Enhancing Business Impact Analysis and Risk Assessment Applying a Risk-Aware Business Process Modelling and Simulation Methodology

Ilayda Tunc

EHL Hospitality Business School (Switzerland), Lausanne, CH

DOI: 10.37648/ijps.v21i01.006

[1]*Received: 28/01/2026; Accepted: 09/02/2026; Published: 23/02/2026*

Abstract

Business Impact Analysis (BIA) and risk assessment are both central to resilience planning, yet many organizations still perform them as separate exercises. That separation creates blind spots: BIA may identify critical processes without modeling how disruptions propagate through real process flows, while risk assessments may score threats without estimating operational and business consequences over time. Earlier work by Tjoa, Jakoubi, and Quirchmayr proposed bridging this gap through the ROPE (Risk-Oriented Process Evaluation) approach, and later work formalized risk-aware business process modeling and simulation for evaluating threats, safeguards, and recovery measures in a unified process view.

This paper presents a human-centered, applied research synthesis and methodology for enhancing BIA and risk assessment using risk-aware business process modeling and simulation. Building on the risk-aware BPM literature, multi-view modeling approaches, BPMN-based risk extensions, and recent integration efforts in crisis management and asset criticality analysis, the paper proposes a stepwise methodology that links process models, resource dependencies, threat scenarios, impact dimensions, and simulation outputs to decision-making.

The contribution is practical: a structured way to move from static risk registers and spreadsheet-style BIA templates toward dynamic, scenario-based analysis that better supports prioritization, recovery strategy design, and resilience investment decisions. The paper also outlines implementation challenges, governance requirements, and a realistic adoption roadmap for organizations that want stronger continuity planning without overengineering the effort.

Keywords: *business impact analysis; risk assessment; business process modeling; business process simulation; risk-aware BPM; resilience; business continuity; scenario analysis*

1. Introduction

Organizations today operate in environments where disruptions are no longer exceptional. Cyber incidents, supplier failures, IT outages, compliance issues, human error, and physical disruptions all affect operations, often in combinations rather than isolation. In practice, however, many firms still run BIA and risk assessment as parallel

---

[1]*How To Cite The Article:* Tunc I (February 2026); Enhancing Business Impact Analysis and Risk Assessment Applying a Risk-Aware Business Process Modelling and Simulation Methodology; *International Journal of Professional Studies*; Jan-Jun 2026, Vol 21, 70-77; DOI: http://doi.org/10.37648/ijps.v21i01.006

workstreams owned by different teams. The result is familiar: one team produces a list of "critical processes," another produces a list of "top risks," and leadership is left to reconcile both lists manually.

The original 2008 ARES paper on this topic argued that BIA and risk assessment can be significantly enhanced by applying a risk-aware business process modeling and simulation methodology (ROPE), specifically to improve identification of critical processes, single points of failure, impact of resource disruptions, and cost-benefit analysis of continuity strategies. That insight remains highly relevant. It addressed a structural problem that many organizations still face: discontinuity between process optimization thinking and continuity/risk thinking.

The later formalization of risk-aware business process modeling and simulation made this bridge stronger by introducing a model capable of representing relations among threats, detection mechanisms, safeguards, recovery measures, and their effects on business processes, including stochastic influences. This is important because business impact is not just a static property of a process. It emerges from dependencies, timing, workload, control effectiveness, and recovery behavior under stress.

Recent literature also supports the need for integration. A broad review of risk-aware business process management (R-BPM) found growth in approaches, but also heterogeneity in scope, functionality, and goals, with persistent research gaps. More recent work has pushed integration further through multi-view modeling tools, BPMN risk extensions, and combined BIA-risk frameworks in crisis management and asset-intensive industries.

This paper builds on that body of work and proposes a practical methodology for enhancing BIA and risk assessment using risk-aware business process modeling and simulation. The emphasis is on decision usefulness, not only modeling sophistication.

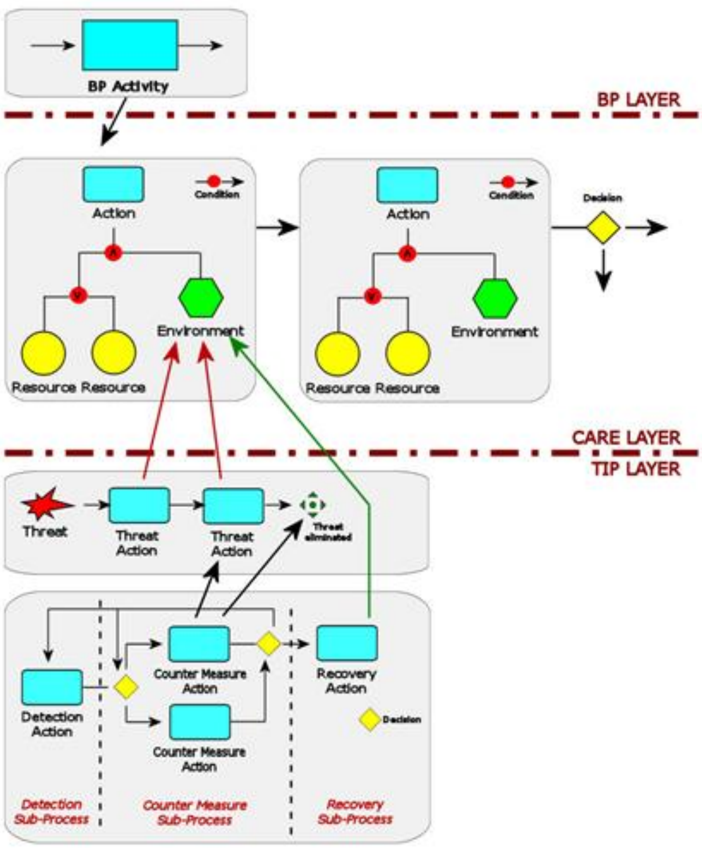

Figure 1. The three layers of ROPE

2. Background and Related Work

2.1 Why traditional BIA and risk assessment often underperform together

BIA usually asks: Which processes, services, and resources are critical, and what happens if they are disrupted for different durations? Risk assessment asks: What threats could occur, how likely are they, and what are their consequences? Both are necessary, but when performed independently, they often fail to capture process dynamics.

The 2011 formal approach by Tjoa et al. highlighted this problem directly, noting that business process modeling/simulation commonly focused on economic aspects, while security and continuity aspects were handled separately, leading to inconsistent improvement decisions (for example, around redundancy investments). In other words, the same decision can look "too expensive" from a process-efficiency lens and "essential" from a continuity lens if both are not modeled together.

2.2 Risk-aware BPM as an integration domain

Risk-aware BPM emerged as a response to this gap. Suriadi et al.'s review synthesized and classified approaches in the field and emphasized that research differed widely in scope and capabilities, while pointing to the need for stronger integration and clearer agendas. That review remains useful because it frames the field as multidisciplinary: process modeling, risk management, simulation, compliance, and runtime control all matter.

Subsequent work expanded implementation options:

- **Formal and simulation-oriented approaches** (e.g., Tjoa et al.) focused on explicit representation of threats and controls and stochastic simulation.
- **Modeling language and engineering approaches** (e.g., XML nets and later BPMN extensions) aimed to encode risk semantics directly in process models. Betz et al. proposed XML nets for risk-aware modeling/simulation, and Cardoso et al. later introduced **riskaBPMN**, a BPMN extension for quantitative risk assessment with likelihood and consequence information.
- **Integrated BPM-risk frameworks and tools** such as BPRIM and multi-view approaches advanced practical adoption by combining process and risk viewpoints in structured modeling environments.

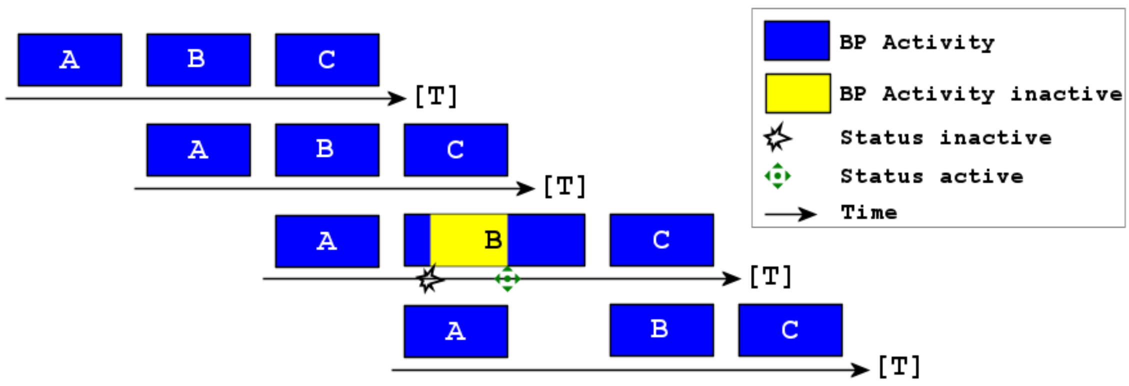

Figure 2. Risk-Aware Business Process Simulation

2.3 Evidence from recent integrated applications

The value of combining BIA and risk assessment is also visible outside “pure BPM” research. Hassel and Cedergren explicitly studied integration of risk assessment and business impact assessment in public crisis management, arguing for alignment between these traditionally separate assessments. Aghabegloo et al. proposed a framework that integrates BIA and risk assessment for physical asset criticality analysis in process industries, showing how BIA concepts can support prioritization decisions under resource constraints.

These studies reinforce a practical point: integration improves prioritization because it ties operational dependencies to business consequences, rather than treating risk scores as standalone outputs.

2.4 Process simulation as the missing operational layer

Foundational BPM literature treats process modeling and analysis as core to process improvement and operational management. What risk-aware simulation adds is the ability to test disruption scenarios and control strategies across time and dependencies. The original ROPE paper already emphasized simulation-supported identification of critical processes and single points of failure. The formal TSC paper further clarified the role of stochastic influences and safeguard effects.

This paper therefore treats simulation not as an optional visualization step, but as the operational engine that makes BIA and risk assessment mutually informative.

3. Research Objective and Contributions

Objective

To propose a practical methodology that enhances BIA and risk assessment by integrating them through risk-aware business process modeling and simulation.

Contributions

i. **A unified methodological flow** linking process models, dependencies, threats, controls, recovery actions, and BIA impact dimensions.
ii. **A simulation-centered decision layer** for comparing continuity strategies and control investments.
iii. **A human-centered implementation approach** that can be adopted incrementally by organizations with limited modeling maturity.
iv. **A governance framing** that aligns outputs with enterprise risk management practices and risk registers, consistent with enterprise-level risk integration guidance.

4. Proposed Risk-Aware Business Process Modeling and Simulation Methodology

The methodology is designed for organizations that already perform some version of BIA and risk assessment but want better decision quality.

Phase 1: Scope and resilience objective framing

Start with a bounded scope, not an enterprise-wide “model everything” effort. Select one value stream or service family (for example, order-to-cash, claims handling, patient intake, or payroll). Define:

- business services in scope
- recovery decision horizon (e.g., 24 hours, 72 hours, 7 days)
- stakeholders (operations, IT, risk, continuity, compliance, finance)
- key decision questions (e.g., “Which controls reduce downtime most?”)

This phase prevents a common failure mode: high-detail modelling without a real decision target.

Phase 2: Process and dependency modelling

Model the process at a level that is operationally meaningful. BPMN is practical for most organizations, and risk-aware extensions such as riskaBPMN show how likelihood and consequence information can be attached to process fragments.

At minimum, capture:

- activities and decision paths
- roles and staffing dependencies
- applications and infrastructure dependencies
- data dependencies
- third-party/supplier dependencies
- manual workarounds (if any)

This is where the original ROPE logic remains useful: business process activities often need further refinement to expose the actual resource and environmental dependencies that matter during disruption.

Phase 3: Threat, control, and recovery modelling

For each critical process fragment, define a threat-control-recovery structure. The Tjoa et al. formal approach is especially relevant here because it distinguishes relationships among threats, detection, safeguards, and recovery measures, and supports stochastic treatment of their effects.

A practical classification is:

- **Preventive controls** (reduce threat likelihood)
- **Detective controls** (reduce time to detection)
- **Blocking/containment controls** (limit propagation)
- **Recovery controls** (restore capability faster)
- **Compensating/manual controls** (maintain minimum service)

This classification helps teams stop treating all controls as equivalent. Two controls with similar implementation cost can have very different impacts on disruption duration and business loss.

Phase 4: BIA impact model design

Traditional BIAs often capture impact categories but not how they evolve over time or across process states. This methodology turns BIA fields into simulation variables.

Recommended impact dimensions:

- financial loss (direct and indirect)
- service degradation / throughput loss
- regulatory / contractual breach exposure
- customer impact / SLA breach
- safety impact (where relevant)
- reputational impact (proxy scoring)

- backlog accumulation and clearance time

Also define continuity thresholds such as:

- maximum tolerable disruption period (MTPD)
- minimum acceptable service level
- target recovery time (RTO-like decision targets, if used internally)

The point is not perfect precision. The point is transparent assumptions that can be improved after each exercise, incident, or test.

Phase 5: Scenario design and simulation execution

Create simulation scenarios that combine process behavior, disruptions, and controls. Early risk-aware BPM work emphasized simulation-based impact analysis and path-aware behavior under uncertainty.

At minimum, include:

1. **Baseline scenario** (normal operations)
2. **Single-point disruption scenarios** (e.g., application outage, key staff absence)
3. **Compound scenarios** (e.g., supplier delay + internal system degradation)
4. **Control alternative scenarios** (with and without selected safeguards/recovery options)

Use discrete-event or event-driven simulation logic with probabilistic inputs where data supports it. If historical data is weak, use ranges and sensitivity analysis instead of pretending certainty.

Phase 6: Decision analysis and prioritization

The simulation outputs should support decisions, not just generate charts. Useful outputs include:

- critical process fragments by expected disruption cost
- single points of failure and dependency concentration
- expected downtime and backlog distribution
- control portfolio comparison (cost vs impact reduction)
- recovery strategy comparison (time, staffing, service levels)
- threshold violations under different scenarios

This directly supports what the original 2008 paper highlighted: stronger cost-benefit analysis of business continuity strategies and better prioritization of threats.

To align with enterprise risk governance, summarize results into risk register entries and escalation thresholds at the enterprise level, consistent with NIST guidance on rolling up lower-level ICT risk information into enterprise risk profiles.

5. Discussion

5.1 Why this methodology improves both BIA and risk assessment

For BIA, it adds process dynamics, dependency visibility, and time-based impact behavior. BIA outputs become less static and more operationally grounded.

For risk assessment, it improves consequence modeling. Instead of broad severity labels, consequences are tied to process states, control behavior, and recovery timelines.

For continuity planning, it supports strategy comparison. This reflects the original promise of risk-aware BPM: integrating economic, risk, and contingency perspectives in one analytical frame.

5.2 Practical adoption barriers

Despite the value, organizations face predictable barriers:

- **Data quality limitations** (missing process times, weak incident data)
- **Model complexity creep** (too much detail too early)
- **Tool fragmentation** (BPM tools, GRC tools, BIA spreadsheets, incident systems)
- **Stakeholder ownership confusion** (who maintains the model?)
- **False precision risk** (overconfidence in uncertain probabilities)

The literature on risk-aware BPM repeatedly shows diversity in approaches and a lack of standardization across implementations, which is one reason adoption is uneven.

5.3 A realistic implementation roadmap

A practical rollout can happen in four steps:

i. **Pilot one critical process** with a limited scenario set.
ii. **Integrate existing BIA and risk data** rather than replacing current templates immediately.
iii. **Validate with one exercise or incident review** and refine assumptions.
iv. **Scale to a small portfolio of critical services** and connect outputs to enterprise risk reporting.

Recent integrated studies in public crisis management and industrial asset continuity suggest that even partial integration yields better prioritization decisions than separate assessments.

6. Conclusion

Enhancing BIA and risk assessment through risk-aware business process modelling and simulation is not just a modelling improvement. It is a decision-making improvement.

The core idea introduced in early ROPE-based work remains compelling: process-aware, simulation-supported analysis can reveal critical dependencies, quantify disruption effects more meaningfully, and improve continuity strategy choices. What has changed is the surrounding ecosystem. Today, organizations have stronger BPM tooling, more mature risk governance expectations, and growing evidence from integrated applications in crisis management and asset-intensive sectors.

The methodology proposed in this paper offers a practical path forward: start with one process, model dependencies that matter, encode threats and controls, simulate realistic scenarios, and use the outputs to improve BIA, risk assessment, and continuity investment decisions together. It is not a silver bullet, and it depends on disciplined assumptions and ongoing validation. But compared with separate, static assessments, it provides a far better basis for resilient operations in uncertain environments.

References

Aghabegloo, M., Rezaie, K., Torabi, S. A., & Yazdani, M. (2024). Integrating business impact analysis and risk assessment for physical asset criticality analysis: A framework for sustainable operations in process industries. *Expert Systems with Applications, 241*, Article 122737. https://doi.org/10.1016/j.eswa.2023.122737

Betz, S., Hickl, S., & Oberweis, A. (2011). Risk-aware business process modeling and simulation using XML nets. In *2011 IEEE 13th Conference on Commerce and Enterprise Computing (CEC)* (pp. 349–356). IEEE. https://doi.org/10.1109/CEC.2011.58

Cardoso, P., Respício, A., & Domingos, D. (2021). riskaBPMN - A BPMN extension for risk assessment. *Procedia Computer Science, 181*, 1247–1254. https://doi.org/10.1016/j.procs.2021.01.324

Dumas, M., La Rosa, M., Mendling, J., & Reijers, H. A. (2018). *Fundamentals of business process management* (2nd ed.). Springer. https://doi.org/10.1007/978-3-662-56509-4

Hassel, H., & Cedergren, A. (2021). Integrating risk assessment and business impact assessment in the public crisis management sector. *International Journal of Disaster Risk Reduction, 69*, Article 102136. https://doi.org/10.1016/j.ijdrr.2021.102136

Lamine, E., Thabet, R., Sienou, A., Bork, D., Fontanili, F., & Pingaud, H. (2020). BPRIM: An integrated framework for business process management and risk management. *Computers in Industry, 117*, Article 103199. https://doi.org/10.1016/j.compind.2020.103199

Quinn, S., Ivy, N., Barrett, M., Feldman, L., Topper, D., Witte, G., Scarfone, K., Gardner, R., & Chua, J. (2023). *Enterprise impact of information & communications technology risk* (NIST SP 800-221). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-221

Suriadi, S., Weiß, B., Winkelmann, A., ter Hofstede, A. H. M., Adams, M., Conforti, R., Fidge, C., La Rosa, M., Ouyang, C., Pika, A., Rosemann, M., & Wynn, M. (2014). Current research in risk-aware business process management—Overview, comparison, and gap analysis. *Communications of the Association for Information Systems, 34*(1), 1099–1139. https://doi.org/10.17705/1CAIS.03452

Thabet, R., Bork, D., Boufaied, A., Lamine, E., Korbaa, O., & Pingaud, H. (2021). Risk-aware business process management using multi-view modeling: Method and tool. *Requirements Engineering, 26*(3), 371–397. https://doi.org/10.1007/s00766-021-00348-2

Tjoa, S., Jakoubi, S., & Quirchmayr, G. (2008). Enhancing business impact analysis and risk assessment applying a risk-aware business process modeling and simulation methodology. In *2008 Third International Conference on Availability, Reliability and Security* (pp. 1041–1048). IEEE. https://doi.org/10.1109/ARES.2008.206

Tjoa, S., Jakoubi, S., Goluch, G., Kitzler, G., Goluch, S., & Quirchmayr, G. (2011). A formal approach enabling risk-aware business process modeling and simulation. *IEEE Transactions on Services Computing, 4*(2), 153–166. https://doi.org/10.1109/TSC.2010.17