

BOARD GOVERNANCE ARTIFACT

Delegated Authority Review for Agentic AI

Seven board-level questions before agentic workflows are approved, deployed, or expanded

Publication Code	PD-ARTIFACT-001
Version	1.0
Published	May 2026
Category	Cyber Risk Governance & Accountability™ (CRGA™)
Issued By	Praesidium Governance, Inc.
Canonical URL	praesidiumoversight.com/publications/artifacts/PD-ARTIFACT-001/
PDF Download	praesidiumoversight.com/publications/artifacts/PD-ARTIFACT-001_Delegated_Authority_Review_v1_0.pdf

Document Status	Board Governance Artifact
Authority Level	Institutional
Applicability	Technology-Enabled Enterprise Risk Governance
Supersession	This document may be revised by subsequent Praesidium publications.

LEGAL NOTICE AND TERMS OF USE

COPYRIGHT

© 2026 Praesidium Governance, Inc. All rights reserved. This publication and all content herein is the proprietary intellectual property of Praesidium Governance, Inc.

PERMITTED USE

This document may be distributed in its complete and unaltered form for non-commercial informational purposes only. Any reproduction, excerpting, or reference must preserve full attribution and may not alter the meaning, context, or presentation of Praesidium's institutional position, including through partial or selective excerpting.

PROHIBITED USE

Reproduction for commercial purposes, redistribution for compensation, modification or derivative works, removal of attribution or copyright notices, and use in any manner that misrepresents the source or authorship of this content are strictly prohibited.

TRADEMARK NOTICE

Praesidium™, Cyber Risk Governance & Accountability™, and CRGA™ are trademarks of Praesidium Governance, Inc. All rights reserved. Unauthorized use of these marks, including use that implies affiliation, endorsement, certification, or authorization by Praesidium Governance, Inc., is strictly prohibited.

NO ENDORSEMENT

Reference to CRGA™ or alignment with its principles does not constitute endorsement, approval, certification, or validation by Praesidium Governance, Inc.

NO ADVISORY RELATIONSHIP

This publication is provided for informational and institutional reference purposes only. It does not constitute legal, financial, regulatory, or operational advice. No advisory, consulting, or fiduciary duty is assumed or created. Recipients should consult qualified professionals for advice specific to their circumstances.

LIMITATION OF LIABILITY

To the fullest extent permitted by applicable law, Praesidium Governance, Inc. shall not be liable for any direct, indirect, incidental, consequential, or special damages arising from or related to the use of, reliance on, or inability to use this publication.

ACCURACY AND UPDATES

Praesidium Governance, Inc. makes no representations or warranties regarding the completeness, accuracy, or applicability of the information contained herein, including without limitation any implied warranties of merchantability or fitness for a particular purpose. The content reflects institutional positions as of the publication date and may be revised or superseded by subsequent publications.

GOVERNING AUTHORITY

This publication is issued under the authority of Praesidium Governance, Inc., the issuing authority for the Cyber Risk Governance & Accountability™ (CRGA™) framework. Questions regarding permitted use or licensing should be directed to Praesidium Governance, Inc. through praesidiumoversight.com.

PURPOSE

Agentic AI becomes a governance issue when software is permitted to initiate, recommend, sequence, escalate, or execute action inside an enterprise workflow.

Before an agentic workflow is approved, deployed, or expanded, boards and executive leadership should be able to evidence how authority, accountability, escalation, and oversight have been defined.

This review provides a board-level governance lens for evaluating whether delegated machine authority has been bounded before it is exercised.

Companion to: PD-NOTE-004, Agentic AI and the Governance of Delegated Authority | praesidiumoversight.com/publications/governance-notes/PD-NOTE-004/

GOVERNANCE REVIEW QUESTIONS

1. What authority is being delegated to the AI system?

Define whether the system is generating information, recommending action, initiating workflow steps, interacting with enterprise systems, escalating issues, or executing tasks.

2. Who approved that delegation?

Identify the executive owner, governance body, committee, or approval authority responsible for permitting the AI system to operate within the workflow.

3. What decisions or actions remain reserved to humans?

Specify which decisions, exceptions, approvals, customer impacts, financial actions, security events, regulatory matters, or material risk conditions require human control.

4. What escalation thresholds apply?

Define when risk conditions, anomalies, uncertainty, system behavior, customer impact, legal exposure, security events, or operational exceptions must be escalated.

5. What evidence will prove oversight occurred?

Retain records showing approval, risk evaluation, authority boundaries, access limitations, testing, monitoring, exception handling, and periodic review.

6. Who owns failures, exceptions, and downstream harm?

Assign accountability to a human role, executive owner, business function, risk owner, or governance body. Accountability cannot be delegated to software.

7. What conditions require suspension, rollback, or board notification?

Define the events that require the workflow to be paused, modified, escalated, reported, or withdrawn from use.

BOARD INTERPRETATION

The central question is not only whether agentic AI can improve a workflow.

The central question is whether the organization can prove that the workflow is governable, accountable, and defensible when software is permitted to act.

Agentic workflows become defensible only when delegated machine authority is bounded before it is exercised.