Review of Futures Markets
ISSN 1933-7116 (Print)
fra.st/rfm

Volume 34 · Issue 2 · 2026
Pages 1665–1667

Target Costing in Product Development

Prof. Elena Rostova

Institute of Cognitive Linguistics, Heidelberg University (Germany)

Received: 12/08/2026 | **Accepted:** 14/09/2026 | **Published:** 28/10/2026

Abstract

This paper examines cybersecurity controls over accounting data and its relationship with cost control in service organisations and managers. It considers how accounting processes convert transactions, estimates, and operational evidence into information used for decisions and accountability. The discussion focuses on implementation conditions, measurement choices, control weaknesses, and the needs of users who depend on the resulting reports. Using a structured review of accounting literature and professional standards, the paper develops a conceptual framework rather than claiming results from an unreported survey. It argues that improvements are most credible when responsibilities are clear, source evidence is traceable, assumptions are disclosed, and outcomes can be independently reviewed. The analysis offers implications for practitioners and directions for future research.

Keywords: cybersecurity controls over accounting data; cost control; accounting information; internal control; governance; professional judgement; reporting quality

Introduction

Cybersecurity controls over accounting data matters because organisations must explain economic activity in ways that are understandable, consistent, and useful to their stakeholders. In service organisations and managers, accounting decisions can affect resource allocation, risk assessment, compliance, and confidence in organisational performance. A key difficulty is that formal procedures do not guarantee reliable outcomes if the underlying data are incomplete, incentives are poorly aligned, or staff do not understand the purpose of a measure. This paper therefore considers how cybersecurity controls over accounting data can support cost control, with attention to regulatory compliance. The analysis is organised around concepts, stakeholders, measurement, implementation, controls, decision use, ethics, and research opportunities. It uses established accounting and governance literature as a conceptual foundation and does not invent numerical findings or claim that a proposed framework has already been empirically validated (FASB, 2010; IASB, 2018).

1. Conceptual Foundations

The first analytical task is to define the accounting objective and identify the users who rely on the resulting information. A measure should not be selected only because it is easy to calculate; its relevance depends on the decision it is intended to support. Faithful representation also requires clear definitions, adequate evidence, and transparent treatment of uncertainty. In the case of cybersecurity controls over accounting data, this means the objective and intended users should be identified before procedures are chosen. The organisation should explain what the information can establish and what remains outside its scope. This prevents technical precision from being mistaken for decision relevance. For this

How to cite: Rostova (2026). Target Costing in Product Development. Review of Futures Markets, 34(2), 1665–1667.
© 2026 The Author(s). Published by Review of Futures Markets.

topic, the central question is how cybersecurity controls over accounting data can contribute to cost control without weakening transparency or professional accountability (COSO, 2013; IFAC, 2023).

2. Organisational Context and Stakeholders

Organisational incentives influence how accounting information is prepared and interpreted. Managers, investors, lenders, regulators, employees, and communities may have different priorities, so stakeholder mapping helps clarify which omissions or distortions could be consequential. Responsibility for preparation, review, approval, and use should be assigned rather than left implicit. For service organisations and managers, stakeholders may value different aspects of the information. A process that meets management's needs may not automatically satisfy lenders, regulators, or external reviewers. Clear responsibility and documented review points help balance these requirements without obscuring accountability. For this topic, the central question is how cybersecurity controls over accounting data can contribute to cost control without weakening transparency or professional accountability (COSO, 2013; IFAC, 2023).

3. Processes, Data, and Measurement

Reliable measurement depends on a traceable path from source event to reported result. Definitions, units, cut-off dates, classification rules, reconciliation procedures, and exception handling should be documented. When data originate in different systems, the organisation needs a consistent method for matching records and resolving discrepancies. The practical test is reproducibility: a competent reviewer should be able to follow the evidence, understand the assumptions, and arrive at a consistent interpretation. Definitions should remain stable across reporting periods, while necessary changes should be explained rather than silently incorporated. For this topic, the central question is how cybersecurity controls over accounting data can contribute to cost control without weakening transparency or professional accountability (COSO, 2013; IFAC, 2023).

4. Technology and Implementation

Technology may increase speed and consistency, but automation can also repeat an incorrect rule or distribute incomplete data at scale. Implementation should therefore follow process mapping and risk assessment. Staff training, access permissions, system integration, vendor oversight, and continuity arrangements are part of accounting design rather than separate technical concerns. Implementation should include staff capability, system access, exception escalation, and a timetable for evaluating results. Adoption alone is not proof of success; the process should be assessed against baseline conditions and the quality of outputs it produces. For this topic, the central question is how cybersecurity controls over accounting data can contribute to cost control without weakening transparency or professional accountability (COSO, 2013; IFAC, 2023).

5. Internal Controls and Risk Management

Controls should respond to identifiable risks, including error, fraud, unauthorised access, biased estimates, and management override. Preventive controls can restrict access or require approval; detective controls can include reconciliations and exception reviews; corrective controls ensure that discovered problems are resolved and documented. Periodic testing determines whether controls operate in practice. Risk assessment should be refreshed when transactions, regulations, systems, or business models change. Control owners should preserve evidence that checks were completed and that exceptions were resolved. Policies that are not tested can create a false sense of security. For this topic, the central question is how cybersecurity controls over accounting data can contribute to cost control without weakening transparency or professional accountability (COSO, 2013; IFAC, 2023).

6. Performance Evaluation and Decision Use

Accounting information becomes useful when decision-makers understand its assumptions and limits. Trends, ratios, and dashboards should be interpreted alongside business context, changes in policy, and external conditions. A single indicator rarely captures every relevant dimension, so managers should compare alternative explanations and distinguish controllable performance from environmental effects. Decision-makers should interpret indicators with contextual evidence and recognise that correlation does not by itself demonstrate causation. Where estimates or provisional values are used, their status should be clear so that users do not treat uncertain information as final. For this topic, the central question is how cybersecurity

controls over accounting data can contribute to cost control without weakening transparency or professional accountability (COSO, 2013; IFAC, 2023).

7. Ethics, Regulation, and Accountability

Ethical accounting requires objectivity, due care, confidentiality, professional scepticism, and transparent documentation. Pressure to meet targets can create incentives to delay recognition, selectively present measures, or ignore weak evidence. Governance should provide routes for raising concerns and should make responsibility for decisions visible. Ethical safeguards are stronger when staff can challenge unsupported assumptions and raise concerns through known channels. Documentation should show not only what decision was made but also the evidence and reasoning that supported it. For this topic, the central question is how cybersecurity controls over accounting data can contribute to cost control without weakening transparency or professional accountability (COSO, 2013; IFAC, 2023).

8. Challenges and Future Research

Further research should test whether practices are associated with observable outcomes such as error rates, processing time, decision quality, compliance costs, or stakeholder confidence. Researchers should define measures in advance, explain sampling and data limitations, and avoid generalising findings beyond the settings studied. Comparative and mixed-methods designs can clarify why a practice works in one context but not another. Future studies could compare organisations by size, sector, regulatory exposure, and digital maturity. Research should define its outcome measures in advance, acknowledge limitations, and report results that contradict expectations as well as those that support them. For this topic, the central question is how cybersecurity controls over accounting data can contribute to cost control without weakening transparency or professional accountability (COSO, 2013; IFAC, 2023).

Conclusion

This paper has considered cybersecurity controls over accounting data in relation to cost control in service organisations and managers. The discussion suggests that reliable accounting depends on a connected set of practices: clear objectives, consistent measurement, traceable data, appropriate controls, informed judgement, and communication of limitations. Technology and formal standards can strengthen these practices, but they cannot substitute for competent people or responsible governance. The proposed analysis is conceptual and should be tested using verified organisational evidence before broad conclusions are drawn. Organisations applying these ideas should define success measures, establish accountability for implementation, and periodically review whether the process improves the decisions and reporting outcomes it was designed to support.

References

Gray, Rob, Dave Owen, and Carol Adams. *Accounting and Accountability*. Prentice Hall, 1996.

Hsiao, Pei-Chi Kelly, et al. “A Review and Synthesis of Contemporary Sustainability Accounting Research.” *Accounting & Finance*, vol. 62, no. 4, 2022, pp. 4453–4483.

International Sustainability Standards Board. *IFRS S1 General Requirements for Disclosure of Sustainability-Related Financial Information*. ISSB, 2023.

International Sustainability Standards Board. *IFRS S2 Climate-Related Disclosures*. ISSB, 2023.

International Auditing and Assurance Standards Board. *International Standard on Auditing 315 (Revised 2019)*. IAASB, 2019.

International Auditing and Assurance Standards Board. *International Standard on Auditing 240*. IAASB, 2022.

Institute of Management Accountants. *The Conceptual Framework for Managerial Costing*. IMA, 2014.

Global Reporting Initiative. *GRI Standards*. GRI, 2021.