RESEARCH ARTICLE

SAMRIDDHI Volume 14, Issue 4, 2022 Print ISSN: 2229-7111 Online ISSN: 2454-5767

Digitizing Risk Management Through Configurable Enterprise Workflow Architecture

Senior Salesforce Developer Santhosh Reddy Basireddy

USAA, San Antonio, Texas, USA

Abstract

Enterprises increasingly confront operational, financial, and regulatory uncertainties that outpace the periodic, document-centric practices historically used to govern them. Configurable enterprise workflow architecture offers a structural foundation for embedding governance directly into the systems where decisions occur, transforming risk activities into executable, adaptable processes rather than isolated records. By separating business logic from application code, such architecture lets administrators model intake, scoring, control, and escalation as declarative definitions that evolve without rewriting underlying software. This article describes how digitization reshapes each stage of the risk lifecycle, from standardized identification and parameterized assessment through automated controls, embedded accountability, and continuous monitoring. It situates the discipline within the broader movement toward risk-aware business process management, where exposures are minimized during design and mitigated during execution. Attention is given to the security, governance, and integration considerations that determine whether automation strengthens resilience or introduces fragility. The resulting framework positions governance as an adaptive, continuous capability aligned with volatile and complex operating conditions.

Keywords: risk digitization; configurable workflow architecture; risk-aware business process management; governance orchestration; continuous monitoring.

SAMRIDDHI : A Journal of Physical Sciences, Engineering and Technology (2022); DOI: 10.18090/samriddhi.v14i04.48

Introduction

For decades, enterprise risk management operated as a periodic, document-centric ritual, detached from the operational systems where exposure actually accumulates. Registers lived in spreadsheets, assessments arrived as static reports, and escalation depended on scattered message threads that fragmented accountability. This separation between where risk is recorded and where decisions are made has long been recognized as the central weakness of the discipline, and it motivated the emergence of risk-aware business process management, a paradigm that unifies two traditionally isolated fields so that risks can be minimized by design and mitigated at run time [9]. Digitizing risk management extends that ambition by embedding governance directly into configurable enterprise workflows, turning risk activities into executable, adaptable processes rather than detached paperwork.

Configuration is the operative word. In a configurable framework, the definitions that govern how risk flows, who must act, and when a control fires are held as editable settings rather than as compiled instructions, so that a change in appetite or obligation becomes an administrative act rather than a software release. This distinction matters because the pace of regulatory and operational change now exceeds the cadence at which bespoke systems can be rebuilt. When governance is expressed as configuration layered over a stable execution engine, the enterprise keeps its controls current without surrendering consistency, and the long-standing divide between written policy and daily execution begins to close. The sections that follow treat that divide as the problem to be solved and configurable workflow architecture as the instrument for solving it.

The commercial momentum behind such automation is substantial. The market for software-driven process automation was projected to approach seven billion euros by 2020 [1], and independent overviews trace a technology moving quickly from novelty toward mainstream capability

Corresponding Author: Santhosh Reddy Basireddy, Senior Salesforce Developer, USAA, San Antonio, Texas, USA, e-mail: santhureddy245@gmail.com

How to cite this article: Basireddy, S.R. (2022). Digitizing Risk Management Through Configurable Enterprise Workflow Architecture. *SAMRIDDHI : A Journal of Physical Sciences, Engineering and Technology,* 14(4), 231-239.

Source of support: Nil

Conflict of interest: None

[14], while evidence gathered across one hundred and ten service enterprises found that almost sixty percent credited software robotics with maintaining continuity of business processes during a period of severe disruption [2]. Integrated frameworks that couple the risk and business process lifecycles, establishing a risk-aware culture across execution, demonstrate that these two concerns can share a single structural foundation [8]. The remainder of the article develops this position across ten connected themes: the intellectual foundations of risk-aware process management, the reference architecture that makes configuration possible, the digitized stages of identification, assessment, control, and monitoring, the market forces driving adoption, the challenges that automation itself introduces, and the directions in which the discipline is advancing.

Foundations of Risk-Aware Business Process Management

The integration of risk and process thinking did not appear suddenly. A sustained line of inquiry established that binding risk management to business process management yields the ability to minimize risks by design and to mitigate them at run time, while also exposing gaps in scope, goals, and tooling that early efforts left unresolved [9]. Subsequent contributions closed part of that gap by proposing an integrated process-risk method that couples the two lifecycles within a shared meta-model, giving practitioners a structured means to embed a risk-aware culture throughout execution rather than treating governance as a separate exercise [8]. In parallel, workflow-driven automation matured into a practical vehicle for executing rule-based tasks as software agents, extending the reach of process governance into day-to-day operations [3],[6].

Progress in the field was slowed for years by a shortage of solid conceptual foundations and dedicated tooling, which left risk-aware practice fragmented across incompatible notations and manual effort [8],[9]. The corrective has been to treat the risk lifecycle and the process lifecycle as a single coupled cycle, so that identification, assessment, treatment, and monitoring are modeled alongside the activities they govern rather than in a separate register [8]. Two complementary timing windows follow from this coupling. During design, exposures are surfaced and controls are specified before a process is ever executed; during operation, the same model supports detection and response as conditions unfold [9]. A configurable architecture is the practical means by which both windows are served from one definition, which is why the intellectual lineage and the engineering that follows are best read together.

These strands converge on a shared insight: risk is a property of processes, not a document filed alongside them. When controls are expressed as executable elements of a workflow, the traditional weakness of first-generation process tools, their inability to recommend the optimal combination of tasks, participants, and timing while reducing cost and risk,

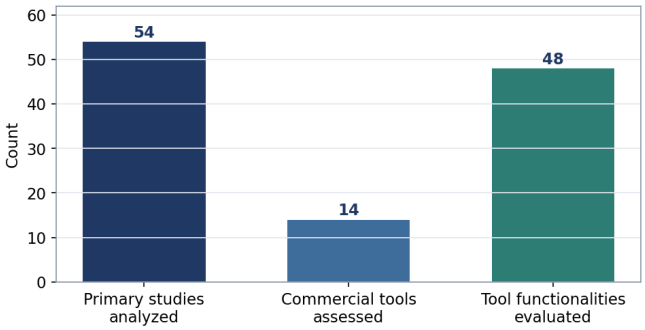

Figure 1: Scope of a systematic mapping of the field: primary studies analyzed, commercial tools assessed, and tool functionalities evaluated [7].

can be addressed through configuration and orchestration [5]. A systematic mapping of the field conveys how far it has matured, drawing on a substantial body of primary studies and evaluating a broad set of commercial tools against a detailed functionality framework [7].

Several threads in the surrounding literature sharpen the picture. The technology at the operational edge of these workflows is best understood as an umbrella term for tools that act on the user interface of other systems in the way a person would, which is what lets governance reach into applications that were never designed to expose their internals [10], [10],[14]. Because such tools are limited in scope on their own, the more mature discipline of business process management supplies the environment in which they thrive, and embedding the two together links their technologies and combines their methods within a single managed setting [11], [16]. Reviews of the field consistently distinguish this operational automation from the broader process discipline while cataloging its benefits and its uneven maturity, a distinction that matters for any enterprise seeking to place governance on a durable footing rather than a novelty [13], [15].

Configurable Workflow Architecture as the Structural Foundation

A configurable architecture rests on one principle: business logic is separated from application code and expressed as declarative definitions that administrators shape through visual tooling rather than programming. Workflow stages, decision gates, approval hierarchies, and escalation paths become adjustable parameters, letting an enterprise encode its particular risk appetite without commissioning bespoke software for every change. Contemporary automation platforms are commonly assembled from three elements: a deployable software component that executes the task, a design studio in which processes are mapped from reusable libraries, and a controller, often called an orchestrator, that governs the creation, review, approval, testing, and deployment of automated tasks while monitoring their performance [3]. This orchestration layer is precisely what a

Table 1: Foundational paradigms linking risk and process governance.

Paradigm or framework	*Core intent*	*Integration point*	*Ref.*
Risk-aware business process management	Unify the risk and process fields	Design time and run time	[9]
Integrated process-risk method	Couple risk and process lifecycles	Shared meta-model and lifecycle	[8]
Workflow-driven process automation	Execute rule-based tasks as software agents	Orchestrated task execution	[3],[6]
Automated controls in regulated domains	Cut cost and error in high-volume controls	Embedded control execution	[5]

digitized risk function needs, because it converts scattered manual steps into governed, observable flows.

Modularity reinforces adaptability. Each risk activity, from intake capture to scoring to audit checkpoint, is expressed as a reusable component, and common sub-processes can be assembled and reassembled across processes without destabilizing the whole [3]. Rule-driven orchestration then determines how items advance, who reviews them, and when controls activate, ensuring that severity and context, not rigid sequence, dictate handling. The architecture therefore behaves as a living framework whose conduct is defined by configuration and whose evolution demands no rewrite of the systems beneath it.

Three properties give this design its durability. Separation of concerns keeps the volatile part of a system, the rules of governance, apart from the stable part, the execution engine, so that each can change on its own schedule. Reusability lets a small library of validated components serve many processes, which shortens the path from a new obligation to a working control and narrows the surface over which errors can be introduced [3]. Observability, supplied by the controller, turns every configured step into a recorded, inspectable event, which is the precondition for both assurance and improvement. Together these properties explain why configurable execution has become a commodity capability rather than a bespoke build, although reaching the full potential of the more sophisticated components still calls for genuine engineering skill rather than casual assembly [3].

The placement of this execution layer is what distinguishes it from earlier automation. Rather than altering the internals of existing systems, the components act at the presentation layer, driving applications through the same interface a person would use, which keeps disruption to underlying systems low while still enforcing governed behavior [10]. Defining that behavior need not be heavyweight, since lightweight requirement practices, including test-driven definition and the recording of on-screen actions, let a control be specified, validated, and revised quickly [17]. When these definitions are expressed in a shared modeling and orchestration language, the configurable layer aligns cleanly with the wider process environment so that automation and management reinforce rather than fragment one another [11], [16].

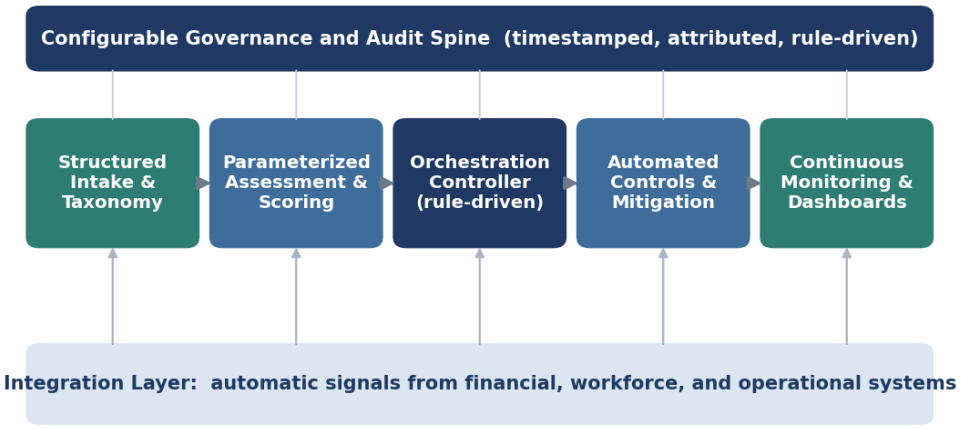

Figure 2: Reference architecture: a configurable pipeline bounded by a governance and audit spine above and an integration layer below.

Table 2: Elements of a configurable workflow architecture and their responsibilities [3].

Element	*Primary responsibility*
Executable component (software agent)	Performs the configured task steps against existing systems
Design studio	Maps processes from reusable, drag-and-drop libraries
Controller or orchestrator	Governs creation, review, approval, testing, and deployment; monitors performance
Reusable modules	Assemble intake, scoring, notification, and audit checkpoints across processes
Rule engine	Routes items by severity and context and activates controls conditionally

Digitizing Risk Identification and Assessment

Digitization begins where risk enters the enterprise. Structured intake channels replace ad hoc observation, capturing exposures from frontline staff, connected systems, and automated triggers into standardized records governed by consistent taxonomies. Standardization is a precondition rather than a convenience, because processes must be well defined and stable before they can be reliably automated, and eliminating non-value-added steps and superfluous decision points is itself part of preparing a process for digital execution [3]. Once captured, exposures are evaluated through configurable scoring models that weigh likelihood, impact, and velocity against organizational criteria; because these models are parameterized, thresholds can be recalibrated as conditions change without discarding historical records.

The transition is rarely frictionless, and the obstacles are well documented. At the organizational level, the inability to prioritize which processes deserve attention has been

Table 3: Dimensions captured by a digitized assessment record.

Dimension	What it captures
Likelihood	Probability that an exposure materializes
Impact	Magnitude of consequence across business domains
Velocity	Speed at which an exposure escalates once triggered
Taxonomy class	Standardized category enabling cross-unit comparison
Ownership and escalation	Accountable party and the path a raised item follows

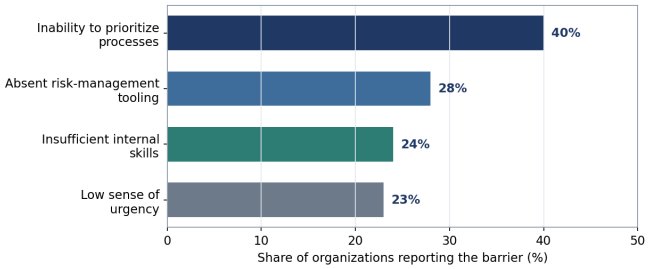

Figure 3: Organizational barriers to process digitization, by share of organizations reporting each [4].

identified as a barrier in roughly forty percent of cases, followed by the absence of dedicated risk-management tooling in about twenty-eight percent, insufficient internal skills in roughly twenty-four percent, and a simple lack of urgency in about twenty-three percent [4]. These figures explain why initiatives that begin without a disciplined selection and governance foundation frequently stall.

Embedding risk awareness directly into process models addresses the first of these barriers by making prioritization an explicit, modeled activity rather than an afterthought, which is the central promise of integrated process-risk frameworks that unify the two lifecycles [8]. The broader value of such integration is the capacity to minimize risk during modeling and to mitigate it dynamically during execution [9], so that assessment ceases to be a periodic snapshot and becomes a continuous property of the workflow itself.

The quality of what enters the system determines the quality of everything downstream. Because automated routines are unforgiving of malformed inputs, standardized capture and disciplined data hygiene are not clerical niceties but controls in their own right, and enterprises burdened with unstandardized or non-digitized processes have found that this deficiency is itself a leading barrier to adoption [2]. Once intake is trustworthy, dynamic questionnaires can adapt to the nature of each exposure, surfacing the factors that matter and suppressing those that do not, while a central repository aggregates individual records into a coherent picture of enterprise-wide exposure. That consolidated view is what allows scarce attention to be directed where vulnerability and consequence intersect most sharply, replacing fragmented judgment with a shared, evidence-grounded footing that every unit can see and trust.

Selecting the right candidates for automated control is itself a discipline. Reviews of practice stress that identifying suitable, stable, high-volume activities is decisive for success, since directing effort at ill-suited processes is a recurrent and costly error [13]. Documented cases show that when a well-chosen process is automated, handling time and error rates fall while throughput rises, which is precisely the profile a risk function seeks when it decides where to apply scarce control capacity [12]. Parameterized assessment supports this by letting the same scoring logic rank exposures consistently

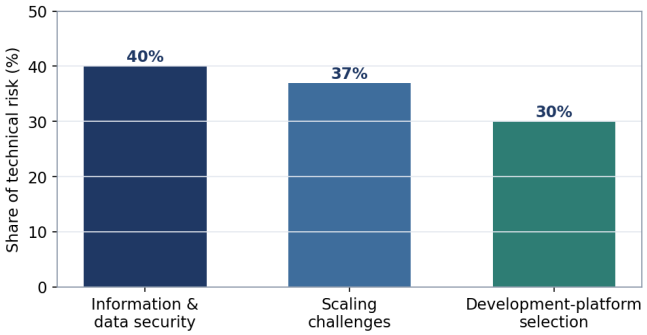

Figure 4: Distribution of technical risk factors in automated process controls [4].

across units, so that prioritization rests on comparable evidence rather than local habit.

Adaptive Controls, Governance, and Embedded Accountability

Once exposures are understood, a configurable architecture operationalizes response by expressing mitigation plans, treatment actions, and control tests as workflow objects with owners, deadlines, and verification steps. Automation advances these items, dispatches reminders, and escalates overdue obligations, and the run-time mitigation this enables is a defining advantage of integrating risk into the process fabric [9]. Yet automating controls introduces its own exposures that governance must anticipate. On the technical side, protecting information and data has been cited as the dominant concern, followed by challenges in scaling and difficulty selecting an appropriate development platform [4].

These distributions argue for governance that is embedded rather than bolted on. Every automated action is timestamped and attributed, producing a durable trail that supports internal oversight and external scrutiny, and a mature governance structure incorporates regular risk assessment of automated activity, restricted access, and continuous logging and tracking, as summarized in Table 4. Because software agents execute deterministically, any fault in input or logic propagates until corrected, which makes error handling and human supervision integral to control design rather than optional refinements [3]. Handled with discipline, this converts automation from a source of latent fragility into a mechanism for organizational resilience, provided that supervision and control keep pace with the reach of the automation itself.

Sound practice treats the security of automated actors as a first-order concern. Because these actors operate with real credentials and act on behalf of people, they raise distinct security and ethical exposures when they impersonate users or move sensitive data, and governance must confront these directly rather than assume them away [10]. The reported concentration of technical difficulty around protecting information and data reinforces the point, as does the weight placed on legal and regulatory constraints once automated

Table 4: Governance controls for automated risk workflows [3],[4],[10].

Control	*Function*
Regular risk assessment of automated activity	Periodic evaluation of agent behavior against policy
Restricted, least-privilege access	Limit what each automated actor can reach or change
Continuous logging and tracking	Maintain an immutable, attributable audit trail
Error handling and exception routing	Contain deterministic fault propagation
Human supervision	Resolve exceptions the rule set cannot

activity enters regulated operations [4]. Encoding safeguards as configurable elements of the workflow, including least-privilege access, verification steps, and mandatory logging, ensures they are applied uniformly and can be audited as readily as any other step, while the controller that governs testing and deployment offers a natural place to enforce them [3].

Integration, Scalability, and Continuous Monitoring

A digitized risk framework realizes its value only when connected to the wider environment, drawing signals automatically from financial, workforce, and operational systems so that emerging patterns surface earlier and manual entry recedes. Scalability follows from the same configurable foundation, since new units, jurisdictions, and risk categories are onboarded through configuration rather than custom development. The economic case is well attested; reported returns during the first year of automation deployments have ranged between roughly thirty and two hundred percent [3], and the labor leverage can be pronounced, with a single digital worker equated in one account to approximately four and a half full-time employees [3]. Beyond cost, the continuity dividend is tangible, as nearly sixty percent of surveyed enterprises reported that automation preserved their processes through acute disruption, with the most highly rated attributes clustering around perceived usefulness among the twenty-two features examined [2].

Continuous monitoring is where digitization most clearly departs from the periodic tradition. Dashboards and automated alerts track control effectiveness and shifting exposure in near real time, giving leadership visibility into the present state rather than a retrospective account. This vigilance is a safeguard rather than a convenience, because immature or poorly trained automated models can reduce productivity and increase errors through unsupported or incorrect decisions [5], and the contemporary literature

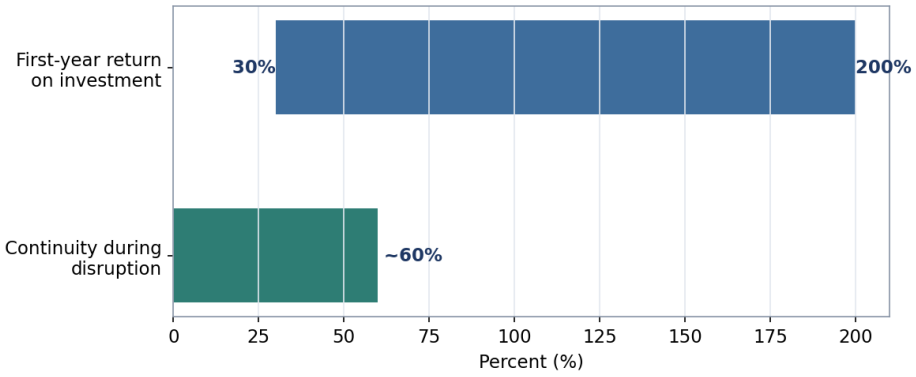

Figure 5: Reported value indicators of workflow automation: first-year return-on-investment range [3] and business-process continuity preserved during disruption [2].

repeatedly emphasizes that persistent challenges accompany the benefits of process automation [6]. Sustained monitoring, coupled with the reusability and rule-driven governance of a configurable architecture, keeps a digitized risk function accurate as the environment around it changes.

Two capabilities turn integration into insight. Process mining extracts the actual sequence of events from the logs that connected systems already produce, exposing where effort is wasted and where exposure concentrates, so that candidate processes for tighter control can be identified from evidence rather than intuition [3]. Continuous assurance then replaces the audit as a scheduled event with oversight as a standing condition, in which control effectiveness is evaluated as work happens rather than reconstructed afterward. Scalability compounds the benefit, because once a control is expressed as configuration it can be extended to a new unit, jurisdiction, or exposure category without a fresh build, preserving a single consistent standard as the enterprise grows. The combination of mined evidence, standing assurance, and configuration-driven scale is what allows a digitized risk function to remain both accurate and affordable as its remit widens.

Table 5: Market and adoption indicators for configurable process automation.

Indicator	*Reported value*	*Ref.*
Software-driven automation market	Approaching seven billion euros by 2020	[1]
Distinct supplier platforms	More than fifty	[3]
Software agents in operation	Approximately four million by 2021	[3]
Compound annual growth rate, 2017 to 2023	Near twenty-nine percent	[3]

Market Trajectory and Adoption Dynamics

The viability of embedding governance into configurable workflows depends on a mature and expanding technology base. Indicators drawn from the surrounding sources describe a field that has moved well beyond experimentation. The market for software-driven automation was projected to approach seven billion euros by 2020 [1], the population of software agents in operation was expected to reach roughly four million by 2021, and the field expanded at a compound annual rate near twenty-nine percent between 2017 and 2023 [3]. The supplier ecosystem is correspondingly broad, comprising more than fifty distinct platforms rather than a single dominant offering [3].

Breadth of supply matters for governance because it signals that configurable execution is a commodity capability rather than a proprietary experiment, allowing enterprises to select tooling that fits their control requirements and to migrate as needs change. Independent reviews of the field describe exactly this breadth, evaluating many commercial tools against a common functionality framework and noting that industrial results have concentrated in finance and outsourcing [7],[14]. Adoption, however, has concentrated on operational benefits such as releasing staff from repetitive tasks and strengthening efficiency, with strategic and external impacts often underweighted during decision-making [3]. A risk-centered agenda reframes that emphasis, treating governance strength as a first-class objective alongside cost reduction.

The way enterprises consume these capabilities also shapes their governance value. Suppliers promote the notion that business users without technical background can build automations directly, a democratizing idea that works well for simple, well-bounded tasks but that demands genuine engineering skill once processes grow sophisticated [3]. Operating models likewise vary, spanning attended components that assist a worker in real time and unattended components that run back-office tasks at scale from the controller [3]. Selection discipline, however, remains uneven,

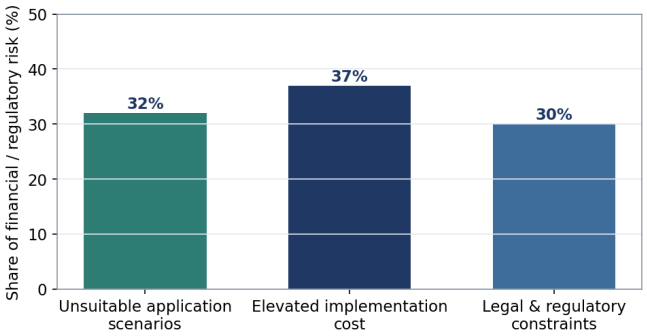

Figure 6: Financial and regulatory risk factors in automated deployments [4].

Table 6: Risk categories in automated deployments and representative concerns [3].

Category	*Representative concerns*
Executive	Over-dependence, loss of expertise, isolated goals
Technical	Integration, agent authorization, cybersecurity
Change management	Employee resistance, communication gaps, skills requirements
Operational	Data quality, scalability, poor documentation, knowledge loss

since only half of the enterprises examined in one account maintained a systematic process for identifying which activities were suitable for automation [3]. For a risk-centered agenda, closing that gap is decisive, because the benefit of a configurable control is realized only when it is applied to the exposures that matter most rather than to whichever process is easiest to reach.

Challenges, Barriers, and Mitigation

The same flexibility that makes configurable workflows powerful also widens the surface over which failure can occur. Beyond the technical concerns already noted, financial and regulatory factors weigh heavily on deployments. Unsuitable application scenarios, elevated implementation cost, and external legal and regulatory constraints each account for a meaningful share of reported financial and regulatory risk [4]. Systematic reviews that catalogue these obstacles group them into structural, technical, and financial-regulatory classes, a division that helps a governance function assign ownership rather than treat risk as undifferentiated [4],[13]. Left unmanaged, these factors turn a promising initiative into a stranded investment.

A structured view of risk categories helps convert these concerns into governable items. Reported deployments distribute risk across executive, technical, change-management, and operational categories, each carrying representative concerns that a governance framework can assign, monitor, and mitigate [3]. Mitigation follows directly from the architecture itself: disciplined process selection reduces unsuitable scenarios, embedded controls and least-privilege access contain technical exposure, transparent communication addresses change resistance, and continuous logging with human supervision limits operational drift [4],[3].

A subtler class of risk arrives with success. As reliance on automated execution deepens, enterprises grow dependent on components that are vulnerable to disturbances in the systems beneath them, and those that have automated extensively report that a change in an underlying application can halt a routine until it is retested and recoded [3]. Because the components act deterministically, a fault in input or logic is reproduced faithfully until a human intervenes, which means the option of reverting to manual handling must be preserved even as manual skill atrophies [3],[5]. Where agents act with real credentials, the security and ethical stakes of an unattended error rise accordingly, which is a further reason to bound their authority tightly [10]. Prudent governance therefore retains fallback capacity and rehearses it, treating the ability to operate without the automation as a control rather than an admission of weakness. Framed this way, the very dependence that automation creates becomes a managed exposure rather than a hidden one.

Future Directions

The trajectory of configurable risk workflows points toward greater cognitive capability and broader scope. Automation is expected to move beyond strictly rule-based execution toward handling unstructured inputs, enlarging the range of risk signals a workflow can absorb [6]. In parallel, the ambition is shifting from automating isolated steps toward orchestrating whole processes from end to end, which raises the importance of robust exception handling and design-time risk modeling [3],[8]. Governance itself is being reframed as a resilience mechanism, where deliberately supervised automation strengthens an enterprise's capacity to absorb disruption rather than merely reducing cost [7]. The direction of travel favors architectures that treat risk as a modeled, first-class concern at every stage of the lifecycle [9].

Realizing this direction will depend on progress along several fronts at once. Cognitive elements drawn from adjacent fields, including recognition of unstructured text and learning from prior decisions, are expected to extend automated handling beyond strictly rule-bound cases, enlarging the set of exposures a workflow can absorb [6]. As ambition grows from automating discrete steps toward orchestrating entire processes, the burden shifts onto robust exception handling and toward modeling risk at design time so that priorities are set before execution rather than after [3],[8]. The persistent tension between operational efficiency and strategic value will likely narrow as governance strength

Table 7: Emerging directions for configurable risk workflows.

Direction	*Expected shift*	*Ref.*
Cognitive augmentation	Handle unstructured inputs beyond rule-based logic	[6]
End-to-end orchestration	Move from isolated steps to whole-process automation	[3]
Strategic and integrated governance	Elevate governance strength alongside efficiency	[3],[11]
Design-time risk modeling	Prioritize exposures during modeling, not after	[8],[9]

is recognized and integrated as an objective in its own right rather than a byproduct of cost cutting [3],[11]. Open research questions around what should be automated and what should remain with people continue to frame the agenda [10], and classification frameworks emerging from systematic mapping give practitioners a vocabulary for positioning their own efforts [15]. What remains constant across these shifts is the premise that risk is best treated as a modeled, first-class concern woven through the workflow rather than appended to it [9].

Conclusion

Digitizing risk management through configurable enterprise workflow architecture reframes governance as an adaptive, continuous capability rather than a periodic obligation. Separating logic from code lets an enterprise model its distinctive risk posture and revise it as circumstances demand, uniting identification, assessment, control, and monitoring within a single executable fabric. The convergence of risk-aware process design with flexible orchestration closes the long-standing gap between where exposures are recorded and where decisions are taken, and it preserves accountability through durable, attributable trails that satisfy internal oversight and external scrutiny. Durable value depends less on any single tool than on disciplined process selection, embedded governance, and vigilant supervision of automated behavior, since flexibility without control merely relocates fragility from people to machines. As connected systems feed richer signals into the fabric, monitoring shifts from retrospective reporting toward anticipatory insight. Enterprises that build these qualities into their governance foundations position themselves to foresee threats, protect value, and sustain resilience across an operating environment defined by accelerating complexity and relentless change.

References

[1] J. Siderska, "Robotic Process Automation — a driver of digital transformation?" Engineering Management in Production and Services, vol. 12, no. 2, pp. 21–31, 2020. https://doi.org/10.2478/emj-2020-0009

[2] J. Siderska, "The Adoption of Robotic Process Automation Technology to Ensure Business Processes during the COVID-19 Pandemic," Sustainability, vol. 13, no. 14, art. 8020, 2021. https://doi.org/10.3390/su13148020

[3] D. Kedziora, A. Leivonen, W. Piotrowicz, and A. Öörni, "Robotic Process Automation (RPA) Implementation Drivers: Evidence of Selected Nordic Companies," Issues in Information Systems, vol. 22, no. 2, pp. 21–40, 2021. https://doi.org/10.48009/2_iis_2021_21-40

[4] D. Choi, H. R'bigui, and C. Cho, "Robotic Process Automation Implementation Challenges," in Proc. Int. Conf. on Smart Computing and Cyber Security (SMARTCYBER 2020), Lecture Notes in Networks and Systems, vol. 149, pp. 297–304, 2021. https://doi.org/10.1007/978-981-15-7990-5_29

[5] M. Romão, J. Costa, and C. J. Costa, "Robotic Process Automation: A Case Study in the Banking Industry," in Proc. 14th Iberian Conf. on Information Systems and Technologies (CISTI), 2019, pp. 1–6. https://doi.org/10.23919/CISTI.2019.8760733

[6] R. Syed et al., "Robotic Process Automation: Contemporary themes and challenges," Computers in Industry, vol. 115, art. 103162, 2020. https://doi.org/10.1016/j.compind.2019.103162

[7] J. G. Enríquez, A. Jiménez-Ramírez, F. J. Domínguez-Mayo, and J. A. García-García, "Robotic Process Automation: A Scientific and Industrial Systematic Mapping Study," IEEE Access, vol. 8, pp. 39113–39129, 2020. https://doi.org/10.1109/ACCESS.2020.2974934

[8] E. Lamine, R. Thabet, A. Sienou, D. Bork, F. Fontanili, and H. Pingaud, "BPRIM: An integrated framework for business process management and risk management," Computers in Industry, vol. 117, art. 103199, 2020. https://doi.org/10.1016/j.compind.2020.103199

[9] S. Suriadi et al., "Current Research in Risk-aware Business Process Management: Overview, Comparison, and Gap Analysis," Communications of the Association for Information Systems, vol. 34, art. 52, pp. 933–984, 2014. https://doi.org/10.17705/1CAIS.03452

[10] W. M. P. van der Aalst, M. Bichler, and A. Heinzl, "Robotic Process Automation," Business & Information Systems Engineering, vol. 60, no. 4, pp. 269–272, 2018. https://doi.org/10.1007/s12599-018-0542-4

[11] M. König, L. Bein, A. Nikaj, and M. Weske, "Integrating Robotic Process Automation into Business Process Management," in Business Process Management: Blockchain and RPA Forum (BPM 2020), Lecture Notes in Business Information Processing, vol. 393, pp. 132–146, 2020. https://doi.org/10.1007/978-3-030-58779-6_9

[12] S. Aguirre and A. Rodriguez, "Automation of a Business Process Using Robotic Process Automation (RPA): A Case Study," in Applied Computer Sciences in Engineering, Communications in Computer and Information Science, vol. 742, pp. 65–71, 2017. https://doi.org/10.1007/978-3-319-66963-2_7

[13] L. Ivančić, D. Suša Vugec, and V. Bosilj Vukšić, "Robotic Process Automation: Systematic Literature Review," in Business Process Management: Blockchain and CEE Forum (BPM 2019), Lecture Notes in Business Information Processing, vol. 361, pp. 280–295, 2019. https://doi.org/10.1007/978-3-030-30429-4_19

[14] P. Hofmann, C. Samp, and N. Urbach, "Robotic Process Automation," Electronic Markets, vol. 30, no. 1, pp. 99–106, 2020. https://doi.org/10.1007/s12525-019-00365-8

[15] J. Wewerka and M. Reichert, "Robotic Process Automation —

A Systematic Mapping Study and Classification Framework," Enterprise Information Systems, vol. 17, no. 2, art. 1986862, 2021. https://doi.org/10.1080/17517575.2021.1986862

[16] I. Stravinskiene and D. Serafinas, "Process Management and Robotic Process Automation: The Insights from Systematic Literature Review," Management of Organizations: Systematic Research, vol. 85, pp. 87–106, 2021. https://doi.org/10.1515/mosr-2021-0006

[17] C. Cewe, D. Koch, and R. Mertens, "Minimal Effort Requirements Engineering for Robotic Process Automation with Test Driven Development and Screen Recording," in Business Process Management Workshops (BPM 2017), Lecture Notes in Business Information Processing, vol. 308, pp. 642–648, 2018. https://doi.org/10.1007/978-3-319-74030-0_51