2024 IEEE International Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation (IATMSI) | 979-8-3503-6052-3/24/$31.00 ©2024 IEEE | DOI: 10.1109/IATMSI60426.2024.10503443

Risk Management in Robotic Process Automation

Dileep Kumar Yendluri
Department of Computer Science
University of the Cumberlands
Williamsburg, USA
dkyendluri55@gmail.com

Ramya Thatikonda
Department of Information Technology
University of the Cumberlands
Williamsburg, USA
ramya.t0211@gmail.com

Reshmi Thatikonda
Department of Computer Information Systems
University of Central Missouri
Williamsburg, USA
reshmi.t03@gmail.com

Jainath Ponnala
Department of Electronics and Communication Engineering
Jawaharlal Technological University
Hyderbad, India
jainath.ponnala@gmail.com

M.Kempanna
Department of Artificial Intelligence and Machine Learning
Bangalore Institute of Technology
Bangalore, India
kempannam@bit-bangalore.edu.in

A.Bhuvanesh
Department of Electrical and Electronics Engineering
PSN College of Engineering and Technology
Tirunelveli, India
bhuvanesh.ananthan@gmail.com

***Abstract*—The paper investigates the nuances of RPA risk management, detailing the difficulties, tendencies, and approaches organizations must adopt to integrate RPA into their operations successfully. From automation to optimization, RPA's impact on industry workflow is revolutionary. However, RPA introduces a spectrum of technical, operational, business, and compliance risks alongside its benefits. Amidst the intricate landscape of RPA, this paper sheds light on key risks. It offers practical strategies for tackling them, enabling organizations to confidently unlock automation's transformative power. Trends like advanced analytics fusion, AI-driven risk analysis, and blockchain utilization will likely influence future RPA risk management. In addition, the paper discusses evolving challenges, including ethical issues, breakneck technology evolution, and digital security dangers. Using an in-depth examination of RPA risk management, this paper prepares organizations for the ever-changing automation environment with informed decisions and proactive measures.**

Keywords—Robotic Process Automation (RPA), risk management, automation, challenges, trends, mitigation strategies, governance, compliance, technical risks, operational risks, business risks, regulatory risks, future trends, AI-driven risk assessment, blockchain integration, cybersecurity threats, ethical considerations, change management.

I. Introduction

RPA integration has revolutionized multiple sectors by accelerating processes, increasing productivity, and decreasing errors. As RPA deployment accelerates, managing risks becomes an essential parallel pursuit. The intricate world of Risk Management in Robotic Process Automation is explored in this paper, showcasing the crucial part played by identifying, assessing, and alleviating potential risks to ensure a smooth and enduring RPA implementation.

Using software robots to automate routine processes, RPA (Robotic Process Automation) can revolutionize productivity and optimize human labor for more complex and creative work [1]. As RPA gains widespread acceptance, many potential risks must be closely examined. These risks span various technical, operational, and strategic elements. Organizations encounter various obstacles, such as technical glitches, insufficient scalability, data leaks, and workplace disruptions, to name a few.

RPA's crucial reliance on risk management techniques underscores the need for proactive risk mitigation measures [1]. Although rare, technical malfunctions can swiftly shut down crucial operations, undermine customer faith, and incur substantial financial burdens. Operational and business risks can threaten the achievement of strategic goals and the promised benefits. By delving into the subtleties of RPA risks, this paper seeks to demonstrate how astute risk management strategies can mitigate potential drawbacks and exploit the advantages of RPA.

This analysis seeks to provide a thorough blueprint for enterprises undertaking RPA initiatives by exploring relevant risk assessment frameworks, mitigation strategies, organizational architectures, and real-world cases. With technological enhancements revolutionizing industry panoramas, this paper's insights are poised to educate professionals, legislators, and scientists on developing a thorough methodology for RPA risk management. In conclusion, incorporating risk management into RPA implementation is essential to ensure long-term success.

II. Fundamentals of RPA

RPA stands at the forefront of innovation, revolutionizing traditional methods and improving efficiency across various sectors. Using software "bots," RPA automates repetitive processes by mimicking human interactions with digital platforms [1]. By combining cutting-edge technologies like AI, ML, and automation, RPA streamlines workflows, boosts operational effectiveness, and minimizes manual mistakes.

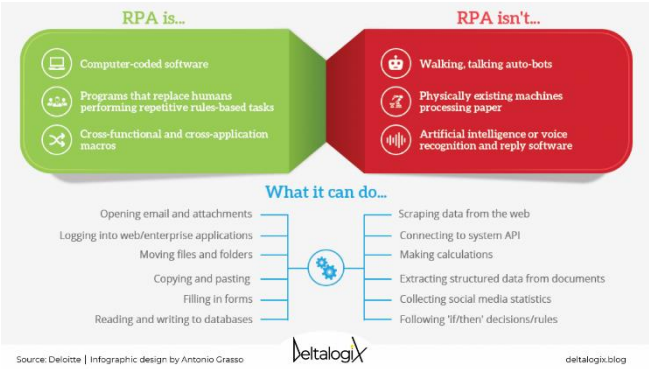

Fig. 1. Robotic Process Automation

(Source: https://deltalogix.blog/en/2021/03/24/robotic-process-automation-what-is-it-and-what-is-it-not/)

RPA offers comprehensive benefits, touching upon various aspects of business operations. Automating uninteresting yet time-intensive tasks, RPA optimizes human productivity [1]. Freeing up human resources allows them to emphasize creativity, strategy, and highly skilled decision-making. Consistency and accuracy in RPA implementation

Authorized licensed use limited to: Sacred Heart University. Downloaded on April 23,2025 at 01:09:01 UTC from IEEE Xplore. Restrictions apply.

greatly reduce errors. One instance where manual data entry is prone to mistakes is when errors occur due to human intervention, leading to financial disparities or regulatory non-compliance [2]. Conversely, RPA's narrow mistake threshold greatly enhances data accuracy and process integrity.

Moreover, RPA's capability to scale up is noteworthy. Virtual bots give businesses an ideal solution when work volumes skyrocket by rapidly increasing capacity without jeopardizing performance or quality [2]. Scalability significantly enhances operational agility, an indispensable trait in today's fast-moving business environment. Significant financial savings are commonly seen as a result of RPA implementation. Streamlined operations, fewer mistakes, and smarter resource management translate into bottom-line benefits for businesses.

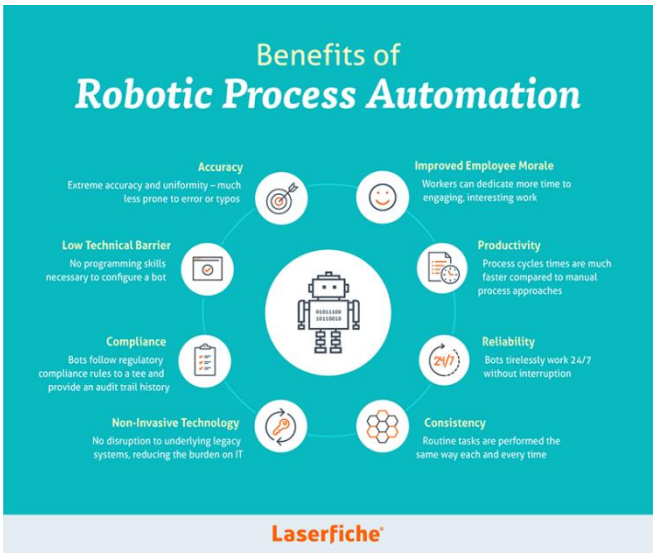

Fig. 2. Benefits of RPA

(Source: https://www.scielo.br/j/jistm/a/m7cqFWJPsWSk8ZnWRN6fR5m/?lang=en)

Abundant case examples witness RPA's positive influence. From finance to healthcare, industries have experienced notable benefits thanks to RPA, including higher productivity, improved customer interactions, and rigorous adherence to regulations [2]. RPA's innovative technology integration paves the way for unparalleled efficiency, precision, and agility in process optimization. Through streamlining mundane tasks, RPA unleashes Human Potential toward more Strategic Ventures, resulting in cost savings and Process Enhancements. More than just efficiency gains, this transformation leads to a groundbreaking evolution in how organizations run and innovate.

III. Types of Risk in RPA

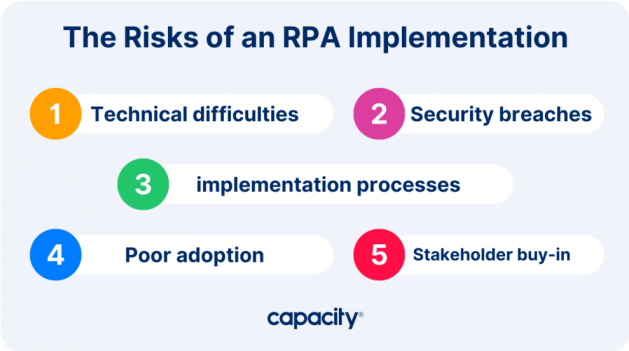

Fig. 3. Risks in RPA

Source:(https://capacity.com/learn/intelligent-automation/rpa-implementation/)

A. *Technical Risks*

With RPA, companies can automate repetitive procedures, unlocking the potential for their workforce to pursue more productive endeavors. Nevertheless, some technical hurdles persist in the landscape of RPA applications, posing significant challenges [3]. Many factors can compromise the functionality, stability, and security of RPA tools.

Software Failures and Bugs: Software defects and bugs pose a substantial technical risk in RPA, ranking highly. RPA software, composed of complex algorithms and scripts, is designed to automate tasks. Moments of carelessness during script creation can cause unwanted behavior or crashes unless rigorous testing occurs. These incompatibilities can lead to unforeseen errors, making the RPA implementation counterproductive or dangerous [3]. Comprehensive testing and quality assurance procedures are essential to mitigate the risk of software faults when utilizing RPA solutions.

Data Security Vulnerabilities: Data security is paramount in every technological implementation, and RPA is no exception. Through interaction with delicate data, RPA systems carry an inherent risk of security breaches if implemented insecurely. Malevolent actors might leverage RPA script flaws, compromising confidentiality and integrity [3]. Safeguarding against threats requires the integration of encryption, access controls, and frequent security assessments.

Lack of Scalability: Scalability obstacles are possible when RPA is used to automatize operations. A robust RPA system will be stretched thin if it can only handle a few processes well. The absence of scaling capacity often brings about speed bumps, hold-ups, or failures during peak hours. It is essential to include load balancing and optimized resource management to maintain peak performance as RPA grows.

Integration Challenges: These systems must integrate flawlessly with an organization's existing applications and IT infrastructure. Data format disparities, communication protocol conflicts, and authentication hurdles can arise during integration [3]. Compromising the anticipated efficiency boost, incomplete or incompatible integrations can obstruct the seamless transfer of information. Organizations may overcome this risk by investing in diligent integration planning, thorough API assessments, and precise communication strategies.

Authorized licensed use limited to: Sacred Heart University. Downloaded on April 23,2025 at 01:09:01 UTC from IEEE Xplore. Restrictions apply.

Reliability and Uptime: Robotic Process Automation (RPA) is frequently leveraged by organizations to execute important business operations reliably. If RPA systems fail to function reliably, this can hinder operations and cause economic losses [3]. Issues emanating from network outages, hardware malfunctions, or upgrade/maintenance activities can compromise the reliability and availability of RPA solutions. Combining redundancy and failover solutions with robust backup plans, we can guarantee the continued uptime of RPA systems.

Change Management: With the introduction of RPA, established procedures and workflows may see modifications. A lack of change management can give rise to employee apprehension regarding RPA, fearing it will replace their roles [3]. When introducing RPA, teaching workers about its advantages, modifying processes to accommodate new approaches, and involving appropriate individuals in the stages of design, introduction, and execution help circumnavigate the difficulty of resistance to change caused by bot adoption.

Maintenance and Updates: Regular upkeep and modifications are necessary to maintain the effectiveness and longevity of RPA technology. Unless tested extensively, newly implemented changes can carry hidden dangers. Upgrades that go against how things are done currently or cause issues can interfere with activities [3]. Change management protocols, thorough testing, and clear update procedures are crucial to reducing these risks.

Lack of Expertise: Technical skills are imperative when designing and maintaining RPA solutions. The possibility of a shortage of skilled professionals to create, deploy, and solve RPA systems looms large [3]. Project timelines may be delayed without resources, and results may not meet expectations. Ensuring the availability of necessary expertise requires investing in employee training and partnering with experienced service providers.

B. *Operational Risks*

Given RPA's surge, a thorough appreciation of the magnitude of the operational risks is essential. RPA's array of advantages is counterbalanced by the complexity it brings to operations. Process Disruption: Automation via RPA may lead to unintended consequences without careful planning and execution. RPA's accuracy, lacking human intuition, can be compromised in complex exceptions and varied tasks, causing errors or inconsistencies [4]. Complex decision-making processes and situations that necessitate human judgment may suffer disruptions. Integrating seamlessly into existing workflows and minimizing the risk of disruption are achieved through systematic process analysis, stakeholder engagement, and ongoing monitoring.

Fig. 4. Reasons for RPA fail

Source: (https://www.xenonstack.com/blog/rpa-projects-fail)

Lack of Scalability: Scalability oversights hinder smooth execution during RPA implementation. Under pressure from an expanding organization and demand for automation, RPA solutions that fail to scale may experience decreased effectiveness and output [4]. By dynamically allocating resources and adjusting to shifting demands, the scalable architecture safeguards against potentially dire consequences related to operational risks.

Inadequate Governance and Oversight: Governance and oversight lapses contribute to poor RPA implementation. Inadequate role definitions, duties, and oversight can open project implementation to irregularities, mistakes, and straying from ideal methods [4]. For effective governance of RPA projects, clear communication channels, standardized processes, and regular reporting must be in place.

C. *Business Risks*

Aligned with promises of enhanced productivity and lower expenses, RPA presents an array of enterprise risks that demand adept handling. The implementation of RPA may well have far-reaching effects on an organization's day-to-day activities, market plans, and employee base.

Lack of Proper Process Assessment: Ignoring a pre-automation process evaluation may result in inheriting difficult-to-solve issues. Organizations without a good understanding of existing workflows risk automating inherently suboptimal workflows [5]. By streamlining ineffective tasks, organizations can attain remarkable efficiencies and marginal improvements. Organizations can minimize risks by prioritizing process analysis and optimization before RPA implementation.

Unrealistic Expectations: Setting unattainable expectations can result in disillusionment and disappointment if RPA does not deliver as expected. Organizations often hope for immediate and substantial cost savings, heightened productivity, or flawless integration, only to encounter obstacles that hinder fulfilling these goals [5]. We can manage expectations and preclude disappointment through unrestricted communication, actionable goals, and knowledge sharing toward RPA's subtle influence.

Impact on Employee Morale and Job Displacement: While automating mundane tasks through RPA can liberate staff for more thoughtful responsibilities, job loss fears cannot be overlooked. Job losses could cause decreased employee morale and reluctance during RPA implementation [5]. By reskilling, upskilling, and effectively communicating the value of RPA, organizations can proactively address these challenges and facilitate a more seamless integration.

Alignment with Business Strategy: Essential to realize substantial benefits, RPA efforts require alignment with the organization's strategic objectives. If RPA is not properly aligned, it can lead to haphazard initiatives lacking cohesion with vital corporate goals [5]. By evaluating the alignment of RPA with their overall strategy, organizations can identify key processes that help achieve sustainable growth.

Vendor Lock-In and Scalability: Fostering a collaboration with RPA providers can lead to an overreliance on a particular vendor's resources. Limited flexibility can hinder addressing

Authorized licensed use limited to: Sacred Heart University. Downloaded on April 23,2025 at 01:09:01 UTC from IEEE Xplore. Restrictions apply.

future requirements or altering course to better solutions. Moreover, some vendors may not adequately prepare themselves to accommodate growing RPA needs [5]. Organizations must conduct rigorous vendor contract assessments, prioritize scalable solutions, and ensure seamless interoperability with other technologies to minimize associated risks.

Integration Complexity: Bridging technological systems with RPA may generate integration issues. Integration gaps between RPA solutions and existing systems can create isolated automation areas, hindering process efficiency and comprehensive automation [5]. Essential to ensuring a seamless technological environment are tactics for efficient integration, such as API utilization and a thorough comprehension of data flows.

Regulatory and Compliance Issues: To conform with regulatory standards, organizations in carefully governed sectors must ensure that their RPA deployments comply. Unpreparedness for regulatory alterations can invite legal and financial penalties [5]. Automatons must adhere to regulatory norms and guidelines set by their respective industries by ensuring compliance through comprehensive examinations.

Return on Investment (ROI) Uncertainty: Significant investment in RPA is required, encompassing expenses for technology, training, change management, and long-term maintenance. Calculating and forecasting ROI's accuracy is often elusive, given the diverse factors affecting its outcome. Organizations can get a clearer picture of the potential return on investment by evaluating the concrete and abstract advantages [5].

IV. Risk Assessment in RPA

RPA's impact on driving organizational productivity and innovation cannot be overstated. While RPA integration carries valuable opportunities, it also introduces various potential risks that need to be deliberately examined, evaluated, and managed to guarantee successful implementation and sustained advantages in the long run. Forming the foundation of successful RPA management, risk assessments facilitate a systematic comprehension of automation's intricacies.

A. Understanding Risk Assessment in RPA

Identifying, examining, and categorizing possible hazards that may hinder the achievement of an RPA endeavor is part of the thorough risk evaluation process. Taking a proactive approach allows potential issues to be averted through strategic planning and early intervention [6]. This project sheds light on the hidden dangers, shortcomings, and ambiguities inherent in RPA, empowering organizations to make educated choices, allocate resources prudently, and establish comprehensive risk management plans.

B. Fundamental Parts of RPA Risk Assessment

Identifying Potential Risks: RPA risk identification comes before any other implementation consideration. These risks have significant impacts covering various aspects such as software glitches, operational disruptions, security threats, limited scalability, etc. Comprehensive risk identification is conducted by involving stakeholders, analyzing processes, and drawing upon past RPA implementations' insight [6].

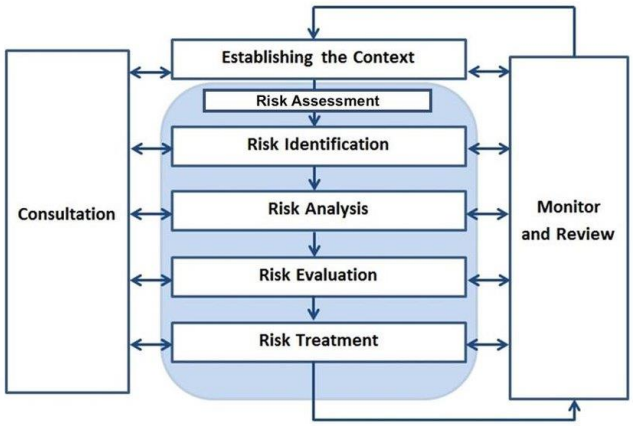

Fig. 5. RPA risk identification

Source: (https://www.researchgate.net/figure/Risk-management-process-ISO-310002009-Reprinted-from-Risk-Management-by-Sivan-R_fig2_328724337)

Assessing Impact and Likelihood: The next step is to evaluate the likely effects and likelihood of the risks after they have been identified. Calculating potential damages means understanding the likelihood of occurrence and its impact on finances, operations, and reputation. Based on historical data, expert opinion, and company-specific circumstances, likelihood assessment calculates the risk occurrence probability.

Prioritizing Risks: Risk levels shift, so some impact more than others. Assessments of impact and likelihood determine the priorities for risks, making them paramount [6]. Organizations can optimize resource allocation to address critical risk management by initially tackling the most pressing threats. Both qualitative and quantitative strategies exist for prioritization, with methods like risk matrices and numerical valuations.

Developing Risk Mitigation Strategies: Strategic plans should be designed to handle identified risks following prioritization. Mitigation strategies tailored to the specific risk can minimize likelihood and impact. Preventive, detective, and corrective strategies can help manage risks effectively.

Monitoring and Continuous Improvement: Risk assessment is a continuous cycle instead of a single event. With each step forward in the RPA initiative, there lies the requirement for continuous monitoring and tweaking [6]. Additional risks could arise as time passes, and existing mitigation methods must be assessed for continued efficacy. Updates to the risk assessment foster the organization's resilience to changing circumstances.

C. Risk Assessment Methodologies for RPA

Various approaches are offered to aid organizations in performing comprehensive risk evaluations for RPA efforts. NIST Risk Management Framework: NIST, a well-established authority in information security, offers a comprehensive framework for addressing risks [7]. An informed risk management plan can be devised by aligning risk assessments with business goals and thresholds. ISO 31000: The preferred global standard for risk management, ISO 31000 boasts widespread acceptance [7]. This method encompasses risk assessment with a specific approach to identification, evaluation, treatment, monitoring, and

Authorized licensed use limited to: Sacred Heart University. Downloaded on April 23,2025 at 01:09:01 UTC from IEEE Xplore. Restrictions apply.

dissemination throughout the organization. COSO ERM Framework: By utilizing COSO's ERM framework, organizations may holistically manage risks related to RPA implementation.

D. *Strategies for Effective Risk Assessment in RPA*

Collaboration: Integrating perspectives from different disciplines through the collaboration of stakeholders from IT, operations, compliance, and finance fosters a complete comprehension of potential risks [7]. By pooling their insights, departments contribute to collective awareness and heighten the likelihood of risk detection.

Process Mapping: Elucidating how processes interact, detailed process mapping reveals areas where automation can improve related functions efficiently. The mapping sheds light on how risks in one sphere might affect the entire network.

Documentation: Documentation must be kept up-to-date and extensive throughout the risk assessment. This documentation includes identified risks, their evaluation, ranking, prevention techniques, and supporting reasoning [7]. Transparency, accountability, and personal and professional development opportunities are attainable through documentation.

Continuous Learning: As risk evaluation is essential, a culture of ongoing learning and improvement should be adopted by organizations [7]. Assessing the efficacy of risk management techniques, learning from triumphs and setbacks, and adjusting methods in response to shifting circumstances enhances risk management's overall impact.

E. *Mitigation Strategies for RPA Risks*

RPA harbors transformative potential, but along with it are various risks that businesses need to tackle promptly. It is crucial to deploy effective strategies to alleviate the potential drawbacks and guarantee RPA's smooth execution.

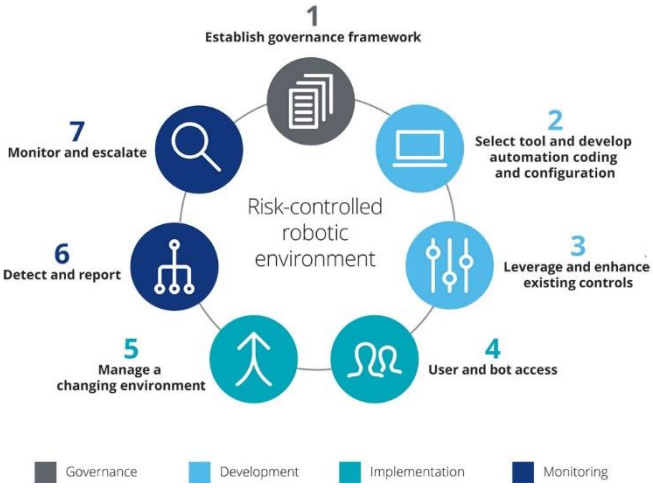

Fig. 6. RPA risks and controls

Source: (https://www2.deloitte.com/us/en/pages/audit/articles/financial-reporting-rpa-risks-and-controls.html)

F. *Technical Risk Mitigation*

Rigorous Testing and Quality Assurance: Identification and correction of software issues demand systematic testing. Thorough testing demands unit, integration and end-to-end testing procedures. Quality assurance practices should encompass the RPA software and its interactions with other systems to ensure a seamless and dependable automation ecosystem [8]. Continuous Monitoring and Updates: Organizations can tackle security concerns and incompatibilities head-on by establishing continuous monitoring systems. Consistent upkeep safeguards software components, security patches, and RPA scripts against obsolescence. Encryption and Data Protection Measures: Encryption comes to the fore when protecting RPA data during transmission and storage. Safeguarding sensitive information through robust encryption methods and secure storage infrastructures offers peace of mind, knowing that unauthorized access is minimized.

G. *Operational Risk Mitigation*

Change Management and Stakeholder Engagement: Organizations can mitigate potential disruptions during changes by incorporating all parties involved. Transparency, education, and employee integration during the shift toward automation guarantee a more tranquil migration. Scalability Planning: While developing RPA solutions, companies must prepare for forthcoming workload expansions [8]. Scalable architectures that can handle expanding process scope are crucial to maintaining efficient automation. Clear Roles and Responsibilities: Establishing clear roles and responsibilities regarding RPA process management is vital. A clear hierarchy of ownership and responsibility speeds up problem-solving and reduces risks of productivity bottlenecks.

H. *Business Risk Mitigation*

Thorough Process Analysis: Automation's hazards can be lessened by systematically examining and optimizing existing processes. Presolving process constraints before automation helps ensure that RPA truly improves processes [8]. Realistic Expectation Setting: Proper communication is vital since it helps to set realistic expectations regarding RPA's advantages and limitations. Setting attainable goals for RPA effectiveness allows organizations to harness the complementary skills of humans and technology. Employee Upskilling and Training: Organizations can fend off worries regarding job replacement by prioritizing employee training and growth. Arming employees with the skills to work with RPA systems minimizes opposition and amplifies organizational capabilities.

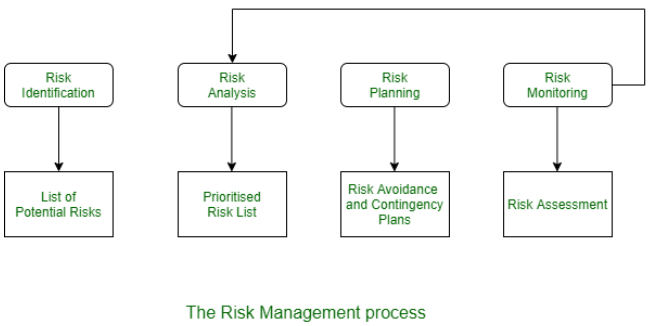

Fig. 7. Risk management process

Source: (https://www.geeksforgeeks.org/risk-mitigation-monitoring-and-management-rmmm-plan/)

I. *Vendor and Technology Risk Mitigation*

Diversification of Vendor Relationships: By diversifying your RPA partnerships, you can defy vendor lock-in's grasp. Diversification unlocks the versatility to accommodate evolving vendor ecosystems [8]. Interoperability Assessment: It is crucial to determine whether a technology will work

Authorized licensed use limited to: Sacred Heart University. Downloaded on April 23,2025 at 01:09:01 UTC from IEEE Xplore. Restrictions apply.

seamlessly with existing systems before adopting it. Innovative solutions and a focus on integration simplify future challenges, guaranteeing success.

J. *Regulatory and Compliance Risk Mitigation*

Regular Compliance Audits: Compliance depends on frequent audits of automated processes, which align with industry standards. Keeping track of regulatory updates, we modify our automated processes [8]. Robust Documentation: Complete documentation of automated processes and data management facilitates compliance proof and reduces legal risks. Inquiry transparency and accountability rely on the documentation's ability to verify.

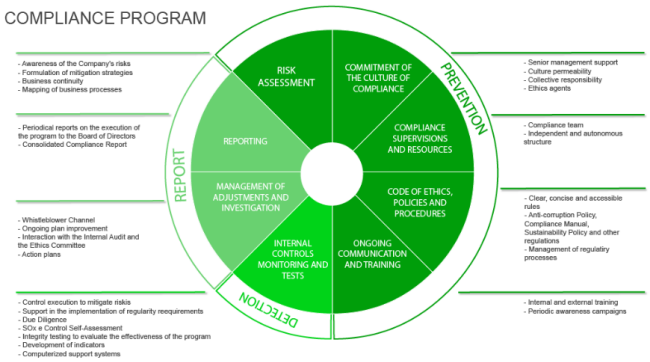

Fig. 8. Compliance Program

Source: (https://ri.oi.com.br/en/corporate-governance/compliance/)

K. *Mitigation Monitoring and Improvement*

Regular Risk Assessments: Regular risk assessments must address emerging challenges and shifts in RPA terrain. Regular assessments enable organizations to improve risk management strategies by adapting to evolving threats [8]. Continuous Learning: Creating a lifelong learning and development culture is crucial in risk mitigation. Integrating lessons from successes and failures into the risk management approach via consistent review boosts its effectiveness.

V. Conclusion and Future Scope

The dynamic duo of advanced analytics and AI-driven risk assessments fuels the future scope of RPA risk management's transformative potential. Organizations adopting a holistic risk management stance may integrate RPA into broader ERM frameworks, possibly blockchain integration, promising increased data safety and regulatory compliance audits. With these encouraging tendencies, businesses must skillfully navigate significant obstacles. Ethical concerns surrounding job displacement, data privacy, regulatory compliance, technological advancements, vendor risks, integration complexities, and cybersecurity threats will significantly influence the future of RPA risk management. Organizations can ensure long-term success and sustainability by adopting a proactive approach to navigating the complex terrain of RPA risk management..

References

[1] S. Moreira, H. S. Mamede, and A. Santos, "Process automation using RPA – a literature review," *Procedia Computer Science*, vol. 219, pp. 244–254, Jan. 2023, doi: https://doi.org/10.1016/j.procs.2023.01.287

[2] D. A. da S. Costa, H. S. Mamede, and M. Mira da Silva, "Robotic Process Automation (RPA) Adoption: A Systematic Literature Review," *Engineering Management in Production and Services*, vol. 14, no. 2, pp. 1–12, Jun. 2022, doi: https://doi.org/10.2478/emj-2022-0012.

[3] C. Lamberton, D. Brigo, and D. Hoy, "Impact of Robotics, RPA, and AI on the Insurance Industry: Challenges and Opportunities," *papers.ssrn.com*, Nov. 29, 2017. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3079495

[4] R. Syed et al., "Robotic Process Automation: Contemporary themes and challenges," *Computers in Industry*, vol. 115, no. 1, p. 103162, Feb. 2020, doi: https://doi.org/10.1016/j.compind.2019.103162.

[5] A.-M. Zaharia-Rădulescu, C. Liviu, D. Shuleski, and A. Cristian Ioan, "The Role of Management in the Economic Paradigm of the XXI st Century" *Proceedings of the 11th International Management Conference and the Future of Workforce*," 2017. Available: http://conferinta.management.ase.ro/archives/2017/pdf/2_16.pdf

[6] L. A. Zarooni and M. E. Khatib, "Robotics Process Automation (RPA) and Project Risk Management," *International Journal of Business Analytics and Security (IJBAS)*, vol. 3, no. 1, pp. 75–91, May 2023, doi: https://doi.org/10.54489/ijbas.v3i1.198.

[7] M. Stamatović, S. Maksimović, and A. Sućeska, "Risk Management as a Part of the Internal System of Financial Controls – Practice in the Public Sector of Serbia," *EMC Review* - Časopis za ekonomiju - APEIRON, vol. 20, no. 2, Sep. 2020, doi: https://doi.org/10.7251/emc2002431s.

[8] O. Y. A. Wijaya, "Risk Management Mitigation in the New Normal Era," *Budapest International Research and Critics Institute (BIRCI-Journal): Humanities and Social Sciences*, vol. 4, no. 1, pp. 1088–1097, Feb. 2021, doi: https://doi.org/10.33258/birci.v4i1.1716.

Authorized licensed use limited to: Sacred Heart University. Downloaded on April 23,2025 at 01:09:01 UTC from IEEE Xplore. Restrictions apply.