R & D QUALITY ROUNDTABLE

Risk and Technology Breakout Series

Integrated Risk Assessment Framework for R&D

Part 1: Framework and Implementation Foundations

CLASSIFICATION |Pre-Competitive Industry Collaboration
STATUS Final | June 2026
AUTHORS| James Irwin[1], Arun Mathew[2], Seth McKinney[3], Simon Ward[4]

REVIEWERS | Keisha Bryant[5], David Carter[6], Lucie Regne-Martos[7], Kyle Young[8]

This white paper is a product of the R&D Quality Roundtable Risk and Technology Breakout Session, a pre-competitive collaboration among pharmaceutical industry professionals. The views expressed represent collective industry perspectives and do not constitute official guidance.

1 Senior Director, Quality Business Partner-Clinical Development, GSK

2 Director, R&D Strategic planning and operations, AbbVie

3 Senior Director, GRDQ Data Analytics, Eli Lilly

4 Lead, Quality Systems – Quality Process and Controls, Astellas

5 Vice President R&D Quality Assurance, AbbVie

6 Risk Management Director R&D, GSK

7 Clinical Quality Performance Head, CQ&CI, Sanofi

8 Head of Analytics & Technology/Systems Team, Merck

NAVIGATION GUIDE

Click any section title to navigate directly. This white paper is organized into four thematic groups.

Reading Key

Tables	Structured data supporting framework concepts; referenced inline as Table 1, Table 2, etc.
Figures	Visual representations of processes and relationships; referenced as Figure 1, Figure 2, etc.
Cross-references	Blue hyperlinked text links to other sections within this document for non-linear navigation.
Part 2 Deferred	Data ontology, system architecture, AI, Gen AI and advanced analytics, are acknowledged but deferred to Part 2.

EXECUTIVE SUMMARY

The Problem: Quality Risk management in pharmaceutical R&D is essential but frequently fragmented. Fragmentation is no longer sustainable in a world of accelerated timelines, modality diversification, and distributed development models. When risk is fragmented, companies are exposed to late-stage surprises that could have been prevented and potentially delay patients receiving access to new medications. Function-specific processes create siloed risk assessments. Multiple assessments for the same product, each with different or even conflicting information, resulting in valuable risk insights generated during development being inaccessible to downstream stakeholders. Inconsistent terminology across ICH, ISO, COSO, and other frameworks further undermines enterprise visibility and inhibits effective automation and integration. ICH Q9(R1) explicitly calls for risk management that builds knowledge across the product lifecycle, yet most organizations lack the structures to deliver on this expectation.

The Solution: This white paper presents a practical framework for Integrated Risk Management (IRM) across the R&D lifecycle. IRM is not a new process- it is a unifying architecture that connects risk knowledge across the lifecycle and accelerates decision making. IRM creates a central risk profile for each product by linking high/significant risks identified by risk processes assessments from all functional silos into a single, visible, and continuously updated view. Rather than replacing existing risk processes, IRM connects them, ensuring that a risk identified in formulation development is visible to clinical operations, that a safety signal informs quality decisions, and that commercialization teams inherit a complete risk history. IRM strengthens decision velocity by ensuring that risk knowledge is visible, connected, and actionable across the lifecycle.

The framework addresses five foundational dimensions: People and Governance (clear ownership, cross-functional forums, and decision rights), Process (standardized lifecycle alignment, common vocabulary, defined triggers), Data (accessible, trusted information, connected systems), Technology (enablement, ontology development, system architecture) and Outcomes (measure value). Part 1 of this series establishes the framework and implementation foundations; Part 2 will address technology enablement including ontology development and system architecture.

Getting Started: IRM requires cultural alignment, governance clarity, and shared vocabulary before tools or workflows can deliver value. Success depends on leadership alignment across functions, not just tools or workflows. Organizations need not undertake a multi-year transformation to begin realizing value. This paper defines five foundational elements that constitute a minimum viable IRM implementation (see Section 7): a common risk vocabulary, a central mechanism for product-level risk visibility, at least one cross-functional governance touchpoint, defined triggers for cross-functional risk communication, and a periodic review cadence.

Expected Outcomes: Organizations that adopt integrated risk management gain resilience, reduce late-stage failures, and strengthen patient and regulatory trust. In addition, regulators gain confidence in organizations that demonstrate connected, lifecycle-wide risk visibility and management.

This framework represents the collective perspective of industry experts from the R&D Quality Roundtable. It is intended as a practical starting point, not a prescriptive standard, that organizations can adapt to their specific context, scale, and maturity.

1 Introduction

Integrated Risk Management (IRM) represents a strategic capability that enables decision velocity, ensures lifecycle continuity, and accelerates commercial readiness across pharmaceutical R&D. Rather than viewing quality risk management as just a series of discrete assessments conducted at fixed intervals, IRM establishes an organizational discipline where high/significant risk knowledge generated at any stage remains visible, actionable, and decision-relevant throughout the entire product lifecycle. This capability transforms risk from a compliance artifact into a strategic asset that informs portfolio prioritization, resource allocation, and go/no-go determinations at critical development milestones.

ICH Q9(R1) reinforces this imperative by emphasizing that risk knowledge must be captured early, maintained continuously, and leveraged across organizational boundaries. The guideline's evolution from periodic risk assessment to lifecycle risk management reflects an industry-wide recognition that fragmented risk information—siloed within functions, locked in point-in-time documents, or disconnected from decision-making processes—undermines both development efficiency and commercial success. Organizations that fail to establish integrated risk capability face predictable consequences: delayed recognition of cross-functional dependencies, reactive escalation of preventable issues, and diminished confidence in regulatory and commercial readiness assessments.

This white paper series defines the governance boundaries, organizational expectations, and operational frameworks necessary to operationalize IRM across pharmaceutical R&D. Part 1 establishes the foundational governance model, clarifies ownership structures that enable accountability without creating bottlenecks, and provides minimum viable implementation guidance for organizations at any maturity level. Subsequent parts will address ontology development, technology enablement, and advanced analytics capabilities. Together, these components constitute an architectural blueprint for organizations committed to transforming risk management from a procedural obligation into a source of competitive advantage.

The level of rigor applied to risk capability should correspond to product lifecycle stage, reflecting the degree of uncertainty, complexity, and proximity to patient impact. However, rigor does not imply bureaucracy but requires disciplined capture of decision-relevant risk information in forms that remain accessible and actionable as products advance from discovery through commercialization. Organizations that establish this capability early create compounding advantages: faster decision cycles, more efficient resource deployment, stronger regulatory submissions, and greater organizational confidence in portfolio strategy.

1.1 Scope

This white paper defines the foundational boundaries for IRM across the pharmaceutical R&D lifecycle, establishing IRM as an enterprise-level architecture for strategic governance, informed decision making, and lifecycle continuity. The intent is to address fragmentation and enable a unified, agile risk capability that supports innovation, patient outcomes, and commercial readiness.

The strategic focus area centers on integrating quality, safety, regulatory, clinical, and supply risk oversight into a connected framework, ensuring that risk intelligence informs and accelerates enterprise-level decisions at every development phase. This cross-industry series sets the principles, governance expectations, and implementation guidance needed to operationalize unified IRM and enable strategic value realization across R&D.

Table 1. *Scope boundaries for Part 1 of this white paper series.*

Boundary	Description
In Scope	Enterprise integration of risk management across the R&D lifecycle for pharmaceuticals specifically quality, safety, regulatory, clinical, and supply risk integration; definition of IRM frameworks, principles, and implementation guidance
Out of Scope	Adjacent domains intentionally excluded to maintain focus: Commercial process and commercial manufacturing, Device risk management (only risks that impact drug is considered) and detailed technology specifications (to be covered in Part 2).

2 Problem Statement

Risk management guidance is well established in documents such as ICH Q9 and ICH E6. However, persistent fragmentation across R&D risk practices—characterized by isolated assessments, lack of standardized terminology, and insufficient cross-functional visibility—compromises decision velocity, lifecycle continuity, and the cohesiveness of control strategies. This fragmentation introduces systemic governance weaknesses that impede the timely translation of risk intelligence into strategic actions, erode organizational alignment, and threaten enterprise readiness for commercialization and sustained innovation. The absence of a unified risk framework limits the scalability and effectiveness of risk oversight, undermining patient outcomes and quality

Table 2. *Core fragmentation challenges in current R&D risk management practices.*

Challenge	Description
Siloed Assessments	Lack of integrated risk management perpetuates redundant assessments, inconsistent risk narratives, and delays execution of risk-based decisions across the lifecycle
Limited Visibility	Insufficient cross-functional transparency restricts timely access to risk intelligence, weakening continuity and impeding enterprise-wide responsiveness
Missing Consolidation	Fragmented stewardship of risk data results in incomplete risk profiles, gaps in lifecycle knowledge, and misaligned control strategies
Vocabulary Barriers	Disparate terminology and data standards create barriers to enterprise harmonization, stifle effective risk automation, and obscure actionable cross-domain insights (Lessons learned).

3 Purpose of This White Paper

The purpose of this white paper is to fill the gap in clear guidance on consolidating high/significant risks from various functional areas and addressing the defined problem statement. It provides the position to industry how the Integrated Risk Management (IRM) framework defines foundational boundaries, core principles, and governance expectations. The paper offers a reference architecture and interpretive guidance that organizations can tailor to their governance models, operational structures, and decision-making processes, helping to ensure continuity throughout the lifecycle. This paper establishes key principles that are necessary conditions for integrated risk management, summarized in Table 3 below.

Table 3. *Five foundational principles for integrated risk management.*

Principle	Summary
People & Governance	Clear ownership models, governance structures, decision rights and effective communication drive accountability and integration.
Process	A standardized, end-to-end product lifecycle process, common vocabulary, defined triggers.
Data	Accessible, trusted and connected risk data and information ensure consistency across functions.
Technology	Enablement, ontology development system architecture and data infrastructure enable seamless risk capture, analysis, and reporting.

Outcomes	Measurable impact criteria confirm that integration delivers value.

Note: Data and Technology are acknowledged as foundational but detailed solutioning (ontology implementation, system architecture) is deferred to Part 2. Part 1 establishes the "what" and "why"; Part 2 will address the "how" for technology enablement.

4 Integrated Risk Management Framework

4.1 Concept

Strategic Piller: Integrated Risk Management (IRM) is an enterprise reference architecture that preserves, validates, and operationalizes risk knowledge across the full R&D lifecycle. The architecture's purpose is strategic: to ensure that program-level risk intelligence is persistent, auditable, and decision-ready as programs move from a product entering phase 1 through clinical development, regulatory approval to support tech transfer, and up to commercial launch. By specifying where high/significant risk knowledge must flow, which governance gateways must validate it, and who holds stewardship and decision rights at each stage, the IRM architecture converts dispersed risk signals into a single program that supports faster, more consistent enterprise decisions.

This architectural stance reflects the intent of ICH Q9(R1): risk knowledge created early must be visible and actionable downstream, so development-phase insights meaningfully strengthen downstream control strategies, regulatory positions, and investment choices. Rather than prescribing tools or local workflows, the model prescribes checkpoints (e.g., milestone reviews, transfer gates, regulatory filings, enterprise escalations), evidence expectations, and accountability constructs that ensure continuity of risk stewardship and enable coherent control strategies at scale.

Integrated Risk Management (IRM) is a systematic, structured process used in R&D to proactively share high/significant quality risks associated with drug products. The IRM process provides a central risk profile, linking risks identified from various risk assessments performed throughout the R&D product lifecycle (products entering Phase I, Phase II/III up to commercialization). The framework components described in this section align with the principles established in Table 3 and are operationalized through the methodology in Section 5. Figure 1: Integrated Risk Assessment Framework illustrates how the integrated risk assessment framework consolidates risks sourced from multiple functional areas, enabling cross-functional visibility and communication. This collective approach supports a comprehensive understanding of potential risks facilitating effective prioritization and mitigations.

To The governance model incorporates cross-functional collaboration, where representatives from different functional areas review consolidated risk information, escalate high/significant risks requiring senior leadership attention, and maintain communication channels to ensure all stakeholders remain informed. Governance decisions and lessons learned are systematically fed back into the risk assessment processes, establishing a

continuous improvement cycle that enhances risk management capabilities over time. The integrated approach works as an enabler to the more future-looking state, where the overall R&D lifecycle moves away from rigid, phase-based approaches with milestones being centered around delivery of document to a more data-centric approach. This transition requires risk to be treated as a continuum rather than assessed at discrete, staged points. By embedding cross-functional collaboration, consolidated risk visibility, and continuous feedback loops into the current operating model, the organization is better positioned to support dynamic, data-driven decision-making that reflects the true, ongoing nature of risk across the full development lifecycle.

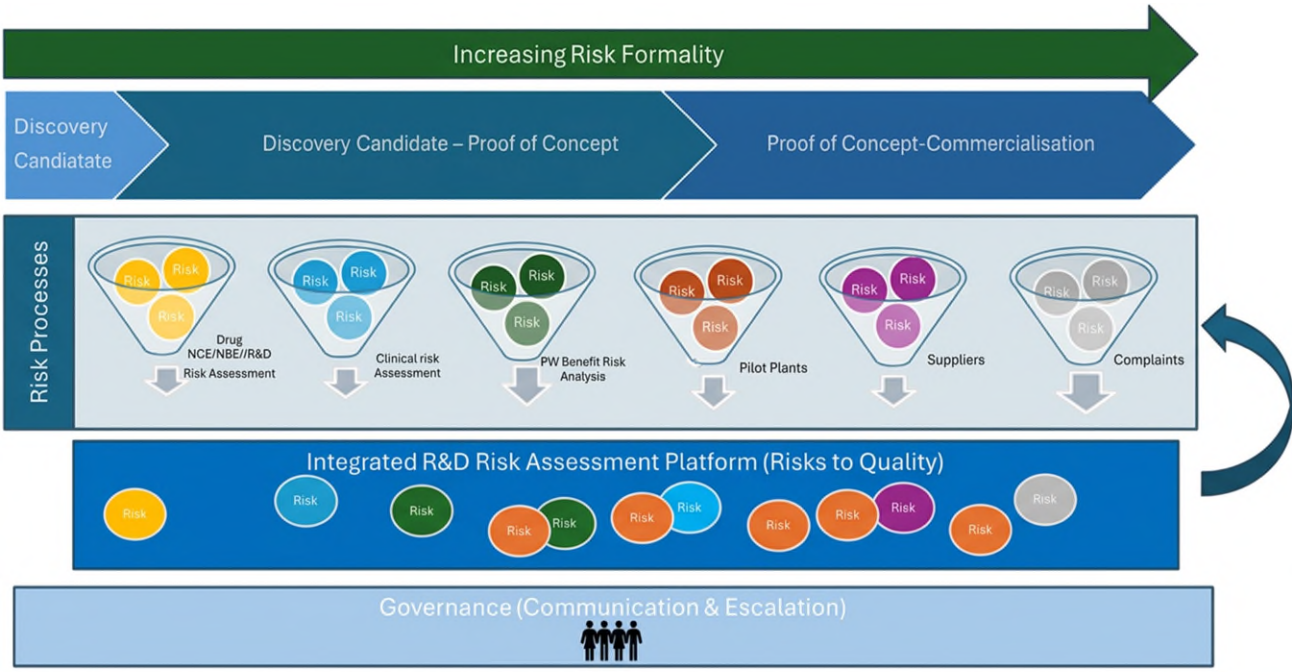

Figure 1: Integrated Risk Assessment Framework

4.2 Framework Components

Table 4. *IRM framework components and their role in the integrated risk lifecycle.*

Component	Description
Risk Identification & Evaluation	Establishes systematic processes for identifying and evaluating risks throughout the product lifecycle. Risks are assessed against defined risk categories (for example Quality, Supply, Regulatory, and Clinical,) using appropriate methodologies. Governance structures ensure accountability for risk identification across all organizational functions and development stages, supporting informed decision-making aligned with ICH Q9(R1) principles.
Risk Control	Defines decision-making authorities and accountabilities for implementing risk mitigation strategies. Ensure risk reduction measures are proportionate to risk significance and are evaluated cross-functionally to prevent unintended consequences. Governance oversight validates that residual risks remain within acceptable thresholds throughout the product lifecycle.
Risk Review	Establishes mechanisms for ongoing risk monitoring and reassessment as knowledge evolves across the product lifecycle. Governance structures facilitate periodic review of significant risks, enabling timely escalation and cross-functional alignment. Supports continuous improvement through systematic evaluation of risk management effectiveness and emerging risk trends.
Risk Communication	Defines governance frameworks for risk transparency and stakeholder engagement throughout the product lifecycle. Establishes accountability for communicating relevant risk information to appropriate stakeholders, with formality and scope proportionate to risk significance and lifecycle stage. Ensures mechanisms exist for effective risk knowledge transfer as products transition through development phases toward commercialization.

5 Implementation Methodology

5.1 Process Steps

Successful IRM implementation requires organizations to establish foundational principles and governance structures that enable systematic risk management throughout the product lifecycle. This section outlines the essential elements organizations should consider when operationalizing IRM, recognizing that specific approaches will vary based on organizational context, product complexity, and lifecycle stage. See Table 5.

Table 5. *Ten-step IRA implementation methodology.*

#	Step	Description
1	**Knowledge Management / Data Collection**	Establish governance for comprehensive knowledge management that captures, integrates, and maintains risk-relevant information across the product lifecycle. Organizations should define accountability for ensuring risk assessments are informed by appropriate data sources, including preclinical findings, clinical evidence, quality assessments, safety surveillance, and historical knowledge.
2	**Risk Identification**	Implement structured approaches for identifying and evaluating risks across all relevant domains (Quality, Clinical, Regulatory, Supply). Organizations should establish clear accountability for risk identification, ensure cross-functional input, and apply consistent evaluation criteria that enable meaningful prioritization and resource allocation.
3	**Sequence of Events Mapping**	Ensure risk assessments consider the mechanisms and pathways through which risks may materialize. Organizations should establish expectations where needed for documenting risk scenarios, including contributing factors, affected stakeholders, and potential consequences, to support informed decision-making.
4	**Risk Scenario Definition**	Define and document the circumstances under which the identified risk could materialize, including contributing factors, affected stakeholders, and potential exposure pathways.
5	**Impact Identification & Evaluation**	Specify possible impacts arising from each risk and assign a severity score using a standardized scale (see Appendix B).
6	**Likelihood Estimation**	Estimate the likelihood of each impact based on available data and knowledge (e.g., complaint data, clinical study findings, or experience with similar products).
7	**Risk Calculation & Categorization**	Ground risk evaluation in available evidence, applying appropriate analytical rigor proportionate to decision significance. Organizations should define governance for impact assessment and likelihood estimation, ensuring consistency, traceability, and alignment with organizational risk tolerance. Use severity and likelihood scores in a risk matrix to categorize each risk as Low, Medium, or High (see Appendix B).
8	**Risk Controls & Mitigation**	Establish decision-making authority and accountability for implementing risk mitigation strategies proportionate to risk significance. Organizations should ensure risk control decisions consider resource constraints, feasibility, and the potential for unintended consequences.
9	**Records & Review**	Ensure transparency, version control, and accessibility of risk information to relevant stakeholders. Organizations should establish processes/systems that support lifecycle knowledge retention
10	**Periodic Review & Updating**	Regularly (at least annually) review and update the IRA as new data emerges, lifecycle stage changes, or risk profiles shift.

5.2 Tools

Selection and integration of risk assessment tools should be guided by organizational context, risk complexity, and the broader risk management architecture rather than adherence to any single methodology. Key principles include:

- Tool-Agnostic Flexibility: Adopt a range of recognized risk assessment approaches (e.g., Hazard Analysis, FMEA, FTA, PHA) and allow their integration or tailoring in alignment with the organization's needs, project specifics, and regulatory requirements.
- Context-Driven Application: Select tools commensurate with the complexity, criticality, and lifecycle stage of the decision at hand, ensuring the approach supports robust identification, evaluation, and documentation of risks.
- Consistency with Governance: Ensure selected tools and frameworks harmonize with established corporate governance standards and remain adaptable to changes in regulatory expectations or business priorities.
- Transparency and Traceability: Structure tool integration to provide clear justifications for tool choice and methodology, facilitate auditability of risk decisions, and support traceable outcomes across the product lifecycle.
- Supporting Lifecycle Continuity: Ensure that tool use enhances continuity and knowledge transfer as risks, data, and projects evolve—avoiding fragmentation or silos.

5.3 Communication Strategy

An effective communication strategy for Integrated Risk Management (IRM) is foundational to transparent governance and organizational agility.

The communication strategy for R&D IRA should ensure transparency, clarity, and timely information flow. Three pillars support effective risk communication, as detailed in Table 6. Communication triggers are further operationalized in Section 7.4.

Table 6. *Communication strategy pillars for IRA implementation.*

Pillar	Approach
Enable Timely Escalation	Define mechanisms for rapid identification and escalation of emerging or changing risks to decision-makers, ensuring swift action where necessary.
Foster Shared Understanding	Establish cross-functional channels and forums that support continuous information flow, alignment of perspectives, and mutual understanding among stakeholders involved in risk identification, evaluation, mitigation, and oversight. While risk and quality-focused roles serve as key facilitators of this pillar, effective cross-functional collaboration extends across all organizational domains.
Deliver Decision-Ready Information	Provide clear, relevant, and current risk summaries tailored to the needs of reviewers, approvers, and other roles as defined by organizational governance (e.g., using RACI models, reporting standards, and centralized information systems).
Govern Process Ownership:	Clearly designate roles and responsibilities for risk communication, review, and approval, making escalation and accountability expectations explicit across the risk management lifecycle.
Ensure Knowledge Management and Traceability	Mandate version-controlled reporting and record-keeping in accessible systems, supporting both transparency and regulatory scrutiny. Ensure data/knowledge is managed to allow records are accessible, supporting both transparency and regulatory scrutiny.

6 People and Governance

A robust governance model is the control plane that makes Integrated Risk Management (IRM) operational at enterprise scale. Section 6 defines a governance approach to ownership: assigning shared accountability where impact is realized, enabling auditable escalation, and providing accountable roles that coordinate cross-functional action. Framing ownership as a governance construct — not only an operational assignment — closes visibility gaps, reduces duplication, and ensures IRM drives strategic decisions across the product lifecycle.

6.1 From Functional to Integrated Risk Ownership

Functional ownership — assigning risks to the function that controls a process or control — preserves operational clarity inside silos but creates a potential knowledge gap across the enterprise. That gap manifests as fragmented visibility, inconsistent prioritization, delayed escalation of cross-cutting risks, duplicate assessments, and uneven engagement with regulators and senior leadership.

Integrated ownership is a governance correction: accountability is shared between the functional owner and business owner (aligned to impact rather than solely to control). Under this model a business Owner (a named business leader or role) holds the governance responsibility to:

- Be the single accountable authority for decisions and trade-offs when a risk affects multiple functions or program outcomes.
- Convene contributors (Functional owners) to design, approve and implement cross-functional mitigation plans.
- Maintain the authoritative IRM profile for the risk (traceability, decisions, artifacts).
- Escalate to the defined governance forum (e.g., program board, enterprise risk committee) when risk thresholds are breached.
- Report status and outcomes to executive governance and regulators as required.

Governance outcomes from this shift include accelerated escalation, consistent prioritization across the portfolio, clearer funding and resourcing decisions tied to enterprise impact, and a streamlined line of accountability for the business .

6.2 Business Risk Ownership

Business based ownership establishes a single governance authority (Business Owner)—the business leader or role accountable for the major outcome if the risk materializes. Functional owners retain responsibility for implementing mitigations, but the Business Owner:

- Sets enterprise priorities for risk mitigation and decision-making
- Drives escalation according to defined triggers
- Responsible for the maintenance of an centralized risk records in the IRM system
- Coordinates across functions and reports to executive governance bodies

This model ensures accelerated escalation pathways, sharper prioritization based on enterprise value, and a single, traceable accountability line for regulators and auditors.

Enterprise Outcomes:

- Strategic Visibility: High/Significant Risks and decisions are transparent to leadership, supporting proactive interventions
- Focused Resource Deployment: Investment and mitigation align to enterprise-critical risks
- Consistent Lifecycle Management: Risks are tracked and governed throughout product development and commercialization
- Audit-Ready Accountability: Ownership and actions are captured for compliance and regulatory assurance

Complex, data-driven R&D ecosystems where critical processes are distributed across global teams call for a shift toward a share functional and business-based risk ownership. This model places accountability with the functional owner and business function or role most affected by consequences of a risk occurring.

Table 7. *Benefits of impact-based risk ownership.*

Benefit	Description
Improved Strategic Visibility	Enterprise risks become more visible to senior leadership when aligned with impact.
Accelerated Escalation	High-impact risks are more likely to be escalated by those anticipating consequences.
Improved Resource Allocation	Budgets align more closely to risks when owned by affected business functions.
Common Focal Point	The impact owner becomes the hub for coordination across contributing functions.
Aligned Accountability	Those closest to impact are best placed to balance trade-offs and orchestrate mitigation.

6.3 Practical Examples

Table 8 demonstrates how business-based ownership complements Functional-based ownership to enable lifecycle continuity and risk-informed decision-making. In each scenario, the control owner maintains technical or functional accountability for mitigation execution, while the business owner holds governance accountability for ensuring the risk is evaluated within the broader product lifecycle context and escalated appropriately. This integrated model ensures that risks are not only managed procedurally but are also positioned within decision-making forums where cross-functional trade-offs can be assessed and strategic actions can be authorized.

The governance value of this model lies in its ability to connect technical risk identification with strategic decision authority, ensuring that risks surface at the appropriate organizational level with sufficient context for timely, informed action.

Table 8. *Worked examples of impact-based vs. control-based risk ownership across R&D functions.*

Typical Risk	Functional Owner	Business Owner	How Integration Improves
CMC/Formulation risks affecting drug product	CMC Development	Drug Product Development Lead	Ensures formulation risks are evaluated against product profile requirements and lifecycle timelines, enabling the Drug Product Lead to make informed decisions about development strategy, backup plans, or resource reallocation.
System outages (EDC, CTMS, eTMF), data integration failures	IT / Digital	Head of Clinical Development	Positions IT incidents within the context of program-critical milestones and submission timelines, allowing senior leadership to prioritize resolution based on strategic impact and authorize cross-functional resource deployment.
Delayed site activation or patient enrollment	Clinical Operations	Global Program Lead	Connects operational delays to submission timelines and commercial commitments, enabling the GPL to assess trade-offs, engage cross-functional support (Medical Affairs, Regulatory), and escalate to portfolio leadership when timeline integrity is threatened.
Query backlog, database lock delays	Data Management	Global Program Lead	Elevates data management delays from technical issues to submission-readiness risks, empowering the GPL to drive escalation, authorize additional resources, or adjust milestone planning based on integrated program impact.
Increased protocol deviations, site non-compliance, inspection readiness gaps	Clinical Operations	Global Program Lead	Elevates operational compliance issues to program-level risks affecting regulatory submission integrity and inspection outcomes, enabling the GPL to assess impact on approval timelines, authorize corrective and preventive actions across sites, and escalate to Regulatory Affairs and Quality Assurance when compliance trends threaten program viability.

7 Minimum Viable Implementation

For organizations beginning their IRM journey, the following five elements constitute the minimum governance conditions necessary for effective integrated risk management. These foundational elements establish the organizational discipline and cross-functional alignment required to operationalize the governance model described in Section 6. Each element represents a governance capability that enables consistent risk interpretation, transparent visibility, and coordinated decision-making across the product lifecycle. Table 9 provides a summary, with each element detailed in the subsections that follow.

Table 9. *Five foundational elements for minimum viable IRM implementation.*

#	Element	Minimum Requirement	Scalable Options
1	**Common Vocabulary**	Governed risk terminology enabling consistent interpretation across function	Harmonized ontology with controlled terminology management (Part 2)
2	**Central Risk Profile**	Lifecycle-continuous risk visibility mechanism accessible cross-functionally	Enterprise-wide risk intelligence with integrated analytics
3	**Governance Touchpoint**	Defined decision-making forum with cross-functional representation and authority	Integrated stage-gate governance with formalized decision rights
4	**Communication Triggers**	Enterprise-level escalation criteria aligned with impact-based ownership	Automated escalation protocols with accountability tracking
5	**Review Cadence**	Risk-informed review frequency tied to lifecycle milestones and decision points	Continuous risk monitoring with dynamic review triggers

7.1 Common Vocabulary

Establish vocabulary alignment as a foundational governance requirement that enables consistent risk interpretation and prioritization across R&D functions. At minimum, the organization must define and govern: risk categories (for example Quality, Supply, Regulatory, Clinical,), severity scale definitions, likelihood scale definitions, and risk acceptance thresholds. This governed glossary ensures that risk assessments are comparable across functions and that escalation criteria are uniformly applied. Appendix A provides an example reference glossary; Appendix B provides example reference scales.

7.2 Central Risk Profile Mechanism

Establish a mechanism that ensures lifecycle continuity and cross-functional visibility of product-level risks. The central risk profile must maintain risk information throughout product development, from when a product enters phase 1 through to commercialization, enabling any authorized function to access current risk status. This mechanism serves as the single source of truth for product risk posture, supporting informed decision-making at critical lifecycle junctures. The emphasis is on governance of information accessibility and continuity, not on specific system implementations.

7.3 Governance Touchpoint

Define a decision-making forum with explicit cross-functional representation where risk information informs product advancement decisions. This governance touchpoint must have defined membership spanning relevant R&D functions, with decision authority, and established criteria for risk-informed go/no-go determinations. The forum operationalizes the ownership framework from Section 6, ensuring that risks are evaluated by those with appropriate functional expertise and decision-making authority. The governance model determines when and how risks are brought to this forum for collective assessment.

7.4 Defined Communication Triggers

Establish enterprise-level escalation criteria that determine when risks must be communicated beyond the identifying function, aligned with the business-based ownership model. These triggers define the thresholds and conditions that mandate risk visibility to senior leadership, cross-functional forums, or enterprise risk governance bodies. Minimum criteria include risks exceeding defined severity or likelihood thresholds, risks with potential cross-functional or cross-product impact, and, regulatory compliance, or strategic objectives. These triggers ensure appropriate ownership engagement as described in Section 7.4 Periodic Review Cadence

7.5 Review Cadence

Establish a review frequency tied directly to lifecycle milestones and decision points, with risk-informed cadence as the minimum viable expectation. Rather than calendar-based reviews alone, the cadence must align with product development stages where risk profiles materially change or where decisions depend on current risk assessment. At minimum, risk profiles must be reviewed at major lifecycle gates (e.g., when a product enters phase 1). Between subsequent milestones, risk-based triggers should determine interim review frequency based on risk severity, velocity of change, or emergence of new information. This ensures risk profiles remain current and decision-relevant throughout development.

8 Outcomes and Success Metrics

A fully integrated risk management capability drives measurable enterprise outcomes aligned to strategic business, regulatory, and patient-impact objectives. Success is defined by clear, quantifiable metrics that align with core themes such as decision velocity, regulatory confidence, and lifecycle continuity. By establishing robust criteria at implementation, organizations ensure IRM practices continuously deliver value and support ongoing improvement. Table 10 presents five recommended metrics spanning leading and lagging indicators.

Table 10. *Recommended success metrics for IRM implementation, with targets.*

Metric	Strategic Outcome	What It Measures	Target
Decision Velocity	Operational agility	Reduction in time from risk identification to mitigation plan adoption across functions.	Establish baseline, then measure improvement over 12 months.
Improved Inspection Readiness	Operational agility	Decrease in inspection/audit findings related to risk documentation or traceability.	Reduction in risk-related observations year-over-year.
Reduced Risk Redundancy	Process Efficiency	Fewer duplicate risk assessments per product as risks are centrally visible.	Single source of truth for product risk profile.
Regulatory Confidence	Compliance & Engagement	Recognition of modernized risk frameworks by regulators as contributing to ICH Q9(R1) compliance.	Positive feedback in regulatory interactions; reduced oversight burden.
Proactive Risk Identification	Preventive Culture	Timeliness of risk discovery via cross-functional sharing	Increasing proportion of risks identified prior to downstream impact

9 Conclusion and Next Steps

Integrated risk management is not a new process layered onto existing work. It is a shift in how organizations understand, communicate, and act on risk across the R&D lifecycle. When practiced with intention, IRM becomes a strategic capability that strengthens decision quality, accelerates development, and ensures that early insights are carried forward with clarity and purpose. The fragmentation that has historically defined R&D risk practices is no longer sustainable in an environment where complexity, speed, and regulatory expectations continue to rise.

This paper establishes the foundation required to move from siloed, function-based assessments to a unified, enterprise aligned model. The journey toward integrated risk management is maturity progression, not a single implementation step. It begins with shared language and measurement, advances through governance and ownership, and ultimately becomes scalable through technology and data connectivity.

A practical maturity arc includes:

1. Establishing shared foundations - aligning on vocabulary, definitions, and measurement principles to ensure consistent interpretation across functions.
2. Harmonizing risk practices - reconciling disparate approaches into a unified model that supports lifecycle continuity and cross-functional clarity.
3. Implementing minimum viable IRM - putting in place the essential governance, visibility, and communication mechanisms that allow integrated behaviors to take root.
4. Embedding governance ownership - shifting accountability to where impact is felt and enabling timely, coordinated decision making.
5. Defining success metrics- selecting a focused set of indicators that measure decision quality, regulatory confidence, and portfolio resilience.
6. Scaling and optimizing - refining practices based on experience and preparing the organization for broader adoption.
7. Enabling Technology - integrating data, platforms, and analytics to create real-time visibility and sustainable enterprise adoption, which will be explored in Part 2.

Appendix A: Glossary

Table 12. *Standardized risk management terminology for cross-functional alignment.*

Term	Definition
Integrated Risk Assessment (IRA)	A systematic process providing a central risk profile linking risks from various assessments across the R&D lifecycle.
Hazard	A potential source of harm (ISO/IEC Guide 51).
Harm	Damage to health, including the damage that can occur from loss of product quality or availability.
Risk	Combination of the probability of occurrence of harm and the severity of that harm (ISO/IEC Guide 51).
Risk Assessment	A systematic process of organizing information to support a risk decision to be made within a risk management process. It consists of the identification of hazards and the analysis and evaluation of risks associated with exposure to those hazards.
Risk Control	Actions implementing risk management decisions (ISO Guide 73).
Severity	A measure of the possible consequences of a hazard.
Likelihood	The probability that harm will occur.
Impact Owner	The business function or role most affected by consequences of a risk occurring.
Control Owner	The function responsible for implementing risk mitigations and sustaining procedural integrity.

Appendix B: Example Reference Risk Matrix

The following scales and matrix provide a starting point for organizations without existing risk rating systems. Organizations should adapt these to their own context and maturity. The severity scale incorporates GxP compliance considerations at levels 3–5, where regulatory impact becomes material. These scales are referenced by the methodology in Section 5, Steps 5–7.

Table 13. *Reference severity scale for IRA risk evaluation.*

Level	Category	Description
1	**Negligible**	No or minimal impact to patient, product, or program.
2	**Minor**	Limited impact; manageable through routine processes.
3	**Moderate**	Significant impact requiring active management; potential GxP compliance implications.
4	**Major**	Serious impact to patient safety, program timeline, regulatory standing, or GxP compliance.
5	**Catastrophic**	Critical impact; potential program termination, serious patient harm, major regulatory action, or systemic GxP failure.

Table 14. *Reference likelihood scale for IRA risk evaluation.*

Level	Category	Description
1	**Rare**	Unlikely to occur during product lifecycle.
2	**Unlikely**	Could occur but not expected.
3	**Possible**	May occur at some point.
4	**Likely**	Expected to occur.
5	**Almost Certain**	Expected to occur multiple times.

Table 15. *5×5 risk matrix combining severity and likelihood. Color coding indicates risk categorization: High (red), Medium (amber), Low (green).*

Likelihood \ Severity	Sev. 1 Negligible	Sev. 2 Minor	Sev. 3 Moderate	Sev. 4 Major	Sev. 5 Catastrophic
5 – Almost Certain	Medium	Medium	High	High	High
4 – Likely	Low	Medium	Medium	High	High
3 – Possible	Low	Low	Medium	Medium	High
2 – Unlikely	Low	Low	Low	Medium	Medium
1 – Rare	Low	Low	Low	Low	Medium

Appendix C: Risk Assessment Tool Template

The following template (Table 16) provides a starting point for IRA documentation. Column headers are generalized to support multiple risk assessment methodologies (Hazard Analysis, FMEA, FTA, PHA). This template operationalizes the ten-step methodology described in Section 5.1.

Table 16. *Generalized risk assessment tool template compatible with FMEA, FTA, Hazard Analysis, and PHA approaches.*

#	Risk Source	Risk Scenario	Potential Impact	Severity	Likelihood	Risk Level	Controls
1	*[Source]*	*[Scenario]*	*[Impact]*	*[1–5]*	*[1–5]*	*[L/M/H]*	*[Controls]*
2							

References

1. International Conference on Harmonisation (ICH). ICH Q9(R1): Quality Risk Management. 2022.
2. International Conference on Harmonisation (ICH). ICH E6(R2): Good Clinical Practice. 2016.
3. ISO 31000:2018. Risk management, Guidelines.
4. Pistoia Alliance. “IDMP Ontology (IDMP-O) Project Charter.” 2024.
5. U.S. Food and Drug Administration (FDA). Final Report: FDA-EMA Pilot Program for Parallel Assessment of Quality-by-Design Applications. 2017.
6. ISPE. GAMP 5: A Risk-Based Approach to Compliant GxP Computerized Systems. 2022.
7. ISO/IEC Guide 51:2014. Safety aspects, Guidelines for their inclusion in standards.
8. ISO Guide 73:2009. Risk management, Vocabulary.