Revue Internationale des Sciences de Gestion
ISSN: 2665-7473
Volume 9 : Numéro 4

Controlling Differently: Internal Control Digitalization as a Dynamic Capability. A Conceptual Framework and Research Propositions

La digitalisation du contrôle interne comme capacité dynamique. Un cadre conceptuel et des propositions de recherche.

BOUBOUH IMAN
PhD Student
National School of Business and Management of Tangier (ENCG Tanger)
Abdelmalek Essaâdi University
Management, Economics, Information Systems and Law
Morocco

GHANIM MOHAMED
Professor-Researcher
National School of Business and Management of Tangier (ENCG Tanger)
Abdelmalek Essaâdi University
Management, Economics, Information Systems and Law
Morocco

Date submitted : 30/09/2026

Date of acceptance : 11/11/2026

To cite this article :

BOUBOUH I. & GHANIM M. (2026) «Controlling Differently: Internal Control Digitalization as a Dynamic Capability. A Conceptual Framework and Research Propositions», Revue Internationale des Sciences de Gestion « Volume 9 : Numéro 4 » pp : 1172 - 1214

Abstract

The digitalization of internal control is widely presented as a lever of performance, yet the mechanisms behind this contribution remain unclear. This article argues that the dominant readings of the phenomenon, whether technical, compliance-based, or resource-based, share a common assumption: they treat digitalization as a state rather than as an ability, which prevents them from explaining why comparable tools produce different outcomes and why well-performing control systems become obsolete. Drawing on an integrative literature review and a theory adaptation approach, the article reinterprets internal control digitalization through dynamic capabilities theory. It distinguishes technological resources, operational capabilities, and dynamic capabilities, and defines internal control digitalization as a capability combining continuous risk sensing, deliberate response, and ongoing reconfiguration of the control system. This reinterpretation uncovers a tension between reconfiguration and the stability on which control reliability rests, and introduces the concept of reconfiguration governance, which is distinguished from IT change management and structured around five dimensions. Six propositions follow. The capability affects organizational performance mainly through two parallel and partial mediators, risk management effectiveness and internal control reliability, provided that data are of adequate quality and that automated controls remain under human oversight. Reconfiguration governance determines whether the capability strengthens or weakens control reliability, environmental dynamism moderates the relationship in an inverted U-shaped manner, and institutional pressures weaken it only when they lead to symbolic adoption. The article confronts these propositions with competing arguments, situates them in the Moroccan textile sector, and proposes an operationalization with a view to their empirical validation.

Keywords : internal control, digitalization, dynamic capabilities, reconfiguration governance, risk management, organizational performance, emerging economies.

Résumé

La digitalisation du contrôle interne est largement présentée comme un levier de performance, sans que les mécanismes de cette contribution soient clairement établis. Cet article soutient que les lectures dominantes du phénomène, qu'elles soient techniques, centrées sur la conformité ou fondées sur les ressources, partagent un présupposé commun : elles pensent la digitalisation comme un état et non comme une aptitude, ce qui les empêche d'expliquer pourquoi des outils comparables produisent des résultats différents et pourquoi des dispositifs performants deviennent obsolètes. À partir d'une revue intégrative de la littérature et d'une démarche d'adaptation théorique, l'article relit la digitalisation du contrôle interne à travers la théorie des capacités dynamiques. Il distingue les ressources technologiques, les capacités opérationnelles et les capacités dynamiques, et définit la digitalisation du contrôle interne comme une capacité articulant la détection continue des risques, la réponse délibérée et la reconfiguration permanente du dispositif. Cette relecture met au jour une tension entre la reconfiguration et la stabilité dont dépend la fiabilité du contrôle, et introduit le concept de gouvernance de la reconfiguration, distinct de la gestion des changements informatiques et structuré autour de cinq dimensions. Six propositions en découlent. La capacité agit sur la performance organisationnelle principalement à travers deux médiateurs parallèles et partiels, l'efficacité de la gestion des risques et la fiabilité du contrôle interne, à condition que les données soient de qualité suffisante et que les contrôles automatisés restent soumis à une supervision humaine. La gouvernance de la reconfiguration détermine si la capacité renforce ou fragilise la fiabilité du contrôle, le dynamisme de l'environnement modère la relation selon une forme en U inversé, et les pressions institutionnelles ne l'affaiblissent que lorsqu'elles conduisent à une adoption symbolique. L'article confronte ces propositions aux arguments concurrents, les situe dans le secteur textile marocain et propose une opérationnalisation en vue de leur validation empirique.

Mots clés : contrôle interne, digitalisation, capacités dynamiques, gouvernance de la reconfiguration, gestion des risques, performance organisationnelle, économies émergentes.

Introduction

Digital transformation has profoundly altered the conditions under which internal control operates. Internal control has long been conceived as a monitoring and compliance mechanism designed to provide reasonable assurance regarding the reliability of financial reporting, the effectiveness of operations, and compliance with laws and regulations. Since the revision of its framework (COSO, 2013), it has been organized around five components and seventeen principles. These components are now permeated by technologies that change their very nature: enterprise resource planning systems, robotic process automation, big data analytics, and artificial intelligence. Monitoring becomes continuous, controls become programmable, and information flows in real time.

This evolution fuels an implicit promise, widely shared by practitioners and software vendors: digitalizing control would improve organizational performance almost mechanically. The literature, however, calls for caution. Solow's (1987) observation that the computer age can be seen everywhere but in the productivity statistics opened a lasting debate on the productivity paradox of information technology (Brynjolfsson, 1993). Subsequent research has shown that the value of technology lies not in its mere acquisition but in its combination with complementary organizational resources and in the processes it transforms (Melville et al., 2004).

Contemporary debates on the transformation of control systems make this question more pressing. Research on information systems governance emphasizes that technology creates value only when its changes are steered and controlled (ISACA, 2018). Work on algorithmic control shows that digital technologies redistribute control within organizations and create new forms of oversight (Kellogg et al., 2020). Research on digital risks highlights the cybersecurity and data vulnerabilities that digitalization itself introduces (Haapamäki & Sihvonen, 2019). Finally, studies on the transformation of auditing practices document both the benefits of new technologies and the risks of excessive reliance on them (Commerford et al., 2022; Eulerich et al., 2023; Fedyk et al., 2022). Together, these debates suggest that the digitalization of control raises not only a question of tools but also a question of how organizations govern the evolution of their control systems.

Applied to internal control, this debate reveals a conceptual weakness. The digitalization of internal control is most often understood as a set of tools, that is, as a technical resource whose possession would confer an advantage, in line with the resource-based view (Barney, 1991). Such a reading remains static. It struggles to explain why two firms with comparable

tools achieve contrasting results, and it overlooks the organization's ability to adapt its control systems as risks, standards, and technologies change.

Dynamic capabilities theory offers a different perspective. Teece et al. (1997) define dynamic capabilities as the firm's ability to integrate, build, and reconfigure competences to address rapidly changing environments. Later refined through the microfoundations of sensing, seizing, and reconfiguring (Teece, 2007), they shift attention from what the firm owns to what it is able to transform. This shift in perspective, however, remains underexploited in internal control research. It would be all the more useful given that firms in emerging economies, facing strong competitive and institutional pressures, are digitalizing their control practices without a stable conceptual framework.

This article addresses this difficulty by asking the following question: **to what extent can the digitalization of internal control be conceptualized as a dynamic capability, and through which mechanisms does this capability contribute to organizational performance?** Three sub-questions follow. The first concerns the constitutive dimensions of internal control digitalization when viewed through the lens of dynamic capabilities. The second concerns the intermediate mechanisms through which this capability is converted into performance. The third concerns the contingency factors that condition this conversion.

The thesis defended here can be stated at the outset: the value of internal control digitalization lies not in the tools it mobilizes but in the ability it gives the control system to transform itself at the pace of its environment. This thesis challenges an assumption that is rarely made explicit in the literature, namely that digitalization is a state that firms reach by acquiring technology. It thus shifts the research question. The issue is no longer whether digital tools improve control, but under what conditions they provide the organization with a control system that learns and renews itself. Challenging an assumption shared by a field, rather than filling a simple gap, is indeed one of the most fruitful ways to generate research questions (Alvesson & Sandberg, 2011).

To answer this question, the article adopts a conceptual approach based on theory adaptation. After setting out this approach and the construction of the corpus, we delineate internal control from neighboring notions and show that existing readings of its digitalization rest on a common assumption that limits their explanatory power. We then present dynamic capabilities theory as our analytical lens, distinguish technological resources, operational capabilities, and dynamic capabilities, and reinterpret internal control digitalization through the microfoundations of sensing, seizing, and reconfiguring. This dialogue uncovers the

tension between reconfiguration and stability that characterizes control functions and leads to the concept of reconfiguration governance. It results in a conceptual framework with six research propositions, which we confront with competing arguments and situate in the context of emerging economies and of Morocco, before discussing their contributions, limitations, and avenues for empirical validation.

1. Methodological Approach

This article is a conceptual study. Unlike an empirical study, it does not draw on data collected in the field: its material is the literature itself, which is compared, connected, and extended in order to produce a new understanding of a phenomenon. As Gilson and Goldberg (2015) note, a conceptual article does not merely summarize the state of knowledge. It bridges previously disconnected theories or streams of research and proposes relationships that had not yet been formulated.

Of the four types of conceptual articles identified by Jaakkola (2020), namely theory synthesis, theory adaptation, typology, and model, our approach falls mainly within theory adaptation and results in a model. Theory adaptation involves revisiting a concept from a given domain using a theory external to that domain. Jaakkola (2020) accordingly distinguishes domain theory, which refers to the body of work on the object studied, from method theory, which provides the lens through which this object is reinterpreted. In our case, domain theory encompasses research on internal control, control systems, and their digitalization, while method theory is dynamic capabilities theory.

This approach relies on importing a theoretical perspective from outside the field of internal control. Such borrowing is one of the surest ways to renew a theory, because it forces a reexamination of assumptions that the host field had taken for granted (Whetten, 1989). The aim is therefore not to transpose a vocabulary but to show what the dynamic capabilities lens reveals about internal control that existing approaches had left out of view.

The corpus was built through an integrative literature review. This type of review is suited to conceptual work that seeks to combine perspectives and generate new frameworks rather than to map a field exhaustively (Snyder, 2019). Consistent with this purpose, the corpus was not assembled through a predefined keyword protocol but constructed iteratively, following the progression of the argument. The starting point was the foundational works of the two bodies of knowledge brought into dialogue: the reference frameworks of internal control and control systems (COSO, 2013; Simons, 1995) and the founding texts of dynamic capabilities theory (Teece et al., 1997; Teece, 2007; Winter, 2003). The corpus was then extended in two ways.

First, backward and forward snowballing from key works on the digitalization of control (Vasarhelyi et al., 2004; Warner & Wäger, 2019) made it possible to identify the main contributions in this stream. Second, targeted bibliographic searches were carried out to answer the specific questions raised at each stage of the argument, such as the delineation of internal control from neighboring notions, the risks associated with automation, or the testing of curvilinear moderation. Particular attention was paid to recent publications on the digitalization of control and auditing, so that the framework reflects the current state of the debate.

Three selection criteria guided this process. Works had to be peer-reviewed journal articles or reference books in accounting, information systems, or management; they had to contribute to the delineation of the concepts or to at least one of the three sub-questions (dimensions of the capability, mediating mechanisms, contingency factors); and they had to offer a conceptual or empirical grounding rather than a purely descriptive account. Professional frameworks issued by standard-setting bodies (COSO, the Institute of Internal Auditors, and ISACA) were retained as authoritative definitions. Synthesis was concept-centric: each work in the analyzed corpus was coded according to its research stream, its implicit assumption about the source of value of digitalized control, and the sub-question it informs. This coding underlies the comparison of existing readings presented in Table 2. Table 1 distinguishes the analyzed corpus, which comprises the works on which the theoretical argument rests, from the supporting references, which frame the research method, the avenues for empirical validation, and the Moroccan context.

Table N°1: Composition of the corpus by research stream

Research stream	Role in the argument	Works
Analyzed corpus		
Internal control, management control, and auditing frameworks	Defines the domain object and its boundaries	11
Digitalization of control, auditing, and accounting	Describes what technologies do to control and the risks they create	20
Dynamic capabilities, resource-based view, and IT business value	Provides the method theory and the link with performance	23
Organizational, institutional, and contingency theories	Grounds the moderators and the competing arguments	9
Subtotal		**63**
Supporting references		
Conceptual research and empirical validation methods	Frames the theorizing approach and the avenues for testing	15
Moroccan institutional and sectoral context	Situates the framework in the Moroccan textile sector	4

Research stream	Role in the argument	Works
Subtotal		**19**
Total		**82**

Source: Prepared by the author

Each work cited in the article is classified once, according to its main contribution to the argument.

The reasoning follows a logic of construction rather than review. A conceptual article is valued not for the number of studies it cites but for the coherence of the explanation it builds (Sutton & Staw, 1995). Each relationship in the framework is therefore justified by an explicit causal mechanism, with the literature serving to support this mechanism rather than to replace it. The figure summarizing the framework is accompanied by an account of the logic it represents, and the whole is organized around a single thesis, stated in the introduction, from which the propositions are derived. To avoid confirmation bias, the main arguments that could contradict the proposed relationships are examined explicitly in Section 5.3.

This choice explains the use of propositions rather than hypotheses. Propositions relate concepts, whereas hypotheses relate measures (Whetten, 1989). The propositions formulated here therefore do not summarize the literature. They state the implications of the theoretical argument and call for subsequent operationalization in the form of testable hypotheses.

Finally, the intended contribution is assessed against the criteria proposed by Whetten (1989), for whom a theoretical contribution must specify which concepts are involved, how they are related, why these relationships hold, and under what conditions they apply. These four questions structure the rest of the article: the clarification of the concept addresses the "what", the dialogue between the two theories the "why", the conceptual framework and propositions the "how", and the examination of contingency factors and boundary conditions the "under what conditions". In terms of the types of conceptual contribution described by MacInnis (2011), the article thus combines the explication of a concept with the delineation of relationships.

2. The Digitalization of Internal Control: A Concept in Search of Theoretical Foundations

2.1. Conceptual Boundaries: Internal Control, Management Control, Internal Audit, and Organizational Control Systems

Four notions are often used interchangeably in research on digitalization, although they do not cover the same scientific objects. A clear delineation is necessary to specify the object of this article.

Internal control, in the sense of the COSO (2013) framework, refers to the organization-wide process designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance. Its center of gravity is assurance: it aims to ensure that risks are identified and managed and that information is reliable.

Management control has a broader and more strategic purpose. It covers the set of mechanisms through which managers ensure that employees' behaviors and decisions are consistent with the organization's objectives and strategy, including planning, cybernetic, reward, administrative, and cultural controls (Malmi & Brown, 2008; Simons, 1995). Internal control overlaps with management control, notably through control activities and monitoring, but it focuses on assurance and risk rather than on strategy implementation and the steering of performance.

Internal audit is of a different nature. According to the Institute of Internal Auditors, it is an independent and objective assurance and advisory activity designed to add value and improve an organization's operations (IIA, 2024). Internal audit evaluates the internal control system; it does not execute it. Accordingly, the digitalization of auditing, such as continuous auditing, must be distinguished from the digitalization of internal control, such as continuous monitoring by management, even though both rely on similar technologies.

Organizational control systems, finally, is an umbrella term that encompasses the formal and informal mechanisms by which organizations direct behavior, of which internal control and management control are components (Malmi & Brown, 2008).

The object of this article is the internal control system in the sense of COSO (2013). Research on management control and on auditing is mobilized only insofar as its findings bear on the design, operation, or evolution of internal control. For instance, studies on continuous auditing are used to understand the continuous monitoring capabilities that digitalization makes available to management, and studies on enabling and coercive control are used to understand how rules can evolve without losing their authority. Throughout the article, the expression "control system" designates the internal control system unless otherwise specified.

2.2. From Traditional to Digitalized Internal Control

The COSO (2013) framework rests on five interrelated components: the control environment, risk assessment, control activities, information and communication, and monitoring activities. More broadly, management control research has shown that control systems do not serve only to constrain behavior. Simons (1995) thus distinguishes four levers, namely belief systems,

boundary systems, diagnostic control systems, and interactive control systems, whose combined use makes it possible both to control and to stimulate the organization.

Digitalization affects several of these components, first and foremost control and monitoring activities. Research on continuous auditing first showed that the automated analysis of transactional data enables a shift from periodic, retrospective control to near-permanent monitoring (Vasarhelyi et al., 2004). The rise of big data and analytics then broadened the scope of possible controls by allowing entire populations, rather than samples, to be examined (Appelbaum et al., 2017). More recently, robotic process automation has made it possible to delegate repetitive and highly structured control tasks to software (Moffitt et al., 2018). Artificial intelligence, for its part, paves the way for controls capable of detecting anomalies that predefined rules fail to identify (Kokina & Davenport, 2017).

Recent literature confirms the scale of this transformation while revealing its conceptual limitations. Management control research emphasizes that digitalization may disrupt both practices and the role of controllers (Fähndrich, 2023; Möller et al., 2020). It also blurs the very boundaries of the accounting function and alters power relations within the organization (Knudsen, 2020). Finally, it challenges the linear sequence long assumed between strategy, structure, and information systems design (Bhimani & Willcocks, 2014). In auditing and control, research now offers frameworks for the use of robotic process automation (Eulerich et al., 2022) and artificial intelligence (Leocádio et al., 2024; Wassie & Lakatos, 2024). Early empirical studies indicate that audit technologies improve task outcomes (Eulerich et al., 2023) and that artificial intelligence is associated with higher audit quality (Fedyk et al., 2022), while raising the question of how far professionals rely on these tools (Commerford et al., 2022). Digitalization is also transforming forms of accountability, including in the public sector (Agostino et al., 2022). These studies share a common feature: they describe precisely what technologies do to control, but rarely what the organization must be able to do for these technologies to create value over time. This is the shift this article seeks to make.

Building on this work, internal control digitalization can be provisionally defined as the integration of digital technologies into the components of the internal control system in order to automate, make continuous, and enrich through data analytics the activities of risk assessment, control, and monitoring. This provisional definition describes digitalization as a process of technological integration. Section 4 will distinguish it from the organizational capability to use these technologies to transform control routines durably.

2.3. Dominant Readings and Adjacent Research Streams

The coding of the corpus shows that studies on internal control digitalization can be grouped into three readings, according to the implicit assumption each makes about the source of value of digitalized control. Rather than describing these studies one by one, it is more useful to identify the assumption underlying each reading, because this assumption determines what the reading can explain and what it leaves unexplained.

The technical reading assumes that the value of digitalized control lies in the tool. It therefore focuses on describing technological features, implementation conditions, and the efficiency gains they provide, as does much of the research on continuous auditing, robotic process automation, and artificial intelligence. This reading explains well what the tool makes possible. It cannot, however, explain why the same tool produces different effects from one firm to another since, by design, it pays no attention to the organization that uses it.

The compliance reading assumes that the purpose of control is defensive: avoiding error, fraud, and sanctions. Digitalization is valued here because it closes loopholes and documents controls, in line with research identifying the organizational factors associated with internal control weaknesses (Doyle et al., 2007) and with research showing that weaknesses in information technology controls are associated with weaknesses in the other components of the control system (Klamm & Watson, 2009). This reading explains why firms digitalize their control. It cannot explain how such control would contribute to performance, since it measures success by the absence of problems rather than by value creation.

The resource-based reading assumes that digitalization is an asset whose possession confers an advantage. It draws on the resource-based view (Barney, 1991) and on research extending it to information technology (Bharadwaj, 2000; Wade & Hulland, 2004). From this perspective, Henri (2006) showed that control systems can contribute to the development of strategic capabilities. This reading is the closest to our purpose, since it already links control to performance. However, it reasons in terms of stocks: it explains why a scarce resource provides an advantage at a given moment, not how this advantage is sustained when the environment changes.

Four adjacent research streams must be examined to verify that this classification covers the main theoretical currents. Research on information systems governance, formalized in frameworks such as COBIT, addresses how organizations direct and control their use of information technology, including through the management of IT changes (ISACA, 2018). It shares with the compliance reading a concern for the integrity of systems, but it treats changes

as technical events to be authorized rather than as the exercise of a capability. Research on algorithmic control examines how digital technologies are used to direct, evaluate, and discipline workers (Kellogg et al., 2020). Its object is the control of people by algorithms, not the evolution of the internal control system itself. Research on digital risk management and cybersecurity documents the new vulnerabilities that digitalization creates (Haapamäki & Sihvonen, 2019); it extends the compliance reading to new categories of risk. Research on the transformation of auditing practices, finally, measures the effects of technologies on audit outcomes (Eulerich et al., 2023; Fedyk et al., 2022) and largely belongs to the technical reading. These streams therefore enrich the three readings without calling their structure into question: none of them takes the control system's ability to change as its object.

2.4. Convergences, Divergences, and Limitations of Existing Readings

Table 2 summarizes the comparison of the existing readings and adjacent streams. It makes their convergences, divergences, and blind spots explicit.

Table N°2: Convergences, divergences, and limitations of existing readings

Reading or stream	Assumed source of value	What it explains	What it leaves unexplained
Technical reading	The tool and its features	What technologies make possible (continuous monitoring, automation, analytics)	Why the same tool produces different effects across firms
Compliance reading	The avoidance of errors, fraud, and sanctions	Why firms digitalize their control	How digitalized control contributes to performance
Resource-based reading	The possession of scarce digital assets	Why control can support strategic capabilities	How the advantage is sustained when the environment changes
Information systems governance	The steering and control of IT changes	How IT changes are authorized and tested	How control rules themselves evolve and create value
Algorithmic control	The direction and evaluation of workers by algorithms	How digital tools redistribute control over people	How the internal control system adapts over time
Digital risk and cybersecurity	The protection of data and systems	Which new risks digitalization creates	How the organization learns from these risks to reconfigure its controls
Audit transformation	The improvement of audit outcomes through technology	The effects of technologies on audit quality and reliance	The capabilities management needs to make these effects last
Dynamic capabilities (this article)	**Organizational processes of sensing, seizing, and reconfiguring**	**Heterogeneity of outcomes and obsolescence of control systems**	**Requires measuring an ability rather than an outcome**

Source: Prepared by the author

The readings diverge on the purpose they assign to control: efficiency for the technical reading, protection for the compliance reading, and competitive advantage for the resource-

based reading. They nonetheless converge on one fundamental assumption: all of them view internal control digitalization as a state. For the first, it is a technical state; for the second, a state of compliance; for the third, a state of resource endowment. This shared assumption creates two blind spots, which can be framed as two anomalies.

The first anomaly concerns heterogeneity. Control technologies are, for the most part, available on the market; they therefore only imperfectly meet the criteria of rarity and inimitability on which the resource-based view rests. If two firms acquiring the same tools achieve different results, the difference cannot stem from the tools themselves. It necessarily stems from the way each organization combines and deploys them, as suggested by research showing that the value of technology depends on complementary resources and on the processes it transforms (Melville et al., 2004). Recent empirical studies confirm this: the effect of digital transformation on internal control quality varies with executive characteristics and ownership structure (Maqsood et al., 2024). However, a state-based reading has no concept with which to name this difference.

The second anomaly concerns obsolescence. Risks evolve, regulatory requirements change, and technologies are rapidly renewed. A digitalized control system that performs well today may thus become inadequate tomorrow, without any tool having been withdrawn. A state-based reading cannot account for this deterioration, since it does not take time into account.

Resolving these two anomalies requires a lens that conceives of internal control digitalization not as a state but as an ability, and that explicitly incorporates change. This is where dynamic capabilities theory offers a genuinely new explanation. It explains heterogeneity by locating value in organizational processes that are specific to each firm rather than in tools available to all. It explains obsolescence by making the capacity to reconfigure routines a distinct object of analysis. Finally, it specifies the conditions under which this capacity creates value, which none of the existing readings does.

3. Dynamic Capabilities as a Theoretical Lens

3.1. From Resources to Capabilities

Dynamic capabilities theory emerged from a question left unanswered by the resource-based view: how can a firm sustain an advantage when its environment changes? Teece et al. (1997) answer this question by defining dynamic capabilities as the firm's ability to integrate, build, and reconfigure internal and external competences to address rapidly changing environments. Advantage no longer rests solely on what the firm owns, but on its ability to renew what it owns.

This perspective introduces an essential distinction between two levels of capability. Winter (2003) contrasts ordinary capabilities, which allow the firm to operate on a day-to-day basis, with higher-order capabilities, which act on the former in order to change them. Helfat et al. (2007) extend this idea by defining a dynamic capability as the capacity of an organization to purposefully create, extend, or modify its resource base. Internal control, in its routine form, clearly belongs to ordinary capabilities. The question then becomes whether its digitalization can give it a higher-order dimension.

The theoretical debate has also addressed the nature of these capabilities. For Eisenhardt and Martin (2000), dynamic capabilities are not abstract entities but identifiable and specific processes, such as product development or strategic alliances, which display commonalities across firms. Zollo and Winter (2002), for their part, show that these capabilities arise from learning mechanisms, namely experience accumulation, knowledge articulation, and knowledge codification, which allow the organization to evolve its operating routines. This contribution is particularly valuable for our purpose, since internal control is itself a set of codified routines.

The rise of the theory has, however, been accompanied by serious criticism, which any rigorous use of the theory must address. The most important concerns the risk of tautology: if a capability is identified by the fact that it produces performance, claiming that it explains performance amounts to explaining nothing (Arend & Bromiley, 2009; Priem & Butler, 2001). The most comprehensive reviews show that the field has gradually responded to this criticism by defining capabilities by their constituent processes rather than by their effects (Barreto, 2010; Schilke et al., 2018). It has also specified the conditions under which they create value. More recently, Helfat et al. (2023) have called for a renewal of the resource-based view that takes new contexts, including digital ones, into account. These two requirements, namely defining capabilities by their processes and specifying the conditions under which they create value, guide the construction of the framework proposed here.

3.2. Microfoundations: Sensing, Seizing, and Reconfiguring

Teece (2007) gave the theory an operational structure by breaking dynamic capabilities down into three clusters of microfoundations. Sensing refers to the capacity to identify and interpret opportunities and threats in the environment. Seizing refers to the capacity to mobilize resources to address these opportunities or neutralize these threats through appropriate decisions and investments. Reconfiguring, finally, refers to the capacity to recombine and

transform the firm's assets and structures in order to maintain its fit with a changing environment.

This decomposition has recently been applied to digital transformation. Warner and Wäger (2019) show that firms engaged in such a transformation develop specifically digital sensing, seizing, and transforming capabilities, and that this development is an ongoing process of strategic renewal rather than a one-off change. Similarly, Vial (2019) emphasizes that digital transformation is not limited to the adoption of technologies but involves structural changes and strategic responses on the part of the organization. Ellström et al. (2022), for their part, identify specific sensing, seizing, and reconfiguring routines that support digital transformation, while Kraus et al. (2022) document the rapid growth of management research devoted to this transformation.

3.3. Why This Lens Suits Digitalized Internal Control

Three reasons justify using dynamic capabilities to reinterpret internal control digitalization, and each points to a contribution that the resource-based view alone does not provide.

The first relates to the control environment. Dynamic capabilities were conceived for turbulent contexts. Internal control now operates in an environment where risks are constantly renewed, notably digital and fraud risks, where standards change, and where technologies themselves quickly become obsolete. Whereas the resource-based view reasons about stable assets, dynamic capabilities explicitly incorporate change.

The second relates to the nature of the tools. As noted above, control technologies are widely available and imitable. Dynamic capabilities theory makes it possible to shift the source of advantage from the tools to the organizational processes that deploy and adapt them, processes that are specific to each firm and difficult to replicate.

The third relates to the affinity between control and capabilities. Internal control is inherently a sensing mechanism, since it identifies and assesses risks, and a response mechanism, since it implements activities to manage them. Its structure thus echoes the microfoundations proposed by Teece (2007). What traditional internal control lacks is the third dimension, namely reconfiguration. Our argument is that digitalization, when conceived as a capability, provides this dimension.

Finally, the choice of this lens must be justified against the available alternatives. Agency theory, the most widely used in internal control research, views control as a mechanism for reducing information asymmetries between principals and agents (Jensen & Meckling, 1976). It explains why organizations control, but not how their control systems evolve. Sociomaterial

approaches, which focus on the entanglement of technologies and work practices (Orlikowski, 2007), describe these transformations in fine detail but are poorly suited to formulating relationships with performance. Organizational learning theory is closer to our purpose. It is, however, embedded in dynamic capabilities theory, which treats learning as one of its generative mechanisms (Zollo & Winter, 2002). Only dynamic capabilities theory connects, within a single framework, changes in the control system and their consequences for performance, which justifies retaining it as our main lens.

4. Reconceptualizing Internal Control Digitalization as a Dynamic Capability

This section constitutes the core of our contribution. It reinterprets the literature on digitalized internal control through the three microfoundations proposed by Teece (2007). The aim is not to impose a new vocabulary on existing practices but to show that digitalization can transform the very nature of control, moving it from the status of an ordinary routine to that of a higher-order capability in the sense of Winter (2003). Before this reinterpretation, it is necessary to specify what distinguishes a dynamic capability from the technologies and routines it relies on.

4.1. Technological Resources, Operational Capabilities, and Dynamic Capabilities

Three levels must be distinguished. Technological resources are the assets the firm owns or rents: an enterprise resource planning system, a software robot, an analytics platform, or a machine learning model. Operational capabilities are the routines through which the firm uses these resources to perform its current activities; they allow it to make a living in the present (Helfat & Winter, 2011; Winter, 2003). Dynamic capabilities, finally, are the capabilities that act on the resource base and on operational routines in order to change them (Helfat et al., 2007).

An example drawn from robotic process automation illustrates these three levels. A software robot that matches purchase orders, receipts, and invoices is a technological resource. When the organization uses this robot to apply the three-way match to all supplier invoices every day, it exercises an operational capability: the control is executed more completely and more consistently than before, but its rules remain the same. The organization exercises a dynamic capability when it is able to detect that a new fraud pattern, such as fictitious suppliers created in small amounts, escapes the existing rule, to decide to modify the control and allocate the necessary resources, and then to redesign the rule, test it, and redeploy the robot. The technology is identical in all three cases. What differs is the object on which the organization acts: the transaction in the first two cases, the control routine itself in the third.

This distinction provides the criterion for qualifying a digitalized control system as a dynamic capability. The criterion lies in the object on which it acts: an operational capability executes routines, whereas a dynamic capability modifies them (Winter, 2003). Software that automates an existing control without ever changing its rules therefore belongs to operational capabilities, however sophisticated it may be. It becomes constitutive of a dynamic capability only when it enables the organization to evolve its own control routines. As Helfat and Winter (2011) note, the boundary between the two types of capabilities is not always sharp, since the same activity can contribute to both. For this reason, the framework does not classify tools or activities but the organizational processes through which control routines are questioned and revised.

The number of dimensions retained must also be justified. Why three, and why these? Because they describe the three necessary moments of any adaptation: perceiving a change, deciding how to respond to it, and then durably transforming the system. Each is indispensable, since the absence of any one of them breaks the cycle. Sensing without seizing produces alerts that lead to no decision. Seizing without sensing acts blindly. Sensing and seizing without reconfiguring produce effective control that is nonetheless doomed to obsolescence, since it handles each anomaly without ever learning from their succession. These three dimensions are also sufficient to account for adaptation, which justifies not adding others and preserving the parsimony of the framework.

4.2. The Sensing Capability: From Periodic Control to Continuous Monitoring

In its traditional form, internal control detects anomalies late. Checks occur at regular intervals and on samples, and irregularities are often discovered after they have produced their effects. Digitalization profoundly changes this temporality. Continuous monitoring systems enable permanent analytical surveillance of transactions (Vasarhelyi et al., 2004), and big data analytics make it possible to examine entire populations rather than mere samples (Appelbaum et al., 2017).

Viewed through the lens of dynamic capabilities, this evolution is more than a gain in speed. It gives the organization a genuine ability to perceive weak signals in its risk environment: process drifts, atypical behaviors, and emerging forms of fraud. Control ceases to be a mere safety net and becomes a listening device for the organization and its environment. Sensing, however, is not limited to the volume of data monitored. It also includes the ability to interpret signals, to distinguish a genuine anomaly from statistical noise, and to recognize

when the risk map itself no longer reflects the organization's exposures. We refer to this dimension as the digital sensing capability of control.

4.3. The Seizing Capability: From Delayed Reaction to Deliberate Response

Sensing is not enough; the organization must also decide and act. In Teece's (2007) formulation, seizing is not a mechanical reaction: it consists of making decisions under uncertainty, choosing among alternative responses, committing resources, and avoiding the decision biases that lead organizations to persist with obsolete solutions. Applied to internal control, this microfoundation covers three types of decisions.

The first concerns the response to alerts. In the traditional model, the response to anomalies relies on an often slow chain of human intervention: reporting, analysis, decision, and corrective action. Digitalization shortens this chain. Robotic process automation makes it possible to execute repetitive controls systematically and to trigger predefined responses (Moffitt et al., 2018), and artificial intelligence makes it possible to handle less structured situations and to inform controllers' decisions (Kokina & Davenport, 2017).

The second concerns the trade-off between the cost of control and the level of residual risk. Not every detected risk justifies a new control. The organization must decide which risks to accept, which controls to automate, which to keep manual, and which to remove because they have become redundant. Digitalization makes this trade-off more explicit, since automated controls generate data on their own cost, their alert rates, and their effectiveness.

The third concerns investment and commitment. Responding to an emerging risk may require acquiring a new analytical module, training controllers, or redesigning a process. These choices commit resources over time and involve the arbitration of top management. Digitalized control frees controllers from repetitive tasks and allows them to focus their expertise on high-stakes situations, but it also requires the organization to decide where this expertise should be directed. We refer to this dimension as the digital seizing capability of control: the organization's ability to turn risk information into decisions about responses, trade-offs, and investments.

4.4. The Reconfiguring Capability: From Fixed to Evolving Control Systems

It is on the third microfoundation that the proposed reinterpretation contributes the most. A traditional internal control system evolves slowly: revising procedures, updating risk matrices, or adapting to new regulatory requirements demands significant effort and often extends over long periods. Control thus lags behind the risks it is supposed to manage.

Digitalization makes the control system itself reconfigurable. Parameterizable control rules can be modified without overhauling procedures, analytical models can be retrained when behaviors change, and the data accumulated through controls feed continuous organizational learning. This process reflects the mechanisms of experience accumulation, knowledge articulation, and knowledge codification that Zollo and Winter (2002) identify as the origins of dynamic capabilities. In Simons's (1995) terms, digitalized control can thus combine diagnostic and interactive use: it monitors deviations while fostering strategic dialogue on emerging uncertainties. We call this dimension the digital reconfiguring capability of control.

4.5. Toward an Integrative Definition

This reinterpretation makes it possible to move beyond the provisional definition put forward in Section 2.2. We propose to define internal control digitalization, as a capability, as the organization's ability to mobilize digital technologies to continuously sense risks, decide on and implement targeted responses, and continually reconfigure its control system as its environment evolves.

This definition has three characteristics. First, it is organizational rather than technical: technologies are a means, and the capability is the object. Second, it is dynamic: it explicitly includes the system's ability to transform itself. Third, it is multidimensional, since it combines sensing, seizing, and reconfiguring. Two firms with the same tools may therefore display very different levels of capability, which helps to explain the heterogeneity of outcomes observed in digitalization.

This definition was constructed so as to avoid the charge of tautology leveled at dynamic capabilities. It does not define the capability by its outcomes but by three processes that can be observed independently of any performance measure: continuous risk monitoring, the conversion of alerts into decisions and actions, and the revision of control rules. It thus becomes possible for a firm to have a strong internal control digitalization capability without deriving any benefit from it, for instance because its environment is stable or because reconfiguration is poorly governed. Far from being a weakness, this possibility is precisely what makes the framework falsifiable.

4.6. Founding Assumptions of the Framework

The proposed reconceptualization rests on three assumptions that must be made explicit, because they are what link the concepts together and allow the reasonableness of the framework to be judged (Whetten, 1989).

The first assumption is competitive. Because control technologies are widely available on the market, they cannot in themselves constitute a durable source of differentiation. Their value depends on the organizational processes that deploy them, processes that, unlike tools, are rooted in each firm's history and routines.

The second assumption is environmental. The risk environment to which internal control must respond is not stable: threats change, regulatory requirements evolve, and technologies themselves age rapidly. A fixed control system therefore gradually loses its fit, whatever its initial quality.

The third assumption is organizational. Internal control is a set of codified routines, and any routine can be modified through deliberate learning mechanisms (Zollo & Winter, 2002). By producing systematic traces of control activity, digitalization multiplies the opportunities for such learning.

From these three assumptions follows the thesis stated in the introduction: the value of internal control digitalization lies not in the tools it mobilizes but in the ability it gives the control system to transform itself at the pace of its environment. The first assumption rules out the tool as a source of value, the second makes transformation necessary, and the third makes it possible. The propositions presented in Section 5 are the implications of this thesis.

4.7. A Constitutive Tension: Reconfiguring Without Destabilizing

The thesis defended here nonetheless raises a difficulty that dynamic capabilities theory, designed for exploration functions such as innovation or alliances, has rarely had to confront. Internal control derives its value from its stability. A control is useful only if its rules are known, consistently applied, and verifiable after the fact; it is this consistency that makes it possible to compare periods, detect deviations, and provide assurance to third parties. However, the reconfiguring capability, by definition, involves modifying these rules. The more the system transforms itself, the more it risks losing its raison d'être. There is thus a constitutive tension: control must change to remain relevant, but every change threatens its reliability.

This tension is far from abstract. Automated systems themselves become objects of control: a software robot whose rules are modified without traceability, validation, or segregation of duties creates new risks at the very heart of the system meant to manage them. This is why recent research has formulated internal control and governance principles specific to robotic process automation (Eulerich et al., 2024). Digitalized control must itself be controlled in its capacity to change.

Control systems research offers two foundations for thinking about this tension. Adler and Borys (1996) showed that formalization is not inherently constraining or enabling: it is enabling when rules are transparent, understandable to those who use them, and repairable by them, and coercive when rules are opaque and imposed. Mundy (2010), for her part, showed that organizations derive distinctive capabilities not from the dominance of one use of control over the other, but from a balance between controlling and enabling uses, a balance that generates productive dynamic tensions. Applied to internal control, these studies suggest that control reconfiguration creates value when it is itself governed. Insufficient reconfiguration condemns control to obsolescence, whereas ungoverned reconfiguration condemns it to instability. The following subsection defines the concept that makes it possible to steer between these two pitfalls.

4.8. Reconfiguration Governance: Definition and Distinctiveness

We define reconfiguration governance as the set of rules, roles, and procedures through which an organization frames the modification of its control routines, so that the control system can change without losing the consistency and verifiability on which its reliability rests. Its object is not information technology in general but the logic of control itself: control rules and thresholds, the parameters of automated controls, the analytical models that generate alerts, and the scope of populations tested.

This concept must be distinguished from two neighboring notions. The first is IT change management. Frameworks such as COBIT include a process dedicated to managing IT changes, which aims to ensure that changes to systems are authorized, tested, and implemented without disrupting operations (ISACA, 2018). Research has also shown that weaknesses in information technology controls are associated with weaknesses in the other components of internal control (Klamm & Watson, 2009). Reconfiguration governance draws on these practices but differs from them in three respects. Its object is the business logic of control rather than the technical infrastructure; a threshold change in an anomaly detection model may involve no change to the software at all. Its criterion is the preservation of assurance, that is, the comparability and auditability of controls over time, rather than the availability and integrity of systems. Its actors are control owners, risk managers, and internal auditors rather than IT teams alone.

The second neighboring notion is information systems governance. This concerns the way the board and top management direct and evaluate the use of information technology as a whole, in particular investment priorities and alignment with strategy (ISACA, 2018).

Reconfiguration governance operates at a more specific level: it concerns how the control system modifies itself once the technological choices have been made.

Reconfiguration governance is treated in this framework as a moderator rather than as a fourth dimension of the capability, for three reasons. First, it does not take part in the adaptation cycle: it neither senses, decides, nor transforms, but frames the way transformation is carried out. Second, it is empirically separable from the capability. A firm may have strict governance and a weak reconfiguring capability, for example when it rarely changes its controls but documents every change carefully. Conversely, a firm may reconfigure intensively without any governance. Third, its theoretical role is not to add to the capability's effect but to determine its direction: the same reconfiguring capability can strengthen or weaken control reliability depending on whether it is governed. This conditional role is precisely what a moderator represents. Table 3 sets out the five dimensions of reconfiguration governance retained in this article.

Table N°3: Dimensions of reconfiguration governance

Dimension	Content	Illustrative practices
Governance of rule modifications	Defines who may propose and decide changes to control rules, thresholds, and models, and on what grounds	Formal change policy; register of change requests; criteria specifying when a rule must be reviewed
Validation and authorization	Requires that new or modified rules be tested before deployment and approved by an authority independent of the requester	Parallel testing of old and new rules; sign-off by the control owner and the risk function
Traceability and documentation	Records each version of rules, parameters, and models, together with its rationale and effective date	Version control of control rules; change logs accessible to internal and external auditors
Segregation of duties	Separates those who design or modify controls from those whose activities are controlled and from those who validate changes	Restricted access rights to robot and model configuration; independent review of changes
Human supervision of automated controls	Ensures that qualified staff periodically review the outputs of automated controls and can override them	Review of alert rates and false positives; periodic performance reports on automated controls; escalation procedures

Source: Prepared by the author

This concept enriches the article's thesis: the value of control digitalization lies in its ability to transform itself, provided that this transformation is itself controlled.

5. Conceptual Framework and Research Propositions

5.1. Overview of the Framework

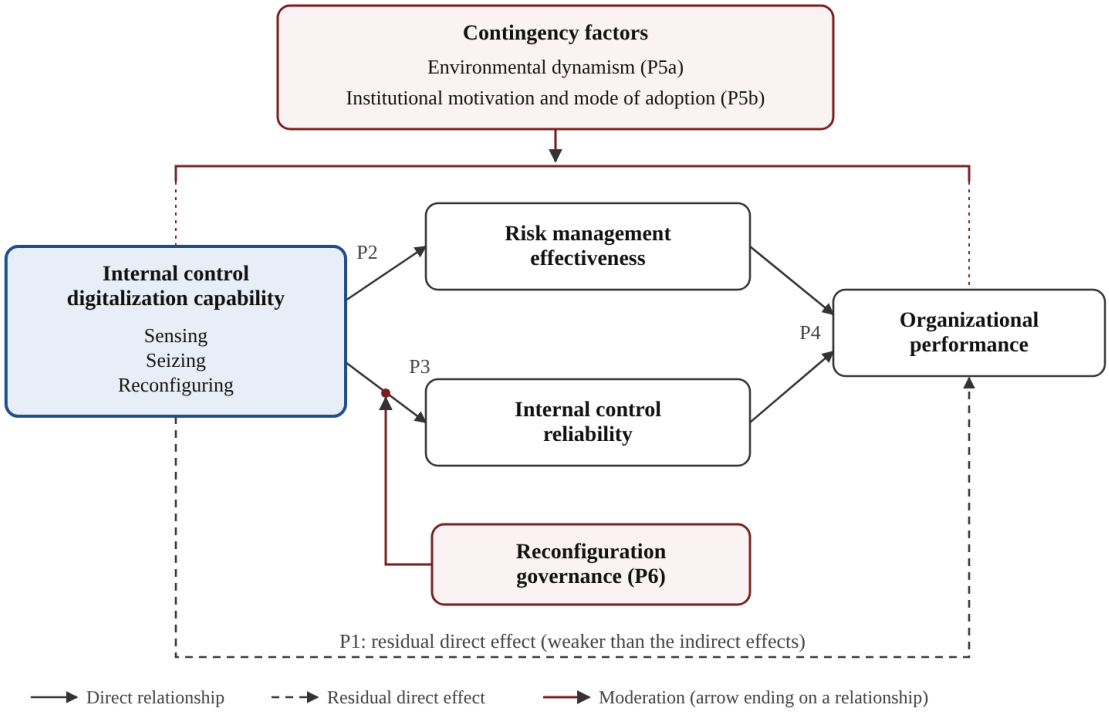
The proposed conceptual framework comprises five blocks. The first is the internal control digitalization capability, captured through its three dimensions of sensing, seizing, and reconfiguring. The second comprises two intermediate mechanisms, risk management

effectiveness and internal control reliability, through which this capability produces most of its effects. The third is organizational performance, understood in a multidimensional sense that covers both financial and non-financial outcomes. The fourth is reconfiguration governance, an internal condition that determines whether the transformation of the system strengthens or weakens its reliability. The fifth comprises the external contingency factors that condition the relationship as a whole.

The logic of the framework rests on a simple principle: the internal control digitalization capability acts on performance mainly by transforming the quality of risk management and control, which in turn conditions performance. This architecture is in line with models of IT business value, which show that technologies create value through the processes they transform (Melville et al., 2004).

The choice of these two mediators reflects the same concern for parsimony. Internal control pursues two main purposes: managing the risks that affect operations and ensuring the reliability of information and control systems (COSO, 2013). If the digitalization capability contributes to performance, it must do so mainly by improving one or the other of these purposes. Other channels, such as innovation or strategic learning, could be considered, but they are not specific to internal control and belong to other functions of the firm; including them would make the framework heavier without strengthening its logic.

Figure N°1: Conceptual framework of internal control digitalization as a dynamic capability



Source: Prepared by the author

Figure 1 reads from left to right as a causal chain. The solid arrows leaving the capability indicate what it transforms first, namely risk management effectiveness (P2) and internal control reliability (P3). The two arrows reaching performance indicate the two parallel channels through which these transformations become value (P4). The dashed line linking the capability directly to performance represents a residual direct effect, which is expected to be weaker than the indirect effect (P1). The moderators are represented by arrows that end on relationships rather than on variables. The contingency factors, placed above, point to a bracket that spans the relationship between the capability and performance as a whole: environmental dynamism (P5a) and institutional motivation combined with the mode of adoption (P5b) condition the strength of this relationship. Reconfiguration governance, placed below, points to the arrow linking the capability to internal control reliability (P6): it conditions the direction of this specific relationship. The figure, however, merely represents the logic of the framework; each relationship is justified by the argument that follows.

5.2. Research Propositions

The following propositions are derived from the thesis stated in Section 4.6. For each one, we first set out the causal mechanism on which it rests, that is, the reason why the relationship

should be observed, before specifying its grounding in the literature and its conditions of validity.

Why would the digitalization capability act on performance mainly indirectly? Because a dynamic capability does not itself produce value: it acts on the organization's operational capabilities, which are the actual producers of value (Helfat et al., 2007; Winter, 2003). Digitalized control neither manufactures nor sells; it changes the way the firm identifies and manages what threatens its operations. Its influence on performance therefore mainly takes a detour through the processes it transforms. A residual direct effect cannot, however, be ruled out. Automating control tasks reduces their labor cost and frees time that can be redeployed to other activities, which may improve efficiency independently of any change in risk management or control reliability. The framework therefore posits partial mediation, in which both indirect and direct effects exist and point in the same direction, which Zhao et al. (2010) call complementary mediation, while predicting that the indirect path dominates. This reasoning also sheds light on the productivity paradox (Brynjolfsson, 1993; Solow, 1987) as applied to control: if the direct effects of technological investment appear weak, it is because most of the value is formed elsewhere.

Proposition 1: The internal control digitalization capability contributes to organizational performance mainly through an indirect path; its direct effect, limited to residual gains such as labor savings on control tasks, is expected to be positive but weaker than its indirect effect (partial mediation with a dominant indirect path).

The mechanism through which the capability improves risk management is informational and temporal. The earlier and more comprehensively a risk is identified, the better it can be managed. Continuous monitoring reduces the time between the occurrence of an anomaly and its detection, while exhaustive data analysis reduces the share of risks that escape scrutiny (Appelbaum et al., 2017; Vasarhelyi et al., 2004). The reconfiguring capability adds a third dimension: by continuously adjusting control parameters, it prevents the risk map from freezing while the environment evolves. Risk assessment, a central component of the system according to COSO (2013), thus becomes more timely, comprehensive, and up to date.

This mechanism nevertheless has two conditions. The first is data quality. An automated control is only as good as the data it processes: incomplete, poorly coded, or inconsistent data produce false alerts or, worse, conceal real anomalies. The second is human judgment. Continuous monitoring generates a large volume of alerts, many of which are false positives. When the volume of alerts exceeds the capacity of controllers to examine them, attention

declines and genuine signals are lost among irrelevant ones, a phenomenon commonly referred to as alert fatigue. Research on human interaction with automation further shows that operators tend to over-rely on automated aids, failing to question their outputs or to look for information the system does not provide (Parasuraman & Manzey, 2010). Evidence from auditing points in the same direction, since professionals' reliance on artificial intelligence varies with the nature of the estimates involved (Commerford et al., 2022). The sensing capability therefore improves risk management only if alerts are calibrated and subjected to qualified human judgment.

Proposition 2: The internal control digitalization capability enhances the effectiveness of the organization's risk management, provided that the data feeding the controls are of adequate quality and that the alerts generated are subject to qualified human judgment.

The effect of the capability on control reliability rests on a different mechanism, namely the reduction of variability. A manually performed control depends on the attention, workload, and judgment of the person performing it; its quality therefore varies from one transaction to another. Automation eliminates much of this variability by applying the same rule to all transactions and keeping a record of each control (Moffitt et al., 2018). It thus reduces the conditions that foster internal control weaknesses, which research has shown to be concentrated in complex or rapidly growing organizations (Doyle et al., 2007). At the same time, the seizing capability frees controllers from repetitive tasks, so that human judgment, a scarce resource, is focused on the situations where it adds the most value (Kokina & Davenport, 2017).

This effect is not unconditional. Automation replaces random human errors with systematic errors: a poorly designed rule is applied with the same consistency as a well-designed one, so that a single design flaw affects every transaction. Digitalization also creates new vulnerabilities, including errors in algorithms, failures in data flows, cyber risks affecting the control tools themselves (Haapamäki & Sihvonen, 2019), dependence on software vendors, and insufficient human supervision of automated controls. Whether the net effect on reliability is positive therefore depends on the quality of design, supervision, and governance of automated controls. This condition is the subject of Proposition 6.

Proposition 3: The internal control digitalization capability improves the reliability and quality of the internal control system when automated controls are adequately designed, supervised, and governed; otherwise, it may create new vulnerabilities, such as algorithmic errors, data failures, cyber risks, technological dependence, or insufficient human oversight.

While Propositions 2 and 3 describe what the digitalization capability transforms, Proposition 4 explains how these transformations become performance. More effective risk management avoids losses, secures business continuity, and allows management to make better-informed decisions about risky commitments. More reliable control improves the quality of management information and strengthens the confidence of partners, customers, and buyers. In both cases, performance results not from technology itself but from the process improvements it has made possible, in line with the IT business value model proposed by Melville et al. (2004). Henri (2006) similarly showed that the influence of control systems on performance operates through the organizational capabilities they help to develop.

The two mediators are conceived as parallel rather than sequential. Each corresponds to a distinct purpose of internal control and to a distinct channel of value creation: risk management protects operations, whereas control reliability secures information and the confidence of stakeholders. The framework does not assume that one mediator causes the other, even though the two are likely to be correlated. Combined with Proposition 1, this specification implies parallel partial mediation: each mediator carries a specific indirect effect, and the capability retains a residual direct effect. Empirically, it calls for a parallel multiple mediator model in which the specific indirect effects are estimated separately and tested by bootstrapping (Preacher & Hayes, 2008).

Proposition 4: Risk management effectiveness and internal control reliability act as two parallel, partial mediators of the relationship between the internal control digitalization capability and organizational performance.

The value of the capability also depends on the environment in which it is exercised. Every dynamic capability has a cost, since it consumes resources to maintain an ability to change. This cost is justified only if the environment actually requires change: in a stable environment, a highly reconfigurable control system adds little to a well-designed routine one. This logic of fit lies at the heart of contingency theory (Donaldson, 2001), whose relevance to control systems has been demonstrated by Chenhall (2003). It must nevertheless be qualified. Schilke (2014) showed that the value of dynamic capabilities is greatest in moderately dynamic environments and declines when dynamism becomes extreme. This nonlinearity takes on particular significance for internal control: in a highly turbulent environment, the permanent reconfiguration it would require would conflict with the stability on which its reliability depends, which echoes the tension analyzed in Section 4.7.

Proposition 5a: Environmental dynamism moderates the relationship between the internal control digitalization capability and organizational performance in an inverted U-shaped manner: the relationship becomes stronger as dynamism rises from low to moderate levels and weakens when dynamism becomes extreme.

Proposition 5a describes a curvilinear moderation, that is, a moderating effect that varies nonlinearly with the level of the moderator. Following Haans et al. (2016) and Schilke (2014), it can be specified as follows, where Perf denotes organizational performance, C the internal control digitalization capability, D environmental dynamism, and ε the error term, with C and D mean-centered:

$$Perf = \beta 0 + \beta 1C + \beta 2D + \beta 3D^2 + \beta 4(C \times D) + \beta 5(C \times D^2) + \varepsilon$$

In this specification, the effect of the capability on performance is given by $\beta 1 + \beta 4D + \beta 5D^2$. Proposition 5a is supported if $\beta 4 > 0$ and $\beta 5 < 0$, which means that this effect first increases and then decreases with dynamism. The effect of the capability reaches its maximum at the level of dynamism $D^* = -\beta 4 / (2\beta 5)$. Two additional conditions must be checked for the inverted U-shape to be established (Haans et al., 2016): the turning point D* must lie within the observed range of dynamism, and the slope of the capability's effect must be significantly positive at low levels of dynamism and significantly negative at high levels.

Institutional pressures introduce a second source of variation, of a different nature. Firms may digitalize their control to comply with buyer requirements, imitate competitors, or follow professional standards (DiMaggio & Powell, 1983). Such pressures are not harmful in themselves: a buyer audit can push a firm to build genuine monitoring routines it would not otherwise have developed. Institutional motivation, which refers to the weight of these external pressures in the decision to digitalize, must therefore be distinguished from internal motivations such as efficiency or risk reduction. The two are not mutually exclusive, since a firm may respond to buyer or regulatory requirements while pursuing its own control objectives. What matters is the way these pressures are translated into practice. Meyer and Rowan (1977) showed that organizations often adopt formal structures for the legitimacy they confer and then decouple them from their actual activities. Bromley and Powell (2012) refine this analysis by distinguishing policy-practice decoupling, where adopted structures are not implemented, from means-ends decoupling, where they are implemented but without a demonstrated link to the goals they are supposed to serve.

Three modes of adoption can therefore be distinguished. Symbolic adoption corresponds to decoupling: the tools are in place and the reports exist, but the processes of sensing, seizing, and reconfiguring do not develop. Substantive adoption corresponds to the effective integration of tools into control routines. Appropriation, finally, refers to the way users actively adapt the tools to their practices; adaptive structuration theory shows that the same technology can be appropriated faithfully, in line with its intended purpose, or in ways that diverge from it (DeSanctis & Poole, 1994). Institutional pressures therefore weaken the relationship between the capability and performance only when they lead to symbolic adoption; when they are translated into substantive adoption and faithful appropriation, they may even reinforce it.

Proposition 5b: Institutional motivation and the mode of adoption jointly moderate the relationship between the internal control digitalization capability and organizational performance: this relationship is weakened when institutional pressures lead to symbolic adoption decoupled from control practices, and it is preserved or strengthened when they lead to substantive adoption and faithful appropriation of the tools.

Section 4.7 showed that the reconfiguring capability is a double-edged sword, and Section 4.8 defined the governance that conditions its effects. When changes to control rules are governed through the five dimensions set out in Table 3, reconfiguration maintains the relevance of the system without compromising its consistency; control remains enabling in the sense of Adler and Borys (1996). When these changes escape any oversight, each change creates an area of uncertainty: the rules applied yesterday are no longer those applied today, comparability is lost, and the new vulnerabilities identified in Proposition 3 emerge within the control tools themselves (Eulerich et al., 2024). Reconfiguration governance therefore determines the direction of the capability's contribution to control reliability and, through it, to performance. Propositions 3 and 6 are thus two sides of the same argument: Proposition 3 states that the effect of the capability on reliability is conditional, and Proposition 6 specifies the organizational variable on which this condition depends.

Proposition 6: Reconfiguration governance, through the governance of rule modifications, the validation and authorization of changes, their traceability and documentation, the segregation of duties, and the human supervision of automated controls, moderates the relationship between the internal control digitalization capability and internal control reliability; this relationship is positive when reconfiguration is governed and weakens, or even reverses, when it is not.

Propositions 5a and 6 both draw on the tension between change and stability, but at two distinct levels. Proposition 5a concerns the external environment: it indicates when reconfiguration is useful, depending on the intensity of change the environment imposes. Proposition 6 concerns the organization itself: it indicates how reconfiguration should be conducted so as not to compromise control reliability. The former thus concerns the demand for change, the latter the way of responding to it. They rest on different variables and can be tested separately.

5.3. Competing Arguments and Alternative Explanations

A conceptual framework gains credibility when it confronts the arguments that could contradict it. Five such arguments deserve attention, together with the evidence that would allow them to be distinguished from the relationships proposed here.

The first argument holds that automation may reduce rather than improve reliability. Automated controls replicate design errors across all transactions, and users tend to trust them excessively (Parasuraman & Manzey, 2010). This argument is not rejected by the framework but incorporated into it: Propositions 3 and 6 posit that the effect of the capability on reliability is conditional on design, supervision, and governance. The framework would be contradicted if well-governed digitalized control systems displayed no greater reliability than manual ones.

The second argument concerns reverse causality. High-performing firms have more slack resources and may therefore be the ones that invest in digitalized control. The observed association between capability and performance would then reflect the effect of performance on the capability rather than the reverse. This argument cannot be ruled out conceptually, which is why Section 6.3 recommends longitudinal designs in which the capability is measured before the mediators and performance, and in which cross-lagged effects in both directions are estimated.

The third argument holds that digitalization may be purely ceremonial. If firms digitalize only to display compliance, the capability described here would never develop, and any observed relationship with performance would be spurious. The framework addresses this argument through Proposition 5b, which makes the mode of adoption an explicit moderator, and through the definition of the capability by observable processes rather than by the presence of tools.

The fourth argument holds that dynamic capabilities are superfluous in stable environments, where well-designed routines are sufficient. The framework accepts this argument, which is

consistent with the lower part of the inverted U-shaped relationship in Proposition 5a. It would be contradicted, however, if the capability's effect did not vary with environmental dynamism at all.

The fifth argument draws on agency theory. From this perspective, digitalized control is primarily a surveillance device that reduces information asymmetries but also increases monitoring intensity, reduces employees' autonomy, and may provoke resistance or gaming. Research on algorithmic control documents such reactions (Kellogg et al., 2020). If this effect dominated, digitalization would improve compliance without improving performance, or even at its expense. The framework does not deny this possibility. It suggests that the outcome depends on whether control remains enabling or becomes coercive (Adler & Borys, 1996), a distinction that reconfiguration governance helps to preserve by making rules transparent and their changes understandable to those affected.

5.4. The Context of Emerging Economies and the Specificities of Morocco

The framework has been formulated in general terms, but its intensity varies with context. It is useful to distinguish the characteristics shared by emerging economies from those specific to Morocco and to its textile sector.

Three characteristics common to emerging economies alter the stakes of the framework. The first is the relative weakness of external control institutions. Khanna and Palepu (1997) used the term institutional voids to describe the absence or fragility, in emerging markets, of the intermediaries that elsewhere ensure the proper functioning of markets, such as regulators, analysts, or contract enforcement mechanisms. Where external control is less dense, internal control bears a heavier share of risk management, so that both the benefits and the failures of the digitalization capability weigh more heavily on performance. The second is dependence on foreign buyers. Industrial firms integrated into global value chains must often comply with control and traceability requirements imposed by their customers. These requirements constitute coercive pressure in the sense of DiMaggio and Powell (1983), which accelerates tool adoption but also increases the risk of symbolic adoption described in Proposition 5b. The third is the relative scarcity of digital skills. Because the reconfiguring capability relies on deliberate learning mechanisms (Zollo & Winter, 2002), it requires skills that tools do not provide. Where such skills are scarce, the gap between technology acquisition and capability building tends to widen, and reconfiguration governance, which requires expertise to validate changes, becomes harder to establish.

Moroccan firms share these characteristics but also operate within a specific institutional framework. The first element is the protection of personal data. Law No. 09-08 regulates the processing of personal data and places it under the supervision of the National Commission for the Control of Personal Data Protection (Kingdom of Morocco, 2009). Digitalized controls that process employee or customer data, such as access logs or behavioral analytics, must therefore comply with this law, which adds a legal dimension to reconfiguration governance. The second element is cybersecurity regulation. Law No. 05-20 on cybersecurity imposes security obligations mainly on administrations, public bodies, and operators of vital importance (Kingdom of Morocco, 2020). Most private industrial firms, including textile firms, are therefore not directly subject to it. In the absence of strong regulatory pressure, the pressure to digitalize control comes mainly from buyers, which reinforces the relevance of Proposition 5b. The third element is public policy. The national strategy Maroc Digital 2030, launched in 2024, aims to accelerate the digital transformation of the economy, including that of businesses (Ministry of Digital Transition and Administrative Reform, 2024). It creates a favorable context for digitalization but does not by itself guarantee that firms will build capabilities rather than acquire tools.

The textile and apparel sector provides a particularly relevant setting for testing the framework, for three reasons. The first is environmental dynamism. The sector produces short series for fast-fashion brands, with tight lead times and frequent changes in orders, which places firms in the zone of high dynamism where Proposition 5a predicts the greatest variation in the value of the capability. The second is buyer pressure. The sector is highly concentrated on a few European markets. In 2024, exports of ready-made garments amounted to 29.6 billion dirhams, of which Spain absorbed 68.7% and France 13.9% (Office des changes, 2025). Firms are therefore exposed to the audit, traceability, and compliance requirements of a small number of large buyers, which creates the conditions for both substantive and symbolic adoption. The third is proximity to European markets. This proximity is the sector's main competitive advantage over Asian competitors, but it can only be exploited if firms are able to respond quickly and reliably to their customers, which makes the reliability of control a direct component of competitiveness. These characteristics make the Moroccan textile sector a setting where the propositions should be particularly visible, without limiting the framework to this sector.

5.5. Boundary Conditions

A theoretical framework is useful only if one knows where it ceases to apply. Specifying the organizations, contexts, and time horizons to which it relates delimits its scope and indicates to future research where to test it (Whetten, 1989). Three conditions bound the proposed framework.

The first concerns the organizations targeted. The framework assumes a minimum level of information system digitalization, without which the capability described cannot develop. It therefore applies primarily to medium-sized and large firms equipped with an enterprise resource planning system or structured transactional systems, rather than to very small firms whose control relies on the owner-manager's direct supervision.

The second concerns context. Consistent with Proposition 5a, the framework should hold most clearly in sectors exposed to turbulent environments and strong external requirements, such as industries integrated into global value chains. Conversely, it should lose explanatory power in stable environments, where the reconfiguring capability is less useful.

The third concerns time. A capability is built gradually, through the accumulation of experience and learning. Its effects on risk management and control reliability should therefore precede its effects on performance, and the latter may appear only with a certain lag. This temporal dimension, which Brynjolfsson (1993) counts among the explanations of the productivity paradox, calls for repeated observations over time rather than one-off measurements.

6. Discussion

6.1. Theoretical Contributions

The first contribution of this article lies in the conceptual shift it brings about. It replaces a reading of internal control digitalization in terms of resources with a reading in terms of dynamic capabilities. By distinguishing technological resources, operational capabilities, and dynamic capabilities, it offers an explanation for a phenomenon that dominant approaches struggle to grasp: the diversity of digitalization outcomes among firms with comparable tools. If value lies in the capability rather than in the tool, this diversity becomes intelligible.

The second contribution concerns the internal control literature itself. By showing that digitalization can give control a reconfiguring capability it previously lacked, the article suggests that digitalized internal control can attain the status of a higher-order capability in the sense of Winter (2003). It thus moves beyond a strictly defensive view of control and joins research that recognizes the contribution of control systems to the development of

strategic capabilities (Henri, 2006; Simons, 1995). It also connects this literature to adjacent debates on information systems governance, algorithmic control, digital risk, and audit transformation, by showing what each of them leaves unexplained about the evolution of control systems.

The third contribution lies in enriching dynamic capabilities theory. Studies applying it to digital transformation have focused mainly on strategic, commercial, or innovation functions (Warner & Wäger, 2019). Internal control occupies a marginal place in this work. By incorporating it, the article extends the theory's scope to a control function too often regarded as purely operational.

This third contribution rests on the tension uncovered in Section 4.7, and it is this tension that distinguishes a theoretical contribution from a mere transposition. Applying a theory to a new domain enriches knowledge only if that domain forces a modification of the theory itself (Whetten, 1989). Internal control is not a neutral field of application for dynamic capabilities: it is a function whose raison d'être is consistency. Introducing a logic of reconfiguration reveals that, in control functions, the value of a dynamic capability depends on the governance of its own exercise. The concept of reconfiguration governance, which the article distinguishes from IT change management and information systems governance, and Proposition 6, which formalizes it, thus constitute the article's most distinctive contribution. They suggest that the theory, built for exploration functions, must incorporate a dimension of change control when applied to functions whose purpose is stability. This result also extends research on the balance between controlling and enabling uses of control (Adler & Borys, 1996; Mundy, 2010) by giving it a temporal dimension. The issue is no longer only to balance two uses at a given moment, but also to balance change and consistency in the control system over time.

Finally, the article refines the institutional reading of control digitalization. Rather than opposing efficiency and legitimacy, it suggests that institutional pressures weaken the value of digitalization only when they lead to symbolic adoption, which shifts attention from the origin of the pressures to the way they are translated into practice.

6.2. Managerial Implications

For executives, the proposed framework cautions against confusing the acquisition of technologies with the development of a capability. Investing in an ERP system or a robotic process automation solution is not enough; the processes that will make it possible to sense,

decide, and evolve the control system must also be organized. Managerial attention should therefore focus as much on skills, learning routines, and control governance as on tools.

For internal control and audit managers, the framework highlights the value of designing parameterizable and evolving systems that can rapidly incorporate new risks. These systems must also subject their own changes to rules of validation, traceability, and segregation of duties, and maintain qualified human supervision of automated controls. Alert volumes should be calibrated to the capacity of controllers to examine them, and data quality should be treated as a control objective in its own right. A system that transforms itself without being governed loses what it claims to strengthen. The framework also encourages managers to treat the data generated by controls as a source of organizational learning.

These implications are particularly relevant for firms in emerging economies, and notably for Moroccan textile and apparel firms. Integrated into global value chains and subject to their buyers' requirements and to strong competitive pressures, these firms are exposed to the risk of symbolic digitalization, driven by compliance or imitation rather than by the development of a genuine capability. Turning buyer requirements into an opportunity to build sensing, seizing, and reconfiguring routines, rather than into a mere display of compliance, is a central managerial challenge for them.

6.3. Limitations and Research Agenda

Like any conceptual work, this article has limitations. The corpus results from an integrative rather than a systematic review: it aims at theoretical coverage and not at exhaustiveness. Because it was built iteratively, following the argument, it also reflects the authors' theoretical choices, and a systematic review could reveal other research streams likely to enrich or nuance the framework. The propositions derive from theoretical reasoning and have not yet been empirically tested. Moreover, the framework focuses on two intermediate mechanisms and, for the sake of parsimony, excludes channels such as strategic learning or innovation, whose exclusion should be tested empirically. Finally, measuring a dynamic capability remains a recognized methodological challenge, since it involves capturing an ability rather than an outcome.

These limitations open several avenues for research. The first is to operationalize the constructs of the framework. Table 4 proposes possible measures for each of them, distinguishing perceptual measures from objective or archival measures in order to limit common method bias (Podsakoff et al., 2003). For the dimensions of the capability, existing scales measuring sensing, seizing, and transforming capacities (Kump et al., 2019) can be

adapted to the control function, and environmental dynamism can be measured with established scales (Jansen et al., 2006). Care must be taken not to confuse the level of technology adoption with the capability itself. For this reason, the perceptual measures of the three dimensions focus on abilities, such as the ability to detect, decide, and revise, whereas usage indicators drawn from information systems are used as complements rather than as proxies of the capability. Likewise, the deficiencies reported by auditors are a meaningful indicator of reliability only if they are weighted by the scope and intensity of the audit work performed. The digital data generated by control systems also open up new methodological possibilities in their own right (Bhimani, 2020).

Table N°4: Possible operationalization of the framework's constructs

Construct	Perceptual measures	Objective or archival measures
Sensing	Perceived ability to detect emerging risks and anomalies early (adapted from Kump et al., 2019)	Share of transactions under continuous monitoring; mean time between an anomaly and its detection; number of data sources analyzed
Seizing	Perceived speed and quality of decisions following alerts; perceived ability to reallocate control resources	Mean time between an alert and corrective action; share of alerts closed; reallocation of control budgets
Reconfiguring	Perceived ability to revise control rules and to integrate new risks or standards	Frequency of rule revisions; time needed to integrate a new risk or regulatory requirement (change logs)
Reconfiguration governance	Perceived formalization of change validation, traceability, segregation of duties, and human supervision	Existence of a change policy; share of changes documented and approved; access rights matrix
Mode of adoption	Perceived extent to which tools are used in daily control routines rather than for external display	Usage logs; share of acquired features actually used; consistency between documented and observed controls
Institutional motivation	Perceived weight of buyer requirements, competitor imitation, and professional standards in the decision to digitalize	Number of buyer audits per year; control requirements included in customer contracts
Environmental dynamism	Perceived rate of change in demand, products, and technologies (Jansen et al., 2006)	Volatility of sales; frequency of order changes; industry data
Risk management effectiveness	Perceived comprehensiveness and timeliness of risk assessment and response	Update frequency of the risk map; operational losses; number of incidents
Internal control reliability	Perceived consistency and auditability of controls	Deficiencies reported by internal and external audit, weighted by the scope and intensity of audit work; errors detected after the fact
Financial performance	Perceived financial performance relative to competitors	Return on assets; operating margin; sales growth (financial statements)
Non-financial performance	Perceived quality, delivery reliability, and customer satisfaction	Defect rate; on-time delivery rate; customer returns; buyer scorecards

Source: Prepared by the author

These measures are offered for illustrative purposes; their use requires prior work on scale development and validation.

The second avenue is to test the propositions using structural equation modeling. This method is suited to the framework for three reasons: the constructs are latent and measured by several indicators, the framework combines direct, mediating, and moderating relationships that must be estimated simultaneously, and it allows measurement error to be taken into account. The unit of analysis should be the firm, with several respondents per firm, for example the chief financial officer, the internal control or audit manager, and an operations manager, in order to reduce single-respondent bias. The measurement model should first be explored through exploratory factor analysis and then validated through confirmatory factor analysis. Reliability can be assessed using composite reliability, with a threshold of 0.70, and convergent validity using the average variance extracted, with a threshold of 0.50. Discriminant validity should be verified using both the Fornell-Larcker criterion (Fornell & Larcker, 1981) and the heterotrait-monotrait ratio (Henseler et al., 2015), which is particularly important to separate the reconfiguring capability from reconfiguration governance. The moderating effects of Propositions 5a, 5b, and 6 require latent interaction terms, including a quadratic term for environmental dynamism, while the indirect effects of Propositions 1 and 4 should be tested by bootstrapping (Preacher & Hayes, 2008).

The third avenue concerns temporal designs. Because capabilities are built gradually and their effects on performance appear with a lag, a longitudinal panel with at least three waves of data collection would be preferable to a cross-sectional design. A cross-lagged design, in which each variable is measured at each wave and its effect on the others is estimated with a lag, would also make it possible to test the reverse causality argument discussed in Section 5.3. Such validation would benefit from being conducted in an industrial sector exposed to international competition, such as the Moroccan textile sector, where the characteristics analyzed in Section 5.4 are particularly pronounced.

The fourth avenue, qualitative in nature, would be to study through in-depth case studies how firms gradually build this capability and govern its reconfiguration, in line with the processual view advocated by Warner and Wäger (2019). Such studies would be particularly useful for observing how the mode of adoption evolves over time and how firms move, or fail to move, from symbolic to substantive adoption.

Conclusion

This article started from a simple observation: internal control digitalization is widely promoted, yet its contribution to performance remains poorly explained. We have argued that this difficulty stems less from the technologies themselves than from the way they are conceived. As long as digitalization is understood as a stock of tools, it can account neither for the diversity of its effects nor for its evolving nature.

Using dynamic capabilities theory as a lens, we have proposed to conceive of internal control digitalization as a capability combining sensing, seizing, and reconfiguring, defined by its processes rather than by its effects and distinguished from both the technologies and the operational routines it relies on. This reinterpretation has revealed a tension specific to control functions, between the need to transform the system and the need to preserve its consistency, which the concept of reconfiguration governance makes it possible to address. The resulting framework, formalized in six propositions, holds that the digitalization capability affects performance mainly through two parallel channels, risk management effectiveness and internal control reliability, while retaining a weaker direct effect. These effects depend on the quality of data and human judgment, on the governance of reconfiguration, on environmental dynamism, and on the way institutional pressures are translated into practice.

Answering the question that opened this article thus amounts to asserting that internal control digitalization can be conceived as a dynamic capability insofar as it gives the control system the ability to transform itself. This capability contributes to performance in an essentially indirect way. Controlling differently, then, does not mean controlling more: it means making control a system that learns, without giving up the consistency on which trust is built. It is now up to empirical research to put this framework to the test, particularly in emerging contexts where the challenge of control digitalization is especially acute.

BIBLIOGRAPHY

Adler, P. S., & Borys, B. (1996). Two types of bureaucracy: Enabling and coercive. Administrative Science Quarterly, 41(1), 61-89.

Agostino, D., Saliterer, I., & Steccolini, I. (2022). Digitalization, accounting and accountability: A literature review and reflections on future research in public services. Financial Accountability & Management, 38(2), 152-176.

Alvesson, M., & Sandberg, J. (2011). Generating research questions through problematization. Academy of Management Review, 36(2), 247-271.

Appelbaum, D., Kogan, A., & Vasarhelyi, M. A. (2017). Big Data and analytics in the modern audit engagement: Research needs. Auditing: A Journal of Practice & Theory, 36(4), 1-27.

Arend, R. J., & Bromiley, P. (2009). Assessing the dynamic capabilities view: Spare change, everyone? Strategic Organization, 7(1), 75-90.

Barney, J. (1991). Firm resources and sustained competitive advantage. Journal of Management, 17(1), 99-120.

Barreto, I. (2010). Dynamic capabilities: A review of past research and an agenda for the future. Journal of Management, 36(1), 256-280.

Bharadwaj, A. S. (2000). A resource-based perspective on information technology capability and firm performance. MIS Quarterly, 24(1), 169-196.

Bhimani, A. (2020). Digital data and management accounting: Why we need to rethink research methods. Journal of Management Control, 31(1), 9-23.

Bhimani, A., & Willcocks, L. P. (2014). Digitisation, 'Big Data' and the transformation of accounting information. Accounting and Business Research, 44(4), 469-490.

Bromley, P., & Powell, W. W. (2012). From smoke and mirrors to walking the talk: Decoupling in the contemporary world. Academy of Management Annals, 6(1), 483-530.

Brynjolfsson, E. (1993). The productivity paradox of information technology. Communications of the ACM, 36(12), 66-77.

Chenhall, R. H. (2003). Management control systems design within its organizational context. Accounting, Organizations and Society, 28(2-3), 127-168.

Commerford, B. P., Dennis, S. A., Joe, J. R., & Ulla, J. W. (2022). Man versus machine: Complex estimates and auditor reliance on artificial intelligence. Journal of Accounting Research, 60(1), 171-201.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2013). Internal control: Integrated framework. COSO.

DeSanctis, G., & Poole, M. S. (1994). Capturing the complexity in advanced technology use: Adaptive structuration theory. Organization Science, 5(2), 121-147.

DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. American Sociological Review, 48(2), 147-160.

Donaldson, L. (2001). The contingency theory of organizations. Sage.

Doyle, J., Ge, W., & McVay, S. (2007). Determinants of weaknesses in internal control over financial reporting. Journal of Accounting and Economics, 44(1-2), 193-223.

Eisenhardt, K. M., & Martin, J. A. (2000). Dynamic capabilities: What are they? Strategic Management Journal, 21(10-11), 1105-1121.

Ellström, D., Holtström, J., Berg, E., & Josefsson, C. (2022). Dynamic capabilities for digital transformation. Journal of Strategy and Management, 15(2), 272-286.

Eulerich, M., Masli, A., Pickerd, J., & Wood, D. A. (2023). The impact of audit technology on audit task outcomes: Evidence for technology-based audit techniques. Contemporary Accounting Research, 40(2), 981-1012.

Eulerich, M., Pawlowski, J., Waddoups, N. J., & Wood, D. A. (2022). A framework for using robotic process automation for audit tasks. Contemporary Accounting Research, 39(1), 691-720.

Eulerich, M., Waddoups, N., Wagener, M., & Wood, D. A. (2024). Development of a framework of key internal control and governance principles for robotic process automation (RPA). Journal of Information Systems, 38(2), 29-49.

ESSAHLI, F. E., & HILMI, Y. (2026). Digitalisation et transformation du contrôle de gestion: vers un rôle de business partner. Agence Francophone, 689-706.

Fähndrich, J. (2023). A literature review on the impact of digitalisation on management control. Journal of Management Control, 34(1), 9-65.

Fedyk, A., Hodson, J., Khimich, N., & Fedyk, T. (2022). Is artificial intelligence improving the audit process? Review of Accounting Studies, 27(3), 938-985.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. Journal of Marketing Research, 18(1), 39-50.

Gilson, L. L., & Goldberg, C. B. (2015). Editors' comment: So, what is a conceptual paper? Group & Organization Management, 40(2), 127-130.

Haans, R. F. J., Pieters, C., & He, Z.-L. (2016). Thinking about U: Theorizing and testing U- and inverted U-shaped relationships in strategy research. Strategic Management Journal, 37(7), 1177-1195.

Haapamäki, E., & Sihvonen, J. (2019). Cybersecurity in accounting research. Managerial Auditing Journal, 34(7), 808-834.

Helfat, C. E., Finkelstein, S., Mitchell, W., Peteraf, M., Singh, H., Teece, D., & Winter, S. (2007). Dynamic capabilities: Understanding strategic change in organizations. Blackwell.

Helfat, C. E., Kaul, A., Ketchen, D. J., Barney, J. B., Chatain, O., & Singh, H. (2023). Renewing the resource-based view: New contexts, new concepts, and new methods. Strategic Management Journal, 44(6), 1357-1390.

Helfat, C. E., & Winter, S. G. (2011). Untangling dynamic and operational capabilities: Strategy for the (n)ever-changing world. Strategic Management Journal, 32(11), 1243-1250.

Henri, J.-F. (2006). Management control systems and strategy: A resource-based perspective. Accounting, Organizations and Society, 31(6), 529-558.

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. Journal of the Academy of Marketing Science, 43(1), 115-135.

Institute of Internal Auditors (IIA). (2024). Global internal audit standards. The Institute of Internal Auditors.

ISACA. (2018). COBIT 2019 framework: Governance and management objectives. ISACA.

Jaakkola, E. (2020). Designing conceptual articles: Four approaches. AMS Review, 10(1-2), 18-26.

Jansen, J. J. P., Van den Bosch, F. A. J., & Volberda, H. W. (2006). Exploratory innovation, exploitative innovation, and performance: Effects of organizational antecedents and environmental moderators. Management Science, 52(11), 1661-1674.

Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. Journal of Financial Economics, 3(4), 305-360.

HAJRIOUI, Z., & HILMI, Y. (2026). Impact de la transformation digitale sur la qualité de contrôle interne: Cas des PME. *International Journal of Economics and Management Sciences*, *5*(3), 339-352.

HILMI, Y., & FATINE, F. E. (2022). The Contribution of internal audit to the corporate performance: a proposal of measurement indicators. *International Journal of Performance and Organizations*, *1*(1), 45-50.

HILMI, y., & NAJI, F. (2016). Audit social et performance de l'entreprise : une étude empirique au sein du champ organisationnel marocain. Revue des Etudes Multidisciplinaires en Sciences Economiques et Sociales, 1(3). doi:https://doi.org/10.48375/IMIST.PRSM/remses-v1i3.5271

Hilmi, Y., & Fatine, F. E. (2022). Transformation digitale des cabinets d'audit par les réseaux sociaux: Cas de KPMG. International Journal of Economics and Management Sciences, 1(1).

HILMI, Y. L'ÉTHIQUE DE L'ENTREPRISE: UN BON MOYEN DE PROTECTION CONTRE LA FRAUDE THE ETHICS OF BUSINESS: A GOOD WAY TO PROTECT AGAINST FRAUD.

HILMI, Y. (2013). L'audit interne au Maroc: Degré d'intégration et spécificités de l'entreprise. *Revue marocaine de recherche en management et marketing*, (8).

HILMI, Y. (2013). L'audit interne au Maroc: Degré d'intégration et spécificités de l'entreprise. *Revue marocaine de recherche en management et marketing*, (8).

Kellogg, K. C., Valentine, M. A., & Christin, A. (2020). Algorithms at work: The new contested terrain of control. Academy of Management Annals, 14(1), 366-410.

Khanna, T., & Palepu, K. (1997). Why focused strategies may be wrong for emerging markets. Harvard Business Review, 75(4), 41-48.

Kingdom of Morocco. (2009). Law No. 09-08 on the protection of individuals with regard to the processing of personal data, promulgated by Dahir No. 1-09-15 of 18 February 2009. Bulletin Officiel.

Kingdom of Morocco. (2020). Law No. 05-20 on cybersecurity, promulgated by Dahir No. 1-20-69 of 25 July 2020. Bulletin Officiel.

Klamm, B. K., & Watson, M. W. (2009). SOX 404 reported internal control weaknesses: A test of COSO framework components and information technology. Journal of Information Systems, 23(2), 1-23.

Knudsen, D.-R. (2020). Elusive boundaries, power relations, and knowledge production: A systematic review of the literature on digitalization in accounting. International Journal of Accounting Information Systems, 36, 100441.

Kokina, J., & Davenport, T. H. (2017). The emergence of artificial intelligence: How automation is changing auditing. Journal of Emerging Technologies in Accounting, 14(1), 115-122.

Kraus, S., Durst, S., Ferreira, J. J., Veiga, P., Kailer, N., & Weinmann, A. (2022). Digital transformation in business and management research: An overview of the current status quo. International Journal of Information Management, 63, 102466.

Kump, B., Engelmann, A., Kessler, A., & Schweiger, C. (2019). Toward a dynamic capabilities scale: Measuring organizational sensing, seizing, and transforming capacities. Industrial and Corporate Change, 28(5), 1149-1172.

Leocádio, D., Malheiro, L., & Reis, J. (2024). Artificial intelligence in auditing: A conceptual framework for auditing practices. Administrative Sciences, 14(10), 238.

MacInnis, D. J. (2011). A framework for conceptual contributions in marketing. Journal of Marketing, 75(4), 136-154.

Malmi, T., & Brown, D. A. (2008). Management control systems as a package: Opportunities, challenges and research directions. Management Accounting Research, 19(4), 287-300.

Maqsood, U. S., Wang, S., & Zahid, R. M. A. (2024). Digital age imperatives and firm internal control quality: Evidence from CEOs' personal traits and type of state-owned enterprises. Managerial Auditing Journal, 39(6), 700-727.

Melville, N., Kraemer, K., & Gurbaxani, V. (2004). Information technology and organizational performance: An integrative model of IT business value. MIS Quarterly, 28(2), 283-322.

Meyer, J. W., & Rowan, B. (1977). Institutionalized organizations: Formal structure as myth and ceremony. American Journal of Sociology, 83(2), 340-363.

Ministry of Digital Transition and Administrative Reform. (2024). Maroc Digital 2030: National strategy for digital transition. Kingdom of Morocco.

Moffitt, K. C., Rozario, A. M., & Vasarhelyi, M. A. (2018). Robotic process automation for auditing. Journal of Emerging Technologies in Accounting, 15(1), 1-10.

Möller, K., Schäffer, U., & Verbeeten, F. (2020). Digitalization in management accounting and control: An editorial. Journal of Management Control, 31(1), 1-8.

Mundy, J. (2010). Creating dynamic tensions through a balanced use of management control systems. Accounting, Organizations and Society, 35(5), 499-523.

Office des changes. (2025). Commerce extérieur du Maroc 2024: Rapport annuel. Office des changes. https://www.oc.gov.ma/sites/default/files/2025-07/Rapport%20Commerce%20Ext%C3%A9rieur%202024%20VF.pdf

Orlikowski, W. J. (2007). Sociomaterial practices: Exploring technology at work. Organization Studies, 28(9), 1435-1448.

Parasuraman, R., & Manzey, D. H. (2010). Complacency and bias in human use of automation: An attentional integration. Human Factors, 52(3), 381-410.

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. Journal of Applied Psychology, 88(5), 879-903.

Preacher, K. J., & Hayes, A. F. (2008). Asymptotic and resampling strategies for assessing and comparing indirect effects in multiple mediator models. Behavior Research Methods, 40(3), 879-891.

Priem, R. L., & Butler, J. E. (2001). Is the resource-based "view" a useful perspective for strategic management research? Academy of Management Review, 26(1), 22-40.

Schilke, O. (2014). On the contingent value of dynamic capabilities for competitive advantage: The nonlinear moderating effect of environmental dynamism. Strategic Management Journal, 35(2), 179-203.

Schilke, O., Hu, S., & Helfat, C. E. (2018). Quo vadis, dynamic capabilities? A content-analytic review of the current state of knowledge and recommendations for future research. Academy of Management Annals, 12(1), 390-439.

Simons, R. (1995). Levers of control: How managers use innovative control systems to drive strategic renewal. Harvard Business School Press.

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. Journal of Business Research, 104, 333-339.

Solow, R. M. (1987, July 12). We'd better watch out. New York Times Book Review, 36.

Sutton, R. I., & Staw, B. M. (1995). What theory is not. Administrative Science Quarterly, 40(3), 371-384.

Teece, D. J. (2007). Explicating dynamic capabilities: The nature and microfoundations of (sustainable) enterprise performance. Strategic Management Journal, 28(13), 1319-1350.

Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. Strategic Management Journal, 18(7), 509-533.

Vasarhelyi, M. A., Alles, M. G., & Kogan, A. (2004). Principles of analytic monitoring for continuous assurance. Journal of Emerging Technologies in Accounting, 1(1), 1-21.

Vial, G. (2019). Understanding digital transformation: A review and a research agenda. Journal of Strategic Information Systems, 28(2), 118-144.

Wade, M., & Hulland, J. (2004). The resource-based view and information systems research: Review, extension, and suggestions for future research. MIS Quarterly, 28(1), 107-142.

Warner, K. S. R., & Wäger, M. (2019). Building dynamic capabilities for digital transformation: An ongoing process of strategic renewal. Long Range Planning, 52(3), 326-349.

Wassie, F. A., & Lakatos, L. P. (2024). Artificial intelligence and the future of the internal audit function. Humanities and Social Sciences Communications, 11, 386.

Whetten, D. A. (1989). What constitutes a theoretical contribution? Academy of Management Review, 14(4), 490-495.

Winter, S. G. (2003). Understanding dynamic capabilities. Strategic Management Journal, 24(10), 991-995.

Zhao, X., Lynch, J. G., & Chen, Q. (2010). Reconsidering Baron and Kenny: Myths and truths about mediation analysis. Journal of Consumer Research, 37(2), 197-206.

Zollo, M., & Winter, S. G. (2002). Deliberate learning and the evolution of dynamic capabilities. Organization Science, 13(3), 339-351.