TEMPLAR shield

servicenow

Accelerating your IRM transformation from legacy GRC platforms to a modern ServiceNow IRM platform in five value-driven phases.

IRM FLIGHTPATH BY TEMPLAR SHIELD - ACCELERATING IRM MATURITY ON SERVICENOW

OVERVIEW

IRM Flightpath is a structured, phased implementation roadmap that seamlessly migrates and transforms your Integrated Risk Management (IRM) program from legacy GRC platforms into a robust, future-ready **ServiceNow Risk** suite. This branded offering is designed for CISOs, Chief Compliance Officers, Chief Risk Officers, and GRC/IRM leaders who seek to modernize their risk and compliance operations with **minimal disruption** and **maximized efficiency.** The five-phase journey emphasizes **transformation, automation, operational resilience,** and **regulatory readiness,** ensuring progressive adoption of advanced IRM capabilities and continuous value realization at each step.

The IRM Flightpath unfolds in five key phases, followed by a Hypercare & Steady State transition. Each phase focuses on specific IRM domains – from establishing a strong foundation to integrating AI-driven risk management – allowing a gradual, controlled rollout of the ServiceNow IRM platform. This phased approach enables risk, compliance, and audit teams to adopt new functionalities in a structured and value-driven manner, maintaining business continuity and building maturity with each step. By the end of the journey, organizations will have fully retired legacy systems and operate a unified, automated, and future-proof IRM program on ServiceNow. This approach of IRM Flightpath emphasizes quick wins and sustained value, enabling organizations to innovate at speed with confidence while building trust with stakeholders.

5-PHASE IRM FLIGHTPATH ROADMAP

Phased IRM Flightpath timeline illustrating five implementation phases and a hypercare transition.

PHASE 01:
FOUNDATION & POLICY MANAGEMENT

IRM Foundation Setup:

Establish foundational entity structures and risk taxonomies aligned with ServiceNow's Common Service Data Model (CSDM) for a consistent data framework.

Policy Lifecycle Management:

Centralize policy management with structured workflows for authoring, approval, publication, and retirement of policies.

Unified Control Library:

Build a single integrated control library mapped to relevant regulations and internal policies, enabling automated compliance attestations and evidence collection.

Knowledge Base Launch:

Deploy a dedicated IRM Knowledge Base for policy dissemination, procedure documentation, and training materials to drive user awareness and adoption.

Benefits:

Enhanced visibility into enterprise-wide risks, automated tracking of issues and remediation efforts, and a consolidated view of risk management activities across the enterprise.

PHASE 02:
RISK & ISSUE MANAGEMENT

Enterprise Risk Modules:

Deploy comprehensive risk management modules for Enterprise, IT, and Operational risks, with customized risk scoring methodologies to quantify and prioritize risk exposure.

RCSA Implementation:

Conduct Risk and Control Self-Assessments (RCSAs) across the organization to regularly evaluate control effectiveness and emerging risk levels.

Unified Issue Management:

Introduce a unified issue and exception management workflow, consolidating all compliance, risk, and audit issues in one repository with automated tracking and remediation workflows.

Exception Handling Governance:

Establish structured policy exception processes with clear governance, approval criteria, and review cycles.

Benefits:

Enhanced visibility into enterprise-wide risks, automated tracking of issues and remediation efforts, and a consolidated view of risk management activities across the enterprise.

PHASE 03:
AUDIT & THIRD-PARTY RISK EXPANSION

Internal Audit Integration:

Roll out the ServiceNow **Internal Audit Management** module, aligning audit plans with real-time risk insights and automating audit findings and issue management.

Third-Party Risk Management:

Implement **Third-Party Risk Management (TPRM)** capabilities, including vendor onboarding assessments, risk tiering of vendors, and continuous monitoring of third-party risk indicators.

Operational Resilience Mapping:

Begin mapping operational resilience by linking critical business services to their supporting vendors, IT assets, and controls. This provides insight into dependencies and helps identify points of failure or concentration risk.

Benefits:

Improved audit effectiveness through risk-aligned auditing and automation, proactive management of vendor and supply-chain risks, and early insights into operational resilience (connecting risk data to business continuity considerations).

PHASE 04:
BUSINESS CONTINUITY & SECURITY OPERATIONS INTEGRATION

Business Continuity Management:

Deploy Business Continuity Management (BCM) modules to develop and maintain continuity plans and disaster recovery strategies for critical business processes. Conduct regular plan testing and governance reviews to ensure preparedness.

Security Operations (SecOps) Integration:

Integrate ServiceNow Security Operations functions, including Vulnerability Response and Security Incident Response. This ties cybersecurity events (vulnerabilities, incidents) directly into the IRM risk register, providing continuous, real-time risk updates driven by security data.

Resilience Dashboards:

Establish comprehensive operational resilience dashboards that consolidate key metrics – enterprise risks, continuity plan status, vendor risk posture, and security incident trends – into a unified view for leadership.

Benefits:

Real-time, holistic visibility into organizational risk and resilience. By linking BCM and SecOps with IRM, the organization enhances its preparedness and compliance posture, achieving embedded operational resilience and a tighter integration of security and risk management practices.

PHASE 05:
CONTINUOUS CONTROLS MONITORING (CCM) INTEGRATION

- **Continuous Controls Monitoring (CCM) Integration:**
  CCM supercharges your risk and compliance processes by **proactively validating controls** and surfacing weaknesses in real time. Key CCM capabilities added in Phase 2 include:

AUTOMATED CONTROL TESTING

Software-driven control tests execute on schedule or trigger-based, automating evidence collection and validation of control effectiveness with minimal manual effort. This ensures controls are functioning as designed and flags any failures immediately.

CONTINUOUS PERFORMANCE MONITORING

Real-time monitoring of control performance through control indicators and data integrations. The system continuously checks control health (e.g. compliance of configurations, completion of tasks) and updates risk scores, providing ongoing assurance instead of periodic snapshots.

COMPLIANCE DASHBOARDS & ALERTS

Interactive dashboards and visual reports that surface compliance breakdowns and gaps at a glance. Stakeholders get instant visibility into control statuses (pass/fail), trend charts, and automated alerts whenever a control deviates from acceptable parameters, enabling quick response.

INTEGRATED ISSUE & RISK WORKFLOWS

CCM is tightly integrated with issue and risk management workflows. If a control test fails or an indicator flags a risk threshold breach, the platform auto-generates an issue record, notifies owners, and ties it to the relevant risk. This seamless linkage ensures immediate remediation action and accountability for control deficiencies.

SECOPS AND POLICY LINKAGE

Continuous monitoring data is linked with Security Operations (SecOps) and policy governance. For example, CCM can pull in security incident data or vulnerability info from SecOps to test controls continuously against emerging threats. It also feeds results back into policy review processes. This closed-loop integration means your security, IT, and compliance teams all work off the same real-time control insights, strengthening overall governance.

PHASE 06:

AI GOVERNANCE & FUTURE-PROOFING

AI Governance (AI Control Tower):

Implement ServiceNow's AI Control Tower to inventory, monitor, and govern AI/ML models and algorithms in use. This ensures oversight and compliance with emerging AI regulations and ethical guidelines as the organization increasingly leverages AI

Intelligent Automation (Agentic AI & Now Assist):

Deploy advanced Agentic AI and Now Assist capabilities within the IRM platform to automate risk assessments, control testing, and regulatory compliance checks. Leverage generative AI to summarize issues and recommend controls, reducing manual effort and accelerating decision-making.

Global Standards Alignment:

Expand the IRM framework to cover additional international standards and regulations, reinforcing multi-jurisdictional compliance readiness (e.g. aligning with ESG criteria, privacy laws, and industry-specific regulations as needed).

Benefits:

Forward-looking AI governance and intelligent automation are now embedded in the risk program. The organization gains a future-proofed IRM platform that adapts to new technological developments and regulatory requirements, ensuring the program remains current, efficient, and globally compliant.

HYPERCARE & TRANSITION TO STEADY STATE

INTENSIVE SUPPORT & TUNING:

In the first months after go-live, provide intensive hypercare support to end-users and administrators. Fine-tune system performance and workflows based on user feedback, and ensure full adoption of all implemented IRM modules across the enterprise.

LEGACY DECOMMISSIONING:

Finalize the retirement of legacy risk systems to eliminate redundancy. Transition ownership of the new IRM solution to a permanent IRM Center of Excellence or governance team to sustain and grow the platform capabilities.

EMBEDDING IRM IN CULTURE:

Establish continuous performance analytics and monitoring. Embed IRM practices into the organizational culture through ongoing training, communication, and leadership reporting, ensuring that risk management and compliance processes are now business-as-usual.

BUSINESS OUTCOMES

By following the IRM Flightpath, your organization achieves tangible and strategic outcomes:

Unified, Scalable Risk & Compliance Operations:

A single, enterprise-wide platform that standardizes and scales all risk, compliance, and audit activities for consistent oversight.

Increased Automation & Reduced Manual Effort:

Significant reduction in manual processes through workflow automation and AI assistance, leading to higher productivity and lower error rates.

Continuous Regulatory Alignment & Audit Readiness:

Ongoing mapping of controls to regulations and standards ensures up-to-date compliance and always-on audit preparedness, even as regulatory requirements evolve.

Embedded Operational Resilience & Proactive Risk Oversight:

Strengthened business continuity and security integration mean resilience is built-in, with leadership gaining proactive insights into emerging threats and operational disruptions.

Future-Proof Platform (AI-Driven & Global Ready):

A modern IRM platform that is ready for the future – capable of governing AI risks, scaling with the organization, and adapting to global risk trends and regulatory changes.

The **IRM Flightpath by Templar Shield** empowers your enterprise to attain advanced, integrated, and future-proof risk management capabilities. With this phased transformation, you not only modernize your GRC/IRM technology but also embed a culture of risk-aware decision-making – ensuring long-term success and resilience for your organization.

Contact Information

+1-619-344-2573
www.templarshield.com
info@templarshield.com
350 10th Ave, Suite 1000, San Diego, CA 92101

TEMPLAR shield