NYCPS TMS: Formal Change & Risk Management Plan

I. Introduction & Integration with Agile/DevOps

This document defines the formal Change Management and Risk Management processes supplementing the core Agile (Scrum) and DevSecOps practices for the NYCPS Transportation Management System (TMS) project. While Agile methodologies embrace iterative refinement within sprints based on feedback and backlog grooming, the scale, complexity, contractual nature, and public sector context of this project necessitate a formal structure for managing significant changes to baselined scope, schedule, or budget, and for proactively managing project risks.

Integration Principle: These formal processes are designed to work *with*, not against, the Agile workflow. They provide a framework for control and accountability for substantial deviations or potential threats, while day-to-day development and refinement continue within the sprint cadence.

- Approved Change Requests (CRs) translate into prioritized Epics/Features/User Stories within the Product Backlog.

- Risk Mitigation actions become tasks within the Sprint Backlog.
- Regular Agile ceremonies (Reviews, Retrospectives, Grooming) serve as inputs for identifying potential changes and risks.
- Automation via Jira/ADO and Confluence streamlines tracking and reporting for both Agile execution and formal PM processes.

Adherence to these Change and Risk Management procedures is mandatory for all project team members and stakeholders to ensure controlled execution, transparency, and successful delivery against commitments.

II. Governance Context for Change & Risk

The effectiveness of these plans relies on the established project governance structure. Key bodies involved include:

- **Project Managers (Vendor & NYCPS):** Co-manage day-to-day execution, facilitate processes, perform initial CR/Risk assessment, prepare reports.
- **Product Owner(s) (NYCPS):** Owns the Product Backlog, key decision-maker for functional scope changes within Agile framework, provides input on CR impact/value.
- **Change Control Board (CCB):** Formal body (membership defined: e.g., PMs, PO, Key Tech Leads, Sponsor Rep) responsible for reviewing and approving/rejecting significant Change Requests impacting baseline

scope, schedule, or cost. Meets regularly (e.g., bi-weekly) or ad-hoc as needed.

- **Technical Review Board (TRB):** Reviews technical impact of changes, assesses technical risks.
- **Security Review Board (SRB):** Reviews security implications of changes, assesses security risks.
- **Steering Committee:** Provides highest-level oversight, resolves escalated risks/issues, approves major strategic changes or budget adjustments recommended by the CCB.

III. Detailed Change Management Plan

A. Purpose & Scope

Purpose: To provide a structured, documented, and controlled process for managing requests to change the agreed-upon project scope, schedule, cost, or technical approach *after* the initial requirements baseline for a major phase or release has been formally approved (typically post Phase 1 requirements sign-off).

Scope - What Requires a Formal Change Request (CR):

- Requests for significant new features or functionality not included in the baselined requirements for the current or upcoming planned release/phase.
- Changes that materially impact the project schedule (e.g., delay a major milestone by more than one sprint) or budget (e.g., require additional resources or licenses).
- Changes impacting contractual obligations or deliverables.
- Significant alterations to the approved technical architecture or core security controls.
- Changes requested by NYCPS stakeholders *after* UAT sign-off for a specific release increment.

Out of Scope (Handled via Agile Backlog Management):

- Clarifications or refinements of existing user stories during backlog grooming or sprint execution.
- Bug fixes for implemented functionality (managed via defect tracking).
- Minor technical implementation details decided by the development team that do not impact external interfaces, NFRs, or overall architecture.
- Reprioritization of *existing* backlog items by the Product Owner (unless it significantly impacts major milestones requiring CCB notification).

B. Change Request (CR) Workflow & Process Steps

1. **Step 1: CR Initiation & Submission**

   ### Description:

   Any project stakeholder (Vendor team member, NYCPS stakeholder) identifies a potential need for change that falls within the scope defined above.

   ### Implementation How-To:

   a. Requestor creates a new issue of type "Change Request" in the project's Jira/ADO board.

   b. Requestor completes the mandatory fields defined in the **Change Request Form Template** (see below). This includes a clear description, strong justification/business value, requestor details, date, and initial thoughts on impact/priority.

   c. Attach any supporting documentation (e.g., mockups, requirement documents).

   Responsibility: Any Stakeholder (Initiation), Requestor (Documentation).

2. **Step 2: CR Logging & Initial Assessment**

Description:

The Project Manager (or designated Change Manager) reviews the submitted CR for completeness and logs it formally.

Implementation How-To:

a. Project Manager reviews the submitted Jira ticket for clarity and required information within 1-2 business days.

b. If incomplete, PM requests clarification from the Requestor via Jira comments.

c. If complete, PM assigns a unique CR ID (can be the Jira key), updates the status to "Under Assessment", and adds it to the central Change Register (maintained as a Jira Filter/Dashboard and potentially summarized on a Confluence page).

d. PM performs a quick initial assessment: Does this clearly require CCB review, or could it potentially be addressed as a backlog refinement/bug? Assigns initial priority estimate.

Responsibility: Project Manager.

3. **Step 3: Detailed Impact Assessment**

Description:

Relevant Subject Matter Experts (SMEs) conduct a thorough analysis of the proposed change's impact across multiple dimensions.

Implementation How-To:

a. PM assigns assessment tasks to relevant SMEs via linked Jira tasks or comments (e.g., Tech Lead for technical feasibility/effort, QA Lead for testing impact, Security Architect for security implications, PO for value/priority reassessment, PM for schedule/cost).

b. SMEs perform analysis within an agreed timeframe (e.g., 3-5 business days).

c. SMEs document their findings using the **Impact Assessment Template** (see below), typically on a linked Confluence page or within dedicated Jira custom fields. Analysis must cover:

- **Scope:** How does this change functionality? What other areas/stories are affected?
- **Schedule:** Estimated effort (e.g., Story Points, Person-Days), impact on

current sprint, impact on major milestones/release dates.

- **Cost:** Additional resource needs, software/licensing costs, AWS GovCloud cost implications.
- **Technical:** Feasibility, architectural impact, complexity, impact on performance/scalability/reliability.
- **Testing:** Additional testing required (automated/manual), impact on existing test suites.
- **Security:** Potential new vulnerabilities, impact on existing controls, compliance implications.
- **Risk:** New risks introduced, impact on existing risks.

- **Dependencies:** Impact on or from other teams/systems/features.

Responsibility: Assigned SMEs (Tech Lead, QA Lead, Sec Lead, PO, PM, Arch, etc.).

4. **Step 4: PM Review & Recommendation**

Description:

The Project Manager consolidates the impact assessment and formulates a recommendation for the CCB.

Implementation How-To:

a. PM reviews the completed impact assessments for thoroughness and consistency.

b. PM synthesizes the findings into a summary.

c. PM develops a formal recommendation: Approve, Reject, Defer, or Request More Information, including rationale based on the impact analysis vs. the original justification/value.

d. PM updates the CR status in Jira/ADO to "Ready for CCB Review" and adds it to the agenda for the next CCB meeting.

Responsibility: Project Manager.

5. **Step 5: Change Control Board (CCB) Review & Decision**

Description:

The formally constituted CCB reviews the CR, impact assessment, and recommendation to make a final, documented decision.

Implementation How-To:

a. CCB meeting held at regular cadence (e.g., bi-weekly) or convened ad-hoc for urgent requests. Agenda circulated beforehand.

b. PM or Requestor presents the CR, justification, and summary of impact assessment.

c. SMEs present details of impact assessment as needed.

d. CCB discusses benefits, costs, risks, and alignment with project goals/constraints.

e. CCB makes a formal decision:

- **Approved:** Change proceeds to implementation.
- **Approved with Conditions:** Change proceeds but specific conditions must be met.

- **Rejected:** Change will not be implemented. Rationale documented.
- **Deferred:** Decision postponed pending more information or strategic timing. CR placed on hold.
- **More Information Required:** CR returned to Impact Assessment stage with specific questions.

f. Decision and rationale are formally documented in CCB meeting minutes (Confluence) and the CR status/resolution updated in Jira/ADO.

Responsibility: CCB Chairperson, CCB Members, PM (Presentation/Documentation).

> **Governance Gate: Formal CCB approval required for any significant changes impacting baselined scope, schedule, or budget.**

6. **Step 6: Implementation & Communication**

Description:

If approved, the change is integrated into the project plan and backlog; the decision is communicated.

Implementation How-To:

a. PM updates project schedule, budget forecast, and potentially risk register based on the approved change.

b. Product Owner works with the BA/Team to translate the approved CR into well-defined Epics/Features/User Stories in the Product Backlog.

c. Prioritize the new backlog items according to standard backlog refinement process.

d. PM communicates the CCB decision and its implications (updated schedule, added features) to the wider project team and relevant stakeholders via meeting minutes summary and status reports.

e. Update the Change Register with the final decision and link to implementation backlog items.

Responsibility: Project Manager, Product Owner, Business Analyst, Scrum Master.

C. Change Management Tools & Artifacts

- **Change Request Tracker:** Jira/ADO Project configured with:
    - Custom Issue Type: "Change Request".
    - Custom Workflow: Submitted -> Under Assessment -> Ready for CCB -> CCB Review -> Approved / Rejected / Deferred -> Implemented / Closed.
    - Custom Fields: CR ID, Requestor, Date Submitted, Justification, Business Value, Priority (Initial/Final), Impact Summaries (Scope, Schedule, Cost, Tech, Sec, Risk), CCB Decision, Decision Date, Link to Implementation Tickets, Link to Confluence Impact Doc.
- **Change Register:** A saved Filter/Dashboard in Jira/ADO showing all "Change Request" issues and their current status. Potentially summarized on a Confluence page.
- **Confluence Space:** Dedicated area for:
    - Change Management Plan (this document).
    - CCB Charter & Membership.
    - CCB Meeting Minutes Archive.
    - Detailed Impact Assessment Documents (using template).

- **Change Request Form Template (Conceptual - implemented as Jira fields):**

  ```
  CR Template Fields:
      - CR ID: (Auto-generated or Jira Key)
      - Title: (Concise summary)
      - Requestor:
      - Date Submitted:
      - Change Description: (Detailed 'What')
      - Justification / Business Value: (Detailed 'Why', benefits, alignment with goals)
      - Proposed Solution (if known):
      - Urgency/Requested Implementation Date:
      - Initial Impact Assessment (Requestor's view – High/Med/Low on Scope/Sched/Cost):
      - Affected Components/Modules:
      - Attachments:
  ```

- **Impact Assessment Template (Conceptual - implemented on Confluence page linked to Jira CR):**

  ```
  Impact Assessment Template Sections:
      - CR ID & Title:
      - Assessment Date:
      - Assessor(s) / Role(s):
  ```

- Scope Impact Analysis: (Detailed changes to functionality, interfaces, data)
- Schedule Impact Analysis: (Estimated effort – Story Points/Days, impact on sprint/milestones)
- Cost Impact Analysis: (Resource needs, licensing, infra costs)
- Technical Impact Analysis: (Feasibility, complexity, architectural changes, performance/scalability effects)
- Testing Impact Analysis: (New test cases needed, automation effort, regression scope)
- Security Impact Analysis: (New threats/vulnerabilities, impact on existing controls, compliance check)
- Risk Impact Analysis: (New risks created, existing risks impacted)
- Dependency Impact Analysis: (Impact on/from other teams/systems)
- Alternatives Considered (Optional):
- Overall Assessment Summary & Recommendation:

D. Roles & Responsibilities Summary (Change Management)

- **Requestor:** Initiates CR, provides justification.
- **Project Manager:** Logs CR, facilitates impact assessment, prepares recommendation, manages Change Register, communicates decisions, updates plans.
- **SMEs (Tech, QA, Sec, PO, etc.):** Perform detailed impact analysis in their area of expertise.
- **Change Control Board (CCB):** Reviews significant CRs, makes Approve/Reject/Defer decisions based on overall project goals and constraints.
- **Product Owner:** Assesses business value/priority, incorporates approved changes into backlog.
- **Development Team:** Implements approved changes via backlog items.

IV. Detailed Risk Management Plan (Enhanced & Prescriptive)

A. Purpose, Scope & Philosophy

Purpose: To establish and mandate a systematic, proactive, documented, and continuously monitored process for identifying, analyzing, planning responses to, tracking, and controlling potential events or conditions (risks) that could negatively impact the successful achievement of the NYCPS TMS project objectives. Our objective is not just to react to risks, but to anticipate and manage them proactively to ensure project success within scope, schedule, budget, quality, security, and compliance constraints.

Scope: This comprehensive plan applies to all project phases, from initiation through deployment and into operations. It covers all categories of risk, including technical, operational, organizational, external dependencies, vendor-related, security, compliance, financial, schedule, and stakeholder-related risks.

Philosophy (Conservative & Proactive): Given the critical public sector nature of this project, our risk management philosophy is inherently conservative. We will prioritize thorough identification, assume risks are potentially higher impact until proven otherwise, favor proactive mitigation over acceptance where feasible, maintain meticulous documentation, and ensure clear communication and escalation pathways. Risk management is an ongoing, integrated activity for the *entire* project team and key stakeholders.

B. Risk Management Methodology & Process Steps

1. **Step 1: Risk Identification (Continuous & Exhaustive)**

   Description:

This stage involves the systematic and ongoing effort to identify any potential risk that could affect the project. We will employ multiple techniques to ensure comprehensive coverage.

Implementation How-To:

a. **Formal Identification Sessions:**

- **Initial Risk Workshop (Phase 1):** Mandatory, facilitated session with core project team (PMs, Leads, Arch, Sec, QA, PO) and key NYCPS stakeholders (OPT, DIIT SMEs). Use brainstorming, SWOT, review of similar project lessons learned. Output populates the initial Risk Register.
- **Phase-Based Risk Reviews:** Dedicated risk identification sessions held at the beginning of major project phases (e.g., before starting complex integrations, before UAT planning).

- **Feature-Specific Risk Assessment:** For complex or high-impact features/epics, conduct mini-risk assessments during design/grooming.

b. **Continuous Identification Techniques:**

- **Checklist Analysis:** Maintain and utilize project-specific checklists covering common risk areas (Technology - AWS GovCloud specifics, new tech adoption; Integration - complexity, vendor dependency; Resources - skill gaps, availability; Schedule - dependencies, estimation accuracy; Scope Creep; Security - vulnerabilities, compliance gaps; External - regulatory changes, SBC readiness). **Checklist stored in Confluence, reviewed quarterly.**

- **Assumption & Constraint Analysis:** Document all key

project assumptions and constraints. Regularly review them and identify risks associated with them proving invalid. Stored in Confluence.

- **Agile Ceremony Input:** Actively solicit potential risks during Daily Stand-ups (blockers often indicate risks), Sprint Reviews (feedback may reveal risks), Retrospectives (process issues are risks), and Backlog Grooming (ambiguity is a risk). Scrum Masters are responsible for facilitating this.
- **Expert Judgment & Interviews:** Regularly consult internal/external SMEs (Cloud Architects, Security Specialists, GIS Experts, experienced OPT personnel) specifically asking about potential risks in their domain.
- **Document Review:** Systematically review RFP,

SOWs, Design Documents, Test Plans, Contracts, and Compliance requirements for potential risks.

- **Trend Analysis:** Monitor project metrics (velocity fluctuations, defect trends, CI/CD failures) for patterns indicating underlying risks.

c. **Logging Risks:**

- **Mandatory Logging:** **Any potential risk identified through any channel *must* be logged immediately by the identifier (or reported to PM/Scrum Master for logging) in the central **Risk Register (Jira/ADO)**.**

- **Required Information:** **Use the "Risk" issue type with standardized fields (see Section IV.C). Initial entry**

requires at minimum: Clear Risk Title, Detailed Description (Cause-Risk-Effect), Date Identified, Identified By, Initial Perceived Priority/Impact.

Responsibility: All Team Members & Stakeholders (Identification Mandate), PM/Scrum Master (Facilitation, Logging Assurance, Workshop Lead), Technical/QA/Sec Leads (Checklist Maintenance, SME Input).

2. Step 2: Qualitative Risk Analysis & Prioritization

Description:

Systematically assess the likelihood and potential impact of each identified risk to determine its overall significance and prioritize further action. All assessments must be documented.

Implementation How-To:

a. **Regular Assessment Cadence:** Newly logged risks are assessed by the PM and relevant SMEs within a defined timeframe (e.g., 3 business days). Existing risks are periodically reassessed (see Monitoring).

b. **Probability Assessment (P):**

- **Estimate likelihood using the defined 1-5 scale (1-Very Low [<10%], 2-Low [10-30%], 3-Medium [31-60%], 4-High [61-90%], 5-Very High [>90%]).**
- **Define criteria for each level (e.g., High = >75% chance) in the Risk Plan (Confluence).**
- ****Document Assumptions:** Record the basis/rationale for the assigned probability rating in the Jira risk ticket (e.g., "Based on complexity of integration point X", "Historical data from similar modules suggests..."). Mandatory Field.**

c. Impact Assessment (I):**

- **Estimate impact across multiple dimensions (Schedule, Cost,**

Scope/Quality, Security, Compliance, Reputation) using the defined 1-5 scale (1-Negligible, 2-Minor, 3-Moderate, 4-Significant, 5-Severe).

- **Define clear, objective criteria for each impact level per dimension (e.g., Severe Schedule Impact = >2 month delay to critical milestone; Significant Security Impact = PII Breach affecting >1000 users). Document these scale definitions in the Risk Management Plan (Confluence).**
- **Use the *highest* impact rating across all dimensions as the overall Impact score for the risk.**
- ****Document Assumptions:** Record the basis/rationale for the**

assigned impact ratings in the Jira risk ticket. Mandatory Field.

d. Risk Score Calculation & Prioritization:**

- Use the approved Probability/Impact (PxI) Matrix (defined in this plan, see template below) to automatically calculate or manually assign the Risk Level (e.g., Low, Medium, High, Critical) based on P and I ratings.
- Store P, I, and Score/Level in mandatory Jira custom fields.
- Prioritize risks for response planning based on Risk Level (Critical > High > Medium > Low). All Critical and High risks *must* have a defined response plan. Medium risks require review and potential response

planning. Low risks are typically accepted but monitored.

Responsibility: Project Manager (Process Owner), Assigned SMEs (Performing Assessment), All Team Members (Input/Challenge during reviews).

Probability/Impact Matrix (PxI) Definition (Example - To be finalized):

Probability (P) ↓	Impact (I) →				
	1 (VL/Neg)	2 (L/Minor)	3 (M/Mod)	4 (H/Sig)	5 (VH/Sev)
5 (VH >90%)	Medium (5)	High (10)	High (15)	Critical (20)	Critical (25)
4 (H 61-90%)	Low (4)	Medium (8)	High (12)	High (16)	Critical (20)
3 (M 31-60%)	Low (3)	Low (6)	Medium (9)	High (12)	High (15)
2 (L 10-30%)	Low (2)	Low (4)	Low (6)	Medium (8)	Medium (10)
1 (VL <10%)	Low (1)	Low (2)	Low (3)	Low (4)	Medium (5)

Score Ranges: Low (1-4), Medium (5-9), High (10-16), Critical (17-25). Score = P * I. Ranges to be finalized and documented in Risk Plan.

3. Step 3: Quantitative Risk Analysis (Mandatory for Critical Risks)

Description:

For all risks assessed as "Critical" (and potentially "High" risks with significant cost/schedule impact), perform quantitative analysis to better understand the potential numerical impact.

Implementation How-To:

a. **Mandatory for risks meeting defined criteria (e.g., Critical score, potential impact >$X or >Y weeks delay).**

b. ****Techniques:****

- ****Expected Monetary Value (EMV):** Calculate EMV = P(%) * Cost Impact($). Used primarily for comparing financial implications of different risks or response strategies. Requires quantifiable cost impact estimates derived from SME input and documented.**
- ****Schedule Network Analysis (PERT/Monte**

Carlo): If the risk significantly impacts schedule dependencies, use PERT estimation (Optimistic, Most Likely, Pessimistic - with documented rationale for each estimate) for affected tasks or Monte Carlo simulation on the project schedule (using tools like Primavera Risk Analysis or simpler Excel add-ins) to determine probabilistic completion dates (e.g., P80 confidence level) and quantify potential schedule delays.**

c. **Document quantitative analysis results, inputs, assumptions, and methodology clearly within the Jira risk ticket or linked Confluence page.**

Responsibility: Project Manager, Lead Scheduler/Planner, Cost Analyst (if applicable), SMEs (for input data).

4. Step 4: Risk Response Planning & Ownership

Description:

Define and document specific, actionable, and time-bound strategies and tasks to address prioritized risks. Assign clear ownership for implementing and monitoring each response plan.

Implementation How-To:

a. **For *every* Critical and High risk, and selected Medium risks, the assigned **Risk Owner** (designated SME or Lead) develops a detailed response plan documented in Jira/Confluence.**

b. **Select primary strategy (document rationale):**

- ****Avoid:** Change the project plan to eliminate the threat entirely (requires CCB approval if baseline impacted). E.g., Choose different AWS service, remove complex feature.**
- ****Mitigate:** Actions to reduce Probability and/or Impact. E.g., Implement additional testing (specify**

what* testing), add redundancy (specify *how*), conduct security training (specify *content/audience*), perform technical spike/prototype *early*, increase monitoring (specify *metrics*). **Most common strategy.

- **Transfer:** Shift impact/ownership to a third party (e.g., enhanced warranty/SLA with hardware supplier, specific cyber insurance coverage - Requires Legal/Contract review). Document contractual basis.
- **Accept (Active vs. Passive):**
    - **Active Acceptance:** No immediate

mitigation, but develop a **Detailed Contingency Plan outlining specific step-by-step actions, required resources, communication steps, and decision points to execute *if* the risk occurs. Define clear, measurable **trigger conditions** for activating the contingency plan (e.g., "If**

integration test failure rate exceeds X% for Y hours"). May involve setting aside pre-approved schedule/budget contingency reserves. Requires documented approval from PM/Steering Committee.

- ****Passive Acceptance:** Take no action, acknowledge the risk. Only acceptable for documented**

Low risks after review by PM.

c. **Response Plan Details:** Document specific, actionable steps (e.g., "Develop automated test suite for module X", "Conduct penetration test on API Y by Z date"), target completion dates for each step, responsible individual(s) for each step, and required resources.

d. **Mitigation/Avoidance Actions -> Backlog:** Create specific Tasks or User Stories in the Product Backlog for implementing mitigation/avoidance actions. Ensure stories have clear acceptance criteria related to risk reduction. Prioritize these appropriately with the Product Owner.

e. **Contingency Plan Documentation:** Store detailed contingency plans in Confluence, linked to the Risk ticket. Ensure plans are reviewed and updated periodically.

f. **Residual Risk Assessment:** *After* defining the response plan, meticulously reassess the Probability and Impact *assuming the plan is successfully implemented*. Document the

Residual Risk Level and the rationale in Jira/Confluence. If residual risk is still unacceptably high (e.g., High/Critical), **mandate escalation** to PM/Steering Committee and development of alternative/additional responses.

Responsibility: Risk Owner (Develops plan), Project Manager (Ensures plan exists, tracks), Product Owner (Prioritizes backlog items), CCB (Approves avoidance impacting baseline), Steering Committee (Accepts high residual risk).

5. **Step 5: Risk Monitoring, Control & Reporting (Continuous & Rigorous)**

Description:

Continuously track the status of risks, response plan execution, and trigger conditions. Identify new risks and report transparently on the overall risk posture.

Implementation How-To:

a. **Risk Register Review Cadence:**
   - **Weekly Project Status Meeting:** Mandatory agenda item. Review status of *all* open Critical and High risks,

progress on their response actions (linked Jira tasks - check actual status), any changes in P/I, and any newly identified Medium+ risks requiring immediate analysis.

- ****Monthly Full Register Review:** Mandatory dedicated meeting (or extended section in MBR prep) to review the *entire* risk register. Re-assess P/I for all open Medium+ risks. Verify status of Low risks (confirm still low). Close resolved/obsolete risks.**
- ****MBR/Steering Committee:** Formal presentation using standardized templates (e.g., Top 5 Risks chart, Risk Matrix summary) showing key strategic risks, status of Critical risk**

mitigations, escalated risks requiring decisions/support, and trend analysis.

b. **Risk Owner Monitoring & Updates:** Risk Owners are accountable for continuously monitoring their assigned risks and triggers. They *must* update the risk status, provide progress updates on response actions, and report any significant changes or concerns to the PM immediately and during weekly reviews via Jira/Confluence.

c. **Response Implementation Tracking:** PM/Scrum Master track progress of mitigation/avoidance tasks in the backlog during standard sprint execution and reviews.

d. **Contingency Plan Activation:** If a trigger is met, the Risk Owner *must* immediately notify the PM and initiate the approved contingency plan. PM escalates as necessary based on the plan's requirements.

e. **New Risk Integration:** Newly identified risks immediately enter the

analysis and response planning cycle (Steps 2-4).

f. **Risk Closure:** Formally close risks in Jira/ADO *only* after verification that the risk is resolved (mitigation complete and effective, risk event passed, etc.). Closure requires PM approval and documented rationale.

g. **Reporting:** Utilize Jira/ADO dashboards (configured with risk fields) for real-time visibility. PM incorporates quantitative and qualitative risk summaries into Weekly Status Reports and MBR Presentations using approved templates. Maintain historical archive of risk status over time.

Responsibility: Project Manager (Overall Process, Reporting, Facilitation), Risk Owners (Monitoring assigned risks & actions), Scrum Masters (Facilitating identification), All Team Members (Ongoing identification & status updates).

6. **Step 6: Risk Escalation (Formalized)**

Description:

Implement a clear, documented pathway for escalating risks that exceed the management threshold or authority at a given level.

Implementation How-To:

a. **Mandatory Escalation Triggers (Examples - To be finalized & documented in Risk Plan):**

- **Risk remains Critical after X weeks of mitigation effort without significant P/I reduction.**
- **Residual Risk score remains High/Critical after response planning, deemed unacceptable by PM.**
- **Contingency Plan activation requires unbudgeted resources or impacts external stakeholders significantly.**
- **High/Critical risk with cross-departmental dependencies unresolved after Y days.**
- **Resource constraints prevent timely**

implementation of critical risk responses.

- **Emergence of a new risk with potential Severe impact (I=5) requires immediate executive visibility.**

b. **Formal Escalation Path & Documentation:**

- ****Risk Owner -> Project Manager:** Initial escalation via Jira status update/comment AND direct communication (meeting/email). PM formally acknowledges.**
- ****Project Manager -> CCB/TRB/SRB:** For risks requiring baseline changes or specialized review. Formal submission via Jira and presentation at relevant board meeting. Decision documented in minutes/Jira.**

- **Project Manager -> Steering Committee:** For strategic/high-impact/unresolved risks. Formal presentation during MBR or dedicated session. Decision documented in minutes.

c. **Tracking:** Escalated status clearly marked in the Jira Risk ticket. Resolution path and final decision documented.

Responsibility: Risk Owner (Initiates), Project Manager (Manages escalation process & documentation), Governance Bodies (Decision-making).

7. **Step 7: Compliance & Legal Integration (Mandatory Checkpoint)**

Description:

Ensure all risks touching upon legal, regulatory, contractual, or compliance mandates receive appropriate expert review and sign-off.

Implementation How-To:

a. **Use mandatory Jira labels/custom fields to tag risks related to specific**

compliance areas (FERPA, NY Ed Law 2-d, WCAG, SLA Contract Terms, Security Policies, Data Privacy).

b. Establish automated Jira notifications or manual workflow steps to ensure the designated NYCPS Compliance Officer and/or Legal Counsel representative is automatically notified or assigned for review of risks tagged with relevant compliance labels, especially those rated Medium or higher.

c. Formal sign-off (via Jira transition or documented approval in Confluence) from Compliance/Legal *must* be obtained for response plans (especially 'Accept' strategies) and residual risk assessments for all High/Critical compliance-related risks *before* final approval by PM or CCB/Steering Committee.

Responsibility: Project Manager (Ensuring process adherence), Compliance Officer/Legal Rep (Review/Approval), Risk Owner (Providing necessary context).

Governance Gate: Explicit sign-off required from Compliance/Legal for managing significant compliance-related risks.

C. Risk Management Tools & Artifacts

- **Risk Management Plan:** This enhanced document (stored in Confluence). Defines methodology, roles, scales, matrix, reporting, escalation triggers.**
- **Risk Register:** **Mandatory & Central:** Jira/ADO Project configured with:**
  - **Custom Issue Type: "Risk".**
  - **Custom Workflow: Open -> Analyzing -> Response Planning -> Responding (Mitigate/Avoid/Transfer) / Monitoring (Accept/Contingency) -> Escalated (Optional) -> Closed / Occurred.**
  - ****Mandatory Custom Fields:** Risk ID (Jira Key), Detailed Description (Cause-Risk-Effect), Category (Technical, Schedule, Budget, Security, Compliance, External, etc.), Date Identified, Identified By, **Probability Rating (1-5 Dropdown/Value)**, **Impact Rating (1-5 Dropdown/Value per dimension)**, **Overall Impact Rating (Highest)**, **Risk Score (Calculated PxI)**, **Risk Level (Calculated - Low/Med/High/Crit)**, **Analysis**

Assumptions (Mandatory Text Field), Response Strategy (Dropdown: Avoid, Mitigate, Transfer, Accept-Active, Accept-Passive), Response Plan Summary (Text/Link to Confluence), **Residual Probability (1-5)**, **Residual Impact (1-5)**, **Residual Risk Level (Calculated)**, **Residual Risk Rationale**, Risk Owner (User Picker), Status, Trigger Conditions (Text - for Contingency), Contingency Plan Link (URL to Confluence), Last Reviewed Date, Link to Mitigation Tasks/CRs, **Compliance Tags (Multi-select list)**, **Escalation Status (Dropdown)**.**

- **Probability & Impact Scales & Matrix:** Formally defined and documented criteria for each P&I level across dimensions, and the PxI matrix mapping. Stored in Confluence (linked from Jira fields).**
- **Risk Breakdown Structure (RBS):** Stored in Confluence, used as input for checklists/workshops.**
- **Meeting Minutes:** Stored in Confluence, explicitly capturing risk discussions, decisions, and action items (linked to Jira).**
- **Reports & Dashboards:** Jira/ADO Dashboards configured for real-time views (Risk Matrix, Risks by Status/Owner/Level, Open Mitigation Tasks). Risk summaries embedded in automated Weekly Status Reports (Confluence macros) and MBR Decks.**

D. Roles & Responsibilities Summary (Risk Management - Enhanced)

- **All Team Members/Stakeholders: Mandatory responsibility to identify and report potential risks immediately using the defined process (Jira). Participate in analysis/response planning when requested.**
- **Project Manager: Owns, facilitates, and enforces the overall risk management process. Ensures register integrity and completeness. Ensures all Medium+ risks are assessed, have owners, and response plans (or documented acceptance). Manages risk reviews, reporting, and escalations. Ensures compliance checks occur.**
- **Risk Owner: Accountable for the end-to-end management of an assigned risk: developing/documenting response & contingency plans, overseeing implementation of actions, continuously monitoring status/triggers, reporting updates, reassessing residual risk, and initiating escalations.**
- **SMEs (Tech, QA, Sec, Ops, BA, etc.): Provide expert input for identification, qualitative/quantitative analysis (including documenting assumptions), and detailed response planning within their domain. Implement mitigation tasks assigned via backlog.**
- **Scrum Master: Facilitates risk identification within sprint ceremonies and helps remove impediments related to risk**

mitigation tasks assigned to the team.

- Product Owner: Provides input on risk impact from a business value/user perspective and prioritizes risk response tasks (mitigation/avoidance stories) in the Product Backlog.
- Governance Bodies (CCB, TRB, SRB, Steering Committee): Review escalated risks, approve significant response plans (especially 'Avoid' strategies impacting baseline), provide strategic direction, formally accept significant residual risks, and allocate contingency resources if needed.
- Compliance Officer/Legal Rep: Reviews and provides input/approval on risks and responses related to compliance and legal matters, acting as a mandatory gate for significant compliance risks.

V. Integrating Formal PM with Agile/DevOps

These formal Change and Risk Management processes are designed to overlay, not replace, the Agile framework:

- **Change vs. Backlog:** The CCB handles changes *to the baseline*. The Product Owner manages priority and refinement *within* the baseline via the backlog. Small adjustments or

clarifications identified during grooming are typically *not* formal CRs. Significant deviations emerging from grooming *should* trigger a CR.

- **Risk Actions in Sprints:** Mitigation or contingency actions identified in the Risk Plan become concrete tasks or User Stories in the Product Backlog, prioritized by the PO alongside features. The work gets done within sprints.
- **Transparency:** Jira/ADO serves as the central hub. CRs and Risks are issue types alongside User Stories and Bugs, providing integrated visibility on project boards and dashboards.
- **Cadence Alignment:** CCB meetings and Risk reviews are scheduled to align with sprint cadences and MBR reporting cycles, ensuring timely information flow.
- **Focus:** Agile focuses on *delivering value iteratively within defined boundaries*. Formal PM focuses on *managing changes to those boundaries* and *proactively addressing threats* to achieving the overall objectives.

VI. Implementation How-To Summary (Tooling & Process Setup)

1. Configure Tools:

- **Set up custom issue types ("Change Request", "Risk"), workflows, and mandatory custom fields (as detailed in Sections III.C & IV.C) in Jira/ADO.**
- **Create Jira/ADO dashboards and saved filters for Change Register and Risk Register visualization and reporting.**
- **Create Confluence space with defined structure. Develop and upload page templates for Plans, Charters, Minutes, Impact Assessments, Risk Matrix/Scales, Decision Log.**

2. **Develop Plans & Charters: Formally write and get approval for the Change Management Plan, Risk Management Plan, CCB Charter, TRB/SRB Charters (if applicable) within Confluence.**
3. **Establish Governance Bodies: Officially designate members and chairs for CCB, TRB, SRB, Steering Committee. Schedule initial meetings and recurring cadence.**
4. **Conduct Initial Workshops: Run project kick-off, initial requirements workshops, and the mandatory Initial Risk Identification workshop. Populate initial backlog and Risk Register.**
5. **Train the Team & Stakeholders: Conduct dedicated training sessions covering:**
    - **Overall project governance structure.**
    - **Detailed Change Management process (when/how to submit CRs, assessment**

process, CCB role).

- Detailed Risk Management process (how to identify risks, assessment scales, response strategies, owner responsibilities, monitoring/reporting).
- How to use Jira/Confluence for CR/Risk tracking and documentation.

6. Integrate into Cadence: Incorporate CCB meetings and Risk Register reviews into the regular project meeting schedule defined in the Communications Plan. Ensure agendas include these items.
7. Monitor & Refine: Use retrospectives and stakeholder feedback to continuously monitor the effectiveness of the Change and Risk processes themselves, making documented adjustments as needed (potentially requiring plan updates and re-approval).

Responsibility: Project Manager, Jira/Confluence Administrator, Scrum Master, CCB Chair, Governance Body Members.