategy-specific fields (conditionally displayed):
  - If Mitigate: New controls to implement, Expected risk reduction (Target L/I)
  - If Transfer: Transfer mechanism (Insurance/Contract/Outsourcing), Insurance/Contract details
  - If Accept: Acceptance justification (required), Approved by, Approval date, Review date
  - If Avoid: Avoidance actions, Business impact, Approved by
- Form validation
- Save treatment plan
- Notification to treatment owner

- Treatment plan appears on risk detail page

Story Points: 13
Priority: P0

User Story 5.2: Update Treatment Plan Progress

As a Treatment Owner
I want to update the progress of my treatment plan
So that stakeholders know the current status

Acceptance Criteria:

- Edit treatment plan from risk detail page or treatment list
- Update fields: Status, Progress %, Actual start date, Actual completion date, Budget actual, Notes
- Progress percentage slider (0-100%) or manual entry
- Status change dropdown
- Add milestone completion notes
- Upload evidence of progress (documents, screenshots)
- Change log tracked (who updated, when, what changed)
- Notification to risk owner on significant updates (status change, completion)
- Last updated date displayed
- Visual progress bar on treatment card

Story Points: 8
Priority: P0

User Story 5.3: Complete Treatment Plan

As a Treatment Owner
I want to mark a treatment plan as completed
So that the risk can be reassessed with the new controls

Acceptance Criteria:

- "Mark as Completed" button on treatment plan
- Confirmation dialog: "Confirm treatment completion"
- Actual completion date captured (defaults to today)
- Progress automatically set to 100%
- Status changed to "Completed"
- Completion notes required
- Evidence of completion upload (optional but recommended)
- Notification to risk owner: "Treatment completed. Please reassess risk."
- Trigger risk reassessment workflow (optional)
- Treatment plan remains visible on risk but marked complete

- Completed treatments included in effectiveness reports

Story Points: 5
Priority: P0

User Story 5.4: Request Risk Acceptance

As a Risk Owner
I want to request formal acceptance of a risk
So that it's documented that the risk is being consciously retained

Acceptance Criteria:

- "Request Acceptance" option when creating treatment plan (Strategy = Accept)
- Acceptance form:
  - Risk to be accepted (pre-populated)
  - Business justification (required, text area)
  - Business reason/benefit (required)
  - Compensating controls (optional, text)
  - Monitoring plan (how will risk be monitored?)
  - Acceptance duration (date range or "until risk changes")
  - Approver selection (must be senior to risk owner, user picker)
  - Supporting documents (optional)
- Submit for approval
- Notification sent to approver
- Acceptance status: Pending, Approved, Rejected
- Approval workflow (see next story)
- Approved acceptances displayed on risk with badge
- Acceptance review reminders (90 days before expiry)

Story Points: 8
Priority: P0

User Story 5.5: Approve Risk Acceptance

As a Business Unit Manager
I want to review and approve risk acceptance requests
So that I ensure risks are consciously accepted with proper justification

Acceptance Criteria:

- Notification when acceptance request submitted
- View acceptance request with full details
- View risk details (score, category, assessment)
- Review justification and compensating controls
- Actions: Approve, Reject, Request More Information

- Approval comments (required for rejection)
- Digital signature or approval confirmation
- Approval date recorded
- Approved by field updated
- Notification to risk owner: Approved or Rejected with reason
- Approved acceptance activates (risk status = "Accepted")
- Rejected acceptance returns to risk owner
- Audit trail of approval decision

Story Points: 8
Priority: P0

User Story 5.6: Track Insurance for Risk Transfer

As a Risk Owner
I want to record insurance details when transferring risk
So that I have a record of risk transfer mechanisms

Acceptance Criteria:

- When treatment strategy = Transfer and mechanism = Insurance
- Insurance details form:
    - Policy Number (text)
    - Insurer Name (text)
    - Coverage Amount (currency)
    - Premium Amount (currency)
    - Deductible (currency)
    - Policy Effective Date
    - Policy Renewal Date
    - Coverage Description (text)
    - Policy Document (file upload)
- View insurance details on treatment plan
- Insurance renewal reminder (90, 60, 30 days before renewal)
- Link multiple risks to same policy (if applicable)
- Report: All risks with insurance coverage
- Insurance expiry dashboard

Story Points: 8
Priority: P1

User Story 5.7: Define Mitigation Controls

As a Risk Owner
I want to specify which controls will be implemented to mitigate a risk
So that the treatment plan is clear and measurable

Acceptance Criteria:

- When treatment strategy = Mitigate
- "New Controls to Implement" section
- Option 1: Link to existing controls from Governance module (select from control library, mark as "to be enhanced")
- Option 2: Describe new controls as free text
- Option 3: Create new control proposal (creates draft control in Governance module)
- Expected risk reduction:
  - Target Likelihood after controls (1-5)
  - Target Impact after controls (1-5)
  - Target Risk Score calculated
  - Shows Current Risk → Target Risk with visual indicator
- Control implementation plan (text)
- Link treatment to control implementation in Governance module
- Treatment completion should update control status

Story Points: 8
Priority: P0

User Story 5.8: View All Treatment Plans

As a Risk Manager
I want to see all active treatment plans across the organization
So that I can monitor overall risk treatment progress

Acceptance Criteria:

- "Treatment Plans" view in navigation
- Table columns: Treatment ID, Linked Risk, Risk Title, Strategy, Owner, Status, Progress %, Target Completion Date, Days Until Due/Overdue
- Color coding: Green (on track), Yellow (due soon), Red (overdue)
- Filter by: Status, Strategy, Owner, Business Unit, Risk Category
- Sort by: Due date, Progress, Risk score
- Search by treatment or risk title
- Click treatment to view details
- Click risk to view risk details
- Export to Excel
- Dashboard summary: Total treatments, In Progress, Completed, Overdue

Story Points: 8
Priority: P0

User Story 5.9: View My Treatment Plans

As a Treatment Owner
I want to see a list of treatment plans assigned to me
So that I can manage my responsibilities

Acceptance Criteria:

- "My Treatments" view (personal dashboard widget or dedicated page)
- Shows treatments where I am the owner
- Same columns as all treatments view
- Highlight overdue and due soon
- Sort by due date (default)
- Quick action buttons: Update Progress, Mark Complete
- Count displayed: "You have X active treatment plans"
- Filter by status
- Export my treatments
- Calendar view option (treatments on timeline)

Story Points: 5
Priority: P0

User Story 5.10: Receive Treatment Due Date Reminders

As a Treatment Owner
I want to receive reminders when treatment plans are due
So that I don't miss deadlines

Acceptance Criteria:

- Automated email notifications:
    - 30 days before due date
    - 14 days before due date
    - 7 days before due date
    - On due date
    - 1 day overdue, then weekly while overdue
- Email content: Treatment ID, Risk title, Current progress %, Due date, Link to treatment
- In-app notification (same schedule)
- Escalation notification to risk owner if treatment overdue >14 days
- Opt-out option for non-overdue reminders (but not for overdue)
- Reminder settings in user preferences

Story Points: 5
Priority: P0

User Story 5.11: View Treatment Plan Dashboard

As a Risk Manager
I want to see treatment plan metrics on a dashboard
So that I can monitor treatment effectiveness

Acceptance Criteria:

- Treatment dashboard showing:
  - **Summary Cards**: Total Treatment Plans, In Progress, Completed (this month), Overdue
  - **Treatment by Strategy**: Pie chart (Mitigate, Transfer, Accept, Avoid)
  - **Treatment by Status**: Bar chart (Planned, In Progress, Completed, On Hold, Cancelled)
  - **Completion Trend**: Line chart showing treatments completed per month (last 12 months)
  - **Overdue Treatments**: List of overdue treatments with owner and days overdue
  - **Progress Breakdown**: Histogram showing progress distribution (0-25%, 26-50%, 51-75%, 76-100%)
- Filters: Date range, Business unit, Risk category
- Drill-down from charts to treatment list
- Export dashboard to PDF
- Refresh button

Story Points: 13
Priority: P1

User Story 5.12: Link Treatment to Project

As a Risk Owner
I want to link a treatment plan to a project
So that risk treatment is integrated with project management

Acceptance Criteria:

- Treatment plan form has "Related Project" field (text)
- Enter project name or ID
- Link to external project management tool (URL)
- Display project info on treatment plan
- Multiple treatments can link to same project
- View all treatments for a project
- Project status influences treatment status (if integration available)

Story Points: 5
Priority: P2 (Nice to have)

User Story 5.13: Calculate Treatment Budget Variance

As a Risk Manager
I want to track treatment plan budget vs. actual costs
So that I can manage risk treatment investments

Acceptance Criteria:

- Budget fields: Estimated, Actual
- Variance calculated: Actual - Estimated
- Variance percentage: (Variance / Estimated) × 100%
- Color coding: Green (under budget), Yellow (within 10%), Red (over budget)
- Budget variance report showing all treatments
- Filter by variance status
- Total budget allocated vs. spent (org-wide)
- Budget by risk category

Story Points: 5
Priority: P2 (Nice to have)

User Story 5.14: Archive Completed Treatments

As a Risk Administrator
I want to archive old completed treatment plans
So that active views remain uncluttered

Acceptance Criteria:

- Auto-archive treatments completed > 6 months ago (configurable)
- Manual archive option for any completed treatment
- Archived treatments not shown in default views
- "View Archived" toggle to show archived treatments
- Restore archived treatment if needed
- Archived treatments included in historical reports
- Archive date recorded

Story Points: 5
Priority: P2 (Nice to have)

Epic 6: Risk Monitoring (KRIs)

User Story 6.1: Create Key Risk Indicator (KRI)

As a Risk Manager
I want to define a KRI for monitoring a risk
So that I can track early warning signs of risk changes

Acceptance Criteria:

- "Add KRI" button on risk detail page or KRI library page
- KRI form fields:
    - KRI ID (auto-generated)
    - KRI Name (required)
    - KRI Description
    - KRI Type: Leading Indicator, Lagging Indicator (required)
    - Linked Risk(s) (multi-select, at least one required)
    - Risk Category (optional, for library KRIs)
    - Measurement Frequency: Daily, Weekly, Monthly, Quarterly (required)
    - Data Source Description (where data comes from)
    - Calculation Method (formula or description)
    - Unit of Measurement: %, Count, Currency, Days, Ratio, Other (required)
    - Thresholds:
        - Target (Green) value (required)
        - Warning (Amber) value (required)
        - Critical (Red) value (required)
        - Threshold Direction: Lower is better / Higher is better (required)
    - KRI Owner (user picker, required)
    - Notification Recipients (multi-select users, who gets alerts)
- Form validation
- Save KRI
- KRI added to KRI library
- KRI appears on linked risk(s) detail page
- Notification to KRI owner

Story Points: 8
Priority: P0

User Story 6.2: Record KRI Measurement

As a KRI Owner
I want to enter the current value for a KRI
So that the risk monitoring data is up-to-date

Acceptance Criteria:

- "Record Measurement" button on KRI detail or from KRI list
- Measurement form:
    - KRI (pre-selected)
    - Measurement Date (defaults to today, editable)
    - Measured Value (required, numeric)
    - Unit displayed (from KRI definition)
    - Notes (optional, context for this measurement)
    - Measured By (defaults to current user)

- Status automatically calculated based on thresholds:
  - Green if value meets/exceeds target
  - Amber if value in warning range
  - Red if value in critical range
- Save measurement
- Measurement added to KRI history
- Current value and status updated on KRI
- If status = Red, trigger threshold breach alert
- Measurement date cannot be in future
- Duplicate date warning (measurement already exists for this date)

Story Points: 8
Priority: P0

User Story 6.3: View KRI Dashboard

As a Risk Manager
I want to see all KRIs with their current status
So that I can monitor risk indicators at a glance

Acceptance Criteria:

- KRI dashboard showing:
  - **Summary Cards**: Total KRIs, Green Status, Amber Status, Red Status, Overdue Measurements
  - **KRI Status Table**: KRI Name, Linked Risk(s), Current Value, Status (colored badge), Last Measured, Trend, Owner
  - **KRIs by Status**: Pie chart (Green/Amber/Red)
  - **Threshold Breaches**: List of KRIs currently in Red status
  - **Recent Measurements**: Activity feed of latest KRI updates
  - **Overdue Measurements**: KRIs past measurement frequency date
- Sort table by: Status (Red first), Name, Last Measured
- Filter by: Status, Risk category, KRI type, Owner
- Click KRI to view details and history
- Export to Excel
- Refresh data button

Story Points: 13
Priority: P0

User Story 6.4: View KRI Trend

As a Risk Owner
I want to see how a KRI has changed over time
So that I can identify improving or deteriorating trends

Acceptance Criteria:

- KRI detail page shows:
  - Current value with status badge
  - Trend indicator: ↑ Deteriorating, → Stable, ↓ Improving
  - Line chart showing KRI values over time (last 12 months or last 20 measurements)
  - Threshold lines on chart (Target, Warning, Critical)
  - Color-coded zones on chart (Green, Amber, Red)
  - Measurement history table (Date, Value, Status, Measured By, Notes)
- Trend calculated:
  - Compare current value to previous 3 measurements
  - Deteriorating if moving away from target
  - Improving if moving toward target
  - Stable if within 10% variance
- Export chart as image
- Export measurement history to Excel

Story Points: 13
Priority: P0

User Story 6.5: Receive KRI Threshold Breach Alert

As a KRI Owner
I want to be notified when a KRI breaches a threshold
So that I can take immediate action

Acceptance Criteria:

- Automated alert when KRI status changes to Amber or Red
- Email notification to:
  - KRI owner
  - Notification recipients (defined in KRI)
  - Risk owner(s) of linked risks
  - Risk manager (if Red)
- Email content: KRI name, Current value, Status, Threshold breached, Linked risk(s), Link to KRI detail
- In-app notification
- Alert only sent once per threshold breach (not repeatedly)
- Clear alert option (acknowledge)
- Alert when status returns to Green (recovery notification)
- Alert history log

Story Points: 5
Priority: P0

User Story 6.6: Create KRI from Template

As a Risk Manager
I want to select a KRI from a pre-defined library
So that I can quickly set up common indicators

Acceptance Criteria:

- "Add from Template" button in KRI section
- KRI template library showing 30+ pre-defined KRIs organized by category:
  - Cybersecurity (10 KRIs)
  - Operational (8 KRIs)
  - Compliance (6 KRIs)
  - Financial (4 KRIs)
  - Third-Party (2 KRIs)
- Template includes: Name, Description, Type, Frequency, Calculation, Unit, Suggested Thresholds
- Preview template before selection
- Select template
- Pre-populate KRI form with template data
- User can edit before saving
- Link to risk(s) before saving
- Assign owner
- Save KRI
- Template-based KRIs can be customized after creation

Story Points: 8
Priority: P1

User Story 6.7: Link KRI to Multiple Risks

As a Risk Manager
I want to associate one KRI with multiple risks
So that a single indicator can monitor several related risks

Acceptance Criteria:

- Multi-select risk picker when creating/editing KRI
- Display all linked risks on KRI detail page
- Display all KRIs on each linked risk detail page
- Remove risk link (unlink) without deleting KRI
- KRI threshold breach notifies all linked risk owners
- View all risks using a KRI (from KRI detail)
- View all KRIs for a risk (from risk detail)
- Search KRIs by linked risk

Story Points: 5
Priority: P0

User Story 6.8: View Overdue KRI Measurements

As a Risk Manager
I want to see which KRIs have not been measured recently
So that I can ensure monitoring is current

Acceptance Criteria:

- "Overdue Measurements" dashboard widget
- Shows KRIs where:
  - Last measurement date + frequency < current date
  - Example: Monthly KRI last measured 35 days ago = overdue
- Table columns: KRI Name, Frequency, Last Measured, Days Overdue, Owner
- Sort by days overdue (most overdue first)
- Click KRI to record measurement
- Notification to KRI owner when overdue
- Escalation to risk manager if overdue > 2× frequency (e.g., monthly KRI overdue >60 days)
- Filter by owner, risk category
- Export overdue list

Story Points: 5
Priority: P0

User Story 6.9: Configure KRI Thresholds

As a Risk Manager
I want to adjust KRI thresholds based on changing circumstances
So that alerts remain relevant and actionable

Acceptance Criteria:

- Edit KRI form allows threshold changes
- Change thresholds: Target, Warning, Critical
- Reason for change (text field, optional but recommended)
- Threshold change logged in KRI history
- Historical measurements not re-evaluated (status at time of measurement preserved)
- New measurements use new thresholds
- Notification to stakeholders if thresholds significantly changed
- Threshold history viewable (who changed, when, old vs. new values)

Story Points: 5
Priority: P1

User Story 6.10: Export KRI Data

As a Risk Analyst
I want to export KRI measurements for analysis
So that I can perform statistical analysis or trending

Acceptance Criteria:

- Export button on KRI list and detail pages
- Export current KRI values (all KRIs) to Excel
- Export measurement history for selected KRI(s) to Excel
- Exported data includes: KRI Name, Date, Value, Status, Thresholds, Notes, Measured By
- Export date range selectable
- Export format: One sheet per KRI or combined sheet
- File naming: "KRI_Export_[Date].xlsx"
- Export activity logged

Story Points: 5
Priority: P1

Epic 7: Risk Review and Reassessment

User Story 7.1: Schedule Risk Review

As a Risk Administrator
I want to define review frequencies based on risk level
So that risks are reviewed appropriately

Acceptance Criteria:

- Configuration page for review frequencies
- Define review frequency by risk level:
  - Critical: Quarterly (default)
  - High: Semi-annually (default)
  - Medium: Annually (default)
  - Low: Biennially (default)
- Override frequency per individual risk (if needed)
- Next review date auto-calculated:
  - At risk creation: Today + Frequency
  - After review: Review Date + Frequency
  - After risk level change: Recalculate based on new level
- Display next review date on risk detail page
- Include in risk list table

Story Points: 5
Priority: P0

User Story 7.2: Receive Risk Review Reminder

As a Risk Owner
I want to be reminded when my risks are due for review
So that I don't miss review deadlines

Acceptance Criteria:

- Automated email reminders:
  - 30 days before review due
  - 14 days before review due
  - 7 days before review due
  - On review due date
  - Weekly while overdue
- Email content: Risk ID, Risk title, Current risk level, Last review date, Next review due date, Link to risk
- In-app notification (same schedule)
- "My Risks Due for Review" dashboard widget
- Count of overdue reviews displayed prominently
- Escalation to risk manager if review overdue >30 days

Story Points: 5
Priority: P0

User Story 7.3: Conduct Risk Review

As a Risk Owner
I want to review a risk and update it if necessary
So that risk information remains accurate

Acceptance Criteria:

- "Conduct Review" button on risk detail page
- Review checklist/wizard:
  - Step 1: Review risk description - Still accurate? (Yes/No, if No → edit)
  - Step 2: Review affected assets - Any changes? (Yes/No, if Yes → update list)
  - Step 3: Review existing controls - Still effective? (Yes/No, if No → reassess or update controls)
  - Step 4: Review risk assessment - Has likelihood or impact changed? (Yes/No, if Yes → reassess)
  - Step 5: Review treatment plan - Is treatment on track? (Yes/No, if No → update treatment)
  - Step 6: Review KRIs - Are KRIs being measured? Are thresholds appropriate? (Yes/No, if No → update KRIs)
  - Step 7: Review risk status - Should status change? (Active, Monitoring, Closed)
  - Step 8: Overall review notes (text area for observations, changes, decisions)

- Option to trigger reassessment if significant changes identified
- Review completion date recorded
- Next review date calculated
- Review history log (who reviewed, when, summary of changes)
- Notification to risk manager that review completed
- Mark review as complete
- Dashboard updated (removes from "due for review" list)

Story Points: 13
Priority: P0

User Story 7.4: Reassess Risk

As a Risk Analyst
I want to perform a new risk assessment
So that the risk rating reflects current conditions

Acceptance Criteria:

- "Reassess" button on risk detail page
- Opens assessment form (same as initial assessment)
- Previous assessment values shown for reference (side-by-side or in help text)
- Conduct new assessment:
  - New likelihood rating
  - New impact rating
  - New risk score and level calculated
  - Confidence level
  - Assessment notes (what changed?)
- Compare to previous assessment:
  - Show change in score (e.g., "+3" if score increased)
  - Show trend direction (↑/→/↓)
- Save new assessment
- Risk score and level updated on risk detail
- Assessment added to history
- If significant change (±5 points or level change), notify stakeholders
- If risk level increases, suggest reviewing treatment plan
- Risk matrix updated with new position

Story Points: 8
Priority: P0

User Story 7.5: Close Risk

As a Risk Owner
I want to close a risk that is no longer relevant
So that the risk register reflects current threats

Acceptance Criteria:

- "Close Risk" button on risk detail page
- Confirmation dialog: "Are you sure you want to close this risk?"
- Closure form:
  - Closure reason (dropdown): Risk Mitigated, No Longer Applicable, Merged with Another Risk, Avoided, Other
  - Closure notes (text area, required)
  - Final assessment (optional but recommended)
- Risk status changed to "Closed"
- Closure date recorded
- Closed by field updated
- Treatment plans automatically marked complete or cancelled
- KRI monitoring stopped (but history preserved)
- Closed risks removed from active views (default)
- "View Closed Risks" toggle to show them
- Reopen risk option (if closed in error)
- Notification to stakeholders
- Audit trail

Story Points: 8
Priority: P0

User Story 7.6: View Risk Review History

As a Risk Manager
I want to see the review history for a risk
So that I can verify review compliance

Acceptance Criteria:

- "Review History" section on risk detail page
- Table showing: Review Date, Reviewer, Review Outcome, Changes Made, Next Review Due
- Review outcome: No Changes, Minor Updates, Reassessed, Major Changes
- Click review to see detailed notes
- Filter reviews by date range
- Export review history
- Visual timeline of reviews
- Highlight overdue reviews (missed review dates)

Story Points: 5
Priority: P1

Epic 8: Integration with Asset Management

User Story 8.1: View Risks Affecting an Asset

As an Asset Manager
I want to see all risks associated with an asset
So that I understand the risk exposure of that asset

Acceptance Criteria:

- "Risks" tab on Asset detail page (in Asset Management module)
- Table showing: Risk ID, Risk Title, Category, Current Risk Level, Status, Risk Owner
- Sort by risk level (Critical first)
- Color-coded risk levels
- Risk count displayed: "This asset is affected by X risks (Y High/Critical)"
- Click risk to view risk details (opens Risk Management module)
- Filter risks by category, status
- Export risk list for asset
- If no risks: Message "No risks identified for this asset. Consider conducting a risk assessment."

Story Points: 8
Priority: P0

User Story 8.2: View Assets Affected by a Risk

As a Risk Owner
I want to see all assets affected by my risk
So that I can understand the scope of potential impact

Acceptance Criteria:

- "Affected Assets" section on Risk detail page
- Table showing: Asset Name, Asset Type, Criticality, Business Unit, Owner
- Asset count displayed
- Color-coded criticality (Critical assets highlighted)
- Click asset to view asset details (opens Asset Management module)
- Add/remove asset links (edit mode)
- Filter assets by type, criticality, business unit
- Export asset list
- Visual indicator if risk affects critical assets (warning icon)

Story Points: 5
Priority: P0

User Story 8.3: Calculate Asset Risk Score

As an Asset Manager
I want to see a composite risk score for an asset
So that I can prioritize asset security investments

Acceptance Criteria:

- Asset risk score calculated as:
  - Sum of all risk scores affecting the asset, OR
  - Highest risk score (if conservative approach), OR
  - Weighted average (asset criticality × risk scores)
- Display asset risk score on Asset detail page (in Asset Management module)
- Risk score badge with color coding
- Comparison: Asset inherent risk vs. current risk
- Asset risk trend (increasing/stable/decreasing)
- Factor in control effectiveness (if controls linked)
- Dashboard: Assets by risk score (highest risk assets)
- Filter assets by risk score range

Story Points: 13
Priority: P1

User Story 8.4: Identify High-Risk Assets

As a Security Manager
I want to see which assets have the highest risk exposure
So that I can prioritize protection efforts

Acceptance Criteria:

- "High-Risk Assets" report
- Table: Asset Name, Type, Criticality, Risk Count, Highest Risk Level, Composite Risk Score
- Sort by composite risk score (descending)
- Combination of asset criticality + risk levels = priority score
- Critical assets with high risks at top
- Filter by asset type, business unit
- Color coding by priority
- Click asset to see risk details
- Export to Excel
- Dashboard widget: Top 10 High-Risk Assets
- Recommendation: "These assets require immediate attention"

Story Points: 13
Priority: P1

User Story 8.5: Trigger Risk Assessment from Asset Creation

As an Asset Manager
I want to be prompted to assess risks when adding a critical asset
So that risks are identified proactively

Acceptance Criteria:

- When creating/editing asset with Criticality = Critical or High
- Prompt/notification: "This is a high-value asset. Would you like to initiate a risk assessment?"
- Options: "Yes, request assessment now" or "No, I'll do it later"
- If Yes: Opens risk assessment request form (pre-populated with asset details)
- If No: Reminder sent after 7 days if no risk assessment initiated
- Track asset-risk assessment linkage
- Dashboard: Assets without risk assessments (critical/high assets only)

Story Points: 8
Priority: P1

User Story 8.6: Filter Risks by Asset Type

As a Risk Analyst
I want to view risks grouped by asset type
So that I can focus on specific technology or business areas

Acceptance Criteria:

- "Risks by Asset Type" view/report
- Group risks by: Physical Assets, Information Assets, Applications, Software, Suppliers, Not Linked to Assets
- Count of risks per asset type
- Bar chart visualization
- Click asset type to see risk list
- Filter by risk level, category
- Export report
- Useful for technology-specific risk analysis (e.g., "Show me all application risks")

Story Points: 8
Priority: P1

Epic 9: Integration with Governance Module

User Story 9.1: View Controls Mitigating a Risk

As a Risk Owner
I want to see which controls are protecting against my risk
So that I understand the current defense posture

Acceptance Criteria:

- "Existing Controls" section on Risk detail page
- Table showing: Control ID, Control Title, Domain, Implementation Status, Effectiveness Rating, Owner
- Control count displayed
- Color-coded implementation status
- Click control to view control details (opens Governance module)
- Add/remove control links (edit mode)
- Filter controls by domain, status
- Control effectiveness influences current risk assessment
- Visual indicator if controls are not implemented or ineffective (warning)
- Export control list

Story Points: 5
Priority: P0

User Story 9.2: View Risks Addressed by a Control

As a Control Owner
I want to see which risks a control is mitigating
So that I understand the control's importance

Acceptance Criteria:

- "Risks Addressed" tab on Control detail page (in Governance module)
- Table showing: Risk ID, Risk Title, Category, Current Risk Level, Status, Risk Owner
- Risk count displayed: "This control mitigates X risks"
- Sort by risk level (Critical first)
- Click risk to view risk details (opens Risk Management module)
- If control fails assessment: Highlight that risks may be exposed
- Export risk list for control
- Useful for prioritizing control implementation (controls protecting most/highest risks = priority)

Story Points: 5
Priority: P0

User Story 9.3: Identify Control Gaps

As a Compliance Officer
I want to see risks that lack adequate controls
So that I can prioritize control implementation

Acceptance Criteria:

- "Control Gap Analysis" report
- Shows risks with:
  - No linked controls, OR
  - Linked controls not implemented, OR
  - Linked controls with low effectiveness (<60%)
- Table: Risk ID, Title, Level, Affected Assets, Control Count, Highest Control Effectiveness, Gap Severity
- Gap Severity = Risk Level × Control Deficiency
- Sort by gap severity (highest first)
- Filter by risk category, business unit
- Recommended actions for each gap
- Export report
- Dashboard widget: Risks with Control Gaps (count)

Story Points: 13
Priority: P1

User Story 9.4: Link Treatment Plan to Control Implementation

As a Risk Owner
I want to link my risk treatment to a control implementation
So that treatment and control efforts are coordinated

Acceptance Criteria:

- In treatment plan form (when strategy = Mitigate)
- "Link to Control Implementation" option
- Select existing control to enhance OR create new control proposal
- If new control: Opens control creation form (in Governance module)
- Treatment completion date should align with control implementation date
- Treatment status synced with control implementation status
- View linked control from treatment plan
- View linked treatment plan from control detail
- Notification when linked control is implemented
- Treatment plan verification includes control testing
- Dashboard: Treatments linked to controls vs. standalone treatments

Story Points: 8
Priority: P1

User Story 9.5: Update Risk When Control Fails Assessment

As a Risk Analyst
I want to be notified when a control protecting my risk fails assessment
So that I can reassess the risk

Acceptance Criteria:

- When control assessment result = "Non-Compliant" or "Failed"
- Identify all risks linked to that control
- Automated notification to risk owners: "Control [ID] failed assessment. This control protects Risk [ID]. Consider reassessing your risk."
- Notification includes: Control details, Assessment findings, Link to risk, Suggestion to re-assess
- Create task/reminder to reassess risk
- Dashboard alert: "Risks requiring reassessment due to control failures"
- Risk detail page shows warning badge if linked control failed
- Option to automatically increase risk likelihood by 1 level (configurable)

Story Points: 8
Priority: P1

User Story 9.6: Generate Risk-Control Coverage Matrix

As a Compliance Officer
I want to see a matrix of risks and controls
So that I can verify comprehensive coverage

Acceptance Criteria:

- "Risk-Control Matrix" report
- Matrix view: Risks (rows) × Controls (columns)
- Cell indicates: Control protects this risk (checkmark), Empty if no relationship
- Color coding: Green (risk has ≥2 controls), Yellow (risk has 1 control), Red (risk has no controls)
- Filter by: Risk category, Control domain, Business unit
- Aggregate view: Risk category × Control domain
- Identify: Risks with most controls (over-controlled?), Risks with no controls (gaps), Controls protecting most risks (critical controls)
- Export to Excel
- Interactive: Click cell to see details
- Print-friendly version

Story Points: 13
Priority: P1

Epic 10: Reporting and Dashboards

User Story 10.1: View Risk Management Dashboard

As a Risk Manager
I want to see a comprehensive risk management dashboard
So that I have real-time visibility into the risk landscape

Acceptance Criteria:

- Main dashboard (landing page) with widgets:
    - **Summary Cards** (top row):
        - Total Active Risks
        - High & Critical Risks (count)
        - Risks Exceeding Appetite (count)
        - Overdue Reviews (count)
        - Active Treatment Plans (count)
        - KRIs in Red Status (count)
    - **Risk Distribution by Level** (pie chart): Critical, High, Medium, Low
    - **Risk Distribution by Category** (bar chart): Top 10 categories by risk count
    - **Risk Heat Map** (5x5 matrix): Current risk positions
    - **Risks by Business Unit** (bar chart): Top 5 BUs by risk count
    - **Risk Trend** (line chart): Total risks over last 12 months
    - **Treatment Status** (donut chart): Planned, In Progress, Completed, Overdue
    - **Recent Activity Feed** (right sidebar):
        - Risks recently identified (last 10)
        - Risks recently assessed
        - Treatment plans completed
        - KRI threshold breaches
        - Reviews completed
    - **Upcoming Items** (left sidebar):
        - Risks due for review (next 7 days)
        - Treatment plans due (next 7 days)
        - KRI measurements due
- Filters: Date range, Business unit
- Refresh button
- Export to PDF
- Customizable layout (future)

Story Points: 21
Priority: P0

User Story 10.2: View My Risks Dashboard

As a Risk Owner
I want to see a personalized dashboard of my responsibilities
So that I can manage my risk portfolio

Acceptance Criteria:

- "My Risks" dashboard showing:
    - **My Summary** (cards):
        - Risks I Own (count)
        - High/Critical Risks I Own
        - My Overdue Reviews
        - My Treatment Plans (count)
        - My KRIs (count)
    - **My Risk List** (table): Risk ID, Title, Level, Status, Review Due, Treatment Status
    - **My Treatment Plans** (table): Treatment ID, Risk, Status, Progress %, Due Date
    - **My KRIs** (table): KRI Name, Current Value, Status, Last Measured
    - **My Action Items**:
        - Risks to review (overdue and upcoming)
        - Treatments to update
        - KRIs to measure
        - Risk acceptances to approve (if manager)
- Sort and filter capabilities
- Click any item to view details
- Export my portfolio
- Email digest option (weekly summary)

Story Points: 13
Priority: P0

User Story 10.3: Generate Risk Register Report

As a Compliance Officer
I want to generate a complete risk register report
So that I can provide it to auditors and management

Acceptance Criteria:

- "Risk Register Report" option in Reports menu
- Report includes all active risks with columns:
    - Risk ID, Title, Description, Category, Sub-category
    - Risk Owner, Business Unit
    - Date Identified, Last Assessed
    - Inherent Risk (L/I/Score/Level)

    - Current Risk (L/I/Score/Level)
    - Target Risk (L/I/Score/Level)
    - Risk Status, Appetite Status
    - Affected Assets (count), Linked Controls (count)
    - Treatment Status, Treatment Owner
    - KRIs (count), Review Due Date
    - Tags
- Filter options: Category, Risk level, Business unit, Status, Date range
- Sort by: Risk score, Date identified, Risk owner
- Format options: Excel, PDF, CSV
- PDF includes: Cover page, Table of contents, Executive summary (stats), Detailed risk list, Risk heat map
- Excel includes: Multiple sheets (Summary, Risk List, High Risks, Treatments, KRIs)
- Branding: Organization logo, date generated, generated by
- Schedule: Option to generate automatically (monthly) and email

Story Points: 13
Priority: P0

User Story 10.4: Generate High & Critical Risks Report

As an Executive
I want to see a focused report on top risks
So that I can prioritize attention and resources

Acceptance Criteria:

- "High & Critical Risks Report" in Reports menu
- Report includes only High and Critical level risks
- Executive summary:
    - Total High risks, Total Critical risks
    - Risks exceeding appetite
    - Treatment coverage (% with active treatments)
    - Top 3 risk categories
- Detailed risk list with:
    - Risk ID, Title, Description (summary), Category
    - Current Risk Level and Score
    - Risk Owner, Business Unit
    - Affected Critical Assets (if any)
    - Treatment Status and Progress
    - Root Cause (if documented)
    - Recommended Actions
- One-page profile per critical risk (detailed)
- Visual: Risk heat map highlighting high/critical risks

- Comparison: Current period vs. previous period (trend)
- Format: PDF (executive-ready, print-friendly)
- Auto-generate monthly and email to executive team

Story Points: 13
Priority: P0

User Story 10.5: Generate Risk Heat Map Report

As a Risk Manager
I want to create visual heat map reports
So that I can communicate risk landscape effectively

Acceptance Criteria:

- "Risk Heat Map" report in Reports menu
- Generate heat maps for:
  - Current Risk (default)
  - Inherent Risk
  - Target Risk
  - Comparison: Current vs. Target (side-by-side)
- Heat map options:
  - All risks (organization-wide)
  - By business unit (one heat map per BU)
  - By category (one heat map per category)
- Risk count or specific risks plotted in each cell
- Color-coded intensity (darker = more risks)
- Export as: Image (PNG/JPEG), PDF, PowerPoint slide
- Include legend and risk list
- Date stamp and title
- Print-friendly format

Story Points: 13
Priority: P0

User Story 10.6: Generate Risks by Category Report

As a Risk Manager
I want to analyze risks by category
So that I can identify risk concentrations

Acceptance Criteria:

- "Risks by Category" report in Reports menu
- Table showing: Category, Total Risks, Critical, High, Medium, Low, Average Score, % of Total Risks

- Sort by: Total risks (default), Average score, Category name
- Visual: Bar chart of risk distribution
- Drill-down: Click category to see risk list
- Comparison: Current period vs. previous period
- Trend: Category risk count over last 6 months
- Insights: Categories with highest average risk, Categories with most critical risks, Categories exceeding appetite
- Export to Excel/PDF
- Filter by business unit

Story Points: 8
Priority: P0

User Story 10.7: Generate Risks by Business Unit Report

As a Business Unit Manager
I want to see risk analysis by business unit
So that I can benchmark and compare risk profiles

Acceptance Criteria:

- "Risks by Business Unit" report in Reports menu
- Table: Business Unit, Total Risks, Critical, High, Medium, Low, Avg Score, Risks Exceeding Appetite, Treatment Coverage %
- Sort by: Total risks, Average score, Exceeding appetite
- Visual: Stacked bar chart (risks by level per BU)
- Heat map: BU × Risk Category
- Drill-down: Click BU to see detailed risk list
- Comparison across BUs (ranking)
- Trend: BU risk profile over time
- Export to Excel/PDF
- Option to email to BU managers

Story Points: 8
Priority: P0

User Story 10.8: Generate Risks Exceeding Appetite Report

As a Chief Risk Officer
I want to see all risks outside acceptable limits
So that I can report to the board and ensure action

Acceptance Criteria:

- "Risks Exceeding Appetite" report in Reports menu
- List of all risks with Current Risk exceeding appetite for their category

- Table: Risk ID, Title, Category, Risk Level, Appetite Tolerance, Gap, Owner, Treatment Status, Acceptance Status
- Sort by: Gap (largest first), Risk score
- Gap = How much risk exceeds appetite (qualitative or score difference)
- For each risk:
  - Why it exceeds appetite
  - Treatment plan status (if any)
  - Acceptance status (if formally accepted)
  - Recommendation: Treat immediately, Accept with justification, Escalate
- Summary: Total exceeding, By category, Trend
- Export to PDF (board report format)
- Auto-generate quarterly

Story Points: 8
Priority: P0

User Story 10.9: Generate Treatment Plan Status Report

As a Risk Manager
I want to report on treatment plan progress
So that I can track risk mitigation efforts

Acceptance Criteria:

- "Treatment Plan Status" report in Reports menu
- Summary:
  - Total treatment plans
  - By status: Planned, In Progress, Completed, On Hold, Cancelled, Overdue
  - By strategy: Mitigate, Transfer, Accept, Avoid
  - Treatment completion rate (completed / total)
  - Average time to complete (for completed treatments)
- Detailed list: Treatment ID, Risk Title, Strategy, Owner, Status, Progress %, Start Date, Due Date, Days Remaining/Overdue
- Overdue treatments highlighted
- Treatment effectiveness (for completed):
  - Expected vs. actual risk reduction
  - Success rate
- Visual: Progress distribution chart, Completion trend over time
- Filter by: Status, Strategy, Owner, Business unit, Date range
- Export to Excel/PDF

Story Points: 13
Priority: P0

User Story 10.10: Generate KRI Summary Report

As a Risk Manager
I want to report on KRI status and trends
So that I can demonstrate proactive risk monitoring

Acceptance Criteria:

- "KRI Summary Report" in Reports menu
- Summary:
    - Total KRIs
    - By status: Green, Amber, Red
    - Threshold breaches (current period)
    - Measurement compliance (% measured on time)
- KRI list: KRI Name, Linked Risk(s), Current Value, Status, Trend, Last Measured, Owner
- Trend analysis: KRIs improving vs. deteriorating
- Red status KRIs detailed section (requires attention)
- Visual: KRI status distribution, Trend charts for top 10 KRIs
- Filter by: Status, Risk category, KRI type (Leading/Lagging), Owner
- Export to Excel/PDF
- Include recommendations for red/amber KRIs

Story Points: 13
Priority: P0

User Story 10.11: Generate Risk Review Compliance Report

As a Risk Administrator
I want to track risk review compliance
So that I can ensure risks are reviewed on schedule

Acceptance Criteria:

- "Risk Review Compliance" report in Reports menu
- Summary:
    - Total risks requiring review
    - Reviews completed on time (%)
    - Reviews overdue (count)
    - Average time between reviews
- Risk list: Risk ID, Title, Risk Level, Last Review Date, Next Review Due, Days Overdue (if applicable), Owner
- Overdue reviews highlighted in red
- Compliance by: Risk owner, Business unit, Risk category
- Trend: Review completion rate over time
- Visual: Review compliance chart, Overdue distribution
- Export to Excel/PDF

- Option to email to risk owners with overdue reviews

Story Points: 8
Priority: P1

User Story 10.12: Generate Risk Trend Report

As an Executive
I want to see how the risk landscape has changed
So that I can assess if risk management is effective

Acceptance Criteria:

- "Risk Trend Report" in Reports menu
- Time period selection: Last 6 months, Last 12 months, Custom range
- Metrics tracked over time:
  - Total risks (line chart)
  - Risks by level (stacked area chart)
  - Risks exceeding appetite (line chart)
  - Treatment plan completions (bar chart)
  - Average risk score (line chart)
  - New risks identified (bar chart)
  - Risks closed (bar chart)
- Net risk change: New - Closed
- Risk score trend: Increasing, Stable, Decreasing (overall)
- Category trends (which categories increasing/decreasing)
- Insights and commentary section
- Comparison: Period vs. period
- Export to PDF/PowerPoint

Story Points: 13
Priority: P1

User Story 10.13: Generate Executive Risk Summary

As a Chief Risk Officer
I want to create a concise executive summary
So that I can brief the board on risk posture

Acceptance Criteria:

- "Executive Risk Summary" report (2-3 pages)
- Page 1: Executive Overview
  - Overall risk rating: Low, Medium, High (based on aggregate risk)
  - Risk appetite status: Green/Amber/Red

    - Key metrics: Total risks, High/Critical count, Risks exceeding appetite, Treatment coverage
    - Risk heat map (current)
    - Top 5 risks (by score)
- Page 2: Risk Landscape
    - Risks by category (chart)
    - Trend: Risk increasing/decreasing/stable
    - Treatment progress
    - KRI status summary
    - Recent significant changes (new critical risks, major incidents)
- Page 3: Actions and Recommendations
    - Key actions taken (this period)
    - Risks requiring board attention
    - Recommendations for board decision/approval
    - Upcoming activities (assessments, treatments)
- Format: PDF, PowerPoint, or Word
- Professional formatting with charts/graphics
- Auto-generate quarterly
- Customizable template

Story Points: 21
Priority: P1

User Story 10.14: Schedule Automated Reports

As a Risk Administrator
I want to schedule reports to generate automatically
So that stakeholders receive regular updates without manual effort

Acceptance Criteria:

- Report scheduling interface
- Select report type
- Define schedule:
    - Frequency: Daily, Weekly, Monthly, Quarterly, Annually
    - Day of week (if weekly)
    - Day of month (if monthly)
    - Specific date range or rolling period
- Define recipients (email list)
- Email subject and message customization
- Report format (Excel/PDF)
- Report parameters (filters to apply)
- Enable/disable schedule
- Test run (generate and email once now)

- Schedule history (view past generations)
- Error notifications if report fails
- Edit/delete scheduled reports

Story Points: 13
Priority: P2 (Nice to have)

Epic 11: Notifications and Alerts

User Story 11.1: Receive Risk Ownership Notification

As a Risk Owner
I want to be notified when a risk is assigned to me
So that I am aware of my responsibilities

Acceptance Criteria:

- Email notification when:
  - New risk created with me as owner
  - Existing risk ownership transferred to me
- Email content:
  - Risk ID and Title
  - Risk category and description (summary)
  - Current risk level
  - Who assigned it and why (notes)
  - Link to risk detail page
  - Next actions (review, assess, create treatment)
- In-app notification
- Acknowledge notification option
- Notification preferences (can't opt out of ownership notifications)

Story Points: 5
Priority: P0

User Story 11.2: Receive Risk Assessment Notification

As a Risk Analyst
I want to be notified when a risk assessment is assigned to me
So that I can conduct the assessment promptly

Acceptance Criteria:

- Email notification when:
  - Assessment request approved and assigned to me
  - Assessment due date approaching (7 days before)
  - Assessment overdue

- Email content:
    - Assessment request details
    - Requester and justification
    - Due date
    - Scope (assets, business units affected)
    - Link to assessment request and risk form
- In-app notification
- Dismiss notification after assessment completed
- Escalation to manager if assessment overdue >14 days

Story Points: 5
Priority: P0

User Story 11.3: Receive Risk Score Change Alert

As a Risk Owner
I want to be notified when my risk score significantly changes
So that I can take appropriate action

Acceptance Criteria:

- Alert triggered when:
    - Risk score increases by ≥5 points OR
    - Risk level changes (e.g., Medium → High)
- Email notification to:
    - Risk owner
    - Risk manager
    - Business unit manager (if critical risk)
- Email content:
    - Risk ID and title
    - Previous score and level
    - New score and level
    - Change reason (from assessment notes)
    - Suggested actions (reassess treatment plan, escalate)
    - Link to risk detail
- In-app notification with prominent alert badge
- Alert log on risk detail page

Story Points: 5
Priority: P0

User Story 11.4: Receive Risk Exceeds Appetite Alert

As a Risk Manager
I want to be notified when a risk exceeds risk appetite
So that I can ensure prompt treatment

Acceptance Criteria:

- Alert triggered when:
  - New risk assessed and exceeds appetite OR
  - Existing risk reassessed and now exceeds appetite
- Email notification to:
  - Risk owner
  - Risk manager
  - Chief Risk Officer (if critical risk)
  - Business unit manager
- Email content:
  - Risk details
  - Category tolerance level vs. current risk level
  - Gap explanation
  - Required actions: Create treatment plan OR Request formal acceptance
  - Link to risk
- Alert displayed on risk detail page (warning badge)
- Alert tracked until resolved (treatment created or risk accepted)
- Dashboard: Risks exceeding appetite (count and list)

Story Points: 5
Priority: P0

User Story 11.5: Receive Treatment Assignment Notification

As a Treatment Owner
I want to be notified when a treatment plan is assigned to me
So that I can begin working on risk mitigation

Acceptance Criteria:

- Email notification when:
  - Treatment plan created with me as owner
  - Treatment plan ownership transferred to me
- Email content:
  - Treatment plan ID
  - Linked risk (ID, title, level)
  - Treatment strategy
  - Treatment description and milestones
  - Target completion date

  - Who assigned it
  - Link to treatment plan
  - Link to risk
- In-app notification
- Cannot opt out
- Acknowledge receipt

Story Points: 3
Priority: P0

User Story 11.6: Receive Risk Acceptance Request Notification

As a Business Unit Manager
I want to be notified when risk acceptance requires my approval
So that I can review and decide promptly

Acceptance Criteria:

- Email notification when:
  - Risk acceptance submitted for my approval
  - Acceptance request waiting for >7 days (reminder)
- Email content:
  - Risk ID and title
  - Current risk level and score
  - Requester and justification
  - Compensating controls (if any)
  - Business benefit of acceptance
  - Recommended decision
  - Link to approval page
- In-app notification with action button (Approve/Reject)
- Reminder every 7 days until decision made
- Escalation to higher management if not approved within 30 days

Story Points: 5
Priority: P0

User Story 11.7: Receive KRI Threshold Breach Alert

As a Risk Owner
I want to be notified when a KRI for my risk breaches a threshold
So that I can investigate and respond

Acceptance Criteria:

- Alert triggered when:
  - KRI status changes to Amber (warning threshold breached)

    - KRI status changes to Red (critical threshold breached)
- Email notification to:
    - KRI owner
    - Risk owner(s) of linked risks
    - KRI notification recipients (defined in KRI)
    - Risk manager (if Red)
- Email content:
    - KRI name and description
    - Current value and status
    - Threshold breached
    - Previous value and trend
    - Linked risk(s)
    - Recommended actions
    - Link to KRI detail
- In-app notification
- Alert priority: Red = High priority, Amber = Medium priority
- Alert cleared when KRI returns to Green status
- Alert log on KRI detail page

Story Points: 5
Priority: P0

User Story 11.8: Configure Notification Preferences

As a User
I want to manage my notification preferences
So that I receive relevant alerts without being overwhelmed

Acceptance Criteria:

- User Preferences page with Notification Settings section
- Notification types with enable/disable toggle:
    - Risk ownership assignments (cannot disable)
    - Risk assessment assignments (cannot disable)
    - Risk review reminders (can disable, defaults to enabled)
    - Treatment plan assignments (cannot disable)
    - Treatment due date reminders (can disable)
    - KRI measurement reminders (can disable)
    - Risk acceptance approvals (cannot disable)
    - Risk score changes (can disable)
    - KRI threshold breaches (can disable for own KRIs only)
- Email notification frequency:
    - Immediate (real-time email for each event)
    - Daily Digest (one email per day with all events)

    - Weekly Digest (one email per week)
- In-app notifications always enabled (cannot disable)
- Save preferences
- Preferences apply immediately
- Reset to defaults option

Story Points: 8
Priority: P1

Epic 12: Administration and Configuration

User Story 12.1: Configure Risk Categories

As a Risk Administrator
I want to customize the risk taxonomy
So that it aligns with organizational structure and terminology

Acceptance Criteria:

- Risk Category management page
- Create new category:
    - Category name (required)
    - Description
    - Color code (for visual identification)
    - Risk appetite tolerance (High/Medium/Low)
    - Icon (optional)
- Edit existing category (name, description, color, tolerance)
- Deactivate category (cannot delete if risks exist)
- Reactivate category
- Reorder categories (drag-and-drop)
- Create sub-categories within categories
- Set default category for new risks
- Category usage statistics (number of risks per category)
- Warning before deactivating category with active risks
- Audit trail of category changes
- Export category list

Story Points: 8
Priority: P0

User Story 12.2: Configure Risk Assessment Methodology

As a Risk Administrator
I want to customize the risk assessment scales and matrix
So that the methodology fits organizational risk culture

Acceptance Criteria:

- Risk Assessment Configuration page
- **Likelihood Scale Configuration**:
  - Edit labels for levels 1-5 (e.g., "Rare" → "Very Unlikely")
  - Edit descriptions for each level
  - Edit probability ranges (optional)
- **Impact Scale Configuration**:
  - Edit labels for levels 1-5
  - Edit descriptions for each level
  - Edit financial impact ranges per level (optional)
  - Configure impact categories to assess (Financial, Operational, Reputational, Compliance, Safety)
- **Risk Matrix Configuration**:
  - Define risk level boundaries (which scores = Low/Med/High/Critical)
  - Customize colors for risk levels (hex codes)
  - Preview matrix with custom settings
- **Assessment Options**:
  - Require confidence level (Yes/No)
  - Require assessment notes (Yes/No)
  - Allow assessments without linked controls (Yes/No)
- Save configuration
- Version control (track changes)
- Export configuration for documentation
- Reset to default option

Story Points: 13
Priority: P1

User Story 12.3: Configure Risk Appetite Statement

As a Chief Risk Officer
I want to update the organizational risk appetite
So that it reflects current board guidance and strategy

Acceptance Criteria:

- Risk Appetite configuration page
- Create/edit appetite statement (rich text editor)
- Define risk tolerance per category
- Set review frequency (annual, biennial)
- Submit for board approval
- Approval workflow
- Version history
- Compare current vs. previous appetite

- Effective date management
- Export appetite statement to PDF
- Communicate appetite to organization (broadcast notification)

Story Points: 8
Priority: P0

User Story 12.4: Manage User Roles and Permissions

As a Risk Administrator
I want to assign users to risk management roles
So that access is controlled appropriately

Acceptance Criteria:

- User Management page (reuses existing from Asset/Governance modules)
- Risk-specific roles available:
  - Risk Administrator
  - Risk Manager
  - Risk Analyst
  - Risk Owner
  - Business Unit Manager
  - Executive/Viewer
- Assign role to user (single or multiple roles)
- Define row-level security (business unit access)
- View all users by role
- User permission matrix display
- Bulk user role assignment (CSV import)
- Remove user from role
- Audit trail of role changes
- Test user permissions (view as user)

Story Points: 8
Priority: P0

User Story 12.5: Configure KRI Library

As a Risk Administrator
I want to manage the KRI template library
So that users can quickly set up standard indicators

Acceptance Criteria:

- KRI Library management page
- Create KRI templates:
  - Template name

    - Description
    - KRI type (Leading/Lagging)
    - Category (Cybersecurity, Operational, etc.)
    - Suggested frequency
    - Calculation method
    - Unit of measurement
    - Suggested thresholds (Target, Warning, Critical)
- Edit existing templates
- Activate/deactivate templates
- Categorize templates
- Template usage count (how many times used)
- Import templates from file (CSV)
- Export template library
- Pre-load with 30 industry-standard KRIs
- Add custom organization-specific KRIs

Story Points: 8
Priority: P1

User Story 12.6: Configure Review Frequencies

As a Risk Administrator
I want to set default review frequencies by risk level
So that risks are reviewed at appropriate intervals

Acceptance Criteria:

- Review Frequency configuration page
- Set frequency for each risk level:
    - Critical: [X] months (default 3)
    - High: [X] months (default 6)
    - Medium: [X] months (default 12)
    - Low: [X] months (default 24)
- Set reminder schedule:
    - First reminder: [X] days before due
    - Second reminder: [X] days before due
    - Third reminder: [X] days before due
    - Overdue reminders: Every [X] days
- Set escalation rules:
    - Escalate to manager if overdue > [X] days
    - Escalate to CRO if critical risk overdue > [X] days
- Allow per-risk override (Yes/No)
- Save configuration
- Apply to existing risks (recalculate due dates)

- Audit trail

Story Points: 5
Priority: P0

User Story 12.7: Configure Notification Settings

As a Risk Administrator
I want to configure system-wide notification rules
So that alerts are sent appropriately

Acceptance Criteria:

- Notification Configuration page
- For each notification type:
  - Enable/disable globally
  - Set trigger conditions
  - Define recipients (by role or specific users)
  - Set reminder intervals
  - Configure escalation rules
- Email template customization:
  - Subject line
  - Body content (with variables)
  - Signature
  - Logo/branding
- Notification delivery settings:
  - Email server configuration (SMTP)
  - From address
  - Reply-to address
- Test notification (send test email)
- Notification log (view sent notifications)
- Notification delivery status (success/failure)
- Retry failed notifications

Story Points: 13
Priority: P1

User Story 12.8: View Audit Logs

As a Risk Administrator
I want to view comprehensive audit logs
So that I can track all risk management activities

Acceptance Criteria:

- Audit Log page (reuses existing shared audit_logs table)

- Filter logs by:
    - Entity type (Risk, Treatment, KRI, Assessment, etc.)
    - Action (Create, Update, Delete, Approve, etc.)
    - User
    - Date range
    - Entity ID (specific risk, treatment, etc.)
- Table columns: Timestamp, User, Action, Entity Type, Entity ID, Changes (before/after), IP Address
- View change details (JSON diff viewer)
- Search within logs
- Export logs to CSV
- Immutable records (cannot be edited or deleted)
- Retention policy (default 7 years)
- Performance optimization for large log volumes

Story Points: 8
Priority: P1

User Story 12.9: Import Initial Risk Data

As a Risk Administrator
I want to bulk import risks from an existing risk register
So that I can migrate historical data

Acceptance Criteria:

- Import function in Risk List page
- Download import template (Excel with required columns)
- Template columns: Risk Title, Description, Category, Sub-category, Owner Email, Business Unit, Inherent L/I, Current L/I, Status, Tags, etc.
- Upload completed template (Excel/CSV)
- Data validation:
    - Required fields check
    - Data type validation
    - User email lookup (map to user IDs)
    - Category validation
    - Business unit validation
- Preview import (show first 10 rows)
- Import options:
    - Create new risks only
    - Update existing risks (match by Risk ID or Title)
- Execute import
- Import results summary:
    - Total rows processed

    - Successful imports
    - Failed imports (with error details)
    - Download error report
- Import activity logged
- Rollback option (within 24 hours)

Story Points: 13
Priority: P1

User Story 12.10: Configure System Settings

As a Risk Administrator
I want to manage global risk management settings
So that the system operates according to organizational policies

Acceptance Criteria:

- System Settings page with sections:
    - **General Settings**:
        - Organization name
        - Fiscal year start (for reporting periods)
        - Default currency
        - Date format
        - Time zone
    - **Risk Management Settings**:
        - Enable/disable risk acceptance workflow
        - Require treatment plan for risks exceeding appetite
        - Allow risks without assets (Yes/No)
        - Minimum controls per risk (default 0)
        - Auto-close risks after treatment completion (Yes/No) - Risk retention period (years, for closed risks)
- **Data Retention**:
    - Audit log retention (years)
    - Assessment history retention (years)
    - Deleted risk retention (days before permanent deletion)
- **Security Settings**:
    - Session timeout (minutes)
    - Password expiration (days)
    - Failed login attempts before lockout
    - MFA requirement for administrators (Yes/No)
- **Integration Settings**:
    - Asset Management module enabled (Yes/No)
    - Governance module enabled (Yes/No)
    - External API access (Yes/No)

    - API rate limits
- Save settings
- Settings change requires admin password confirmation
- Settings change logged in audit trail
- Export settings for documentation
- Reset to defaults option (with confirmation)

Story Points: 8
Priority: P1

Story Summary by Priority

P0 (Must Have) - 73 Stories

Core functionality essential for Phase 1 launch:

- Risk Governance and Appetite: 4 stories
- Risk Identification and Registration: 10 stories
- Risk Assessment: 5 stories
- Risk Evaluation and Prioritization: 6 stories
- Risk Treatment: 10 stories
- Risk Monitoring (KRIs): 8 stories
- Risk Review and Reassessment: 5 stories
- Integration with Asset Management: 3 stories
- Integration with Governance: 2 stories
- Reporting and Dashboards: 10 stories
- Notifications: 6 stories
- Administration: 4 stories

Estimated Story Points: ~580 points

P1 (Should Have) - 31 Stories

Important features that enhance value but not critical for initial launch:

- Risk Governance and Appetite: 3 stories
- Risk Identification and Registration: 2 stories
- Risk Assessment: 5 stories
- Risk Evaluation and Prioritization: 0 stories
- Risk Treatment: 3 stories
- Risk Monitoring (KRIs): 2 stories
- Risk Review and Reassessment: 1 story
- Integration with Asset Management: 3 stories
- Integration with Governance: 4 stories
- Reporting and Dashboards: 2 stories

- Notifications: 1 story
- Administration: 5 stories

Estimated Story Points: ~210 points

P2 (Nice to Have) - 6 Stories

Enhancement features for future phases:

- Risk Treatment: 2 stories
- Reporting: 1 story
- Other enhancements: 3 stories

Estimated Story Points: ~60 points

Implementation Recommendations

Sprint Planning (2-week sprints)

Sprint 0 (Weeks 1-2): Foundation

- Database schema implementation
- API framework setup
- UI component library setup
- Development environment configuration
- Initial data model and migrations

Sprint 1-2 (Weeks 3-6): Risk Governance and Core Registration

- Stories: 1.1, 1.2, 1.3, 1.4, 1.6, 2.1, 2.2, 2.3, 2.4, 2.5, 2.6
- Deliverable: Can create/edit risks, define risk appetite, link to assets/controls
- Story Points: ~70

Sprint 3-4 (Weeks 7-10): Risk Assessment

- Stories: 3.1, 3.2, 3.3, 3.4, 3.5, 4.1, 4.2, 4.3, 4.5, 4.6
- Deliverable: Can assess risks qualitatively, view heat maps, compare to appetite
- Story Points: ~80

Sprint 5-6 (Weeks 11-14): Risk Treatment

- Stories: 5.1, 5.2, 5.3, 5.4, 5.5, 5.7, 5.8, 5.9, 5.10
- Deliverable: Can create and track treatment plans, request risk acceptance
- Story Points: ~70

Sprint 7-8 (Weeks 15-18): Risk Monitoring (KRIs) and Review

- Stories: 6.1, 6.2, 6.3, 6.4, 6.5, 6.7, 6.8, 7.1, 7.2, 7.3, 7.4, 7.5
- Deliverable: Can define KRIs, record measurements, conduct reviews
- Story Points: ~80

Sprint 9-10 (Weeks 19-22): Integration and Reporting

- Stories: 8.1, 8.2, 9.1, 9.2, 10.1, 10.2, 10.3, 10.4, 10.5, 10.6, 10.7, 10.8, 10.9, 10.10
- Deliverable: Full integration with Asset/Governance, core reports and dashboards
- Story Points: ~110

Sprint 11 (Weeks 23-24): Notifications and Administration

- Stories: 11.1, 11.2, 11.3, 11.4, 11.5, 11.6, 11.7, 12.1, 12.2, 12.3, 12.4, 12.6
- Deliverable: Notifications operational, system configuration complete
- Story Points: ~60

Sprint 12 (Weeks 25-26): Testing, Bug Fixes, Polish

- User acceptance testing
- Bug fixes from UAT
- Performance optimization
- Documentation completion
- Training material creation

Sprint 13 (Weeks 27-28): Deployment and Training

- Production deployment
- Data migration (if needed)
- User training sessions
- Go-live support

Definition of Done (DoD)

For each user story to be considered "done":

✅ **Development**:

- Code written and peer-reviewed
- Unit tests written and passing (80% coverage minimum)
- Integration tests passing
- Code merged to main branch

✅ **Quality**:

- Acceptance criteria met and verified
- No critical or high-priority bugs
- Cross-browser tested (Chrome, Firefox, Edge, Safari)
- Responsive design verified (desktop, tablet)
- Performance acceptable (page load < 2 seconds)

✅ **Documentation**:

- User documentation updated

- API documentation updated (if applicable)
- Code comments for complex logic
- Release notes entry created

✅ **Demo/Approval**:

- Demo to Product Owner
- Product Owner acceptance
- Deployed to staging environment
- Stakeholder feedback incorporated

Acceptance Criteria Template

For consistency, all user stories follow this pattern:

```
**As a** [User Role]
**I want to** [Action/Goal]
**So that** [Business Value/Reason]

**Acceptance Criteria:**
- [Criterion 1]
- [Criterion 2]
- [Criterion 3]
- [etc.]

**Story Points:** [1, 2, 3, 5, 8, 13, 21]
**Priority:** [P0, P1, P2]
```

User Story Sizing Guide

- **1-2 points**: Simple CRUD operation, minor UI change, configuration update
- **3-5 points**: Standard feature with moderate complexity, single entity management
- **8 points**: Complex feature with multiple components, integration work, complex business logic
- **13 points**: Very complex feature, multiple integrations, sophisticated algorithms, major UI work
- **21 points**: Epic-level work, likely should be broken down further

---

Next Steps

1. **Review and Prioritization**: Stakeholders review stories and confirm priorities
2. **Story Refinement**: Development team reviews stories for technical feasibility
3. **Sprint Planning**: Map stories to sprints based on dependencies and capacity
4. **Backlog Grooming**: Detailed breakdown of Sprint 1-2 stories
5. **Environment Setup**: Development, staging, and production environments prepared
6. **Kickoff**: Sprint 0 begins

Appendix: Epic Dependencies

```
Epic 1 (Governance/Appetite) → Must complete first (foundation)
    ↓
Epic 2 (Risk Registration) → Requires Epic 1
    ↓
Epic 3 (Risk Assessment) → Requires Epic 2
    ↓
Epic 4 (Risk Evaluation) → Requires Epic 3
    ↓
Epic 5 (Risk Treatment) → Requires Epic 4
    ↓
Epic 6 (KRIs) → Requires Epic 2 (can run parallel with Epic 5)
    ↓
Epic 7 (Review) → Requires Epic 3
    ↓
Epic 8 (Asset Integration) → Requires Epic 2 (can run parallel with Epic 3-7)
Epic 9 (Governance Integration) → Requires Epic 2 (can run parallel with Epic 3-
7)
    ↓
Epic 10 (Reporting) → Requires all data capture epics (2-7)
Epic 11 (Notifications) → Can run parallel with all epics
Epic 12 (Administration) → Can run parallel with all epics
```

Ready to proceed with detailed PRD and database schema for Risk Management Module?

Wagieh

Risk Management Module - PRD & Database Schema (Compressed)

---

1. PRD Summary

1.1 Product Overview

Risk Management Module enabling end-to-end risk lifecycle: identification → assessment → treatment → monitoring. Integrates with Asset Management and Governance modules.

Phase 1 Duration: 16 weeks (28 weeks with testing/deployment)
Target Users: 50+ users managing 100-200 risks

1.2 Core Features (P0)

✅ Risk Appetite Framework

✅ Risk Register (CRUD)

✅ Qualitative Risk Assessment (5×5 matrix)

✅ Risk Treatment Plans (4 strategies)

✅ KRI Management (30 indicators)

✅ Risk Review Workflows

✅ Asset & Control Integration

✅ 10 Standard Reports

✅ Notifications & Alerts

1.3 Key Workflows

Risk Identification → Assessment → Treatment → Monitoring

```
1. Create Risk → Link Assets/Controls
2. Assess: Inherent → Current → Target Risk
3. Compare to Appetite → Create Treatment
4. Define KRIs → Monitor
5. Review Periodically → Reassess
```

---

2. Database Schema

Shared Tables (Existing)

```
-- Reuse from Asset/Governance modules:
users, roles, business_units, audit_logs, tags, notifications
```

2.1 Risk Appetite & Governance

```
CREATE TYPE risk_tolerance_enum AS ENUM ('high', 'medium', 'low');

CREATE TABLE risk_appetite_statements (
    id UUID PRIMARY KEY DEFAULT gen_random_uuid(),
    statement_text TEXT NOT NULL,
    version VARCHAR(50) DEFAULT '1.0',
    status VARCHAR(50) DEFAULT 'draft', -- draft, approved, archived
    effective_date DATE,
    next_review_date DATE,
    approved_by UUID REFERENCES users(id),
    approval_date DATE,
    created_by UUID REFERENCES users(id),
    created_at TIMESTAMP DEFAULT CURRENT_TIMESTAMP,
    updated_at TIMESTAMP DEFAULT CURRENT_TIMESTAMP
);

CREATE TABLE risk_categories (
    id UUID PRIMARY KEY DEFAULT gen_random_uuid(),
    name VARCHAR(200) NOT NULL,
    description TEXT,
    color_code VARCHAR(7), -- Hex color
    risk_tolerance risk_tolerance_enum DEFAULT 'medium',
    is_active BOOLEAN DEFAULT true,
    display_order INTEGER,
    created_at TIMESTAMP DEFAULT CURRENT_TIMESTAMP
);

-- Pre-populate with 12 categories
INSERT INTO risk_categories (name, risk_tolerance, display_order) VALUES
('Strategic Risks', 'medium', 1),
('Operational Risks', 'medium', 2),
('Technology/Cybersecurity Risks', 'low', 3),
('Financial Risks', 'low', 4),
('Compliance & Legal Risks', 'low', 5),
('Reputational Risks', 'low', 6),
('Third-Party/Vendor Risks', 'medium', 7),
('Human Resources Risks', 'medium', 8),
('Environmental/Physical Risks', 'medium', 9),
('Project Risks', 'medium', 10),
('Data Privacy Risks', 'low', 11),
('Business Continuity Risks', 'low', 12);
```

2.2 Risk Register

```
CREATE TYPE risk_status_enum AS ENUM ('active', 'monitoring', 'closed', 'accept-
ed');
CREATE TYPE risk_velocity_enum AS ENUM ('slow', 'medium', 'fast', 'immediate');
CREATE TYPE threat_source_enum AS ENUM ('internal', 'external', 'natural', 'in-
tentional', 'accidental');

CREATE TABLE risks (
    id UUID PRIMARY KEY DEFAULT gen_random_uuid(),
    risk_id VARCHAR(50) UNIQUE NOT NULL, -- RISK-2025-001
    title VARCHAR(500) NOT NULL,
    description TEXT,
    risk_statement TEXT, -- If [cause], then [event], resulting in [impact]

    -- Classification
    category_id UUID REFERENCES risk_categories(id),
    sub_category VARCHAR(200),

    -- Ownership
    risk_owner_id UUID REFERENCES users(id),
    risk_analyst_id UUID REFERENCES users(id),
    business_unit_ids UUID[], -- Array of business_unit IDs

    -- Risk Scenario
    threat_source threat_source_enum,
    vulnerabilities TEXT,
    risk_velocity risk_velocity_enum,
    early_warning_signs TEXT,

    -- Status
    status risk_status_enum DEFAULT 'active',
    date_identified DATE DEFAULT CURRENT_DATE,
    date_closed DATE,
    closure_reason TEXT,

    -- Review
    last_review_date DATE,
    next_review_date DATE,
    review_frequency_months INTEGER, -- Override default

    -- Metadata
    tags VARCHAR(100)[],
    custom_fields JSONB,

    -- Audit
    created_by UUID REFERENCES users(id),
    created_at TIMESTAMP DEFAULT CURRENT_TIMESTAMP,
    updated_by UUID REFERENCES users(id),
    updated_at TIMESTAMP DEFAULT CURRENT_TIMESTAMP,
    deleted_at TIMESTAMP
);

CREATE INDEX idx_risks_risk_id ON risks(risk_id);
CREATE INDEX idx_risks_owner ON risks(risk_owner_id);
CREATE INDEX idx_risks_category ON risks(category_id);
CREATE INDEX idx_risks_status ON risks(status) WHERE deleted_at IS NULL;
CREATE INDEX idx_risks_review_due ON risks(next_review_date) WHERE status = 'active';
CREATE INDEX idx_risks_search ON risks USING gin(to_tsvector('english',
    coalesce(title, '') || ' ' || coalesce(description, '')));
```

2.3 Risk-Asset Relationships

```
CREATE TABLE risk_asset_links (
    id UUID PRIMARY KEY DEFAULT gen_random_uuid(),
    risk_id UUID REFERENCES risks(id) ON DELETE CASCADE,
    asset_type asset_category_enum NOT NULL, -- From Asset Management
    asset_id UUID NOT NULL,
    created_at TIMESTAMP DEFAULT CURRENT_TIMESTAMP,
    CONSTRAINT unique_risk_asset UNIQUE (risk_id, asset_type, asset_id)
);

CREATE INDEX idx_risk_assets_risk ON risk_asset_links(risk_id);
CREATE INDEX idx_risk_assets_asset ON risk_asset_links(asset_type, asset_id);
```

2.4 Risk-Control Relationships

```
CREATE TABLE risk_control_links (
    id UUID PRIMARY KEY DEFAULT gen_random_uuid(),
    risk_id UUID REFERENCES risks(id) ON DELETE CASCADE,
    control_id UUID NOT NULL, -- References unified_controls from Governance
    control_effectiveness_rating INTEGER CHECK (control_effectiveness_rating BETWEEN 1 AND 5),
    notes TEXT,
    created_at TIMESTAMP DEFAULT CURRENT_TIMESTAMP,
    CONSTRAINT unique_risk_control UNIQUE (risk_id, control_id)
);

CREATE INDEX idx_risk_controls_risk ON risk_control_links(risk_id);
CREATE INDEX idx_risk_controls_control ON risk_control_links(control_id);
```

2.5 Risk Assessments

```
CREATE TYPE assessment_type_enum AS ENUM ('inherent', 'current', 'target');
CREATE TYPE confidence_level_enum AS ENUM ('high', 'medium', 'low');

CREATE TABLE risk_assessments (
    id UUID PRIMARY KEY DEFAULT gen_random_uuid(),
    risk_id UUID REFERENCES risks(id) ON DELETE CASCADE,
    assessment_type assessment_type_enum NOT NULL,

    -- Likelihood & Impact (1-5 scale)
    likelihood INTEGER CHECK (likelihood BETWEEN 1 AND 5),
    impact INTEGER CHECK (impact BETWEEN 1 AND 5),

    -- Impact by category (optional)
    financial_impact INTEGER CHECK (financial_impact BETWEEN 1 AND 5),
    operational_impact INTEGER CHECK (operational_impact BETWEEN 1 AND 5),
    reputational_impact INTEGER CHECK (reputational_impact BETWEEN 1 AND 5),
    compliance_impact INTEGER CHECK (compliance_impact BETWEEN 1 AND 5),
    safety_impact INTEGER CHECK (safety_impact BETWEEN 1 AND 5),

    -- Calculated
    risk_score INTEGER, -- likelihood × impact (1-25)
    risk_level VARCHAR(50), -- Low, Medium, High, Critical

    -- Assessment metadata
    assessment_date DATE DEFAULT CURRENT_DATE,
    assessor_id UUID REFERENCES users(id),
    confidence_level confidence_level_enum,
    assessment_notes TEXT,
    assumptions TEXT,

    -- Comparison to appetite
    appetite_status VARCHAR(50), -- within, near, exceeds

    created_at TIMESTAMP DEFAULT CURRENT_TIMESTAMP
);

CREATE INDEX idx_assessments_risk ON risk_assessments(risk_id);
CREATE INDEX idx_assessments_type ON risk_assessments(assessment_type);
CREATE INDEX idx_assessments_date ON risk_assessments(assessment_date DESC);

-- Trigger to calculate risk_score and risk_level
CREATE OR REPLACE FUNCTION calculate_risk_score()
RETURNS TRIGGER AS $$
BEGIN
    NEW.risk_score := NEW.likelihood * NEW.impact;
    NEW.risk_level := CASE
        WHEN NEW.risk_score <= 6 THEN 'Low'
        WHEN NEW.risk_score <= 12 THEN 'Medium'
        WHEN NEW.risk_score <= 20 THEN 'High'
        ELSE 'Critical'
    END;
    RETURN NEW;
END;
$$ LANGUAGE plpgsql;

CREATE TRIGGER set_risk_score
    BEFORE INSERT OR UPDATE ON risk_assessments
    FOR EACH ROW EXECUTE FUNCTION calculate_risk_score();
```

2.6 Risk Treatment Plans

```
CREATE TYPE treatment_strategy_enum AS ENUM ('mitigate', 'transfer', 'accept',
'avoid');
CREATE TYPE treatment_status_enum AS ENUM ('planned', 'in_progress',
'completed', 'on_hold', 'cancelled');

CREATE TABLE risk_treatments (
    id UUID PRIMARY KEY DEFAULT gen_random_uuid(),
    treatment_id VARCHAR(50) UNIQUE NOT NULL,
    risk_id UUID REFERENCES risks(id) ON DELETE CASCADE,

    -- Strategy
    strategy treatment_strategy_enum NOT NULL,
    description TEXT NOT NULL,

    -- Ownership
    treatment_owner_id UUID REFERENCES users(id),
    supporting_team_members UUID[], -- Array of user IDs

    -- Schedule
    target_start_date DATE,
    target_completion_date DATE,
    actual_start_date DATE,
    actual_completion_date DATE,

    -- Progress
    status treatment_status_enum DEFAULT 'planned',
    progress_percentage INTEGER DEFAULT 0 CHECK (progress_percentage BETWEEN 0
AND 100),

    -- Budget
    budget_estimated DECIMAL(15,2),
    budget_actual DECIMAL(15,2),
    -- Details
    milestones TEXT,
    dependencies TEXT,
    success_criteria TEXT,
    notes TEXT,

    -- Strategy-specific fields (JSONB for flexibility)
    strategy_details JSONB, -- See structure below

    created_by UUID REFERENCES users(id),
    created_at TIMESTAMP DEFAULT CURRENT_TIMESTAMP,
    updated_at TIMESTAMP DEFAULT CURRENT_TIMESTAMP
);

/*
strategy_details JSONB structure by strategy:

MITIGATE: {
  "new_controls": ["text description or control_ids"],
  "expected_target_likelihood": 2,
  "expected_target_impact": 3
}

TRANSFER: {
  "mechanism": "insurance|contract|outsourcing",
  "insurance": {
    "policy_number": "...",
    "insurer": "...",
    "coverage_amount": 1000000,
    "premium": 50000,
    "deductible": 10000,
    "renewal_date": "2025-12-31"
  },
  "contract": {
    "contract_ref": "...",
    "counterparty": "...",
    "terms": "..."
  }
}

ACCEPT: {
  "justification": "...",
  "approved_by_id": "uuid",
  "approval_date": "2025-01-15",
  "review_date": "2025-07-15",
  "compensating_controls": "...",
  "monitoring_plan": "..."
}

AVOID: {
  "avoidance_actions": "...",
  "business_impact": "...",
  "approved_by_id": "uuid"
}
*/

CREATE INDEX idx_treatments_risk ON risk_treatments(risk_id);
CREATE INDEX idx_treatments_owner ON risk_treatments(treatment_owner_id);
CREATE INDEX idx_treatments_status ON risk_treatments(status);
CREATE INDEX idx_treatments_due ON risk_treatments(target_completion_date)
    WHERE status IN ('planned', 'in_progress');
```

2.7 Key Risk Indicators (KRIs)

```
CREATE TYPE kri_type_enum AS ENUM ('leading', 'lagging');
CREATE TYPE kri_frequency_enum AS ENUM ('daily', 'weekly', 'monthly', 'quarter-
ly');
CREATE TYPE kri_status_enum AS ENUM ('green', 'amber', 'red');

CREATE TABLE kris (
    id UUID PRIMARY KEY DEFAULT gen_random_uuid(),
    kri_id VARCHAR(50) UNIQUE NOT NULL,
    name VARCHAR(300) NOT NULL,
    description TEXT,
    kri_type kri_type_enum NOT NULL,

    -- Measurement
    measurement_frequency kri_frequency_enum NOT NULL,
    unit_of_measurement VARCHAR(50), -- %, count, currency, days, ratio
    data_source_description TEXT,
    calculation_method TEXT,

    -- Thresholds
    target_value DECIMAL(10,2), -- Green
    warning_threshold DECIMAL(10,2), -- Amber
    critical_threshold DECIMAL(10,2), -- Red
    threshold_direction VARCHAR(20), -- lower_is_better, higher_is_better

    -- Current state
    current_value DECIMAL(10,2),
    current_status kri_status_enum,
    last_measurement_date DATE,

    -- Ownership
    kri_owner_id UUID REFERENCES users(id),
    notification_recipients UUID[], -- Array of user IDs

    created_by UUID REFERENCES users(id),
    created_at TIMESTAMP DEFAULT CURRENT_TIMESTAMP,
    updated_at TIMESTAMP DEFAULT CURRENT_TIMESTAMP,
    deleted_at TIMESTAMP
);

CREATE TABLE kri_risk_links (
    id UUID PRIMARY KEY DEFAULT gen_random_uuid(),
    kri_id UUID REFERENCES kris(id) ON DELETE CASCADE,
    risk_id UUID REFERENCES risks(id) ON DELETE CASCADE,
    created_at TIMESTAMP DEFAULT CURRENT_TIMESTAMP,
    CONSTRAINT unique_kri_risk UNIQUE (kri_id, risk_id)
);

CREATE TABLE kri_measurements (
    id UUID PRIMARY KEY DEFAULT gen_random_uuid(),
    kri_id UUID REFERENCES kris(id) ON DELETE CASCADE,
    measurement_date DATE NOT NULL,
    measured_value DECIMAL(10,2) NOT NULL,
    status kri_status_enum NOT NULL,
    notes TEXT,
    measured_by UUID REFERENCES users(id),
    created_at TIMESTAMP DEFAULT CURRENT_TIMESTAMP
);

CREATE INDEX idx_kris_owner ON kris(kri_owner_id);
CREATE INDEX idx_kris_status ON kris(current_status);
CREATE INDEX idx_kri_measurements_kri ON kri_measurements(kri_id);
CREATE INDEX idx_kri_measurements_date ON kri_measurements(measurement_date
DESC);
```

2.8 On-Demand Risk Assessments

```
CREATE TYPE assessment_request_status_enum AS ENUM ('submitted', 'under_review',
'approved', 'in_progress', 'completed', 'rejected');

CREATE TABLE risk_assessment_requests (
    id UUID PRIMARY KEY DEFAULT gen_random_uuid(),
    request_id VARCHAR(50) UNIQUE NOT NULL,
    title VARCHAR(500) NOT NULL,
    description TEXT,

    -- Requester
    requested_by UUID REFERENCES users(id),
    business_justification TEXT NOT NULL,

    -- Trigger
    trigger_type VARCHAR(100), -- new_product, regulatory_change, etc.
    scope_description TEXT,
    affected_asset_ids JSONB, -- {asset_type, asset_id}[]
    affected_business_units UUID[],

    -- Priority
    priority VARCHAR(50), -- high, medium, low
    requested_due_date DATE,

    -- Status
    status assessment_request_status_enum DEFAULT 'submitted',
    assigned_to UUID REFERENCES users(id),

    -- Results
    resulting_risk_ids UUID[], -- Risks created from this assessment

    created_at TIMESTAMP DEFAULT CURRENT_TIMESTAMP,
    updated_at TIMESTAMP DEFAULT CURRENT_TIMESTAMP
);

CREATE INDEX idx_assessment_requests_status ON risk_assessment_requests(status);
CREATE INDEX idx_assessment_requests_assigned ON risk_assessment_requests(assigned_to);
```

2.9 Supporting Tables

```
-- Risk Review History
CREATE TABLE risk_reviews (
    id UUID PRIMARY KEY DEFAULT gen_random_uuid(),
    risk_id UUID REFERENCES risks(id) ON DELETE CASCADE,
    review_date DATE NOT NULL,
    reviewer_id UUID REFERENCES users(id),
    review_outcome VARCHAR(100), -- no_changes, minor_updates, reassessed, major_changes
    changes_made TEXT,
    review_notes TEXT,
    next_review_date DATE,
    created_at TIMESTAMP DEFAULT CURRENT_TIMESTAMP
);

CREATE INDEX idx_risk_reviews_risk ON risk_reviews(risk_id);
CREATE INDEX idx_risk_reviews_date ON risk_reviews(review_date DESC);

-- Risk Relationships (for future phases)
CREATE TABLE risk_relationships (
    id UUID PRIMARY KEY DEFAULT gen_random_uuid(),
    source_risk_id UUID REFERENCES risks(id) ON DELETE CASCADE,
    target_risk_id UUID REFERENCES risks(id) ON DELETE CASCADE,
    relationship_type VARCHAR(50), -- related_to, causes, contributes_to, parent_of
    description TEXT,
    created_at TIMESTAMP DEFAULT CURRENT_TIMESTAMP,
    CONSTRAINT unique_risk_relationship UNIQUE (source_risk_id, target_risk_id, relationship_type),
    CONSTRAINT no_self_relationship CHECK (source_risk_id != target_risk_id)
);
```

3. Key Views

```
-- Complete Risk Profile
CREATE VIEW vw_risk_profile AS
SELECT
    r.id, r.risk_id, r.title, r.status,
    rc.name AS category,
    u.first_name || ' ' || u.last_name AS owner_name,

    -- Current Assessment
    (SELECT likelihood FROM risk_assessments WHERE risk_id = r.id AND assessment_type = 'current'
     ORDER BY assessment_date DESC LIMIT 1) AS current_likelihood,
    (SELECT impact FROM risk_assessments WHERE risk_id = r.id AND assessment_type = 'current'
     ORDER BY assessment_date DESC LIMIT 1) AS current_impact,
    (SELECT risk_score FROM risk_assessments WHERE risk_id = r.id AND assessment_type = 'current'
     ORDER BY assessment_date DESC LIMIT 1) AS current_score,
    (SELECT risk_level FROM risk_assessments WHERE risk_id = r.id AND assessment_type = 'current'
     ORDER BY assessment_date DESC LIMIT 1) AS current_level,

    -- Assets & Controls
    (SELECT COUNT(*) FROM risk_asset_links WHERE risk_id = r.id) AS asset_count,
    (SELECT COUNT(*) FROM risk_control_links WHERE risk_id = r.id) AS control_count,

    -- Treatment
    (SELECT COUNT(*) FROM risk_treatments WHERE risk_id = r.id AND status IN ('planned', 'in_progress')) AS active_treatments,

    -- KRIs
    (SELECT COUNT(*) FROM kri_risk_links WHERE risk_id = r.id) AS kri_count,
    (SELECT COUNT(*) FROM kri_risk_links krl
     JOIN kris k ON krl.kri_id = k.id
     WHERE krl.risk_id = r.id AND k.current_status = 'red') AS kri_red_count,

    -- Review
    r.next_review_date,
    CASE WHEN r.next_review_date < CURRENT_DATE THEN TRUE ELSE FALSE END AS review_overdue

FROM risks r
LEFT JOIN risk_categories rc ON r.category_id = rc.id
LEFT JOIN users u ON r.risk_owner_id = u.id
WHERE r.deleted_at IS NULL;

-- Risk Dashboard Summary
CREATE VIEW vw_risk_dashboard_summary AS
SELECT
    COUNT(*) AS total_risks,
    COUNT(*) FILTER (WHERE current_level IN ('High', 'Critical')) AS high_critical_risks,
    COUNT(*) FILTER (WHERE review_overdue) AS overdue_reviews,
    COUNT(DISTINCT CASE WHEN active_treatments > 0 THEN id END) AS risks_with_treatments
FROM vw_risk_profile;
```

---

4. Sample Queries

```
-- Top 10 Risks by Score
SELECT risk_id, title, current_level, current_score, owner_name
FROM vw_risk_profile
WHERE status = 'active'
ORDER BY current_score DESC NULLS LAST
LIMIT 10;

-- Risks Exceeding Appetite
SELECT r.risk_id, r.title, ra.risk_level AS current_level,
       rc.risk_tolerance AS appetite,
       CASE
           WHEN rc.risk_tolerance = 'low' AND ra.risk_level NOT IN ('Low') THEN 'EXCEEDS'
           WHEN rc.risk_tolerance = 'medium' AND ra.risk_level IN ('High', 'Critical') THEN 'EXCEEDS'
           ELSE 'WITHIN'
       END AS appetite_status
FROM risks r
JOIN risk_categories rc ON r.category_id = rc.id
JOIN LATERAL (
    SELECT risk_level FROM risk_assessments
    WHERE risk_id = r.id AND assessment_type = 'current'
    ORDER BY assessment_date DESC LIMIT 1
) ra ON TRUE
WHERE r.status = 'active'
HAVING CASE
    WHEN rc.risk_tolerance = 'low' AND ra.risk_level NOT IN ('Low') THEN 'EXCEEDS'
    WHEN rc.risk_tolerance = 'medium' AND ra.risk_level IN ('High', 'Critical') THEN 'EXCEEDS'
    ELSE 'WITHIN'
END = 'EXCEEDS';

-- Treatment Plans Due in Next 30 Days
SELECT t.treatment_id, r.risk_id, r.title, t.strategy, t.status,
       t.target_completion_date, t.target_completion_date - CURRENT_DATE AS days_remaining,
       u.first_name || ' ' || u.last_name AS owner
FROM risk_treatments t
JOIN risks r ON t.risk_id = r.id
LEFT JOIN users u ON t.treatment_owner_id = u.id
WHERE t.status IN ('planned', 'in_progress')
AND t.target_completion_date BETWEEN CURRENT_DATE AND CURRENT_DATE + INTERVAL '30 days'
ORDER BY t.target_completion_date;
```

---

5. API Endpoints (RESTful)

```
# Risk Management
GET    /api/risks                       # List all risks
GET    /api/risks/{id}                  # Get risk details
POST   /api/risks                       # Create risk
PUT    /api/risks/{id}                  # Update risk
DELETE /api/risks/{id}                  # Delete risk
```

```
GET    /api/risks/{id}/assessments     # Get assessment history
POST   /api/risks/{id}/assess          # Create assessment
GET    /api/risks/{id}/treatments      # Get treatments for risk
GET    /api/risks/{id}/kris            # Get KRIs for risk

# Risk Assessments
POST   /api/assessments                # Create assessment
GET    /api/assessments/{id}           # Get assessment details

# Treatment Plans
GET    /api/treatments                 # List treatments
GET    /api/treatments/{id}            # Get treatment details
POST   /api/treatments                 # Create treatment
PUT    /api/treatments/{id}            # Update treatment
PUT    /api/treatments/{id}/progress   # Update progress

# KRIs
GET    /api/kris                       # List KRIs
GET    /api/kris/{id}                  # Get KRI details
POST   /api/kris                       # Create KRI
POST   /api/kris/{id}/measure          # Record measurement
GET    /api/kris/{id}/measurements     # Get measurement history

# Assessment Requests
GET    /api/assessment-requests        # List requests
POST   /api/assessment-requests        # Create request
PUT    /api/assessment-requests/{id}   # Update status

# Reports
GET    /api/reports/risk-register      # Export risk register
GET    /api/reports/heat-map           # Generate heat map
GET    /api/reports/dashboard          # Dashboard data

# Configuration
GET    /api/config/categories          # List categories
POST   /api/config/categories          # Create category
GET    /api/config/appetite            # Get risk appetite
PUT    /api/config/appetite            # Update appetite
```

---

6. Integration Points

With Asset Management

```
-- Query: Get risks for an asset
SELECT r.* FROM risks r
JOIN risk_asset_links ral ON r.id = ral.risk_id
WHERE ral.asset_type = 'physical' AND ral.asset_id = $asset_id;

-- Query: Get asset risk score
SELECT SUM(ra.risk_score) AS total_risk_score
FROM risk_asset_links ral
JOIN risk_assessments ra ON ral.risk_id = ra.risk_id
WHERE ral.asset_id = $asset_id
AND ra.assessment_type = 'current'
AND ra.id IN (
    SELECT MAX(id) FROM risk_assessments
    WHERE risk_id = ral.risk_id
    GROUP BY risk_id
);
```

With Governance Module

```
-- Query: Get risks for a control
```

```
SELECT r.* FROM risks r
JOIN risk_control_links rcl ON r.id = rcl.risk_id
WHERE rcl.control_id = $control_id;

-- Query: Control gap analysis (risks without controls)
SELECT r.risk_id, r.title, r.current_level
FROM vw_risk_profile r
WHERE r.control_count = 0
AND r.status = 'active'
AND r.current_level IN ('High', 'Critical');
```

---

7. Performance Optimization

```
-- Materialized view for dashboard (refresh hourly)
CREATE MATERIALIZED VIEW mv_risk_dashboard AS
SELECT
    COUNT(*) AS total_risks,
    COUNT(*) FILTER (WHERE current_level = 'Critical') AS critical_risks,
    COUNT(*) FILTER (WHERE current_level = 'High') AS high_risks,
    COUNT(*) FILTER (WHERE review_overdue) AS overdue_reviews,
    COUNT(*) FILTER (WHERE active_treatments > 0) AS risks_with_treatment
FROM vw_risk_profile
WHERE status = 'active';

CREATE UNIQUE INDEX ON mv_risk_dashboard ((1));

-- Refresh schedule
CREATE OR REPLACE FUNCTION refresh_risk_dashboard()
RETURNS void AS $$
BEGIN
    REFRESH MATERIALIZED VIEW CONCURRENTLY mv_risk_dashboard;
END;
$$ LANGUAGE plpgsql;

-- Call from cron job or application scheduler
```

---

8. Data Migration

```
-- Import risks from CSV
CREATE TABLE risks_import_staging (
    title VARCHAR(500),
    description TEXT,
    category_name VARCHAR(200),
    owner_email VARCHAR(255),
    business_unit_name VARCHAR(200),
    inherent_likelihood INTEGER,
    inherent_impact INTEGER,
    current_likelihood INTEGER,
    current_impact INTEGER,
    status VARCHAR(50),
    tags TEXT -- comma-separated
);

-- Transform and load
INSERT INTO risks (risk_id, title, description, category_id, risk_owner_id,
business_unit_ids, status, tags)
SELECT
    'RISK-' || LPAD(nextval('risk_id_seq')::TEXT, 4, '0'),
    s.title,
    s.description,
    rc.id,
    u.id,
    ARRAY[bu.id],
    COALESCE(s.status, 'active'),
    string_to_array(s.tags, ',')
FROM risks_import_staging s
LEFT JOIN risk_categories rc ON rc.name = s.category_name
LEFT JOIN users u ON u.email = s.owner_email
LEFT JOIN business_units bu ON bu.name = s.business_unit_name;

-- Insert assessments
INSERT INTO risk_assessments (risk_id, assessment_type, likelihood, impact, assessor_id)
SELECT r.id, 'inherent', s.inherent_likelihood, s.inherent_impact, r.created_by
FROM risks r
JOIN risks_import_staging s ON r.title = s.title
WHERE s.inherent_likelihood IS NOT NULL;
```

Total Schema: 14 main tables + 4 junction tables + 4 views

Estimated Database Size: ~500MB for 200 risks with 5 years of history

Query Performance: <100ms for dashboard, <500ms for complex reports