Change Management - Recommended Implementation Sequence

Legend:

Realize value with every phase deployed.

Your maturity path is unique. This guidance helps maximize platform potential to achieve business outcomes.

Suggested to setup left to right

* Requires ITSM Pro+ - check your licensing

Use the Best Practices to execute the implementation.

Before you start

1. Understand Change Management
2. Understand DevOps Change Velocity
3. Understand NOW Assist for Change Management

Service Response: Correlate & Remediate

Phase 1: Stabilize core operations with strong foundations and out-of-the-box features

Standard Change Management	Enable Normal, Standard, Emergency change types and set minimal mandatory fields
Change Policies	Set up simple approval rules and define specific scenario for Emergency changes
Change Calendar	Define and set up blackout windows and business hours (non-CI conflict detection)
Basic CAB	Define and set schedule change meetings and use manual approvals
Risk Assessments	Define and use basic impact + urgency for risk (static)
Service Operations Workspace - CAB	Ensure it's visible to agents and they can see them with incidents
Base Metrics	Use basic, OOTB change success rate and emergency change volume
CMDB CIs	Ensure setup is done for CIs in CMDB as it relates to change

Phase 2: Accelerate delivery with automation, policy-driven compliance & risk control

SoW – CAB Workbench	Set up and use CAB agenda, approvals in workspace and impacted services are visible
Change in SoW	Actively using change tasks and managing them in SoW, unified view with incident/problems
*Multi-Modal Change Requests	Set up UI-based forms, record producers and ensure API-based change creation is CI/CD friendly
*Change Risk Intelligence	Risk now uses CI health, past change failures and business service criticality
*Change Routing	Changes are now auto-assigned by CI, service or risk
*Change Success Scoring	Basic use of post-implementation evaluations and dashboard
*NOW Assist with Change	Basic/introduction to using NOW Assist for change summaries and suggested plans / roll backs
*DevOps Change Velocity	Introduce DevOps with deployment frequency tracking and changes created automatically from the pipeline

Service Resilience: Prevent and Govern

Phase 2: Accelerate delivery with automation, policy-driven compliance & risk control

*ML-Driven Change Risk	Utilize real-time risk prediction and auto-escalation of high-risk changes for review
*Change Success w/ ML	Utilize predictive success scoring and pattern detection across failed changes
*Policy-Driven Automation	All low-risk changes are auto-approved and use of dynamic approval chains active
*Change Impact – Mapping	Actively using mapped CIs to services which use customer impact visualizations
*Advanced Change Routing	Actively using skill based and workload-based routing for assignments
*NOW Assist for Change Agent	(Advanced) Actively using auto-generated implementation plans, AI driven roll back plans, and NL CAB summaries, conversational change
*DevOps Change Velocity	Actively integrated with change records created/closed automatically and metrics align with ITSM
Quality Governance	Active use of failed change root cause analysis

Phase 3: Proactive management with AI & self healing

*Self-Healing	Active use of auto-rollbacks on anomaly detection
*Business Outcome Driven Changes	Actively using changes that are prioritized by revenue and customer experience impacts
*Change Automation	Actively using "closed-loop" automation for lifecycle (incident to change to deploy to validation)
*DevOps Change / AI	Actively using AI driven release governance and humans only intervene if the system asks

Value Driver:

- Standardization of changes (intake, paths, visibility)
- Standardization of change governance
- Standardization of risk visibility for leadership

- Risk based decision acceleration
- CAB Optimization and team autonomy with governance
- Failure pattern detection and monitoring (change success & risk)
- Automation at scale with prevention and proactivity

- Autonomous recovery & validation
- Preventative change governance
- Business-impact prioritization

Move to the next phase when:

- Executive sponsorship is in place
- Customers are encouraged to reset Change and embrace modern approaches

General:
- Types: Normal, Standard and Emergency change types are actively used
- Change policies are enforced
- CAB cadence defined and followed
- Emergency changes reviewed post-implementation
- Blackout Windows set and enforced, conflict detection in use for all changes

Data:
- Required change fields are at least 95% populated (CI, planned start/end, backout plans)
- Impacted services with CI selection enforced (no free text) and *basic service mapping exists for Tier-1
- **Dependent on service setups at overall ITSM "Walk" levels or overall "Phase 2" value levels*

Operational Metrics Tracked:
- Change Success rate – at least 85% or more
- Emergency Changes – 15-20%
- Unauthorized Changes – 0 or explained

Other:
- **CAB is NOT using email threads, excel, SharePoint, etc**

General:
- Standard changes around 30-40% of volume
- Multi-modal change intake live/in use
- Low-risk Approvals automated

Metrics Tracked:
- Change success rate at least 90%
- Emergency changes trending down for min. 2 quarters

Data/Risk:
- Risk is calculated on CI Criticality / historic change outcomes
- *Services – risk model validated against historical failures and high-risk changes follow separate approval path

AI Usage:
- NOW Assist generating change summaries and implementation suggestions
- Users actively using AI outputs

General:
- ML-based prediction fully enabled
- Predicted risk vs actual outcomes tracked

AI/Autonomous:
- Low-risk changes auto-approved
- Dynamic approval chains working
- Human approval only when risk thresholds exceeded

DevOps & Velocity:
- Change records auto-created from pipelines
- Rollbacks auto-linked to change failures

Governance:
- Failed change RCA automated or templated
- Repeat failure patterns detected and addressed
- Business impact measured**
- Leadership uses dashboards and trusts data
- NO shadow change processes exist

General (Advanced):
- MTTR is consistently low
- Change success is at least 97%
- Incident spikes AFTER changes are rare
- AI rollbacks better than humans

Example Success Measures

- Change Success %
- Emergency Change Count

- Approval time
- Standard change usage

- Predicted vs. actual risk accuracy

- MTTR
- Autonomous change rate