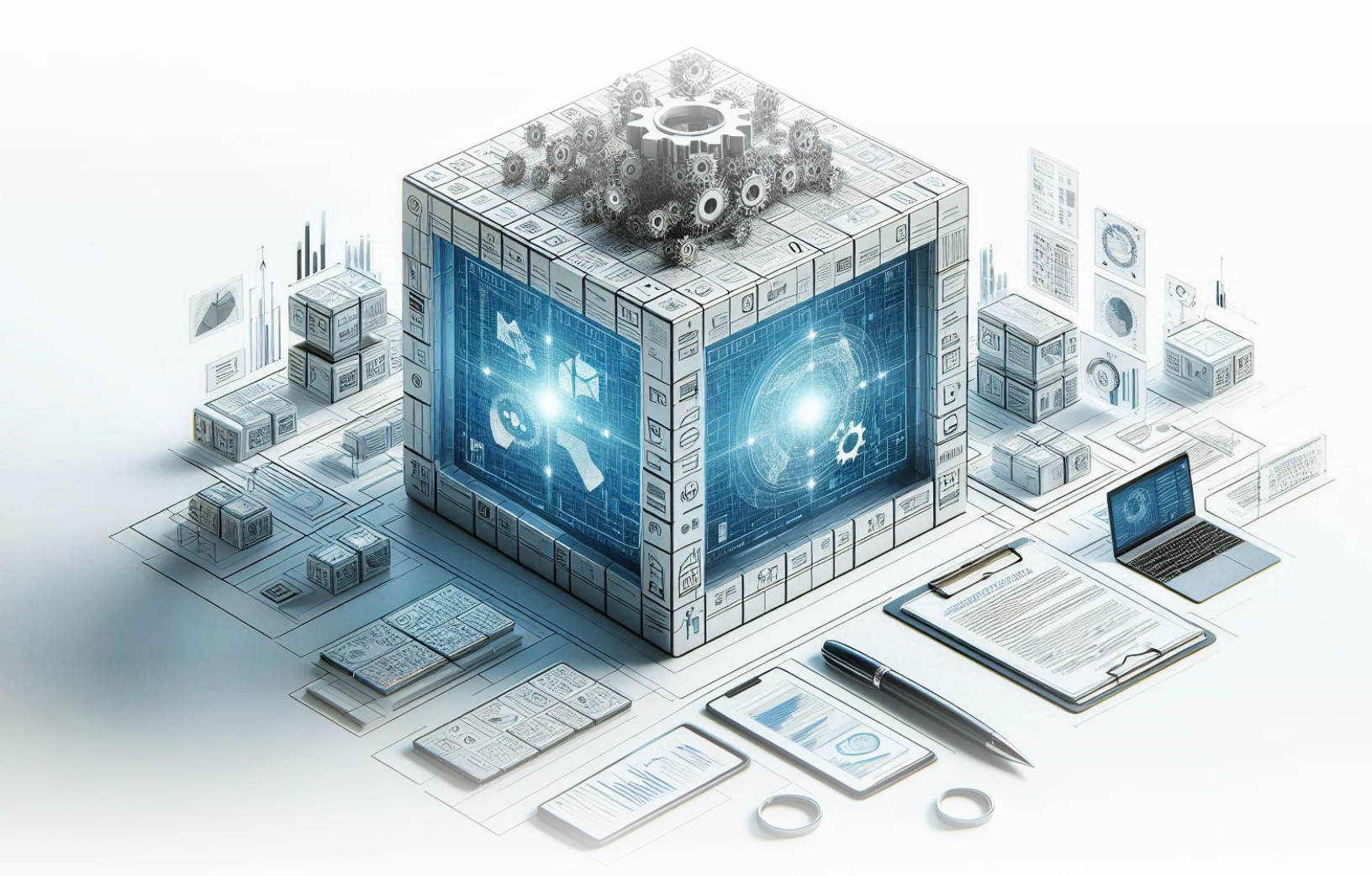
COSO

Achieving Effective Internal Control Over

Robotic Process Automation

RPA



ALIGNING WITH THE COSO INTERNAL CONTROL-INTEGRATED FRAMEWORK

Authors

Prof. Dr. Marc Eulerich, Jan Gruene and Dr. David A. Wood.

Acknowledgements

We would like to recognize and thank Dr. David Wood for his leadership on this project. Additional thank you goes to the COSO Board, and COSO Board Chair and Executive Director Lucia Wind for providing input, assistance, and valuable feedback in developing this paper. We also thank Professor and Doctor Marc Eulerich, Jan Gruene, Martin Wagener and Nathan Waddoups for their technical input and advice.

COSO Board Members

This project was commissioned by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), which is dedicated to helping organizations improve performance by developing thought leadership that enhances internal control, risk management, governance, and fraud deterrence.

COSO is a private-sector initiative jointly sponsored and funded by the following organizations:

American Accounting Association (AAA)

American Institute of CPAs (AICPA)

Financial Executives International (FEI)

The Institute of Management Accountants (IMA)

The Institute of Internal Auditors (IIA)

Design and layout: Sergio Analco

COSO

Committee of Sponsoring Organizations
of the Treadway Commission

coso.org

Contents

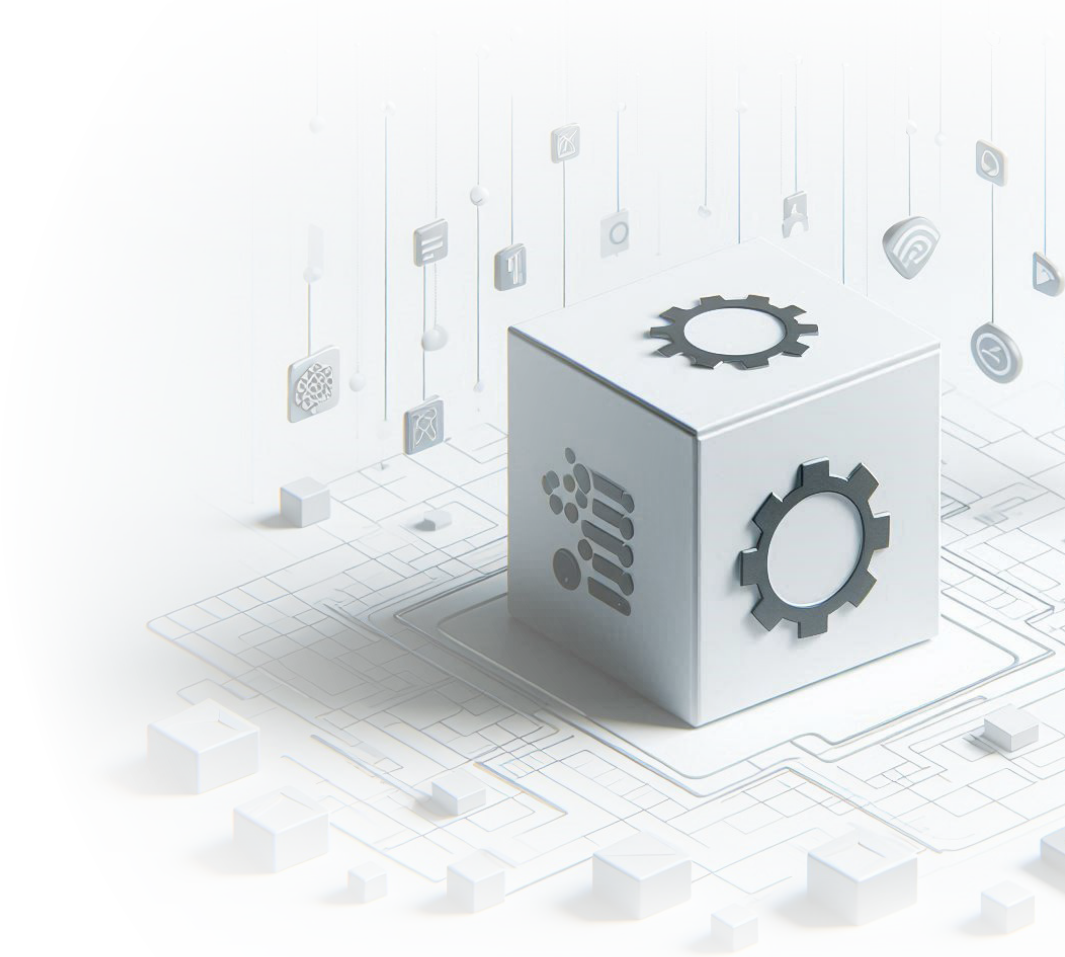
Executive summary

Robotic Process Automation (RPA) is impacting organizations by automating repetitive, rules-based tasks traditionally performed by humans. However, this technology comes with significant governance and control challenges that must be addressed to maximize RPA's benefits while mitigating associated risks. This white paper provides a guide for integrating RPA governance requirements with the COSO Internal Control Integrated Framework (ICIF).

The RPA governance requirements are based on research by Eulerich, Waddoups, Wagener, and Wood (2024). Their study developed an RPA governance framework to address the internal control and governance challenges of RPA. The framework, validated through feedback from professionals across various organizations, includes key governance areas and control requirements designed to maximize RPA benefits and minimize risks.

COSO-ICIF provides a comprehensive approach for designing and implementing effective systems of internal controls, consisting of five components: Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring Activities. By aligning key RPA governance requirements to the five components of COSO-ICIF, we offer a structured approach for organizations to enhance their RPA governance and overall effectiveness of their internal control. This alignment also addresses common challenges of operating RPA, such as security issues, hidden costs, organizational complexities, and knowledge loss.

By following the guidelines and best practices outlined in this document, industry professionals and auditors can better govern RPA initiatives, ensuring compliance with established standards and enhancing the overall effectiveness of their internal control systems.



Introduction to COSO Internal Control-Integrated Framework

The Committee of Sponsoring Organizations of the Treadway Commission's Internal Control-Integrated Framework (COSO-ICIF) has long been the gold standard for designing and implementing effective systems of internal control. As organizations increasingly adopt RPA to streamline operations and boost efficiency, it becomes more important to integrate RPA governance principles with the COSO-ICIF.

COSO-ICIF provides a comprehensive approach for designing and implementing effective systems of internal controls, consisting of five components:

1. **Control Environment**
2. **Risk Assessment**
3. **Control Activities**
4. **Information and Communication**
5. **Monitoring Activities**

These components are supported by 17 principles that represent the fundamental concepts associated with each component. Together, they provide a comprehensive approach to designing and implementing effective internal controls.

In today's rapidly evolving business landscape, the COSO-ICIF remains a critical tool for organizations seeking to:

- Adapt to changing business and operating environments.
- Mitigate risks to acceptable levels.
- Make informed decisions about internal control.
- Reduce the risk of fraud and errors.

COSO-ICIF forms the basis for all control governance, including RPA-related controls. This paper assumes that strong internal controls have already been established for non-RPA areas using COSO-ICIF. Building on that foundation, we focus on key considerations to address the unique risks introduced by RPA, ensuring that these automated processes are effectively governed and integrated into the broader internal control framework.

Understanding Robotic Process Automation (RPA)

Robotic Process Automation (RPA) refers to the use of autonomous computer programs to automate structured, rules-based, and repetitive business processes. As RPA becomes increasingly common, its adoption is driven by the promise of efficiency, cost savings and improved accuracy in routine task performance such as variety of reconciliations, data extraction, accounts receivable or talent management.

Despite these benefits, RPA has introduced significant challenges related to internal controls and governance. Research has found that many organizations, including Fortune 500 companies, report difficulties in managing the risks associated with RPA, such as security vulnerabilities, uncontrolled bot proliferation, and the loss of critical process knowledge (Eulerich, Waddoups, Wagener, and Wood 2024a). This research draws on interviews with RPA stakeholders, including internal and external auditors, chief audit executives, IT specialists, and other RPA stakeholders. Their insights highlight the critical need for a robust governance structure to ensure the successful implementation and operation of RPA technologies.

The "dark side" of RPA highlighted by this prior research is compounded by RPA's ease of use, low cost, and minimal integration requirements, which can lead to ad-hoc implementations and insufficient oversight. Unlike conventional IT controls, RPA introduces a unique set of governance challenges due to its ease of deployment, scalability, and minimal need for integration with existing systems. These characteristics, while advantageous for rapid automation, also create vulnerabilities that traditional IT controls may not fully address.

For instance, RPA's ability to be implemented by non-IT personnel (often termed "citizen developers") can lead to inconsistencies in bot-deployment, inadequate oversight, and increased risk of security breaches. Additionally, the non-intrusive nature of RPA means that it often operates outside the usual IT governance frameworks, potentially leading to gaps in control and oversight.

To avoid these problems and maximize the benefits of RPA, practitioners should conduct a thorough RPA readiness assessment. This assessment should evaluate the organization's preparedness for RPA implementation or expansion across several key areas. These include identifying processes suitable for automation, assessing the current IT infrastructure's ability to support RPA, evaluating the team's skills and knowledge in RPA, and reviewing existing governance structures and policies.

By conducting this comprehensive assessment, organizations can identify potential challenges early and develop strategies to address them, ensuring a smoother and more successful RPA implementation that aligns with their internal control framework.

RPA Bot Governance Framework

The RPA Bot Governance Framework, developed by Eulerich et al. (2024), provides a structured approach to managing RPA implementations. It addresses key governance areas to ensure effective control and risk management in RPA environments. This framework is designed to help organizations navigate the complexities of RPA governance and aligns well with the principles of the COSO-ICIF.

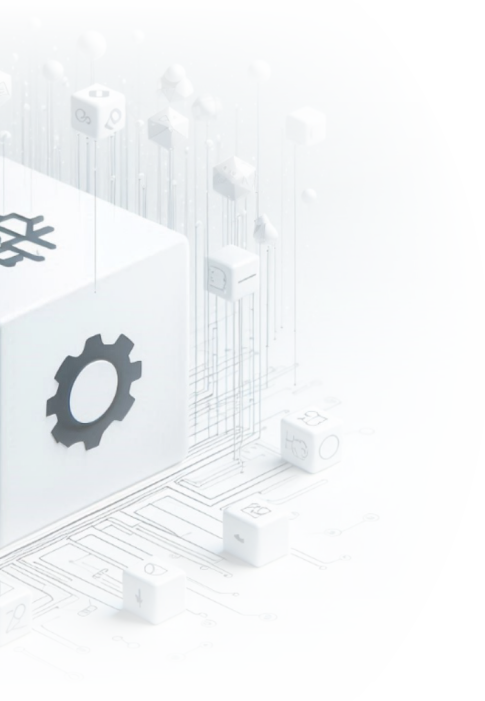
The framework is divided into four main governance areas:

1. **Bot Usage Decision**
2. **Access and Authorization Management**
3. **Managing RPA Process Changes**
4. **IT Operations**

Each of these governance areas encompasses specific control requirements designed to address potential risks and ensure proper management of RPA initiatives. A summary of the specific control requirements (as numbered in the research paper) for each governance area is listed in Figure 1 below.

Figure 1. **Summary of the RPA framework specific control requirements**

1 Bot Usage Decision	2 Access and Authorization Management	3 Managing RPA Process Changes	4 IT Operations
• **1.1** Determine if the process can be automated with existing software. • **1.2** Determine if an existing bot can perform the process. • **1.3** Ensure bots comply with existing IT rules and standards. • **1.4** Ensure bot developers are competent and adhere to governance policies. • **1.5** Identify bots relevant to internal controls.	• **2.1** Restrict access to bot program code based on job responsibilities. • **2.2** Implement password and cybersecurity policies.	• **3.1** Maintain an accurate inventory of all unattended bots. • **3.2** Establish a formal change management process for bots. • **3.3** Restrict access for migrating bot changes into the production environment.	• **4.1** Configure and monitor servers that run bots according to defined standards. • **4.2** Implement an incident management process for bots. • **4.3** Monitor and log deviations from scheduled bot usage. • **4.4** Document and implement backup/recovery policies for bots.



The Bot Usage Decision area focuses on determining whether a process is suitable for automation and if existing bots or software can perform the required tasks. It includes control requirements such as:

- Determining if the process can be automated with existing software
- Determining if an existing bot can perform the process
- Ensuring bots comply with existing IT rules and standards
- Ensuring bot developers are competent and adhere to governance policies
- Identifying bots relevant to internal controls (ICIF)[1]

1. Identifying the risks for bots relative to all COSO objectives (e.g., financial reporting, operations, compliance) is important. The framework focused specifically on financial reporting because of the heightened regulatory requirements, increased scrutiny on financial accuracy, and the critical role of financial data in corporate governance. Generally, an RPA-enhanced risk assessment should cover all relevant COSO objectives specified for each individual organization.

Access and Authorization Management deals with restricting access to bot program code based on job responsibilities and implementing robust password and cybersecurity policies. This area is crucial for maintaining the integrity and security of RPA systems.

Managing RPA Process Changes focuses on maintaining an accurate inventory of all unattended bots, establishing a formal change management process, and restricting access for migrating bot changes into the production environment. This area is essential for maintaining control over the evolving RPA landscape within an organization.

Lastly, the IT Operations area covers configuring and monitoring servers that run bots, implementing incident management processes, monitoring deviations from scheduled bot usage, and documenting backup and recovery policies. This area ensures the smooth and secure operation of RPA systems.

For practitioners, developing a comprehensive RPA governance checklist based on this framework is an important step in ensuring effective control over RPA. This checklist should cover all four governance areas and include specific questions or criteria to assess compliance with each control requirement. It should also provide space for documenting current status, identifying gaps, and outlining action plans for improvement.

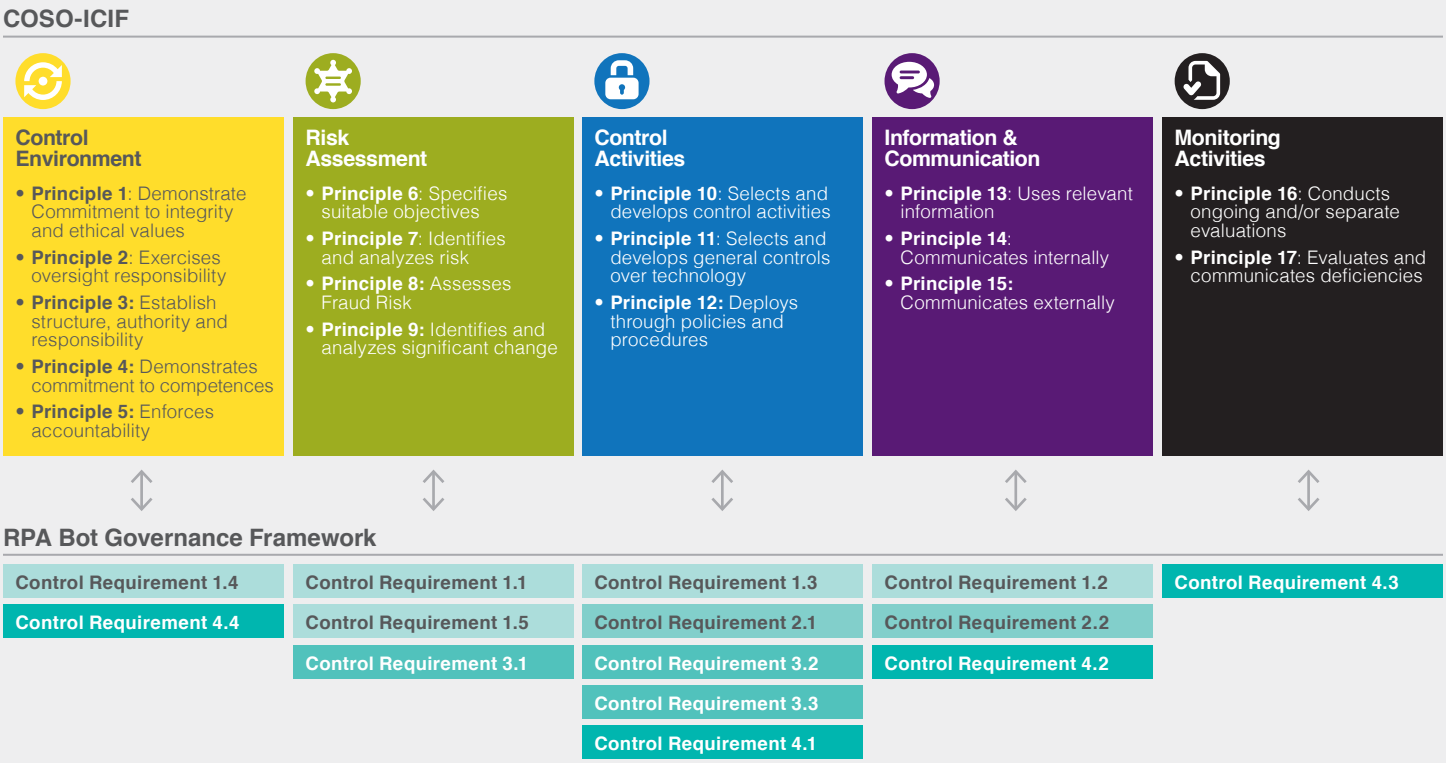
Regular review and updating of this checklist is essential to identify changes in the RPA environment and to ensure ongoing alignment with organizational goals and control objectives. By systematically working through this checklist, organizations can identify areas of weakness in their RPA governance and take proactive steps to address them, thereby strengthening their overall internal control framework.

Aligning RPA Bot Governance with COSO-ICIF

Aligning the RPA Bot Governance Framework with the COSO-ICIF involves mapping specific RPA control requirements to COSO's five components and their associated 17 principles of effective internal control. This alignment ensures that RPA initiatives are integrated effectively into the organization's overall internal control framework. By applying the 17 principles across COSO's five components, organizations can maintain a comprehensive approach to managing both traditional and RPA-specific processes.

The Figure 2 below illustrates how the control requirements of the RPA Bot Governance Framework align with each of the COSO-ICIF components. It demonstrates which specific RPA control requirements map to the corresponding COSO principles, ensuring that all RPA initiatives are coherent with the broader internal control framework. Some of the RPA control requirements correspond to several COSO principles; however, we map them to just one below to avoid duplication.

Figure 2. **RPA Bot Governance Framework aligning with COSO-ICIF components**



We provide a detailed discussion of this mapping in the remainder of the document. Before doing so, we give an example of the mapping. "Control Requirement 1.4" maps to the COSO ICIF component "Control Environment", emphasizing the importance of having skilled bot developers who adhere to governance policies. Similarly, "Control Requirement 3.2" aligns with "Control Activities," highlighting the need for effective change management processes when managing bot changes.

To begin aligning the RPA Bot Governance Framework with COSO-ICIF, practitioners should conduct a thorough maturity assessment of their current RPA-specific internal controls and procedures, using COSO-ICIF as a benchmark. This includes creating an inventory of RPA-specific controls, aligning with to COSO ICIF, and identifying areas that need improvement. Some RPA-specific controls and procedures may be entirely new to the organization's control framework, such as specialized training for bot developers or maintaining an inventory of bots, while others may involve enhancing existing measures, like incorporating bots into IT change management processes.

The initial maturity assessment is not just a procedural step—it is the foundation upon which an effective and resilient RPA governance strategy is built. Establishing RPA governance procedures that align with the organization's internal control framework are important for ensuring that RPA delivers its full benefits without compromising control, security, nor compliance. This mapping exercise provides clarity and direction, helping organizations identify gaps where controls are needed, anticipate potential risks, and proactively strengthen their governance systems to support ongoing innovation.

Much like COSO ICIF, effective RPA Bot Governance is not a one-time effort; it must evolve alongside RPA deployments. As automation technology continues to develop and becomes more deeply integrated into business processes, new risks and control gaps will emerge. Regularly revisiting and adapting control structures ensures ongoing alignment with COSO principles, thus safeguarding organizational integrity and preventing vulnerabilities that could arise from unchecked automation. In essence, continuous alignment helps organizations not only mitigate risks but can also maximize the operational efficiencies and cost savings that RPA promises.

The following sections will provide a detailed discussion of each COSO component, outlining how specific RPA governance principles can be integrated effectively. By referencing the provided graphic, we will demonstrate how this alignment can be put into practice, ensuring that RPA initiatives are not only effective but also secure, compliant, and aligned with the organization's broader control environment. These practical strategies will help create a structured approach that enables organizations to confidently scale their RPA initiatives while maintaining robust internal controls.

A Control Environment

The Control Environment sets the tone for the organization, influencing the control consciousness of its people. In the context of RPA, this component focuses on ensuring that the organizational structure, policies, and culture support effective governance of automated processes. Relevant RPA control requirements in this area include ensuring bot developers are competent and adhere to governance policies, and establishing clear roles and responsibilities for RPA management. These requirements help create a strong foundation for RPA governance by setting clear expectations and accountability measures.

To address the challenges in this area, organizations should implement the following strategies based on the RPA control requirements **1.4** and **4.4**.

Control Requirement 1.4: Ensure bot developers are competent and adhere to governance policies.

- Training and certification programs: Establish training programs that provide bot developers with the necessary skills and knowledge related to RPA development, governance policies, and compliance requirements. Implement certification programs to validate developers' competence and ensure ongoing learning.
- Regular auditing and assessments: Conduct periodic audits and assessments of the bot development process to identify any deviations from governance policies. This can include reviewing documentation, inspecting code repositories, interviewing developers, and analyzing development artifacts for compliance with policies and standards.
- Experience and project portfolio review: Request candidates to submit their project portfolio, showcasing their past work and experience in bot development or similar automation projects during recruiting, to assess technical skills, adherence to best practices, and ability to deliver quality solutions.
- Certifications and qualifications: Hire (or upskill) candidates holding relevant certifications or qualifications e.g. in RPA, automation, or related fields.

Control Requirement 4.4: Document and implement backup/recovery policies for bots.

- Backup policy documentation: Establish a clear and comprehensive backup policy specifically for bots. Document the frequency, timing, locations, and methods for backing up bot configurations, code, databases, and any related data. Specify the required retention periods for backups and outline the roles and responsibilities of personnel involved in backup and recovery processes.

- Off-site backup storage: Store backups in secure off-site locations or cloud-based storage to protect against physical disasters or events that may affect the primary environment. Implement strong access controls and encryption mechanisms for the storage of backups, ensuring their confidentiality and integrity.

- Recovery procedure documentation: Develop documented recovery procedures outlining step-by-step instructions for restoring bots from backups. Include details on the restoration process, necessary hardware, software, and dependencies. Clearly define roles and responsibilities during the recovery process to ensure proper execution and minimize downtime.

- Regular recovery testing: Conduct periodic recovery testing to validate the effectiveness and reliability of the backup/recovery procedures. Test the recovery of bot configurations, code, and data from backups in a controlled environment. This allows you to identify and resolve any issues or gaps in the recovery process proactively.

- Documentation review and updates: Regularly review and update the documentation related to backup/recovery policies and procedures. Ensure that changes in bot configurations, dependencies, or infrastructure are reflected in the documentation. This keeps the policies relevant and accurate, allowing for efficient and effective recovery operations.

To further strengthen the Control Environment, it is important to align the objectives of RPA initiatives with the overall digitalization strategy. Therefore, organizations should:

- Define clear goals and KPIs for automation: Defining specific KPIs helps ensure that automation aligns with strategic goals, facilitates performance tracking, and provides clarity regarding RPA's expected contributions to business outcomes.

- Establish a central unit for coordination and operation: A centralized unit for RPA governance—such as a Center of Excellence for Process Excellence—serves as a coordination hub that enforces consistent standards, best practices, and governance policies across RPA deployments. This central unit can also help mitigate risks related to the miscalculation of effort and costs associated with running, maintaining and troubleshooting of bots.

Strategic Alignment in RPA Governance
Clear goals and KPIs for automation, combined with a centralized coordination unit, ensure that RPA initiatives align with the organization's broader digitalization strategy. This helps prevent underestimations of effort and avoid unexpected license costs.

By fostering a strong Control Environment that embraces RPA governance, organizations lay the foundation for successful automation initiatives. This cultural shift towards accountability, competence, and ethical considerations in RPA deployment ensures that automated processes align with organizational values and control objectives. A robust Control Environment not only mitigates risks associated with RPA but also promotes innovation and efficiency within a well-governed framework.

B Risk Assessment

The Risk Assessment component of COSO-ICIF takes on new dimensions in the context of RPA. Organizations must not only consider traditional risks but also those specifically introduced or amplified by automation technologies.

Key RPA control requirements in this area include identifying bots relevant to internal controls over critical areas and assessing their impact on existing control processes. This ensures that organizations maintain a comprehensive understanding of how their automated processes interact with and potentially impact their critical processes and control systems.

To address the challenges in this area, organizations should implement the following strategies based on the RPA control requirements **1.1**, **1.5**, and **3.1**.

Control Requirement 1.1: Determine if the process can be automated with existing software.

- Check for software compatibility: Verify if the existing software has the necessary features and capabilities to automate the process, by reviewing the software's documentation.
- Analyze workflow complexity: Examine the complexity of the process workflow and determine if the existing software can handle the required steps and decision-making logic. Consider if the software allows for conditional branching, looping, or parallel processing.
- Test automation feasibility: Conduct a proof-of-concept or pilot test with the existing software to determine if it can successfully automate the process. Evaluate the accuracy, efficiency, and reliability of the automation.

Control Requirement 1.5: Identify bots relevant to internal controls.

- Impact assessment: Assess the impact of bot implementation on the design and effectiveness of existing internal controls. Verify that the bots and their automated processes do not weaken or bypass any vital control activities.
- Periodic reassessment: Regularly review and reassess the relevance of bots to internal controls as business processes evolve. This ensures that changes in processes or bot functionalities are reflected in the internal control framework.

Control Requirement 3.1: Maintain an accurate inventory of all unattended bots.

- Centralized (bot) management system: Establish a centralized system or tool specifically designed for managing and tracking bots, serving as a repository for maintaining details and information about each bot, including its purpose, location, version, and assigned responsibilities.
- Regular inventory reconciliation: Conduct regular review of the bot inventory against the actual deployed and unattended bots.
- Version control and change management: Implement version control practices for the bot code and change management processes for bot deployment. Any updates or changes made to the bots should be documented and reflected accurately in the inventory system.

Another key aspect of effective Risk Assessment is managing the dependency on automation and ensuring business continuity:

- High dependency on automation and lack of backup systems: When organizations become too reliant on automated processes, they may overlook the risks associated with bot failures, which can create operational bottlenecks.
- Measures:
  - Establish a specific backup and business continuity plan for RPA: A well-defined backup plan ensures that in the event of a bot failure, critical operations can continue without significant interruption.
  - Implement readily available redundancy systems for particularly critical bots: Redundancy systems act as immediate alternatives to maintain business process continuity, reducing the risk posed by automation failures.

Risk Mitigation for Critical Bots

Establishing redundancy and backup plans for critical bots is essential to ensure that the benefits of automation do not come at the cost of increased vulnerability to operational disruptions.

Effective Risk Assessment in the RPA context is important for maintaining a balance between innovation and control. By consistently evaluating and addressing RPA-specific risks, organizations can confidently expand their automation initiatives while safeguarding against potential pitfalls. This proactive approach to risk management enables businesses to harness the full potential of RPA while maintaining the integrity of their control systems and reporting processes.

C Control Activities

Control Activities in the context of RPA governance involve the policies, procedures, and process controls that help ensure management directives are carried out and risks are mitigated. These activities become particularly crucial in an automated environment where bots are performing tasks previously done by humans.

Key RPA control requirements in this area include restricting access to bot program code based on job responsibilities and implementing a formal change management process for bots. Hence helping to maintain the integrity of automated processes and ensure that changes to bots are properly controlled and documented.

To address the challenges in this area, organizations should implement the following strategies based on the RPA control requirements **1.3**, **2.1**, **3.2**, **3.3**, and **4.1**.

Control Requirement 1.3: Ensure bots comply with existing IT rules and standards.

- Security controls: Ensure that the RPA bot follows the established IT-security protocols and standards (e.g. access controls, encryption, and adherence to authentication and authorization requirements).
- Change management: Implement a change management process for the RPA bot to ensure that any updates or modifications to the bot undergo proper testing, documentation, and approval, including version control practices and maintaining a log of changes made.
- Compliance with data privacy regulations: Implement features like data anonymization, proper consent management, and data retention policies.
- Compliance with software licensing: Ensure that all software used by the RPA bot is appropriately licensed and complies with licensing agreements, e.g. by obtaining and reviewing a comprehensive record of the software licenses and their usage.

Control Requirement 2.1: Restrict access to bot program code based on job responsibilities.

- Role-based access control (RBAC): Implement RBAC to assign specific roles or permissions to individuals based on their job responsibilities.
- User authentication and authorization: Employ robust user authentication measures to ensure that only authorized individuals can access the bot program code, including e.g. username/password combinations, multi-factor authentication, or integration with your organization's single sign-on infrastructure. Authorize users based on their job responsibilities or assigned roles to restrict their access accordingly.
- Access control lists (ACL): Utilize ACLs to define and control user access to specific files or folders containing the bot program code.

Control Requirement 3.2: Establish a formal change management process for bots.

- Change request submission: Require bot developers or stakeholders to submit formal change requests that document the proposed changes to the bot, including details such as the nature of the change, the reason for the change, the expected impact, and any associated risks.
- Change request evaluation and prioritization: Designate a change management team or committee responsible for evaluating change requests.
- Testing and validation: Develop a rigorous testing and validation process for bot changes. This includes testing the changed functionality, verifying its compatibility with other systems or processes, and ensuring continued compliance with governance policies. Test results should be reviewed and documented.
- Change documentation and communication: Maintain documentation of approved changes, including updated specifications, configurations, and dependencies.

Control Requirement 3.3: Restrict access for migrating bot changes into the production environment.

- Change management approval: Require formal approval from designated change management authorities before migrating bot changes to the production environment. This ensures that changes go through a proper review and authorization process before being deployed.
- Segregation of duties: Ensure that the individuals responsible for developing and testing bot changes are not the same individuals with access to migrate those changes into the production environment. This segregation of duties helps prevent unauthorized or unintentional changes from being introduced into the production environment.
- Access controls: Implement access controls and permissions within the production environment to restrict who can migrate bot changes. Grant access only to authorized individuals who have undergone the necessary change management training and adhere to established policies and procedures.

Control Requirement 4.1: Configure and monitor servers that run bots according to defined standards.

- Server configuration management: Establish a standardized configuration management process for servers that run bots. This includes defining baseline configurations, hardening guidelines, and security standards.
- Access controls: Implement access controls and permissions within the production environment to restrict who can migrate bot changes. Grant access only to authorized individuals who have undergone the necessary change management training and adhere to established policies and procedures.
- Logging and monitoring: Set up comprehensive logging and monitoring systems on servers to capture and analyze logs for anomalous activities, security events, and operational issues. Establish alerting and reporting mechanisms to promptly detect and respond to any unauthorized access attempts or potential security incidents.

To ensure effective Control Activities for RPA, the organization should focus on evaluating the practical value of each RPA implementation:

- Evaluation of cost-effectiveness of use cases: It is important to regularly assess whether automating a particular process adds measurable value compared to maintaining it as a manual process. Automations that do not yield significant returns should be re-evaluated or adjusted.
- Measures:
  - Embed RPA into the existing internal control system environment: Integrating bots into the existing control structure ensures that bots follow the same compliance and control standards as other IT processes.
  - Ensure audit logs in the operation of relevant individual bots: Maintain comprehensive audit logs for all bots to enhance transparency, allowing for effective review and oversight of bot activities.

Audit Trail for Bots
Ensure that all activities performed by bots independently (i.e. unattended bots), are retraceable and can be reproduced in an (Internal) Audit.

Implementing comprehensive Control Activities for RPA governance strikes a necessary balance between operational efficiency and risk mitigation. By adapting traditional control mechanisms to the unique challenges of automated processes, organizations can ensure the integrity, security, and compliance of their RPA initiatives. These tailored Control Activities not only protect against potential vulnerabilities but also enhance the overall reliability and effectiveness of automated operations.

D Information and Communication

In an RPA environment, the Information and Communication component of COSO-ICIF takes on new significance. With bots performing tasks previously done by humans, ensuring effective communication and maintaining transparency in bot operations becomes crucial.

Key RPA control requirements in this area include maintaining an accurate inventory of all unattended bots and implementing an incident management process for bots. This helps organizations to maintain visibility into their automated processes.

To address the challenges in maintaining effective communication in a highly automated environment, organizations should implement the following strategies based on the RPA control requirements **1.2**, **2.2**, and **4.2**.

Control Requirement 1.2: Determine if an existing bot can perform the process.

- Input validation: Ensure that the inputs required for the selected process match the inputs the RPA bot needs for processing. Validate if the required data is available and in the correct format.
- Test scenarios: Create test scenarios that cover different possible paths and variations within the selected process. Evaluate the RPA bot‘s ability to navigate through these scenarios accurately and efficiently.
- Performance testing: Conduct performance testing to assess the RPA bot‘s ability to handle the volumes of data or actions within the selected process. Evaluate if the bot can maintain acceptable response times and handle the needed transaction volumes.

Control Requirement 2.2: Implement password and cybersecurity policies.

- Password requirements: Enforce strong password policies that require employees to create passwords that are long and not easily guessable.
- Using Multi-factor authentication (MFA)
- User account lockout policy: Implement an account lockout policy that temporarily locks user accounts after a certain number of failed login attempts.
- Cybersecurity education: Provide regular training and education on cybersecurity best practices, especially for "citizen developers" and other non-IT personnel involved in RPA initiatives.

Control Requirement 4.2: Implement an incident management process for bots.

- Incident reporting and classification: Implement a formal incident reporting mechanism that allows users or stakeholders to report bot-related incidents promptly. Establish a clear classification system to categorize incidents based on severity and impact. This classification helps prioritize incident response and resolution efforts.
- Incident identification and assessment: Develop incident identification processes that monitor bot performance, logs, and user feedback to proactively detect potential issues. Once an incident is identified, conduct thorough assessments to determine its impact, root cause, and potential mitigation strategies. This includes analyzing bot logs, system metrics, and other relevant information to facilitate accurate understanding and resolution of the incident.
- Incident communication and escalation: Establish clear communication channels and escalation procedures for incident management. Promptly notify relevant stakeholders, such as management, impacted users, or business continuity teams, about the incident. Implement defined escalation paths to involve higher-level support or leadership as necessary, ensuring timely resolution and effective coordination.
- Post-incident review: Conduct "lessons learned" sessions after significant incidents to identify areas for improvement in the incident management process and prevent similar issues in the future.

Effective Information and Communication are critical for managing RPA at scale. The following additional measures can help maintain an effective communication framework:

- Lack of overview of bots in the organization: Without a full inventory of bots in operation, it is difficult to maintain visibility and control, leading to inconsistencies and potential compliance gaps.
- Measures:
  - Ensure interfaces and information exchange between relevant stakeholders: Regular communication between IT teams, business process owners, and RPA developers ensures that all parties are aware of current RPA deployments and any changes being made.
  - Maintain audit logs in bot operations: A robust logging system ensures that relevant stakeholders can quickly understand the performance and behavior of bots, reducing the risk of inconsistencies.

Cost-Effectiveness Assessments
Regularly assessing cost-effectiveness and embedding RPA into internal controls ensures that automated solutions remain efficient, transparent, and fully accountable.

In an RPA-driven environment, robust Information and Communication practices are vital for maintaining transparency and operational oversight. By establishing clear channels for sharing RPA-related information and fostering open communication among stakeholders, organizations can more quickly identify and address issues, promote continuous improvement, and ensure that automated processes remain aligned with business objectives. This emphasis on information flow and communication strengthens the overall governance structure and supports informed decision-making at all levels.

E Monitoring Activities

The Monitoring Activities component of COSO-ICIF takes on new dimensions in an RPA environment. With bots performing tasks autonomously, continuous monitoring becomes essential to ensure that automated processes are functioning as intended and that controls remain effective.

A key RPA control requirement in this area is to monitor and log any deviations from scheduled bot usage. Following this practice will help organizations quickly identify and respond to issues with their automated processes and ensure business continuity in case of bot failures.

To address the challenges in ensuring continuous monitoring of bot activities, organizations should implement the following strategy based on the RPA control requirement **4.3**.

Control Requirement 4.3: Monitor and log deviations from scheduled bot usage.

- Automated monitoring system: Deploy an automated monitoring system specifically designed to track bot usage and activities. This system continuously monitors the execution of scheduled bot runs and compares them against predefined schedules and expected patterns, generating alerts or notifications when deviations are detected.
- Real-time event logs: Implement a logging mechanism that captures information about bot activities and usage in real-time. Log relevant events such as bot start and stop times, execution durations, successful runs, failures, or any other significant deviations from the scheduled usage. Ensure that the logs are timestamped and securely stored for later analysis.
- Logging of exceptions and errors: Configure the bots to log any exceptions, errors, or unusual behaviors encountered during their execution. Capture information about the nature of the deviation, error codes or messages, affected processes, and relevant contextual data. This helps in identifying and diagnosing the causes of deviations from scheduled bot usage.
- Threshold-based alerts: Set up threshold-based alerting mechanisms within the monitoring system to trigger notifications when certain predefined thresholds are exceeded. For example, if a bot exceeds its allocated runtime for a scheduled task by a specified percentage, an alert is generated. This helps identify significant deviations requiring attention.

Continuous monitoring is important for managing the unique challenges posed by RPA. Key areas to address include:

- Lack of audit logs in the bot environment: Without detailed audit logs, it can be difficult to track bot activities and identify the root causes of any issues.
- Measures:
  - Conduct regular functional and integrity tests for all relevant bots: Regular testing ensures that bots are operating as expected and helps identify issues before they impact business processes.
  - Document, track, and implement improvement potentials: Learning from operational incidents and logging these lessons are critical to improving bot performance and reliability.

Enhancing Monitoring Through Regular Testing

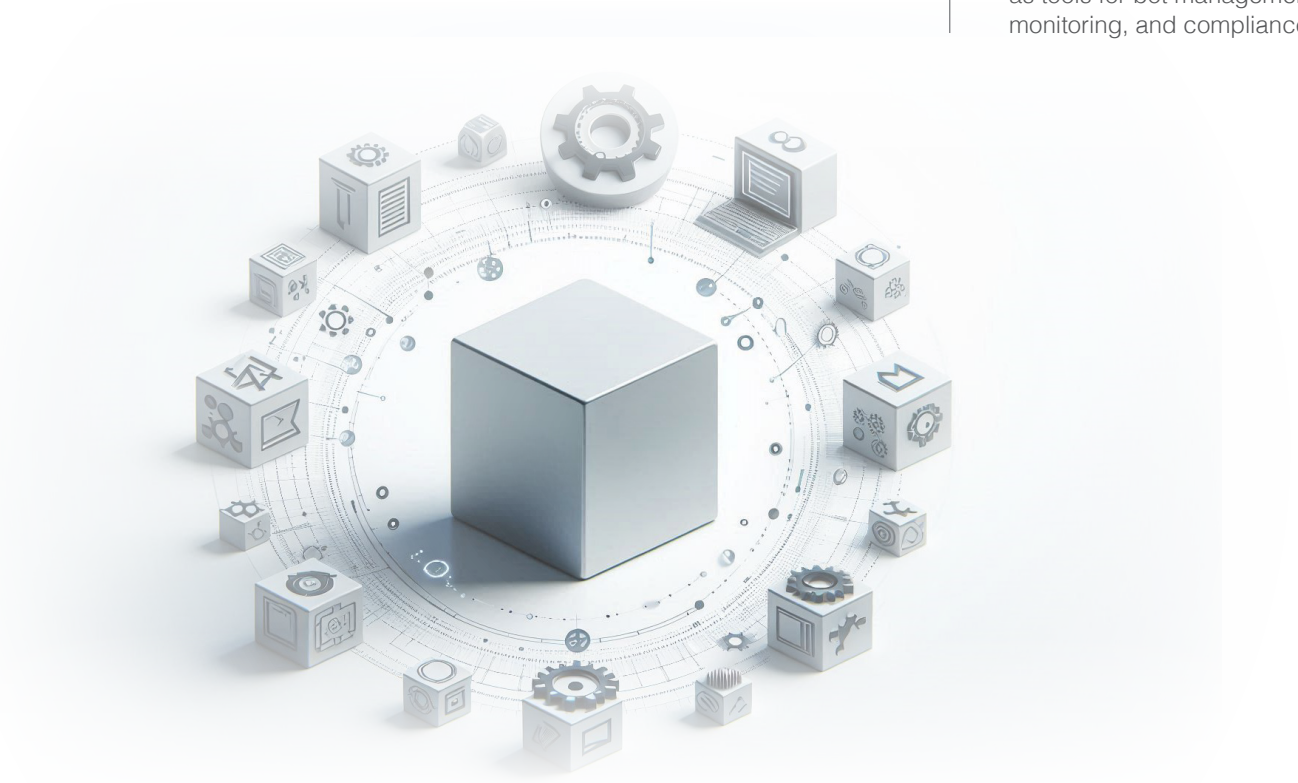
Conducting regular functional testing and documenting bot performance helps ensure consistency, reduce the risk of data integrity issues, and drive improvements in bot quality.

Continuous and effective Monitoring Activities are the cornerstone of successful RPA governance. By implementing comprehensive monitoring strategies, organizations can ensure the ongoing effectiveness of their automated processes and swiftly adapt to changing risks or business needs. This vigilant approach not only enhances the reliability and efficiency of RPA initiatives but also provides valuable insights for refining governance practices, ultimately driving continuous improvement in the organization's use of automation technologies.

Practical Implementation Guidelines

Implementing an integrated COSO-ICIF RPA governance approach requires a structured and thoughtful process. The following guidelines provide a roadmap for practitioners to effectively align their RPA initiatives with established internal control principles:

1. Conduct a comprehensive assessment of your current RPA landscape and internal control environment, mapping existing RPA processes to the COSO-ICIF components and identifying any gaps or areas of misalignment.
2. Develop a detailed implementation plan that outlines specific steps for aligning RPA governance with each COSO-ICIF component, including timelines, resource allocations, and clear accountability for each action item.
3. Establish a cross-functional RPA governance committee to oversee the integration process, make key decisions, and ensure that RPA governance remains aligned with broader organizational goals and control objectives.
4. Develop comprehensive policies and procedures that address each aspect of RPA governance within the COSO-ICIF framework, covering areas such as bot development standards, change management processes, access controls, monitoring protocols, and incident response procedures.
5. Implement robust training programs that cover not only the technical aspects of RPA but also the principles of internal control and the importance of governance.
6. Establish a centralized repository for all RPA-related documentation, including bot inventories, risk assessments, control matrices, and audit logs.
7. Implement a continuous improvement process for your RPA governance framework, regularly reviewing and updating your governance practices based on lessons learned, changes in the business environment, and evolving best practices in RPA and internal control.
8. Consider leveraging technology solutions to support your RPA governance efforts, such as tools for bot management, performance monitoring, and compliance tracking.



Conclusion

The integration of RPA governance principles with the COSO Internal Control-Integrated Framework represents a significant opportunity for organizations to enhance their control environments while leveraging the benefits of automation. By aligning RPA initiatives with established internal control principles, organizations can ensure that their automation efforts not only drive efficiency and productivity but also maintain robust governance and risk management practices.

The approach outlined in this paper provides a comprehensive framework for practitioners to navigate the complexities of RPA governance within the context of COSO-ICIF. By addressing each component of the COSO framework in relation to RPA, organizations can develop a holistic approach to governance that supports both innovation and control.

Appendix

This appendix provides a comprehensive set of checklists designed to guide practitioners in implementing effective RPA governance aligned with the COSO-ICIF. These checklists serve as practical tools to ensure that all critical aspects of RPA governance are addressed, helping organizations maximize the benefits of RPA while mitigating associated risks.

Checklists Aligned with COSO Components

A Control Environment

Governance and Oversight

- ☐ Have you established an RPA governance framework aligned with COSO-ICIF?
- ☐ Is there a cross-functional RPA governance committee in place?
- ☐ Are roles and responsibilities for RPA management clearly defined and communicated?
- ☐ Does the organization have a central unit (e.g., Center of Excellence) overseeing RPA initiatives?
- ☐ Are RPA objectives aligned with the organization's overall digital strategy and risk appetite?

Competence and Accountability

- ☐ Are bot developers properly trained and certified in RPA technologies and internal control principles?
- ☐ Do bot developers understand and adhere to established governance policies and procedures?
- ☐ Are processes in place to verify the competence and experience of bot developers, including "citizen developers"?
- ☐ Is ongoing training provided to keep skills current with evolving RPA technologies?

Integrity and Ethical Values

- ☐ Does the RPA governance framework promote integrity and ethical behavior in bot development and deployment?
- ☐ Are policies in place to address ethical considerations, such as data privacy and security in RPA initiatives?
- ☐ Is there a code of conduct that includes expectations for RPA-related activities?

B Risk Assessment

Identification and Analysis of Risks

- ☐ Have you conducted a comprehensive risk assessment specific to RPA initiatives?
- ☐ Are all processes proposed for automation evaluated for risks, including security vulnerabilities and impacts on existing controls?
- ☐ Is there an evaluation to determine if existing software or bots can perform the required tasks before developing new bots?
- ☐ Are bots that are relevant to Internal Controls over critical areas identified and documented?
- ☐ Have you assessed the risk of bot failure and its impact on business operations?

Assessment of Fraud Risks

- ☐ Have potential fraud risks associated with RPA been identified, such as unauthorized access or data manipulation?
- ☐ Are controls in place to mitigate identified fraud risks, including access restrictions and monitoring?

Changes in Operating Environment

- ☐ Is there a process to assess risks arising from changes in the RPA operating environment, such as software updates or regulatory changes?
- ☐ Are dependencies on automation evaluated, including the risk of high reliance without adequate manual backups?

Backup and Continuity Planning

Are backup systems and business continuity plans in place for critical bots?
Have redundancy systems been implemented for essential automated processes?
Is there a documented recovery plan in case of bot or system failure?

C Control Activities

Policies and Procedures

- ☐ Are comprehensive policies and procedures established for RPA control activities?
- ☐ Is there a formal change management process for bots, including approval workflows, testing, and documentation?
- ☐ Are bots integrated into the organization's existing internal control system and IT governance frameworks?
- ☐ Are procedures in place to ensure bots comply with IT rules and standards?

Access Controls

- ☐ Are access controls in place to restrict access to bot program code based on job responsibilities?
- ☐ Is role-based access control (RBAC) implemented for bot development and deployment environments?
- ☐ Are segregation of duties enforced to prevent conflicts of interest in bot development, testing, and deployment?
- ☐ Are access permissions reviewed and updated regularly?

Backup and Recovery

- ☐ Are documented backup and recovery policies for bots established and implemented?
- ☐ Are backups performed regularly and stored securely, with encryption if necessary?
- ☐ Are recovery procedures tested periodically to ensure they work effectively?

Server and Infrastructure Configuration

- ☐ Are servers running bots configured and monitored according to defined IT standards?
- ☐ Are security measures such as firewalls, antivirus software, and intrusion detection systems in place?
- ☐ Is there regular maintenance, including updates and patches, for servers and infrastructure supporting RPA?

Evaluation of Cost-Effectiveness

- ☐ Is there an ongoing evaluation of the cost-effectiveness and practical value of each RPA implementation?
- ☐ Are processes automated only when they provide measurable value and efficiency gains?
- ☐ Are KPIs established to measure the performance and ROI of bots?

D Information and Communication

Information Quality and Availability

- ☐ Is there an accurate and up-to-date inventory of all bots, including unattended bots?
- ☐ Are audit logs maintained for all bot operations, capturing relevant activities and events?
- ☐ Is critical RPA documentation centralized and accessible to authorized personnel?
- ☐ Are logs regularly reviewed for anomalies or unauthorized activities?

Internal Communication

- ☐ Are effective communication channels established between IT, bot developers, business units, and other stakeholders?
- ☐ Is there regular reporting on RPA performance, issues, and governance matters to relevant stakeholders?
- ☐ Are updates and changes to RPA policies and procedures communicated promptly to all affected personnel?
- ☐ Do teams collaborate to ensure alignment of RPA activities with business objectives?

External Communication

- ☐ Are external stakeholders, such as auditors and regulatory bodies, provided with necessary information regarding RPA initiatives and controls?
- ☐ Is there transparency in communicating RPA-related incidents that may impact critical areas?
- ☐ Are disclosures related to RPA included in financial statements if required?

Cybersecurity Policies

- ☐ Are robust password and cybersecurity policies implemented and enforced for all users involved in RPA?
- ☐ Is multi-factor authentication used where appropriate to enhance security?
- ☐ Are users educated on cybersecurity best practices and aware of their responsibilities?
- ☐ Are cybersecurity policies regularly reviewed and updated to address emerging threats?

E Monitoring Activities

Ongoing Monitoring

- ☐ Is there continuous monitoring of bot performance and adherence to control requirements?
- ☐ Are automated monitoring systems in place to detect deviations from scheduled bot usage?
- ☐ Are alerts configured for significant events or anomalies in bot operations?
- ☐ Are functional and integrity tests conducted regularly for all bots?

Separate Evaluations

- ☐ Are periodic independent evaluations of RPA governance and controls conducted, such as internal or external audits?
- ☐ Is there a process for documenting findings from evaluations and implementing corrective actions?
- ☐ Are audit results communicated to senior management and the governance committee?

Reporting Deficiencies

- ☐ Are mechanisms in place for personnel to report issues or deficiencies in RPA operations or controls without fear of reprisal?
- ☐ Are incidents and control deficiencies reported to appropriate levels of management and the governance committee in a timely manner?
- ☐ Is there a tracking system for reported issues to ensure they are addressed promptly?

Incident Management

- ☐ Is there an established incident management process for bots, including identification, assessment, escalation, and resolution procedures?
- ☐ Are responsibilities clearly defined for incident response teams?
- ☐ Are incidents analyzed for root causes, and are lessons learned used to improve controls and processes?
- ☐ Is there documentation of all incidents and responses for future reference?

Continuous Improvement

- ☐ Is there a process for documenting, tracking, and implementing improvement opportunities identified through monitoring activities?
- ☐ Are changes resulting from monitoring activities communicated and integrated into the governance framework?
- ☐ Are best practices and lessons learned shared across the organization to enhance overall RPA governance?

By utilizing these comprehensive checklists, practitioners can systematically address critical aspects of RPA governance in alignment with the COSO-ICIF. This structured approach ensures that RPA initiatives are effectively integrated into the organization's internal control environment, enhancing operational efficiency while maintaining robust governance and risk management practices.

About the authors

Prof. Dr. Marc Eulerich is a professor of internal auditing at the Mercator School of Management, University Duisburg-Essen, a position he has held since 2011 with the backing of the German Institute of Internal Auditors (DIIR). As the head of the "Center for Internal Auditing Excellence" and chair of the scientific committee of the German IIA, he is at the forefront of bridging academic inquiry with practical auditing standards. With a portfolio of over 150 publications spanning corporate governance, internal auditing, and strategic management, his insights have found a home in revered international journals. Marc is a CIA and is enriching the internal auditing profession through numerous talks and consulting projects. His relentless efforts aim at intertwining theoretical acumen with practical engagements, ensuring a vibrant dialog between academia and the industry. He is the founder and academic head of the "Mercator Audit & Artificial Intelligence Research Center" and one of the leaders in the field of AI-related Internal Audit research.

Jan Gruene is a leader for Digital Internal Audit at Deloitte Germany's Risk Advisory Practice. He has more than 15 years' experience in evaluating and optimizing corporate governance systems and business processes with a specific focus on Internal Control and Internal Audit. Throughout his career he has advised businesses on strategy, transformation and digitization of their 2nd and 3rd line functions. In this area he leads the design and implementation of solutions around data analytics, GenAI, and automation. With his team he leads the development around optimization, streamlining and automation of internal controls, business processes as well as (internal) audit procedures. He also has a strong focus on integrating and aligning corporate governance functions and their activities towards new, technology-driven risks.

Dr. David A. Wood works as the Glenn D. Ardis professor accounting at Brigham Young University. At BYU, David teaches accounting data analytics and accounting information systems. He has published over 175 articles in a combination of respected academic and practitioner journals, monographs, books, and cases. David has developed numerous resources for academia and practice. For the academy, he is one of the founders of https://experience.eyarc.site/ and https://www.techhub.training, which provide free resources to thousands of students throughout the world. For practice, he is a cofounder of a free generative AI governance framework (see http://genai.global/), and of a training company that uses cutting-edge technology to help train accountants and business professionals (skillabyte.com). He is currently working on developing other products and companies related to GenAI in accounting.

About COSO

Originally formed in 1985, COSO is a joint initiative of five private sector organizations and is dedicated to helping organizations improve performance by developing thought leadership that enhances internal control, risk management, governance, and fraud deterrence. COSO's supporting organizations are the American Accounting Association (AAA), the American Institute of Certified Public Accountants (AICPA), Financial Executives International (FEI), the Institute of Management Accountants (IMA), and The Institute of Internal Auditors (IIA).

Achieving Effective Internal Control Over

Robotic Process Automation

RPA

ALIGNING WITH THE COSO INTERNAL CONTROL-INTEGRATED FRAMEWORK

COSO

Committee of Sponsoring Organizations
of the Treadway Commission

coso.org