ServiceNow Autonomous IT Value Journeys

Building Autonomous IT on Your ITSM Foundation

Key Themes

- Preventive Endpoint Health
- Omni-Channel Self-Service
- Agentic Triage & Resolution
- Compound Future Gains
- Preventive Operations
- Proactive AIOps
- Responsive Ops
- Continuous Improvement

Value Journey

ZERO TOUCH IT SUPPORT → ZERO SERVICE OUTAGES

Phase Intent

Organizational Capability
Phase I: "Activate core service desk workflows & use data to identify and prioritize top support drivers"
Phase II: "Deliver AI-powered omni-channel support & automate repetitive tasks for higher-value work"
Phase III "Optimize IT operations through improved endpoint experience & enable self-resolution with minimal human input"

What Success Looks like
Phase I (Insight): Digitized service delivery + clarity on where to automate
Phase II (Automation): AI-assisted workflows + reduced manual effort + readiness for agents
Phase III (Autonomy): AI agents resolving issues with minimal human input + continuous improvement

Organizational Capability
Phase I: "Digitized incident, problem & change management • Knowledge base and service catalog • End-to-end visibility to prevent service disruptions"
Phase II: "Deliver full IT estate visibility & intelligent Service Graph, automating incident detection and accelerating resolution""
Phase III "Deploy AI-driven automation & self-healing to prevent outages and eliminate service disruptions"

What Success Looks like
Phase I (Insight): See your estate, detect issues, respond with structure
Phase II (Automation): AI reduces noise, accelerates response, prevents self-inflicted outages
Phase III (Autonomy): AI agents predict and prevent outages with human oversight

Scope

Activate

Phase I: INSIGHT

1. PLATFORM & DATA FOUNDATION
Why: Establish the data backbone that powers everything - AI automation, and analytics all depend on clean connected data

AI Platform Foundation
- Organizations, Locations, Groups, Users/Roles
- Active Directory (LDAP, SSO)
- Now Assist Admin Console - Intro to AI [PRO]

AI Readiness (Introduction)
- AI Platform Overview
- Data Quality Assessment
- AI Governance Awareness

CMDB Foundation
- Logical Cls (Business Processes, Contracts)
- CI Classes & CSDM Guardrails
- Identification & Reconciliation Rules
- CMDB 360 Workspace

Integration Foundation
- Endpoint Management Integrations (Intune, Jamf)
- Service Graph Connector - SCCM

2. WORKSPACE & USER EXPERIENCE
Why: Create unified experiences for employees and agents - fragmented portals and tools kill adoption and hide insights.

Employee Experience (Employee Center)
- Taxonomy, Quick Links, Actions
- Record Producers
- Branding & Theme
- Employee Center Service Catalog
- "IT Help" Service

Agent Experience / Service Operations Workspace (SOW)
- Landing Page Designer
- Form & List Configuration
- Role-Based Access Control

3. CORE ITSM WORKFLOWS
Why: Digitize and standardize how work flows through IT - this structured data feeds everything that follows (analytics, AI, automation).

Incident Management
- Incident Management SOW
- Setup Category and Subcategory
- Assignment Groups & On-call
- Schedules Incident Investigation Process Flows
- SLA Definitions

Problem Management
- Problem Management SOW Setup
- Problem-to-Incident Linking
- Known Error Database (KEDB)
- Basic Root Cause Documentation

Change Management
- Change Management SOW Setup (incl. CAB)
- OOTB Change Models (std, normal, emergency)
- Basic Change Governance (approvals, risk, conditions)
- Conflict Detection (maintenance & blackout windows)

Request Management (Service Catalog)
- Service Catalog SOW Setup
- Request SOW Setup
- Standard Request & Approval Workflows
- AI Search [PRO]

Knowledge Management
- Knowledge Management SOW
- Setup Configure Knowledge Articles for Requests
- Knowledge-Centered Service (KCS) Basics

4. VISIBILITY [Light]
Why: You can't support what you can't see - endpoint visibility is the foundation for proactive support and accurate impact analysis.

Endpoint Visibility
- Endpoint Management Data (via SCCM/Intune)
- Asset-to-User Relationships
- Basic CI Health

5. REPORTING & ANALYTICS
Why: You can't automate what you can't measure - this is how you identify where automation will have the biggest impact.

Performance Analytics Foundation
- OOTB ITSM Dashboards
- Top Support Drivers Reporting
- SLA Performance Tracking
- Self-Service Adoption Metrics
- Knowledge Gap Analysis
- Assignment Group Workload Distribution

6. MOBILE [Optional]
Why: Meet employees where they are - mobile self-service increases adoption and deflects tickets before they're created.

Performance Analytics Foundation
- Mobile App Configuration
- Mobile Agent Experience
- Push Notifications

Phase II: AUTOMATE

1. PLATFORM & DATA FOUNDATION
Why: Extend the data foundation to power AI - Knowledge Graph connects data across workflows, enabling smarter recommendations and automation.

Knowledge Graph [PRO]
- Knowledge Graph Designer
- Knowledge Graph activation
- Workflow Data Fabric (foundation)

Data Quality Enhancement
- CMDB health improvements (based on Phase I insights)
- CI relationship enrichment
- Service-to-asset mapping refinement

2. WORKSPACE & USER EXPERIENCE
Why: Meet employees wherever they are - omni-channel removes friction and captures demand that previously went untracked.

Omni-Channel Experience
- Employee Portal (enhanced from Phase I)
- MS Teams integration
- Slack integration
- Agent Chat & Dynamic Translation

Agent Experience (Enhanced SOW) [PRO]
- Unified Workspace enhancements
- Sidebar & Chat for collaboration
- Cross-team visibility

3. CORE ITSM WORKFLOWS (Enhanced)
Why: Layer intelligence onto digitized workflows - AI handles the routine, humans handle the exceptions.

Incident Management (AI-Assisted) [PRO]
-Automated Work Assignment (AWA)
- Incident Summarization
- Similar incidents suggestions
- Resolution Note Generation
- SLA Extraction

Request Management (AI-Assisted)
- Intelligent Request Routing [PRO]
- Auto-fulfillment for standard requests
- Approval automation

Knowledge Management ! (AI-Assisted) [PRO]
- Knowledge Generation from resolutions
- Article recommendations during incident work
- Knowledge gap identification

4. AI & AUTOMATION
Why: This is the core of Zero Touch - AI agents and skills deflect tickets, accelerate resolution, and free humans for complex work.

Now Assist Skills (Requestors) [PRO]
- Now Assist Virtual Agent (VA)
- Now Assist Voice Agent
- Conversational self-service
- Intent detection & topic routing

Now Assist Skills (Fulfillers) [PRO]
- Triage & Categorization (Agent)
- Investigation & Resolution guidance (Agent)
- Resolution Note & Knowledge Generation (Skills)
- Incident Summarization (Skills)
- SLA Explanation (Agent)

Recommended Actions [PRO]
- Recommended Actions Engine
- Guidance-based recommendations Field-based recommendations
- Playbook suggestions

Workflow Automation [PRO]
- Flow Designer (enhanced workflows)
- Automated Work Assignment (AWA)
- Scheduled automations Event-triggered flows

5. VISIBILITY [Enhanced]
Why: Expand on Phase I visibility - deeper endpoint insights enable proactive engagement and set the foundation for self-healing

Enhanced Endpoint Visibility
- Expanded device telemetry
- Application performance visibility
- User-to-device-to-service mapping

6. DIGITAL END-USER EXPERIENCE (DEX)
Why:Shift from reactive to proactive - see issues before users report them and engage employees before they create tickets.

DEX Capabilities [PRO]
- DEX self-help and proactive engagement
- Proactive endpoint monitoring
- Employee sentiment tracking Self-healing triggers (foundation for Phase III)

7. REPORTING & ANALYTICS [Enhanced]
Why: Measure automation effectiveness - track deflection, AI accuracy, and identify next automation candidates.

Automation Performance [PRO]
- Virtual Agent deflection rates
- AI skill accuracy & feedback
- Self-service adoption trends
- Agent handle time impact

Continous Improvement [PRO+]
- Automation candidate identification
- Knowledge gap trends
- Repeat incident patterns
- AI recommendation acceptance rates

8. AI GOVERNANCE (Introduction)
Why: As AI does more, governance matters more - lay the foundation for responsible AI that scales in Phase III.

AI Control Tower (Foundation) [PRO+]
- AI Discovery setup (Self Service)
- Playbooks (Self Service)
- AI usage visibility
- Baseline AI metrics

9. SKU EXPANSIONS (When Ready) SAM & HAM
Why: Extend automation into asset lifecycle - reclaim unused software, automate hardware fulfillment, optimize spend..

Software Asset Management (ITAM SKU) [PRO]
-Fulfill software requests (automated)
- Software license checks
- Software reclamation workflows
-License compliance visibility

Hardware Asset Management (HAM SKU) [PRO]
- Track & Manage Hardware requests
- Hardware lifecycle automation
- Procurement integration
- Asset refresh workflows

Phase III: AUTONOMY

1. PLATFORM & DATA FOUNDATION (Autonomous)
Why: AI agents are only as good as the data they access - Workflow Data Fabric enables cross-domain intelligence for autonomous decision-making.

Workflow Data Fabric (Full) [PRO+]
- Cross-workflow data connections
- Real-time data access for agents
- Decision context enrichment

Now Assist Data Kit [PRO+]
- Create & Configure skills
- Custom skill development
- Skill performance tuning

Data Quality (Continuous) [PRO+]
- Automated data quality monitoring
- Self-correcting data workflows
-AI-driven data enrichment

2. WORKSPACE & USER EXPERIENCE (Autonomous)
Why: In autonomy, the workspace shifts from "where work happens" to "where humans oversee Autonomous Agents" - transparency, governance and control become critical.

Employee Experience (AI-First) [PRO+]
- AI-driven personalized portal
- Predictive self-service (anticipate needs)
- Proactive notifications & resolutions

Agent Experience (Oversight Mode) [PRO+]
- AI agent activity dashboard
- Human override controls
- Exception queue management
- Escalation monitoring

3. CORE WORKFLOWS (Autonomous)
Why: Workflows shift from human-executed to AI-executed with human oversight - the goal is resolution without human touch for routine issues.

Incident Management (Autonomous) [PRO+]
- End-to-end incident resolution (AI agents)
- Auto-resolution for known patterns
- Human escalation understanding for exceptions
- Resolution verification & closure

Request Management (Autonomous) [PRO+]
- Full auto-fulfillment for standard requests
- Zero-touch provisioning
- Autonomous approval for low-risk requests
- Self-service conversations handling

Knowledge Management ! (Self-Improving) [PRO+]
- Auto-generated knowledge from resolutions
- AI-curated article improvements
- Knowledge accuracy scoring
- Continuous content optimization

Problem Management (Predictive) [PRO+]
- AI-identified problem patterns
- Proactive problem creation from trends
- Automated root cause suggestions
- Preventive action recommendations

4. AI AGENTS & SKILLS (Full Autonomy)
Why: This is the heart of Zero Touch - AI agents with specific skills resolve issues end-to-end, learning and improving continuously.

AI Agent Studio [PRO+]
- Ready-made Agents (ITSM)
- Agent Builder (custom agents)
- AI Agentic Activity monitoring
- Agent orchestration

Agentic Triage & Resolution[PRO+]
- Autonomous incident triage
- Investigation without the need for human input
- Resolution execution
- Verification & closure

Advanced Skills [PRO+]
- Multi-step resolution skills
- Cross-system action skills
- Decision-making skills
- Learning & adaptation

Human-AI Collaboration [PRO+]
- Escalation protocols (when agents must stop)
- Human-in-the-loop checkpoints
- Confidence thresholds for autonomy
- Feedback loops for agent improvement

5. VISIBILITY (Predictive)
Why: Move from "see issues" to "predict issues" - visibility becomes forward-looking, enabling prevention over reaction.

Predictive Endpoint Intelligence [PRO+]
- Issue prediction models
- Risk scoring for devices
- Proactive alerts (before failure)
- Trend-based maintenance triggers

PUser Experience Prediction [PRO+]
- Employee friction prediction
- Sentiment trend analysis
- Proactive engagement triggers

6. DIGITAL END-USER EXPERIENCE (Auto-Healing)
Why:DEX moves from monitoring to acting - issues are detected AND resolved automatically without user awareness.

DEX Auto-Healing [PRO]
- Issue prevention
- Automated remediation actions
- Self-healing scripts & workflows
- Silent resolution (no user action needed)

App & Asset Intelligence [PRO]
- Application health auto-correction
- Asset performance optimization
- Automated patching & updates
- Resource rebalancing

7. REPORTING & ANALYTICS (Autonomous Ops)
Why: Measure autonomous performance - how much is truly zero-touch, where do humans still intervene, and how is AI improving?

Autonomous Performance Metrics [PRO+]
- Zero-touch resolution rate
- Human intervention rate (& reasons)
- AI agent success/failure rates
- Mean time to autonomous resolution

Continous Improvement [PRO+]
- Automation candidate identification
- Knowledge gap trends
- Repeat incident patterns
- AI recommendation acceptance rates

Executive Dashboards [PRO]
- Autonomy maturity scorecard
- ROI on AI investments
- Human capacity reallocation metrics

8. AI GOVERNANCE (Full)
Why: With AI agents acting autonomously, governance is non-negotiable - you need visibility, control, and compliance at scale..

AI Control Tower (Full) [PRO+]
- AI lifecycle management
- Enterprise AI strategy alignment
- Risk & compliance monitoring
- AI usage policies & enforcement

Agent Governance [PRO+]
- Agent permissions & boundaries
- Action audit trails
- Compliance verification Bias & fairness monitoring

Continuous Oversight [PRO+]
- "Real-time" AI performance monitoring
- Anomaly detection in agent behavior
- Automated governance alerts
- Periodic AI reviews & recertification (via Strategic Portfolio Management)

9. SKU EXPANSIONS (Full Value) SAM, HAM, SPM & Risk and Security
Why: Expand autonomous capabilities into asset lifecycle, strategic alignment, and risk management for enterprise-wide impact

Software Asset Management (Autonomous) (ITAM SKU) [PRO]
- Autonomous software reclamation
- AI-driven license optimization
- Predictive license needs
- Auto-compliance remediation

Hardware Asset Management (Autonomous) [PRO]
- Predictive hardware refresh
- Autonomous procurement triggers
- Lifecycle optimization
- Auto-End of Life workflows

Strategic Portfolio Management [PRO]
- AI Portfolio Strategies
- Enterprise Strategies alignment
- Investment prioritization (AI-assisted)

Risk and Security [PRO]
- AI-driven risk assessment
- Autonomous compliance checks
- Security posture automation

Phase I: INSIGHT

LEVERAGED FROM ZERO TOUCH PHASE I:
→ AI Platform Foundation (Orgs, Users, LDAP/SSO, Now Assist Admin Console)
→ CMDB Foundation (CI classes, CSDM, ID & Reconciliation rules)
→ Incident Management (SOW, categories, assignment, SLAs)
→ Problem Management (SOW, Problem-to-Incident linking, KEDB)
→ Change Management (SOW, change models, basic governance)
→ Knowledge Management(SOW, article, KCS basics)
→ Reporting & Analytics Foundation (OOTB dashboards)

If not done, complete these first or in parallel.
Reference: Zero Touch Phase I

1. PLATFORM & DATA FOUNDATION (Extended)
Why: Zero Outages requires deeper infrastructure data - you can't prevent outages you can't see. Discovery and Service Mapping extend CMDB from "what we have" to "how it's connected.

CMDB Core (Extended) ITOM
- Define CI classes, inheritance for Infrastructure
- CSDM guardrails for operational CIs
- Validate ID, Reconciliation,
- Data Source rules CMDB 360 Workspace (infrastructure focus)

Integration Foundation (Extended)
- Service Graph Connector - Microsoft SCCM
├─ Normalize SCCM hardware & software data
├─ Auto-populate CMDB with trusted endpoint details
└─ Improve license reconciliation and SAM coverage

2. DISCOVERY [ITOM Visibility]
Why: Discovery is the foundation of Zero Outages - you need to know what exists before you can monitor it, map it, or protect it from failure.

Discovery - Agentless IP-Based
- Discovery Administrator Workspace
- Map IP ranges to schedules
- Classify hosts; detect SNMP network and storage devices
- Populate CMDB with Discovery patterns
- Balance coverage across on-prem and cloud data centers

Discovery - Cloud (AWS / Azure / GCP)
- Discover cloud-native compute, network, and storage
- Capture dynamic topology and real-time relationships
- Normalize multi-cloud attributes into one CMDB model
- Support service maps, dashboards, and governance

Service Graph Connectors
- Microsoft SCCM (if not done in Zero Touch)
- Cloud provider connectors (AWS, Azure, GCP)
- Third-party infrastructure connectors

3. SERVICE MAPPING [ITOM Visibility]
Why: Discovery shows what exists; Service Mapping shows how it connects. Understanding service dependencies is critical for impact analysis and preventing cascading outages.

Service Mapping Foundation
- Service Mapping patterns and schedules
- Application service definitions
- Entry point identification
- Upstream/downstream dependency mapping

Service Map Visualization
-Service maps for critical business services
-Dashboard integration Governance and ownership assignment

4. WORKSPACE & USER EXPERIENCE (Operators) [ITSM] [ITOM]
Why: Operators need a unified view of infrastructure health - fragmented tools hide problems and slow response.

Operator Experience (Service Operations Workspace)
- Service Operations Workspace (SOW) for ITOM
- Unified operator console Alert and event visibility
- Infrastructure health dashboards

Agent Experience (Enhanced)
- Incident workspace (Ops-focused views)
- Change workspace (Ops-focused views)
- Cross-team collaboration tools

5. MAJOR INCIDENT MANAGEMENT [ITSM]
Why: When services go down, every second counts. MIM is the cornerstone of Zero Outages - structured response reduces MTTR and business impact.

On-Call & Escalation
- Setup On-Call schedules and rosters
- Escalation paths and policies
- Role definitions (Incident Commander, Comms Lead, etc.)

Communications
- Communication Plans & Templates
- Stakeholder notification workflows
- Status page integration (if applicable)
- Bridge/war room protocols

Investigation & Response
- Investigation framework in SOW
- OOTB Playbooks (Procedural MIM Playbook)
- Incident timeline tracking
- Workaround documentation

Post Incident Review
- Post Incident Review process (manual documentation)
- Root cause capture
- Action item tracking
- Knowledge article creation (manual)

6. CHANGE MANAGEMENT (Ops-Enhanced) [ITSM]
Why: Most outages are caused by change. Ops-aware change management prevents self-inflicted wounds from poorly planned or conflicting changes.

Change Process
- Change models for infrastructure changes
- CAB process for high-risk changes
- Conflict detection (maintenance & blackout windows)
- Change-to-CI impact visibility Basic change risk assessment

Change Visibility
-Change calendar (Ops view)
- Upcoming change awareness for Ops teams
- Change freeze/blackout enforcement

7. PROBLEM MANAGEMENT (Ops-Enhanced) [ITSM]
Why: Outages repeat when root causes aren't addressed. Problem Management closes the loop from incident to prevention.

Problem Process
- Infrastructure problem patterns
- Root cause documentation (Ops focus)
- Known Error DB (Infrastructure entities)
- Problem-to-Incident linking Workaround documentation

8. EVENT MANAGEMENT [ITOM Health]
Why: Events are the early warning system for outages - capturing, normalizing, and correlating events is how you detect issues before they become incidents..

Event Management Foundation
- Define event ingestion strategy
- Normalize and classify events
- Configure event rules & transformations
- Set up Alert Management
-Build operator workflows
-Validate alert & CI linkage

Alert Management
-Alert correlation rules
-Alert-to-incident creation rules
-Alert prioritization
-Noise reduction (foundation)

9. REPORTING & ANALYTICS (Ops) [Platform] [ITOM]
Why: You can't prevent outages you can't measure - operational dashboards reveal patterns, bottlenecks, and early warning signs.

Operational Dashboards
- Infrastructure health overview
- Alert volume and trends
- Event-to-incident correlation rates
- Change success/failure rates
- Traffic, MTTR, MTTD baselines

Outage Analysis
- Top outage causes
- Repeat incident patterns
- CI-based incident clustering
- Business service impact visibility

10. SKU EXPANSIONS (When Ready) SecOps, Risk & Business Continuity
Why: Security incidents often cause or escalate outages - when ready, integrate SecOps to unify security and operations response.

Security Operations (SecOps SKU)
- Major Security Incident Management
- Security event visibility in ops console
- Escalation paths between SecOps and IT Ops
- Security-to-Ops alert correlation

Integrated Risk Management (IRM SKU)
- Proactive Risk Identification and Assessment
- Integrated Incident and Crisis Workflow
- CMDB-integrated Service Dependency Mapping

Business Continuity Management (BCM SKU)
- Business Continuity Planning
- Business Impact Assessment
- Disaster Recovery for IT
- Scenario Analysis

Phase II: AUTOMATE

LEVERAGED FROM ZERO TOUCH PHASE II:
→ Knowledge Graph (Platform & Data Foundation)
→ AI Governance Introduction (AI Control Tower foundation)
→ Now Assist Skills patterns (for fulfillers)
→ Recommended Actions framework
→ Workflow Automation patterns (Flow Designer, AWA)

LEVERAGED FROM ZERO OUTAGES PHASE I:
→ Discovery (IP-based, Cloud)
→ Service Mapping (foundation)
→ Event Management (ingestion, normalization, alerts)
→ Major Incident Management (process, playbooks)
→ Change Management (ops-enhanced)
→ Operator Workspace (SOW) if not done.

Complete these first or in parallel.

1. PLATFORM & DATA FOUNDATION (Intelligent) [PLATFORM] [ITOM]
Why: AI needs connected, high-quality data. Service Graph and Knowledge Graph power intelligent automation across operations.

Service Graph (Enhanced) ITOM [PRO]
- Knowledge Graph integration
- Service Graph Connectors (expanded)
- Real-time topology updates
- Cross-domain data connections

Workflow Data Fabric TOM [PRO]
- Operational data vectors
- Cross-workflow intelligence
- Decision context for AI agents

Data Visibility & Traceability
- Planning tool integration (e.g., Jira, SPM)
- Dev-Ops tool integrations (coding, archestration, testing, security)
- Cross-platform data lineage

Data Quality (Continuous) [PRO]
- Automated CMDB health monitoring
- CI relationship validation
- Service map accuracy scoring
- Data quality dashboards

2. SERVICE MAPPING (Enhanced) [ITOM Visibility]
Why: Expand discovery to cover the full estate - cloud-native, containers, and dynamic infrastructure require advanced discovery patterns.

Service Mapping Workspace [PRO]
- Service Mapping Plus Workspace
- Enhanced mapping capabilities
- Hybrid/cloud service map onboarding

Service Mapping - Tag Based [PRO]
- Trace services from entry points through real traffic
- Use ML to suggest service dependencies connections
- Tag-based service identification

Service Mapping - Top Down with ML [PRO]
- ML connection suggestions
- Recommended Actions Engine for mapping
- Pattern-based service discovery

Tag Governance
- Enforce required cloud tags across VMware/AWS/Azure/GCP
- Standardize ownership, environment, cost center, lifecycle metadata
- Enable automated remediation and continuous compliance
- Tag policy enforcement

4. OPERATOR WORKSPACE (Enhanced) [ITSM] [ITOM]
Why: Ops Teams need a unified, intelligent workspace. Express List and SOW enhancements transform how operators triage, investigate, and remediate alerts.

Service Operations Workspace (Enhanced) [PRO]
- SOW for ITOM (enhanced from Phase I)
- Unified operator console
- Cross-workflow visibility (alerts, incidents, changes)

Express List ITOM Health [PRO]
- Live alert feed (real-time updates)
- Dynamic filtering (priority, CI, services, tags)
- Integrated triage and remediation actionsAlert preview pane

Express List - Link View ITOM Health [PRO]
-Tag-based alert group visualization
-Shared attribute identification
- CMDB-less mapping for RCA Alert group timeline

Integration Launchpad ITOM Health [PRO]
- External tool connections
- Cross-platform data exchange
-Simplified integration management

AIOps Dashboards ITOM Health [PRO]
- KPI monitoring
- Service health visualization
- Operational insights dashboards

5. AIOps (TELEMETRY & INTELLIGENCE) [ITOM Health] [ITOM AIOps]
Why: AIOps transforms raw data into actionable intelligence. Metrics, logs, and telemetry feed AI that detects anomalies, predicts issues, and reduces noise before operators see it.

Agent Client Collector (ACC-V/M) [PRO]
- Define deployment model
- Configure ACC-V hub
- Deploy collectors to infrastructure
- Enable CI enrichment
- Validate data quality Telemetry-to-CI mapping

Metric Intelligence (MI) ! [PRO]
- Identify telemetry owners & metrics sources
- Configure metric ingestion
- Build MI indicators & baselines
- Create MI Signals & Anomaly Detection
- Integrate MI signals with Alerts
- Tune thresholds and reduce false positives
-Trend-based alerting Capacity prediction indicators

Health Log Analytics (HLA) [PRO]
- Identify log sources & access methods
- Configure log ingestion pipelines
- Define log classification patterns
- Enable anomaly detection for logs
- Surface insights within the AIOps console
- Log-based alert generation
- Error pattern recognition
- Log correlation with events

6. MAJOR INCIDENT MANAGEMENT (AI-Assisted) [ITSM]
Why: When outages happen, AI accelerates response. Summarization, recommendations, and auto-generated knowledge reduce MTTR.

AI-Assisted Investigation [PRO+]
- Incident Summarization
- Recommended Actions for operators
- Similar Incident suggestions
- Impact analysis automation

AI Assisted Communications [PRO+]
- Auto-generated status updates
- Stakeholder notification suggestions
- Timeline summarization

Post Incident Review (AI-Enhanced) [PRO+]
- Post Incident Review & Knowledge Generation
- Auto-generated PIR drafts
- Root cause suggestions
- Action item extraction

7. CHANGE MANAGEMENT (Intelligent) [ITSM]
Why: Most outages are caused by change. Intelligent change management prevents self-inflicted wounds through AI-driven risk assessment and automation.

Change Planning Agent [PRO+]
- Write test plans (AI-generated)
- Implementation plans (AI-generated)
- Back-out plans (AI-generated)

Conversational Change [PRO+]
- Conversational change via agentic workflows
- Natural language change creation
- Change summarization

Advanced Change Governance [PRO+]
- Success scores, calculated risk score
- Agentic workflow assessing change data quality
- Advanced approval policies using risk and operational data
- Change-incident correlation analysis

Change Simplification & Acceleration [PRO]
- Fit-for-purpose change via custom change models
- Shift validations left into release
- Standard change auto-approval (low risk)

8. PROBLEM MANAGEMENT (Predictive) [ITSM]
Why: Don't wait for incidents to find problems. AI identifies patterns and predicts issues before they cause outages.

AI-Enhanced Problem Management [PRO+]
- Problem Management (AI-assisted)
- Known Error DB (AI-enriched)
- Root Cause Analysis suggestions (Pro+)

Predictive Problem Identification [PRO+]
- Pattern detection across incidents
- Repeat incident clustering
- Proactive problem creation from trends

9. AI-POWERED OPERATIONS [ITOM AIOps] [ITOM Health]
Why: This is the heart of Phase II - LEAP playbooks, Alert Assist, and agentic workflows automate response and reduce operator toil.

LEAP Playbooks [PRO+]
- LEAP Playbooks (automated remediation)
- Playbook builder
- Pre-built operational playbooks
- Playbook execution tracking

Alert Assist [PRO+]
- Alert Assist (AI-powered triage)
- Alert correlation and grouping
- Noise reduction automation
- Priority recommendations

Alert Automation [PRO+]
- No-code automation builder
- Event rules automation
- Tag-based clustering automation
- Alert management rules

Gen AI for Event Management [PRO]
- Gen AI for Event Management
- Natural language alert investigation
- Event summarization
- Recommended remediation actions

Agentic Workflows [PRO+]
- Agentic Workflows for operators
- Automated diagnostic routines
- Self-service remediation triggers
- Escalation automation

10. SERVICE RELIABILITY MANAGEMENT [ITOM]
Why:SRM brings SRE discipline to operations. SLIs, SLOs, and Error Budgets define what "healthy" means - this is foundational for Phase III autonomous decisions.

SRM Foundation
- Incident Response (SRE model)
- Service Level Indicator (SLI) / Service Level Objective (SLO) / Error
- Budget definition Service health scoring

Reliability Visibility
- Service reliability dashboards
- Error budget consumption tracking
- SLO breach alerting

Phase III Zero Outage Foundation
- Baseline service health metrics
- Define acceptable error thresholds
- Establish service tier priorities

11. REPORTING & ANALYTICS (Intelligent Ops) [Platform] [ITOM]
Why: Measure AI effectiveness and operational improvement. Dashboards show noise reduction, MTTR gains, and automation ROI.

AIOps Performance [PRO+]
- Alert noise reduction metrics
- ML/HLA detection accuracy
- Playbook execution success rates
- False positive trends

Operational Metrics[PRO+]
- MTTR / MTTA / MTTD trends
- Automation coverage & ROI
- Service health trends (feeds SRM)
- Incident-to-change correlation

12. AI GOVERNANCE (Operational) [Platform]
Why: As AI makes operational decisions, governance ensures it's accurate, compliant, and trustworthy.

AI Control Tower (Ops Focus) [PRO+]
- AI usage visibility (AIOps)
- AI accuracy monitoring
- Operational AI policies

AIOps Governance [PRO+]
- Alert Assist accuracy tracking
- Playbook audit trails ML/HLA model performance
- Threshold tuning governance

13. SKU EXPANSIONS (When Ready) SecOps, Risk, Third-Party Risk and SPM
Why: Extend intelligent operations into security and strategic planning for enterprise-wide impact..

Security Operations (SecOps SKU) [PRO]
- Security Posture Control
- Now Assist for SIR & VR
- Security-Ops alert correlation
- Unified incident response (Security + IT)

Integrated Risk Management (IRM SKU)
- Automated Compliance Checks
- Integrated Incident and Crisis Workflow
- Regulatory Reporting for Breaches
- Continuous Resilience Monitoring and Metrics

Third-Party Risk Management (TPRM SKU)
- 3rd Party Communications
- 3rd Party Change Management
- 3rd Party Root Cause

Strategic Portfolio Management (SPM SKU) [PRO]
- Project Portfolio Management (AI & Enterprise Strategies)
- Resource Management
- Change-to-project visibility

Phase III: AUTONOMY

LEVERAGED FROM ZERO TOUCH PHASE III:
→ AI Agent Studio (agents, builder, agentic activity)
→ Now Assist Data Kit (custom skills)
→ AI Control Tower (full governance)
→ Human-AI Collaboration protocols
→ Autonomous workflow patterns

LEVERAGED FROM ZERO OUTAGES PHASE II:
→ AIOps stack (MI, HLA, ACC-V) - mature and tuned
→ LEAP Playbooks - proven and effective
→ Alert Assist - noise significantly reduced
→ Express List - operators efficient
→ SRM - SLIs/SLOs defined, baselines established
→ Change governance - risk scoring mature Phase III activates autonomy on this foundation.

Phase III activates autonomy on this foundation.

1. PLATFORM & DATA FOUNDATION (Autonomous) [PLATFORM] [ITOM]
Why: Autonomous operations require real-time, connected data. Workflow Data Fabric enables Autonomous Workers to access cross-domain context for independent decision-making.

Workflow Data Fabric (Full) [PRO+]
- Cross-workflow data connections (full)
- Real-time data access for agents
- Decision context enrichment
- Operational data vectors (complete)

Now Assist Data Kit [PRO+]
- Create & configure custom skills
- Ops-specific skill development
- Skill performance tuning
- Continuous skill improvement

Kubernetes Visibility Agent [PRO+]
- Collect live workload, node, pod, and service metadata
- Map cluster to namespace to workload relationships
- Visualize service-to-service flows
- Enable dynamic topology for ITOM + Service Mapping

2. AUTONOMOUS OPERATIONS [PLATFORM] [ITOM]
Why: This is the heart of Phase III - AI detects, decides, and acts without waiting for humans. Self-healing resolves issues before users are impacted.

Self-Healing Automation [PRO+]
- Proactive issue prevention
- Automated remediation actions
- Self-healing scripts & workflows
- Silent resolution (no user awareness needed when governed)

LEAP Playbooks (Autonomous Mode) [PRO+]
- Auto-execution for known patterns
- Confidence-based triggers
- No-approval remediation (within guardrails)
- Autonomous escalation decisions

Alert-to-Resolution (End-to-End) [PRO+]
- Alert → Triage → Investigate → Remediate → Close
- Full cycle without a nee for human touch (based on governance)
- Pattern-based auto-resolutionException-only escalation to humans

Predictive Operations [PRO+]
- AIOps-driven issue prediction
- Capacity-based preventive actions
- Anomaly-triggered remediation
- Trend-based maintenance automation

3. AUTONOMOUS CHANGE & RELEASE [ITSM]
Why: Most outages come from change. Autonomous change governance prevents self-inflicted wounds while accelerating safe delivery

E2E Change Automation [PRO+]
- Automated change creation -DevOps Chang Velocity (DCV)
- Automated change approval via advanced policies (DPR & DCV)
- Risk-based auto-approval (low-risk = no human)
- Auto-scheduling within safe windows

Autonomous Release Governance [PRO+]
- Data-driven release policies
- Automated validation gates
- Autorollback on failure detection
- Release health scoring

MIM Automation [PRO+]
- Innovate on playbook - add Technical Resolution Steps
- Auto-resolution for known incident patterns
- Autonomous bridge/war room initiation
- Autonomous stakeholder comms notifications

4. SERVICE HEALTH-DRIVEN AUTOMATION [ITOM]
Why: SRM moves from measurement to action. Error budgets and SLOs drive autonomous decisions - AI protects service health without human intervention.

Error Budget Enforcement [PRO+]
- Auto-freeze changes when budget exhausted
- SLO breach prevention automation
- Service tier-based prioritization
- Autonomous protection actions

Service Health-Driven Decisions [PRO+]
- Health score triggers automation
- Degradation-based auto-scaling
- Predictive SLO breach prevention
- Service-aware incident prioritization

Continuous Reliability [PRO+]
- Automated reliability improvements
- Pattern-based stability actions
- Self-optimizing service configurations

5. AI GOVERNANCE (Full) [PLATFORM]
Why: With AI acting autonomously, governance is non-negotiable. Full visibility, control, and compliance at scale ensures trust and accountability.

AI Control Tower (Full) [PRO+]
- AI lifecycle management (complete)
- Enterprise AI strategy alignment
- Risk & compliance monitoring
- AI usage policies & enforcement

Agent Governance [PRO+]
- Agent permissions & boundaries
- Action audit trails (complete)
- Compliance verification
- Bias & fairness monitoring

Autonomous Operations Governance [PRO+]
- Confidence thresholds for auto-action
- Escalation rules enforcement
- Human override protocols
- Autonomous action results review

Continuous Oversight [PRO+]
- "Real-time" AI performance monitoring
- Anomaly detection in agent behavior
- Automated governance alerts
- Periodic AI reviews & recertification

6. SKU EXPANSIONS (Full Value) SecOps, Risk, BCM & SPM
Why: Extend intelligent operations into security and strategic planning for Autonomous IT enterprise-wide impact.

Security Operations (SecOps SKU) [PRO+]
- Autonomous security incident response
- AI-driven threat remediation
- Security-Ops unified automation Auto-compliance enforcement

Integrated Risk Management (IRM SKU)
- Autonomous Compliance Checks and Remediation
- Continuous Resilience Monitoring and Metrics

Business Continuity Management (BCM SKU)
- Business Continuity Planning in action
- Recovery of Integrated Services

Strategic Portfolio Management (SPM SKU) [PRO+]
- AI Portfolio Strategies
- Enterprise Strategies alignment
- Autonomous investment prioritization
- Resource optimization (AI-driven)

NOTE: *If SPM is not in scope, Digital Portfolio Management (DPM) within ITSM provides lighter-weight portfolio visibility for product-centric operating models.*

Intelligent Automation [PRO+]
- Integration Hub (advanced)
- Workflow Studio (autonomous patterns)
- Cross-platform orchestration

Outcomes + Answers

After completing Phase I you should be able to answer:

Insight Question	Enabled By	Why It Matters for Phase II
What are my top 10 incident categories by volume?	Incident categorization + Reporting	Prioritize which workflows to automate first
Which requests are repetitive & high-volume?	Service Catalog analytics	Candidates for Virtual Agent deflection
What's my self-service adoption rate?	Self-service metrics	Baseline to measure automation impact
Where are my knowledge gaps?	KB gap analysis (incidents without article matches)	Target content creation for AI-assisted resolution
Which assignment groups are overloaded?	Workload distribution reporting	Focus automation on bottlenecks
Am I meeting my SLAs?	SLA Performance Tracking	Identify where speed improvements are needed
Is my CMDB healthy enough for automation?	CMDB 360 + Data Quality Assessment	AI/automation fails with bad data
What incidents repeat for the same users/assets?	Problem-to-Incident linking	Candidates for proactive remediation

After completing Phase II you should be able to answer:

Insight Question	Enabled By	Why It Matters for Phase III
What % of tickets are being deflected by Virtual Ag