



IT Sophistication 2.0 : Towards a Comprehensive Framework for Assessing IT Capabilities in the Digital Age

Sambas Ade Kesuma^{1*}, Risanty², Sonya Putri³

Universitas Sumatera Utara

Corresponding Author: Sambas Ade Kesuma sambas.usu@gmail.com

ARTICLE INFO

Keywords: IT Sophistication, IT Usage, IT Management, IT Security

Received : 21 April

Revised : 23 May

Accepted: 23 June

©2025 Kesuma, Risanty, Putri: This is an open-access article distributed under the terms of the [Creative Commons Attribution 4.0 International](https://creativecommons.org/licenses/by/4.0/).



ABSTRACT

While accelerating digital transformation, many frameworks for evaluating IT sophistication, such as the classic model of Raymond and Paré (1992), have yet to capture key contemporary elements, including cybersecurity maturity, user digital capability, and strategic IT alignment. This study introduces IT sophistication 2.0, a new conceptual framework that remaps organisational IT capabilities into nine dimensions grouped under three core clusters: IT Usage, IT Management, and IT Security. The novelty of the model lies in (1) the integration of security sophistication across preventive, detective, and responsive layers; (2) the inclusion of user sophistication to reflect end-user digital maturity; and (3) the use of a multi-tiered measurement scale, moving beyond traditional intensity or dichotomous approaches. This framework offers theoretical and practical contributions, developed through synthesising classical and recent literature (up to 2024). Theoretically, it integrates previously fragmented perspectives and provides a more explicit classification of IT capabilities. It presents a diagnostic tool comprising 45 measurable indicators applicable across business, public, and social sectors. This model is particularly suited to support digital strategy assessments and IT maturity diagnostics in diverse organisational contexts. Future studies are recommended to empirically validate the framework, adapt it across sectors, and examine its relevance to organisational resilience and innovation outcomes

INTRODUCTION

The digital transformation era has significantly changed how organisations adopt, deploy, and secure their information technology (IT) resources. As digital devices become increasingly integrated with strategic operations, the evaluation and measurement of the level of IT sophistication of an organisation becomes increasingly essential (Bharadwaj, 2000; Kane et al., 2015; Jayawardena et al., 2020).

According to Polozhentseva et al. (2024), "modern technology helps service organisations to increase the volume of services provided, effectively control quality, speed up and automate business processes. In addition, digital transformation requires a proactive approach to addressing ethical and regulatory issues related to data-intensive use and cybersecurity (Cheng et al. 2024). The reality is that an organisation's digital transformation has significantly impacted various aspects of business operations, leading to increased operational agility" (Mishra & Varshney, 2024). Zheng et al. (2024) stated that organisational culture values innovation and sustainability, which ultimately increases the effectiveness of digital transformation efforts. Keen (1991) and Weill and Broadbent (1998) view IT sophistication as an essential resource of an organisation. Raymond and Paré (1992) define IT sophistication as a processing models, operational types, application portfolios, decision level, and position of the SI function. Cheney and Dickson (1982) categorise IT sophistication into three main criteria: (1) Technological sophistication, (2) Organisational sophistication, and (3) System performance.

Based on previous research, the concept of IT sophistication is a multidimensional concept. To integrate these concepts, Raymond and Paré (1992) proposed the integration of IT sophistication variables, namely information content, technology support, functional support, and management information systems.

Despite the growing interest in digital integration and capability frameworks, existing models often fail to comprehensively yet pragmatically capture the multidimensional nature of IT sophistication (Sándor & Gubán, 2021). One of the most influential early models, developed by Raymond and Paré (1992), provides a fundamental approach by conceptualising IT sophistication along four dimensions: technological, informational, managerial, and functional. This model has been widely referenced and applied in small and medium-sized enterprises (SMEs) studies and IT management research (Chen & Hsiao, 2012; Cragg et al., 2011; Sinambela et al., 2023).

However, the rapidly evolving digital landscape has revealed essential gaps in these legacy models. In particular, this model does not adequately reflect the growing importance of cybersecurity management, user empowerment, and the strategic role of IT in organisational value creation (Cram et al., 2017; Gonzalez & Sol, 2012; Nambisan et al., 2017; Sinambela et al., 2023). In addition, the advent of cloud computing, data-driven decision-making, and hybrid work activities has added a significant layer of complexity that requires an updated framework to guide researchers and practitioners (Kamariotou & Kitsios, 2023). This study proposes IT sophistication 2.0, an expanded and integrative conceptual framework that builds on the foundations of previous models while

incorporating new dimensions that reflect the realities of today's organisations. The proposed model covers nine dimensions in three core groups: IT Usage, IT Management, and IT Security. The model also introduces User sophistication as an essential element of IT sophistication. The rest of the paper is structured as follows: Part 2 reviews the literature on IT sophistication and its evolution. Part 3 introduces the IT sophistication 2.0 model. Part 4 discusses its theoretical and practical implications, and Part 5 concludes with suggestions for future research.

LITERATURE REVIEW

1. The Evolution of IT Sophistication

The concept of IT sophistication was first introduced systematically by Raymond and Paré (1992), who viewed it as a multidimensional construct to measure how organisations use and manage information technology (IT). The model consists of three main dimensions, namely: Technological sophistication (the diversity and complexity of the technologies used), information sophistication (the scope of application and integration), and functional sophistication (the structure and role of IT functions in the organisation). This model is particularly suitable for small and medium enterprises (SMEs). The dimension of IT sophistication proposed by Raymond and Paré (1992) was initially developed in the context of SMEs. However, some recent studies have attempted to apply the dimension of IT sophistication in different contexts, such as the context of state-owned banking (Kesuma et al., 2016), healthcare organisations (Paré & Sicotte, 2001), manufacturing listed on the stock exchange (Al-Eqab & Adel, 2013), cooperative contexts (Alannita & Suaryana, 2014), manufacturing SMEs (Raymond et al., 1992) and listed companies (Al-Eqab & Ismail, 2011). This concept offers a practical perspective for understanding IT adoption and management variations in different companies (Raymond & Paré, 1992). Despite its age, this framework continues to inform studies on IT capabilities, digital maturity, and digitalisation of SMEs (Cragg et al., 2011; Chen & Hsiao, 2012; Sinambela et al., 2023).

However, such models have fundamental limitations in today's digital context. This model does not explicitly account for information security management, user enablement, or strategic alignment of the IT aspects now central to the organisation's IT capabilities.

In response to the evolving needs of organisations, several studies have proposed more nuanced IT strategy and capability models. For example, Bharadwaj (2000) emphasises IT as an organisational capability in a resource-based (RBV) view, highlighting its impact on company performance. Similarly, Chen et al. (2010) and Cragg et al. (2011) have explored how IT competence and maturity affect strategic alignment and value creation. The Digital Transformation Capability Maturity Model (DX-CMM) developed by Gökalp and Martinez (2021) is designed to help organisations assess the maturity level of digital transformation, identify capability gaps, and develop an improvement roadmap. Maturity in IT security sophistication reflects the organisation's readiness to manage cyber risks systematically. This maturity model helps assess security capabilities and adapt to threats (Brezavšek & Baggia, 2025).

Similarly, the literature on digital transformation has emphasised broader dimensions, including leadership, culture, and security (Kane et al., 2015; Jayawardena et al., 2020). Newer frameworks, such as Cram et al. (2017) on IT security policy and Gonzalez & Sol (2012) on security maturity models, demonstrate the important role of cybersecurity in the contemporary IT environment. In addition, the role of users is becoming increasingly significant. Studies on end-user readiness, digital skills, and computing underscore the importance of incorporating user sophistication into any IT capability framework (Nambisan et al., 2017). This perspective aligns with socio-technical systems theory, emphasising the interaction between technology and human actors in achieving performance outcomes (Trist, 1981; Chabot et al., 2024).

Digital transformation requires a robust IT infrastructure, systems, efficient data management, and flexible procedures to foster an innovative environment (Mollah et al., 2024). Organisations rely heavily on data to improve products and services, turning information into valuable assets (Gebremeskel et al., 2023). Adopting a strategy that embraces the implications of digital transformation is essential to drive better operational performance, emphasising that technology is just one aspect to stay competitive in the digital world (Vial, 2019).

Given these developments, there is a growing need to expand traditional IT sophistication models to capture modern organisations' broader and more complex nature of IT capabilities. The power of IT 2.0 is built on the Raymond and Paré framework by incorporating four new dimensions:

1. Strategic sophistication – the degree to which IT aligns with and enables long-term organisational goals;
2. User sophistication – the user's competence, attitude, and proactive behaviour in utilising IT devices;
3. Preventive Security sophistication – the maturity of protective measures (e.g., access control, firewall);
4. Detective and Responsive Security sophistication – the ability to detect and respond to incidents (e.g., intrusion detection, incident handling).

This expanded framework aims to bridge the gap between traditional IT use and modern digital resilience, providing a more holistic and actionable model for researchers and practitioners.

2. IT Sophistication Model 2.0

In this section, the conceptual framework of IT sophistication 2.0 is introduced in detail, which expands on the model of Raymond & Paré (1992) by adding dimensions of security and user sophistication, as well as emphasising aspects of IT strategy. The model is organised into three main clusters: (1) IT usage, (2) IT management, and (3) IT security (see figure 1). Below each cluster are complementary dimensions to describe the organisation's IT capabilities holistically. The IT Usage Cluster consists of:

1. Technological sophistication is the complexity and complexity of IT infrastructure (hardware, software, network) and processing modes, continuing the technological dimension of Raymond & Paré (1992).
2. Information sophistication is the scope of the application portfolio and the level of data integration (compact databases, LANS), building on the information dimension of Raymond & Paré (1992).
3. User sophistication is the competence, engagement, and initiative of the end user in making optimal use of IT; complements end-user computing viewpoints (Js & Venkatesh, 2023; Nyathani, 2023).

Furthermore, it continues to the second cluster, namely IT management, which consists of several dimensions, which are as follows:

1. Functional sophistication is the role of IT structure and function, the number of specialists, user participation, and the formality of the application development process (Raymond & Paré, 1992).
2. Managerial sophistication Refers to implementing IT planning, control, and evaluation, including budgeting and documentation (Raymond & Paré, 1992).
3. Strategic sophistication shows the alignment of IT with the organisation's long-term goals, describing the role of IT as a source of competitive advantage (Bharadwaj, 2000; Jayawardena et al., 2020).

The last cluster is IT security, where this cluster also consists of several dimensions, namely:

1. Preventive sophistication is the level of maturity of preventive measures, access control, firewalls, encryption, answering cybersecurity needs (Magklaras & Furnell, 2004; Rockart & Flannery, 1983; Gonzalez & Sol; Gonzalez & Sol, 2012).
2. Detective sophistication is the ability to detect and monitor security events (audit logs, intrusion recognition) in line with the security maturity framework (Al-Matari et al., 2020; Rabii et al., 2020; Cram et al., 2017).
3. Responsive sophistication is the incident response and recovery process, incident handling, and business continuity to maintain organisational resilience (Dube & Mohanty, 2020; Nist, 2013; Xiao-yan et al., 2011).

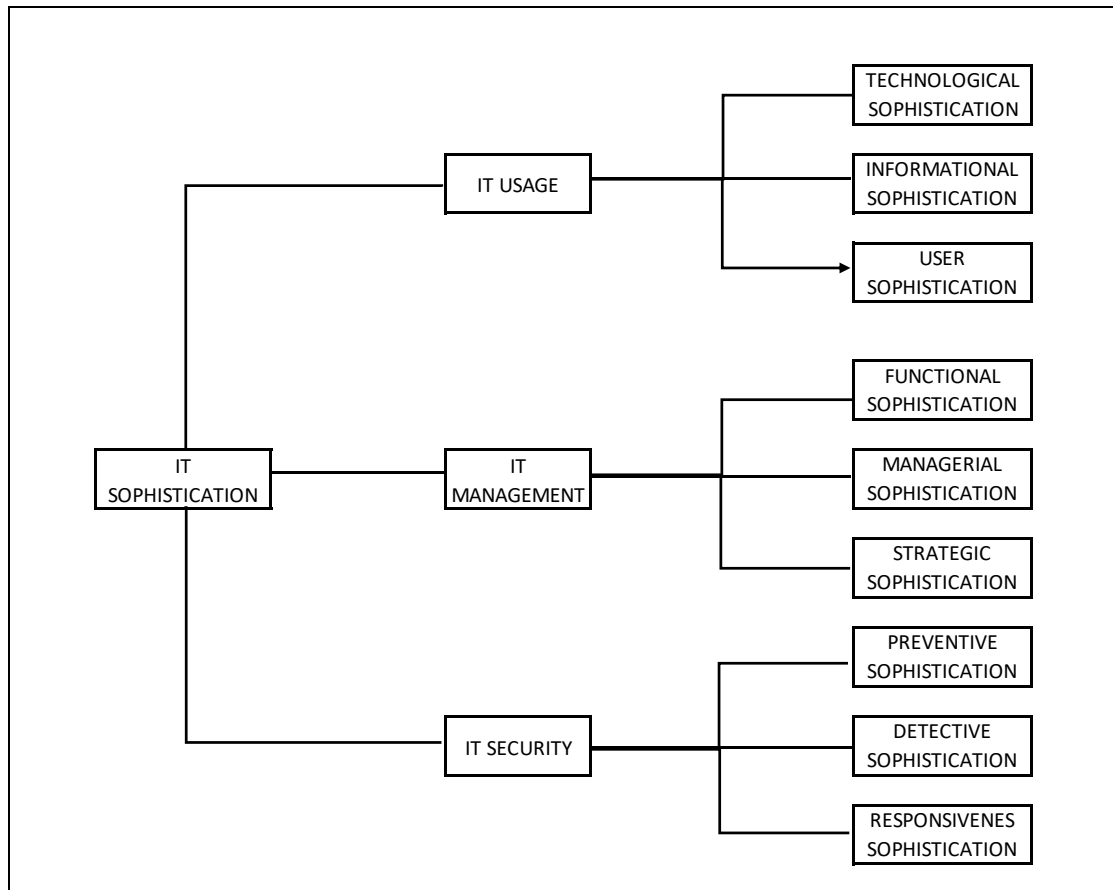


Figure 1. IT sophistication Concept Framework 2.0

METHODOLOGY

A Systematic Literature Review (SLR) is a rigorous and structured approach to reviewing existing research on a particular topic by identifying, evaluating, and synthesizing relevant studies in a transparent and replicable manner. This method is describe about IT sophistication 2.0 model as a comprehensive framework for assessing the maturity and advancement of an organization's information technology. Building upon the foundational model by Raymond and Paré (1992), it incorporates additional dimensions that reflect contemporary digital priorities, such as user sophistication and IT security sophistication. The model is organized into three core clusters—usage, management, and security—encompassing nine dimensions and 45 indicators derived from both established and modern literature. Its well-grounded theoretical basis and practical design make it a valuable tool for evaluating and understanding an organization's IT capabilities.

RESULTS AND DISCUSSION

This study integrates the original dimensions of Raymond and Paré's (1992) IT sophistication model and enriches it by prioritising the relevance of the current IT atmosphere. IT Sophistication 2.0 maintains the original four-dimensional, technological, informational, functional, and managerial foundations, which have proven to be reliable for measuring IT maturity (Raymond & Paré, 1992), while complementing the model with strategic dimensions (RBV; Bharadwaj, 2000), user sophistication (end-user computing; DeLone & McLean, 2003), and IT security sophistication (maturity model; Gonzalez & Sol, 2012; Cram et al., 2017).

The Digital Age's relevance has changed how individuals view life and work, with transformative effects comparable to those of previous industrial revolutions. In the cloud, big data, and cyber threats era, organisations need a framework that looks at infrastructure and applications and user readiness, management strategies, and end-to-end security mechanisms (Chan, 2020). Actionability for IT Practitioners and Advanced Managers focuses on improving, measuring, and aligning IT sophistication with business strategy objectives, aiming to mitigate risks that may arise and optimise IT investments (Adekanye & Rahman, 2018). A deep understanding of architectural system information is essential in the contemporary business landscape, encompassing the design, implementation, and complex management systems to ensure operational efficiency and informed decision-making (Vartanyan, 2020). With its scalable dimensions, it can be used as a diagnostic tool to assess the strengths and weaknesses of IT capabilities and guide the development of a digital transformation roadmap. Thus, IT sophistication 2.0 provides a comprehensive, measurable, and practically relevant conceptualisation framework, as a basis for further research and implementation of IT policies in different organisations.

To concretise the constructs in the IT sophistication 2.0 model, each dimension is operationally defined based on a synthesis of classical and current literature. This operational definition aims to provide clear measurement boundaries for each dimension, linking it simultaneously to specific indicators that can be observed empirically.

1. IT Usage Clusters

The IT Usage cluster has three main dimensions, each described as follows: Technology sophistication is the utilisation and integration of technologies (hardware, software, cloud systems, and multiplatform) within an organisation. Indicators used include various IT platforms, level of integration between units, real-time application usage, adoption of cloud computing, and the ability to access systems across devices (Raymond & Paré, 1992; Ciriello et al., 2021; Wang & Su, 2022; Winkler & Xiao, 2021; Gfrerer & Krcmar, 2023).

Information sophistication reflects the level of application coverage of an organisation, database integration, and information automation to support decision-making. Indicators measured include the scope of application functions, database usage, automated dashboards, presence of active internal networks, and level of system integration (Saunders & Keller, 1983; Raymond & Paré, 1992; Ciriello et al., 2021; Ein-Dor & Segev, 1982; Winkler & Xiao, 2021).

User sophistication represents the level of competence, independence, and technological exploration carried out by IT users in an organisation. The indicators developed include user ability in advanced features, participation in IT development proposals, personal initiative in participating in IT training, technical independence, and a culture of exploration of new technologies (Nambisan et al., 2017; Gfrerer & Krcmar, 2023; Bottle, 2021; Kane et al., 2015; Winkler & Xiao, 2021).

Table 1. Cluster A. IT Usage

Dimension	Operational Definition	Indicators	Reference
Technological sophistication	The level of utilisation and integration of technologies (devices, systems, cloud, multiplatform).	1. IT Variety Platform 2. Integration level between units 3. Real-time app usage 4. Cloud computing adoption, as well as capabilities 5. Cross-device system access	Raymond & Paré, 1992; Ciriello et al., 2021; Wang & Su, 2022; Winkler & Xiao, 2021; Gfrerer & Krcmar, 2023
Information sophistication	Application coverage levels, database integration, and information automation.	1. Scope of application functions 2. Database usage learned 3. Automated dashboard 4. Active internal network presence 5. System integration level	Saunders & Keller, 1983; Raymond & Paré, 1992; Ciriello et al., 2021; Ein-Dor & Segev, 1982; Winkler & Xiao, 2021
User sophistication	The level of competence, independence, and technological exploration by users.	1. User capabilities in advanced features 2. Participation in IT development proposals 3. Personal initiative in IT training 4. Technical independence 5. Culture of exploration of new technologies	Nambisan et al., 2017; Gfrerer & Krcmar, 2023; Kane et al., 2015; Winkler & Xiao, 2021

2. IT Management

In the IT Management cluster, the IT sophistication 2.0 model outlines the three main dimensions related to the organisation's structural, managerial, and IT management strategies. Functional sophistication is defined as the level of existence of a formal organisational structure for IT functions, documented procedures, and cross-functional coordination. Indicators used include the presence of internal IT staff, user involvement in the early stages of the development system, documentation of development procedures, the formation of specialised IT units or teams, and collaboration between functions using IT (Benbasat et al., 1980; Raymond & Paré, 1992; Luftman & Kempaiah, 2007; Ciriello et al., 2021; Winkler & Xiao, 2021).

Managerial sophistication Refers to the level of formalisation in IT strategy planning, annual budgeting, and post-implementation evaluation systems. Indicators in this dimension include the existence of an IT strategic plan, a formal IT budget, the implementation of an evaluation after the implementation system, the integration of IT in the organisation's long-term plan, and the use of key performance indicators (KPIs) in measuring the success of IT projects (Cheney & Dickson, 1982; Gremillion, 1984; Weill & Woerner, 2015; Coltman et al., 2015; Susanti et al., 2021). Strategic sophistication measures the contribution of IT to the achievement of an organisation's strategic goals, both in terms of strategy formulation and implementation. Indicators used include the use of IT to achieve strategic goals, leadership involvement in IT decision-making, evaluation of IT strategy contributions, alignment of IT initiatives with organisational strategies, and organisational views of IT as a strategic asset (Bharadwaj, 2000; Bottle, 2021; Luftman, 2004; Reich & Benbasat, 2000; Susanti et al., 2021). The operational definition and complete indicators for the IT Management cluster can be seen in Table 2 below.

Table 2. Cluster B. IT MANAGEMENT

Dimension	Operational Definition	Indicators (abbreviations)	Reference
Functional sophistication	IT team attendance levels, process documentation, and cross-functional coordination.	1. Presence of internal IT staff 2. User engagement in the early stages of system development 3. Documentation of development procedures 4. Formation of a dedicated IT unit or team 5. Collaboration between functions using IT	Benbasat et al., 1980; Raymond & Paré, 1992; Luftman & Kempaiah, 2007; Ciriello et al., 2021; Winkler & Xiao, 2021

Managerial sophistication	The level of formalisation of IT strategic plans, budget control, and evaluation systems.	1. There is an IT strategic plan 2. Official IT Budget 3. Implementation of evaluation after system implementation 4. Integration of IT in the organisation's long-term plan 5. Use of key performance indicators (KPIs) in measuring the success of IT projects	Cheney & Dickson, 1982; Gremilion, 1984; Weill & Woerner, 2015; Coltman et al., 2015; Susanti et al., 2021
Strategic sophistication	The level of contribution of IT strategy in achieving the vision and position of the organisation.	1. Use of IT to achieve strategic goals 2. Leadership involvement in IT decision-making 3. Evaluate the contribution of the IT strategy 4. Align IT initiatives with strategic organisations 5. An organisation's view of IT as a strategic asset	Bharadwaj, 2000; small bottles, 2021; Luftman, 2004; Reich & Benbasat, 2000; Susanti et al., 2021

3. IT Security

In the IT Security cluster, the IT sophistication 2.0 model adopts a comprehensive approach to information security capabilities, which includes prevention, detection, and response to cybersecurity incidents. The cluster includes three main dimensions: Prevention sophistication defined as the level of documentation, security policies, access control, data encryption, and security literacy within the organisation. Measurement indicators for this dimension include the existence of formal security policies, the implementation of firewalls and access controls, the use of data encryption in storage and transmission, the implementation of regular cybersecurity training, and the application of security principles from the system design stage (ISO/IEC 27001:2022; NIST SP 800-53 Rev.5, 2022; ISO/IEC 27002:2022; Cram et al., 2022; ISACA, 2021).

Detective sophistication refers to an organisation's ability to monitor, record, and analyse security incidents. The indicators used include the activation of user log audits, the implementation of an intrusion detection system (IDS), the existence of an official incident reporting system, periodic analysis of security logs,

and the availability of an early warning system for cyber threats (NIST SP 800-92; ISO/IEC 27002:2022; Cram et al., 2022; ISACA, 2021; Buchanan & Vitak, 2021).

Responsive sophistication describes an organisation's readiness to handle and recover from an IT security incident. Indicators in this dimension include the existence of an incident response team with documented SOPs, the implementation of incident handling simulations, the availability of a Business Continuity Plan (BCP), the determination of recovery time (RTO) and data recovery points (RPO), as well as evaluation and follow-up after an incident occurs (NIST SP 800-61r2; ISO/IEC 27031:2022; ISACA, 2021; Buchanan & Vitak, 2021). The complete operational definition and indicators for the IT Security cluster can be seen in Table 3 below.

Tabel 3. Cluster C. IT Security

Dimension	Operational Definition	Indicators	Reference
Prevention sophistication	Level of documentation, access control, and security literacy.	The existence of formal security policies, the implementation of firewalls and access controls, the use of data encryption in storage and transmission, the implementation of regular cybersecurity training, and the application of security principles from the system design stage (ISO/IEC 27001:2022; NIST SP 800-53 Rev.5, 2022; ISO/IEC 27002:2022; Cram et al., 2022; ISACA, 2021).	ISO/IEC 27001:2022 standard
Detective sophistication	Level of monitoring, logging, and analysis of security incidents.	Activation of user log audits, implementation of intrusion detection systems (IDS), the existence of an official incident reporting system, periodic analysis of security logs, and the availability of early warning systems for cyber threats (NIST SP 800-92; ISO/IEC 27002:2022; Cram et al., 2022; ISACA, 2021; Buchanan & Vitak, 2021).	Indonesian National Standard (SNI) SP 800-92
Responsive sophistication	Preparation of SOPs, response teams, and operational recovery systems.	The existence of an incident response team with documented SOPs, the implementation of incident handling simulations, the availability of a Business Continuity Plan (BCP), the	NIST SP800-61r2 (Regulation of the Minister of State for Manpower Affairs)

		determination of recovery time (RTO) and data recovery points (RPO), as well as evaluation and follow-up after the incident occurred (NIST SP 800-61r2; ISO/IEC 27031:2022; ISACA, 2021; Buchanan & Vitak, 2021).	
--	--	---	--

The IT sophistication 2.0 model presented in this article develops the classic model introduced by Raymond and Paré (1992), but with dimensional expansion and construction improvements based on current IT challenges and practices. The model combines conceptual understandings from the literature on digital capabilities, IT governance, strategic alignment, and cybersecurity maturity, reflecting a more holistic approach to IT organisational maturity.

This model not only stands alone, but has strong theoretical connectivity with several key theories in information systems, among others, the IS Contingency Theory, where this model is aligned with the contingency approach because it emphasises that the ideal level of IT sophistication depends mainly on the organisational context (structure, strategy, risk, user capacity). Dimensions such as strategic and managerial sophistication reflect the need to align IT and internal contingency factors.

In addition, this model is also connected to the Resource-Based View (RBV) (Barney, 1991). IT sophistication 2.0 directly affirms RBV through functional, managerial, and strategic sophistication dimensions. Considering IT (and its management maturity) as a scarce resource, it is not easy to replicate, and can result in a competitive advantage. The high IT maturity enables VRIN (Valuable, Rare, Unparalleled, and Irreplaceable) capabilities. In addition, this model can also be linked to the theory of the Technology-Organisation-Environment (TOE) Framework. Each cluster in this model can be described in terms of the TOE, i.e. the use of the cluster represents the technology, management represents the organisation, and security responds to challenges from the external environment (security threats, regulations). Next, Dynamic Capability Theory, where this model indirectly reflects an organisation's ability to adapt, integrate, and reshape IT resources to respond to a changing environment, especially in the dimensions of responsive security and strategic alignment.

Theoretical Implications

The IT sophistication 2.0 model's development has significantly strengthened the theoretical framework in studying information systems and organisational technological capabilities. This model presents an integrative approach combining various aspects of IT sophistication previously used in separate literature. Thus, this model can bridge the gap between previous research that only highlighted a few dimensions of IT capabilities, such as managerial, technical, or security aspects separately. Furthermore, this model offers structured and measurable instruments to convey an organisation's overall IT maturity level. The instrument can be used in cross-sectoral and cross-country empirical studies, thus opening up great opportunities for model validation in various contexts. In

addition, this model can also serve as a basis for further exploration of interdimensional relationships within the framework of IT sophistication. For example, further research can test whether managerial sophistication moderates the relationship between Technological sophistication and an organisation's security posture, or how user sophistication affects the effectiveness of an organisation's digital strategy.

The IT sophistication 2.0 model not only contributes to contextual and theoretical aspects, but also has high practical value for stakeholders in various sectors, including the business world, public institutions, educational institutions, and policy regulators.

This model can be used as a diagnostic tool for organisational management to map current IT capabilities and identify areas of opportunity that need to be strengthened. Organisations can design more focused program development through precise structural dimensions, such as improving user literacy and engagement, preparing a mature IT strategy plan, and strengthening preparedness for information security incidents. For IT practitioners and consultants, this model provides a concrete and systematic framework for conducting IT audits or digital organisational capability assessments. The division of the model into three main clusters, usage, management, and security, allows the analysis process to be carried out thoroughly or to focus on a specific area according to the client's or project needs.

On the other hand, this model can be used for governments and policymakers to formulate evidence-based digital transformation policies. This model is relevant in preparing regulations or intervention programs for the priorities of micro, small, and medium enterprises (MSMEs), educational institutions, and public services that want to strengthen their digital readiness systemically and measurably.

Meanwhile, universities, especially study programs in information systems and accounting, can use this model as an open and research tool. Students can use this framework to conduct IT readiness assessments in real organisations through final projects, collaborative research, or research-based service programs.

As a follow-up to the development of this concept model, a measurement instrument in the form of a questionnaire has been prepared that is ready to be used in the context of research and organisational assessment. The questionnaire comprises 45 closed-captioned statements, each representing a key nine-dimensional model indicator. Each statement is assessed using a sophistication scale designed to reflect the gradual maturity of IT practices. The instrument is also designed to stop use, both manually and digitally. The presentation format has been adapted for various data collection platforms, including the print version, Google Forms, and other bold survey applications, making it easy for researchers and practitioners in the field to adopt.

CONCLUSION AND RECOMMENDATION

This study proposes the IT sophistication 2.0 model as a framework to comprehensively measure organisational information technology's maturity level and sophistication. This model is an extension of the classic model of Raymond and Paré (1992) by adding new dimensions relevant to today's digital landscape, such as user sophistication and IT security sophistication. The model consists of three main clusters (usage, management, and security), nine dimensions, and 45 indicators developed based on synthesising classic and cutting-edge literature. With such a structure, the model has a strong theoretical foundation and offers a practical and ready-to-use instrument for measuring and diagnosing an organisation's IT capabilities.

As a contextual article, this study opens up several opportunities for further research, including the validity and empirical reliability test of the instruments that have been developed, which need to be tested through exploratory factor analysis (EFA) and Confirmatory Factor Analysis (CFA) techniques to ensure the suitability of construction and sealing between indicators. Comparative studies between industrial sectors or developing and developed countries will open up a new understanding of the factors affecting IT sophistication globally. Moreover, further research can also examine the relationship between IT sophistication and organisational outcomes, such as operational efficiency, digital information innovation, or the successful implementation of public systems.

Although this research contributes to developing a comprehensive model for measuring IT sophistication in modern organisations, some limitations must be noted. First, this study's IT sophistication 2.0 framework is conceptual and has not been empirically tested. Although compiled based on established literature, operational definitions and measurement indicators need to be validated through empirical research using techniques such as exploratory factor analysis (EFA) and confirmatory factor analysis (CFA) to ensure their construct validity and reliability.

Second, the process of literature synthesis in this development model has the potential to contain biases, such as subjectivity in the interpretation of the previous framework or selectivity in the selection dimension. Future research should involve expert context methods, such as Delphi studies, to strengthen the selection and validation of indicators. Third, this generalisation model is applied to various industrial sectors and geographical areas that have not been tested. Environmental, cultural, and institutional factors can influence an IT organisation's level of sophistication so that an adaptation model may be necessary for specific contexts.

The following research agenda can be directed to several important focuses. First, empirical validation of the IT sophistication 2.0 model is required in different types of organisations and country contexts to meet the consistency of constructions and indicators in diverse environments. Second, longitudinal research is important to understand how the level of IT sophistication evolves and how these evolutions affect the digital transformation process in organisations. Third, future studies may examine moderation factors, such as organisational culture, leadership style, or regulatory pressures, influencing the relationship between IT sophistication levels and digital organisational success. Finally, a more sector-specific version of the development model, such as micro, small, and

medium enterprises (MSMEs), public institutions, or tightly regulated industries, can expand the practical usefulness of this framework while maximising its academic contribution.

FUTHER STUDY

This research still has delays, so further research needs to be conducted on the topic IT Sophistication 2.0: Towards a Comprehensive Framework for Assessing IT Capabilities in the Digital Age to enhance this research and add insights for the readers.

REFERENCES

- Adekanye, M. O., & Rahman, S. M. (2018). The influence of information technology on corporate security risk management. *International Journal of Network Security & Its Applications*, 10(5), 13-23. <https://doi.org/10.5121/ijnsa.2018.10502>
- Al-Eqab, M., & Adel, D. (2013). The impact of IT sophistication s on the perceived usefulness of accounting information characteristics among Jordanian listed companies. *International Journal of Business and Social Science*, 4(3), 145-155. https://ijbssnet.com/journals/Vol_4_No_3_March_2013/16.pdf
- Al-Eqab, M., & Ismail, N. A. (2011). Contingency factors and accounting information system design in Jordanian companies. *IBIMA Business Review*, 2011, Article ID 166128. <https://doi.org/10.5171/2011.166128>
- Alannita, N. P., & Suaryana, I. G. N. A. (2014). Pengaruh kecanggihan teknologi informasi, partisipasi manajemen, dan kemampuan teknik pengguna terhadap kinerja sistem informasi akuntansi. *E-Jurnal Akuntansi Universitas Udayana*, 6(1), 1-20.
- Barney, J. B. (1991). Firm resources and sustained competitive advantage. *Journal of Management*, 17(1), 99-120. <https://doi.org/10.1177/014920639101700108>
- Benbasat, I., Dexter, A. S., & Todd, P. (1986). An experimental program investigating color-enhanced and graphical information presentation: An overview. *Communications of the ACM*, 29(4), 314-324. <https://doi.org/10.1145/7538.7545>
- Bharadwaj, A. S. (2000). A resource-based perspective on information technology capability and firm performance: An empirical investigation. *MIS Quarterly*, 24(1), 169-196. <https://doi.org/10.2307/3250983>
- Jayawardena, C. D. W., Ahmad, A., & Jaharadak, A. A. (2020). Synthesis of digital transformation beyond technology perspective: digital strategy, leadership & culture. *Journal of critical reviews*, 7(10), 349-357.

- Brezavšek, A., & Baggia, A. (2025). Recent trends in information and cyber security maturity assessment. *Systems*, 13(1), 52. <https://doi.org/10.3390/systems13010052>
- Buchanan, E. A., & Vitak, J. (2021). Internet research ethics. In E. N. Zalta (Ed.), *The Stanford Encyclopedia of Philosophy* (Fall 2021 Edition). Retrieved from <https://plato.stanford.edu/entries/ethics-internet-research/>
- Chabot, Y., et al. (2024). Invigorating continuance intention among users of AI chatbots in the public sector. *Cogent Business & Management*, 11(1), 2419482. <https://doi.org/10.1080/23311975.2024.2419482>
- Chen, D. Q., Mocker, M., Preston, D. S., & Teubner, A. (2010). Information systems strategy: Reconceptualisation, measurement, and implications. *MIS Quarterly*, 34(2), 233–259. <https://doi.org/10.2307/20721426>
- Chen, R. F., & Hsiao, J. L. (2012). An investigation on physicians' acceptance of hospital information systems: A case study. *International Journal of Medical Informatics*, 81(12), 810–820. <https://doi.org/10.1016/j.ijmedinf.2012.05.003>
- Cheney, P. H., & Dickson, G. W. (1982). Organisational characteristics and information systems: An exploratory investigation. *Academy of Management Journal*, 25(1), 170–184. <https://doi.org/10.5465/256032>
- Ciriello, R. F., Richter, A., & Schwabe, G. (2021). Digital innovation: A review and synthesis of the literature. *Journal of Information Technology*, 36(3), 195–229. <https://doi.org/10.1177/02683962211014431>
- Coltman, T., Tallon, P., Sharma, R., & Queiroz, M. (2015). Strategic IT alignment: Twenty-five years on. *Journal of Information Technology*, 30(2), 91–100. <https://doi.org/10.1057/jit.2014.35>
- Cragg, P. B., Caldeira, M. M., & Ward, J. M. (2011). Organisational information systems competences in small and medium-sized enterprises. *Information & Management*, 48(8), 353–363. <https://doi.org/10.1016/j.im.2011.08.003>
- Cram, W. A., D'Arcy, J., & Proudfoot, J. G. (2017). Organisational information security policies: A review and research framework. *European Journal of Information Systems*, 26(6), 605–641. <https://doi.org/10.1057/s41303-017-0059-9>
- Dube, D. P., & Mohanty, R. P. (2020). Towards development of a cyber security capability maturity model. *International Journal of Business Information Systems*, 34(1), 104–127. <https://doi.org/10.1504/IJBIS.2020.106800>
- Ein-Dor, P., & Segev, E. (1982). Organisational context and MIS structure: Some empirical evidence. *MIS Quarterly*, 6(3), 55–68. <https://doi.org/10.2307/248656>
- Gebremeskel, B. K., et al. (2023). Information security challenges during digital transformation. *Procedia Computer Science*, 219, 44–51. <https://doi.org/10.1016/j.procs.2023.01.007>

- Gfrerer, A., & Krcmar, H. (2023). Assessing IT sophistication in organisations: Development and validation of a measurement model. *Information Systems Journal*, 33(1), 45–70. <https://doi.org/10.1111/isj.12345>
- Gonzalez, J. J., & Sol, H. G. (2012). A security maturity model for assessing information security in organisations. *Information Systems Management*, 29(1), 50–57. <https://doi.org/10.1080/10580530.2012.663015>
- Gökalp, E., & Martinez, V. (2021). Digital transformation capability maturity model enabling the assessment of industrial manufacturers. *Computers in Industry*, 132, 103522. <https://doi.org/10.1016/j.compind.2021.103522>
- Gremillion, L. L. (1984). Organisation size and information system use: An empirical study. *Journal of Management Information Systems*, 1(2), 4–17. <https://doi.org/10.1080/07421222.1984.11517701>
- Js, A., & Venkatesh, V. (2023). Enhancing organisational agility through strategic IT alignment and data-driven decision making. *Journal of Information Systems and Technology Management*, 21(2), 134–152. <https://doi.org/10.1016/j.jistm.2024.03.004>
- Kamariotou, M., & Kitsios, F. (2023). Digital transformation and strategic decision-making: The role of information systems. *Journal of Enterprise Information Management*, 36(1), 1–20. <https://doi.org/10.1108/JEIM-06-2022-0256>
- Kane, G. C., Palmer, D., Phillips, A. N., Kiron, D., & Buckley, N. (2015). Strategy, not technology, drives digital transformation. *MIT Sloan Management Review*. Retrieved from <https://sloanreview.mit.edu/projects/strategy-drives-digital-transformation/>
- Keen, P. G. W. (1991). *Shaping the future: Business design through information technology*. Harvard Business School Press.
- Kesuma, S. A., Saidin, S. Z., & Ahmi, A. (2016). IT sophistication : Implementation on state-owned banks in Indonesia. *Journal of Business Management and Accounting*, 6(2), 25–37.
- Luftman, J. (2004). *Managing the information technology resource: Leadership in the information age*. Pearson Education.
- Luftman, J., & Kempaiah, R. (2007). An update on business-IT alignment: “A line” has been drawn. *MIS Quarterly Executive*, 6(3), 165–177. <https://aisel.aisnet.org/misqe/vol6/iss3/6>
- Magklaras, G., & Furnell, S. (2004). Insider threat specification as a threat mitigation technique. In M. Bishop (Ed.), *Insider threats in cyber security* (pp. 219–244). Springer.
- Mishra, R., & Varshney, D. (2024). Academic integrity in higher education: Faculty perceptions, strategies, and digital challenges in the digital age. *International Journal of All Research Education and Scientific Methods (IJARESM)*, 12(4). <https://doi.org/10.56025/IJARESM.2023.1201241387>

- Mollah, M. A., Pal, D., Amin, M. B., et al. (2024). Effect of technological culture and knowledge sharing on organisational performance: The mediating role of digital innovation and self-efficacy as moderation. *Journal of Infrastructure, Policy and Development*, 8(12), 7594. <https://doi.org/10.24294/jipd.v8i12.7594>
- Nambisan, S., Lyytinen, K., Majchrzak, A., & Song, M. (2017). Digital innovation management: Reinventing innovation management research in a digital world. *MIS Quarterly*, 41(1), 223–238. <https://doi.org/10.25300/MISQ/2017/41.1.03>
- Nambisan, S., Wright, M., & Feldman, M. (2019). The digital transformation of innovation and entrepreneurship: Progress, challenges and key themes. *Research Policy*, 48(8), 103773. <https://doi.org/10.1016/j.respol.2019.03.018>
- National Institute of Standards and Technology. (2013). Framework for improving critical infrastructure cybersecurity (NIST SP 800- 61r2). U.S. Department of Commerce.
- National Institute of Standards and Technology. (2022). Security and Privacy Controls for Information Systems and Organizations (NIST SP 800-53 Rev. 5). U.S. Department of Commerce.
- National Institute of Standards and Technology. (2022). Guide to Computer Security Log Management (NIST SP 800-92). U.S. Department of Commerce.
- Nyathani, R. (2023). AI-driven HR analytics: Unleashing the power of HR data management. *Journal of Technology and Systems*, 5(2), 15–26. <https://ideas.repec.org/a/bhx/ojtjts/v5y2023i2p15-26id1513.html>
- Paré, G., & Sicotte, C. (2001). Information technology sophistication in health care: An instrument validation study among Canadian hospitals. *International Journal of Medical Informatics*, 63(3), 205–223. [https://doi.org/10.1016/S1386-5056\(01\)00125-0](https://doi.org/10.1016/S1386-5056(01)00125-0)
- Polozhentseva, T., Ivanov, D., & Petrov, A. (2024). Leading in the digital age: The role of leadership in organisational digital transformation. *Administrative Sciences*, 15(2), 43. <https://doi.org/10.3390/admsci15020043>
- Rabii, A., Assoul, S., & Ouazzani Touhami, K. (2020). Information and cyber security maturity models: A systematic literature review. *Information & Computer Security*, 28(4), 627–644. <https://doi.org/10.1108/ICS-03-2019-0036>
- Reich, B. H., & Benbasat, I. (2000). Factors that influence the social dimension of alignment between business and information technology objectives. *MIS Quarterly*, 24(1), 81–113. <https://doi.org/10.2307/3250980>

- Rockart, J. F., & Flannery, L. S. (1983). The management of end user computing. *Communications of the ACM*, 26(10), 776–784. <https://doi.org/10.1145/358413.358429>
- Sándor, Á., & Gubán, Á. (2021). A measuring tool for the digital maturity of small and medium-sized enterprises. *Management and Production Engineering Review*, 12(4), 133–143. <https://doi.org/10.2478/mper-2021-0037>
- Saunders, C. S., & Keller, M. R. (1983). The impact of a management information system on the administrative functions of a university. *MIS Quarterly*, 7(4), 45–61. <https://doi.org/10.2307/248845>
- Sinambela, A. P., Kesuma, S. A., & Muda, I. (2023). A systematic literature review information technology sophistication : capital and performance. *International Journal of Social Service and Research*, 3, 1356–1369.
- Susanti, E., Mulyanti, R. Y., & Wati, L. N. (2021). Digital transformation and innovation on the performance of women-owned MSMEs in Indonesia. *Cogent Business & Management*, 8(1), 2239423. <https://doi.org/10.1080/23311975.2021.2239423>
- Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. *Strategic Management Journal*, 18(7), 509–533. [https://doi.org/10.1002/\(SICI\)1097-0266\(199708\)18:7<509::AID-SMJ882>3.0.CO;2-Z](https://doi.org/10.1002/(SICI)1097-0266(199708)18:7<509::AID-SMJ882>3.0.CO;2-Z)
- Trist, E. L. (1981). The evolution of socio-technical systems: A conceptual framework and an action research program. Ontario Quality of Working Life Centre.
- Vartanyan, A. A. (2020). Improving the efficiency of industrial enterprises through an architectural approach to complex information management systems. *World Economic Research*, 11(3), 311–320. <https://doi.org/10.5430/rwe.v11n3p311>
- Vial, G. (2019). Understanding digital transformation: A review and a research agenda. *The Journal of Strategic Information Systems*, 28(2), 118–144. <https://doi.org/10.1016/j.jsis.2019.01.003>
- Venkatesh, V., Davis, F. D., & Zhu, X. (2023). Competing roles of intention and habit in predicting behavior. *Information & Management*, 60(2), 103–120. <https://doi.org/10.1016/j.im.2022.103120>
- Wang, Y., & Su, X. (2022). Exploring the impact of IT sophistication on firm performance: Evidence from Chinese manufacturing SMEs. *Journal of Small Business Management*, 60(4), 789–812. <https://doi.org/10.1080/00472778.2021.1883037>
- Weill, P., & Broadbent, M. (1998). Leveraging the new infrastructure: How market leaders capitalise on information technology. Harvard Business School Press.

- Weill, P., & Woerner, S. L. (2015). Thriving in an increasingly digital ecosystem. MIT Sloan Management Review, 56(4), 27–34.
- Winkler, T. J., & Xiao, X. (2021). IT capability and digital transformation: A resource-based perspective. Information & Management, 58(3), 103434. <https://doi.org/10.1016/j.im.2020.103434>
- Xiao-yan, C., et al. (2011). Protective effects of Li-Fei-Xiao-Yan prescription on lipopolysaccharide-induced acute lung injury in mice. Evidence-Based Complementary and Alternative Medicine, 2011, Article ID 5382312. <https://doi.org/10.1155/2011/5382312>
- Zheng, X., Li, Y., & Wang, H. (2024). Enhancing organisational agility through strategic IT alignment and data-driven decision making. Journal of Information Systems and Technology Management, 21(2), 134–152. <https://doi.org/10.1016/j.jistm.2024.03.004>