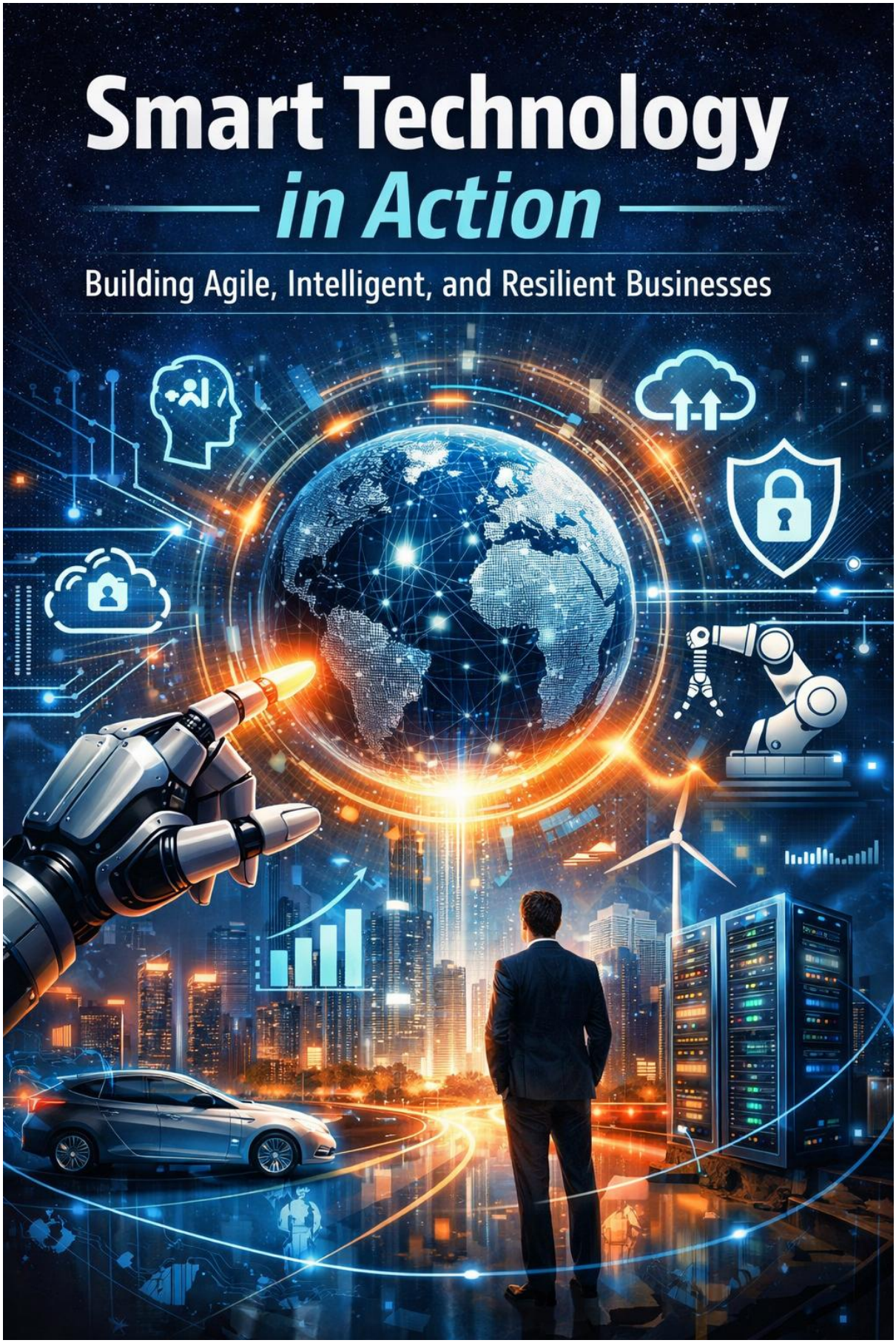
Smart Technology
in Action
Building Agile, Intelligent, and Resilient Businesses

By:
Prof Ir Rudy C Tarumingkeng, PhD
Professor of Management NUP: 9903252922
Rector, Cenderawasih State University, Papua (1978-1988, dan
Head, AGRO Manokwari Campus, (now Universitas Papua Manokwari)
Coordinator, CIDA/DIKTI SFU Burnaby BC Canada 1988-1991
Rector, Krida Wacana Christian University, Jakarta (1991-2000)
Chairman, Board of Professors, IPB-University, Bogor (2005-2006)
AI - Data Analyst, dan Chairman Academic Senate, IBM-ASMI, Jakarta 2024-

---

rudyct75@gmail.com
22 March 2026

SMART TECHNOLOGY IN ACTION: BUILDING AGILE, INTELLIGENT, AND RESILIENT BUSINESSES

Abstract

This essay examines how smart technology can be used in practice to build businesses that are agile in response, intelligent in decision-making, and resilient under disruption. It argues that digital maturity is not defined by technology ownership alone, but by the ability to integrate artificial intelligence, data systems, automation, cloud infrastructure, and cybersecurity into a coherent business architecture. In this framework, agility refers to the capacity to sense change early and respond quickly; intelligence refers to the ability to convert data into sound managerial judgment; and resilience refers to the capability to absorb shocks, adapt under pressure, and continue functioning in unstable conditions. The essay shows that smart technology strengthens these capabilities by improving visibility, prediction, coordination, and process redesign. At the same time, it emphasizes that technology is not inherently beneficial. Its value depends on data governance, workforce capability, leadership discipline, trustworthy AI practices, cyber resilience, and strategic purpose. The discussion also highlights a digital paradox: the same technologies that improve efficiency and adaptability can also increase energy demand, cyber exposure, and inequality if deployed without proper governance. Drawing on recent evidence from the OECD, World Bank, NIST, IFRS Foundation, IEA, UN Trade and Development, and the World Economic Forum, the essay concludes that the most successful firms will be those that combine technological capability with

organizational judgment, human development, and long-term responsibility. (OECD)

Keywords

Smart technology; digital transformation; business agility; business intelligence; business resilience; artificial intelligence; data governance; cyber resilience; workforce capability; sustainable digitalization.

Smart Technology in Action: Building Agile, Intelligent, and Resilient Businesses

Introduction

The contemporary business environment is being reshaped by a convergence of forces that are both technological and structural. Artificial intelligence, cloud computing, connected devices, advanced analytics, digital platforms, automation, and cybersecurity systems are changing not only how firms operate, but also how they compete, innovate, and survive. At the same time, businesses face an external environment marked by volatility in supply chains, rising cyber risk, demanding customers, workforce disruption, sustainability pressure, and accelerating regulatory expectations. In such a context, the value of smart technology does not lie merely in novelty. Its significance lies in action: in the way it helps firms become more agile in response, more intelligent in decision-making, and more resilient in the face of disruption. The OECD describes the current phase as a new stage of digital transformation characterized by rapid technological change, while also emphasizing that digital transformation depends on foundations such as connectivity and skills, and on trust-related capabilities such as digital security and data governance. (OECD)

The phrase “smart technology in action” is important because it shifts attention away from technology as possession and toward technology as

capability. Many businesses today can purchase software, subscribe to cloud services, and experiment with AI tools. That alone does not make them digitally mature. What matters is whether these technologies are integrated into the firm's ability to sense change, process information, coordinate action, reduce waste, anticipate threats, support workers, and create sustainable value. In this respect, smart technology is less a collection of devices than an architecture of organizational intelligence. The World Bank's 2025 report on AI foundations argues that effective and inclusive AI ecosystems depend on the "four Cs": connectivity, compute, context, and competency. This framework is highly relevant to firms as well, because it shows that digital transformation succeeds only when infrastructure, data, and human capability evolve together. (World Bank)

This essay argues that businesses become agile, intelligent, and resilient not by deploying the largest number of tools, but by learning how to connect technology with strategy, process redesign, workforce development, governance, and purpose. An agile business is one that can perceive changes early and respond quickly. An intelligent business is one that can convert data into judgment. A resilient business is one that can absorb shocks, adapt under pressure, and continue functioning when conditions become unstable. Smart technology can strengthen all three, but only if it is managed deliberately. When managed poorly, the same technology can produce the opposite outcomes: faster confusion, deeper dependence, higher cyber exposure, greater energy demand, and widening inequality between firms and workers. UN Trade and Development warns that digitalization can promote inclusion and sustainability, but that unregulated digitalization can also intensify raw-material depletion, energy use, water use, pollution, and waste. (UN Trade and Development (UNCTAD))

The modern managerial challenge, therefore, is no longer simply to digitize. It is to build a business that can use digital systems intelligently

under real-world conditions of uncertainty. That challenge is especially significant because AI adoption by firms has accelerated rapidly in OECD countries. OECD data released in early 2026 indicate that 20.2% of firms reported using AI in 2025, up from 14.2% in 2024 and 8.7% in 2023, meaning that firm-level adoption more than doubled over two years. Yet this growth remains uneven across industries and firm sizes, which suggests that the next wave of competition will be shaped not merely by access to tools, but by the ability to govern and scale them productively. (OECD)

The Meaning of Agility in a Digital Business Age

In everyday business language, agility is often reduced to speed. A firm is called agile if it launches quickly, responds rapidly, or changes direction with minimal delay. Yet a deeper understanding is needed. True agility is not simple acceleration. It is the capacity to reconfigure intelligently in response to change. An agile firm can detect shifts in demand, recognize emerging risks, interpret signals from customers and suppliers, and alter operations without losing coherence. Smart technology becomes crucial here because it changes the firm's sensing ability. Through digital platforms, analytics, sensors, and AI-supported forecasting, businesses can observe what was previously invisible: changing consumption patterns, equipment stress, supplier delays, quality anomalies, and operational bottlenecks. OECD work on the digital economy underscores that data, technologies, and new business models are major drivers of the ongoing transformation of economies and organizations. (OECD)

To appreciate this, consider a retailer facing volatile customer demand and fragmented channels. In the past, the company might have relied on delayed sales reports, seasonal assumptions, and managerial intuition. In a digitally integrated environment, it can track demand in near real time, compare online and offline behavior, identify regional variation, and

predict which product lines are gaining momentum. This does not eliminate uncertainty, but it changes the quality of the response. The firm moves from reacting late to adapting early. Agility in this sense is informational before it is operational. It begins when the organization can see clearly enough to act with purpose rather than improvisation.

The same applies in manufacturing, logistics, finance, health services, and education. Smart technology allows organizations to shorten the distance between event and response. Cloud systems make information more accessible across teams. AI tools improve pattern recognition. IoT devices create continuous visibility into physical operations. Digital workflows reduce friction in cross-functional coordination. When these systems are well designed, agility becomes embedded in the structure of the organization. But when they are fragmented, the opposite occurs: firms collect vast data yet remain slow because the data does not move meaningfully into decisions. This is why agility is inseparable from integration. Technology must support organizational choreography, not just information accumulation.

A helpful way to think about this is to distinguish between digitized firms and agile firms. A digitized firm may have online processes, dashboards, and digital tools. An agile firm can redeploy resources, revise priorities, and adapt workflows because its digital infrastructure supports coordinated change. In that sense, agility is not a feature of the technology alone. It is a feature of the relationship between technology and management. This is consistent with OECD evidence that the benefits of AI and related tools depend on complementary assets such as management practices, workforce skills, and ICT capabilities. (OECD)

Building Intelligent Businesses: Data, AI, and Better Judgment

If agility is about response, intelligence is about judgment. An intelligent business is not simply a firm with large datasets or advanced algorithms. It is a firm that can turn information into better decisions. This requires

much more than software acquisition. It requires relevant data, appropriate models, context-sensitive interpretation, and clear accountability. In modern enterprises, this intelligence operates at multiple levels. At the operational level, it helps optimize processes and reduce inefficiencies. At the tactical level, it supports forecasting, pricing, scheduling, and service quality. At the strategic level, it informs investment, risk management, product development, and competitive positioning. NIST's AI Risk Management Framework emphasizes that AI should be managed in ways that improve trustworthiness and public trust, which makes clear that the value of AI depends not only on performance, but on how it is governed in context. (NIST Publications)

This is a critical point because organizations often confuse information abundance with intelligence. They accumulate data from customers, sensors, transactions, and digital platforms, but still fail to make good decisions because the data is incomplete, inconsistent, poorly governed, or disconnected from workflow. Smart technology becomes genuinely intelligent only when the firm builds the discipline needed to use it well. That discipline includes data governance, model oversight, workflow integration, role clarity, and mechanisms for human review. Without these, AI may produce outputs that appear impressive but are strategically weak.

One of the most important lessons from current research is that AI's value is highly task-dependent. OECD evidence suggests that AI can improve performance in many specific tasks, yet those benefits vary widely across use cases and sectors, and broader productivity effects depend on complementary investments in management, skills, and digital infrastructure. This means that smart firms are selective. They do not deploy AI merely because it is fashionable. They deploy it where prediction, classification, generation, or optimization materially improves the economics or resilience of the business. (OECD)

Imagine a logistics firm trying to reduce failed deliveries, fuel costs, and warehouse congestion. A superficial AI strategy might install dashboards and claim digital transformation. A more intelligent approach would identify the key points where better prediction changes outcomes: route optimization, demand anticipation, maintenance schedules, inventory positioning, and disruption detection. In that scenario, AI is not an abstract symbol of modernization. It is a decision-support layer embedded in concrete business problems. Intelligence, then, is the capacity to apply technology precisely where judgment can be improved.

At this stage, a crucial managerial insight emerges: intelligent business is not equivalent to fully automated business. The more powerful AI becomes, the more important it is to define the boundary between machine assistance and human responsibility. NIST's framework explicitly highlights issues such as validity, reliability, safety, security, transparency, explainability, and fairness. These qualities matter because many business decisions are not purely technical. Credit assessment, hiring, healthcare triage, procurement screening, and customer service escalation all involve context, ethics, and potential reputational consequences. Smart technology should improve judgment, not replace accountability. (NIST Publications)

Data Governance as the Hidden Foundation of Business Intelligence

An intelligent business rests on a foundation that is often neglected because it is less visible than AI applications or user interfaces. That foundation is data governance. Data governance is not a bureaucratic add-on to digital transformation. It is what makes transformation credible. Without reliable, consistent, secure, and well-structured data, firms cannot forecast effectively, report accurately, automate responsibly, or defend the outputs of their systems. The World Bank's "four Cs" framework places "context," meaning locally relevant data and content,

at the heart of AI readiness, while also emphasizing the importance of competency and governance to ensure responsible use. (World Bank)

Why does this matter so much? Because organizations are increasingly judged not only by what they do, but by whether they can explain how and why they do it. This applies to customer decisions, financial decisions, supplier decisions, and sustainability claims. If a firm uses AI to prioritize clients, detect fraud, optimize inventory, or evaluate risks, it must know what data enters the system, how that data is validated, who oversees the model, and how errors are escalated. Otherwise, it does not truly manage intelligence; it merely consumes it.

This issue is becoming even more important because sustainability and digital transformation are converging. IFRS S1, effective for annual reporting periods beginning on or after 1 January 2024, requires entities to disclose sustainability-related risks and opportunities that could reasonably be expected to affect cash flows, access to finance, or cost of capital, and it also requires disclosure of governance processes, strategy, and risk management. This means that firms increasingly need integrated information systems capable of linking operational, strategic, and sustainability-related data. Businesses that cannot manage their data architectures will find it difficult to satisfy both internal decision needs and external disclosure expectations. (IFRS Foundation)

A hypothetical example shows how this works in practice. Consider a food company under pressure to reduce waste, improve traceability, and provide more transparent sustainability disclosures. If its procurement data sits in one system, manufacturing data in another, logistics data in a third, and sustainability data in manually updated spreadsheets, then even a sophisticated AI layer will struggle to add real value. But if the company builds a governed data structure across procurement, production, inventory, and reporting, then smart technology can begin to identify spoilage risks, optimize batch planning, support supplier

traceability, and generate more reliable disclosures. The intelligence does not come first. The data discipline does.

Smart Technology and the Reinvention of Operations

One of the clearest arenas in which smart technology acts is operations. This is where agility, intelligence, and resilience often converge most visibly. Operations include production, logistics, service workflows, maintenance, scheduling, and quality control. In all these areas, the business challenge is similar: too much waste, too much delay, too little visibility, and too much dependence on reactive management. Smart technology helps by transforming operations from opaque systems into observable systems.

Sensors, for instance, allow equipment conditions to be monitored continuously. Predictive models can identify abnormal patterns before failure occurs. Workflow analytics can reveal where approvals are delayed. Digital twins can simulate changes before they are executed physically. Cloud-based systems can allow geographically dispersed teams to work from common information. When these tools are connected to managerial action, firms can reduce downtime, improve throughput, lower energy use, and respond more quickly to disruptions.

The energy dimension is especially significant because smart operational technology is increasingly tied to resource efficiency. The IEA emphasizes that there is no AI without energy, and that affordable, reliable, and sustainable electricity supply is a crucial determinant of AI development. At the same time, AI can optimize energy use and support system-wide efficiency improvements. This means that operational intelligence has two directions: technology consumes energy, but it can also reduce wasteful consumption elsewhere. (IEA)

In industry, this can be seen in predictive maintenance, process optimization, and energy monitoring. In logistics, route optimization and

dynamic scheduling can reduce idle time, travel distance, and fuel use. In commercial buildings, smart controls can reduce unnecessary heating, cooling, and lighting loads. In agriculture, digital tools can improve irrigation and input management. The World Bank's 2025 AI report includes case studies on how AI is being used in agriculture and energy to improve efficiency and service delivery, showing that the operational value of AI is not confined to large tech firms or office environments. (World Bank)

But a caution is necessary. Not all operational technology produces resilience. Some technologies optimize narrowly for normal conditions while leaving firms more vulnerable to unusual events. A tightly optimized supply system with little redundancy may be efficient under stable conditions but brittle under disruption. Smart thinking therefore requires businesses to redesign operations not only for efficiency, but for adaptive capacity. Operational excellence in the digital age must include the ability to switch modes under stress, not merely the ability to run faster when everything is working well.

Resilience: Why Smart Businesses Must Be Designed for Shock

If agility is the capacity to respond and intelligence is the capacity to decide well, resilience is the capacity to endure. This has become especially important because the business environment now includes multiple, overlapping sources of disruption: cyberattacks, geopolitical fragmentation, supply-chain vulnerabilities, infrastructure failures, climate-related events, and sudden shifts in labor or regulation. Smart technology can help firms withstand these shocks, but it also creates new dependencies that must be managed carefully.

Cybersecurity is perhaps the most obvious example. The more connected a business becomes, the more exposed it becomes to cyber risk. Cloud services, connected devices, automated workflows, third-party software, remote access, and AI-enabled tools all enlarge the attack

surface. The World Economic Forum's Global Cybersecurity Outlook 2025 reports that cyber resilience is highly uneven and that public-sector organizations, in particular, report significantly weaker resilience and larger talent gaps than medium-to-large private-sector organizations. The report also notes that large organizations identify supply-chain challenges as the biggest barrier to achieving cyber resilience, highlighting how lack of visibility into supplier security has become a leading risk. (World Economic Forum)

NIST's Cybersecurity Framework 2.0 is directly relevant here because it is designed to help organizations of all sizes and sectors manage and reduce cybersecurity risks, and to address cyber risks alongside broader enterprise risks such as financial, reputational, technological, supply-chain, and physical risks. This perspective is important because cyber resilience is not just an IT issue. It is an enterprise issue. A ransomware attack can halt operations, damage customer trust, disrupt suppliers, and trigger financial losses. A data breach can undermine strategy, compliance, and reputation simultaneously. Firms that treat digital resilience as a technical matter confined to specialists misunderstand the nature of the threat. (NIST Publications)

Resilience also has an informational side. In times of disruption, organizations need trusted data and clear decision rights. If systems fail or become compromised, can the firm still operate? Can teams access critical information? Are dependencies on particular vendors or platforms understood? Is there visibility across the supply chain? These are not glamorous questions, but they often determine whether a business weathers disruption or collapses into confusion.

A narrative illustration may help. Imagine a regional distributor hit by simultaneous shocks: a cyber incident affecting logistics software, a supplier delay caused by geopolitical restrictions, and a spike in demand from customers attempting to build inventory. A conventional firm might

respond with ad hoc firefighting. A resilient smart business would already have mapped critical dependencies, segmented systems, tested backup workflows, diversified key suppliers, and built dashboards that distinguish essential from non-essential demand. Technology matters in such a scenario, but what matters more is the design of the system around the technology. Resilience is engineered through preparation, not improvised through panic.

Workforce Transformation: Skills, Augmentation, and Human Capability

No business becomes agile, intelligent, and resilient without people. One of the most persistent myths about smart technology is that it reduces the importance of the human element. In reality, it increases the importance of certain human capabilities even as it automates some tasks. The World Economic Forum's Future of Jobs Report 2025 finds that employers expect 39% of workers' core skills to change by 2030, and that skills gaps are the primary barrier to business transformation, cited by 63% of surveyed employers. These findings are highly relevant because they show that digital transformation is not merely a procurement problem. It is a workforce problem. (World Economic Forum)

What kinds of capabilities matter most in smart businesses? Technical skills certainly matter: data literacy, AI familiarity, cybersecurity awareness, cloud and software fluency, and analytical reasoning. But so do broader human capacities: problem framing, interpretation, communication, adaptability, ethical reasoning, and collaborative judgment. A firm can install advanced tools and still fail if managers cannot ask good questions, if employees do not trust the systems, or if teams cannot translate digital insights into real operational change.

The World Bank's "competency" pillar emphasizes that robust digital skills are indispensable for adopting, adapting, and innovating with AI.

This suggests that digital capability should be treated as core business infrastructure, not as an optional HR initiative. Firms that invest in systems but underinvest in people create a structural imbalance. They possess tools without the human capacity to absorb them. Conversely, firms that build digital fluency across the workforce can often derive significant value from relatively modest technological investments. (World Bank)

There is also a crucial distinction between replacement and augmentation. Policy discussions increasingly emphasize that AI should complement and augment human workers rather than simply replace them. The World Bank explicitly notes this as a policy challenge, and the point is equally valid at firm level. When technology is introduced in a way that strips workers of autonomy, creates surveillance without trust, or treats staff mainly as costs to be removed, resistance and disengagement often follow. When technology is introduced as a support system—reducing routine burdens, improving learning, and enabling higher-value work—the organization is more likely to gain both productivity and legitimacy. (World Bank)

A practical example would be a customer service company introducing AI-assisted support tools. A poorly managed approach might use the technology mainly to measure and control workers more intensely. A better approach would define which repetitive tasks the AI handles, where human empathy and judgment remain essential, how errors are corrected, and how staff are trained to work with the system confidently. In the second case, technology becomes a partner in service quality. In the first, it becomes a source of stress and mistrust.

Leadership and Governance: The Difference Between Adoption and Maturity

Technology adoption is easy to announce and difficult to govern. This is where leadership becomes decisive. Many businesses proclaim digital

transformation because they have deployed tools. Far fewer can demonstrate digital maturity, meaning the ability to align technology with goals, integrate it into decision structures, manage its risks, and adapt it over time. Leadership in smart businesses is therefore less about celebrating innovation than about orchestrating it.

A first responsibility of leadership is prioritization. Not every technology deserves equal attention. Smart leaders identify which digital capabilities are most strategically material for the organization. In one firm, the priority may be better forecasting. In another, cyber resilience. In another, supply-chain traceability. In another, sustainability reporting. The question is not what technology is most fashionable, but what capability most strengthens the business under current and future conditions.

A second responsibility is governance. This includes who owns data quality, who oversees AI use, how digital risks are escalated, how vendors are assessed, how models are validated, and how compliance, operations, HR, finance, and strategy coordinate around technology decisions. NIST's AI RMF and CSF 2.0 both reflect the idea that risk management must be organizational, not merely technical. They are designed to be intelligible to executives and managers, not just specialists, precisely because digital risk now sits at the center of enterprise decision-making. (NIST)

A third responsibility is timing. Not every organization should pursue the same digital ambitions at the same pace. Some need to fix data architecture before they scale AI. Some need stronger cybersecurity before they expand cloud dependence. Some need workforce upskilling before they automate more aggressively. Smart leadership recognizes sequencing. It understands that foundations often matter more than visible applications. This perspective aligns with the World Bank's argument that connectivity, compute, context, and competency are

bedrocks of effective AI ecosystems, and with OECD findings that AI productivity gains depend on complementary organizational investments. (World Bank)

Leadership also requires narrative clarity. Employees, investors, customers, and partners need to know why the business is investing in smart technology. If the story is only about efficiency, transformation may look threatening. If the story includes better service, more adaptive operations, higher-quality decisions, stronger resilience, and sustainable value creation, then the organization has a clearer basis for commitment. Purpose is not a cosmetic addition to technology strategy. It is what gives transformation legitimacy.

Sustainability, Inclusion, and the Limits of Technological Optimism

A serious essay on smart technology cannot end with efficiency and growth alone. Businesses now operate in a world where questions of sustainability, inclusion, and long-term responsibility are unavoidable. Smart technology can help firms reduce waste, optimize routes, improve energy use, enhance transparency, and support circular business models. But the digital economy itself has material consequences. UNCTAD stresses that digital infrastructure relies heavily on raw materials and that the production and disposal of devices, alongside growing water and energy needs, are taking an increasing toll on the planet. The IEA, in turn, emphasizes that AI development depends on large and power-hungry data centres, making reliable and sustainable electricity supply a crucial determinant of AI's future. (UN Trade and Development (UNCTAD))

This creates a digital paradox. On one side, smart technology can make businesses leaner, cleaner, and more adaptive. On the other, it can increase resource demand, deepen digital inequality, and create new forms of dependence. The answer is not to reject technology, but to govern it more wisely. Firms need to ask not only whether a digital investment improves performance, but also how it affects energy use,

supply-chain complexity, workforce equity, and institutional trust. The OECD's digital economy work explicitly links digital transformation with net-zero goals and environmental protection, suggesting that the digital and green transitions should be treated as intertwined rather than separate agendas. (OECD)

Inclusion is equally important. The benefits of smart technology are not evenly distributed across firms, sectors, or countries. The World Bank notes a stark divide in the global AI landscape, with most innovations concentrated in high-income countries, while low- and middle-income countries are more likely to rely on "small AI" solutions and still need investment in foundational capabilities. This has implications for businesses everywhere. Large firms may capture disproportionate gains unless ecosystems are strengthened to help smaller firms access affordable tools, digital skills, cloud services, and trusted infrastructure. A truly resilient digital economy cannot be built on concentration alone. (World Bank)

Thus, the mature business view of smart technology is neither utopian nor cynical. It recognizes technology as a powerful lever whose value depends on stewardship. A firm that uses digital tools to reduce waste, support workers, strengthen decisions, improve traceability, and prepare for shocks is likely to build more durable value than a firm that uses them only to accelerate transactions or intensify extraction. In the long run, intelligence without responsibility is not resilience. It is fragility disguised as progress.

Conclusion

Smart technology in action is not fundamentally about machines. It is about how organizations learn to act under conditions of complexity. Businesses become agile when technology helps them sense change earlier and reconfigure more quickly. They become intelligent when they can convert data into sound judgment through governed, context-

sensitive systems. They become resilient when they can absorb shocks, manage cyber risk, diversify dependencies, and continue operating when disruption occurs. These capabilities are connected. Agility without intelligence becomes impulsiveness. Intelligence without resilience becomes vulnerability. Resilience without agility becomes rigidity. Smart technology matters because, when governed well, it can help firms build all three at once. (OECD)

The evidence from OECD, NIST, the World Bank, the World Economic Forum, the IEA, UN Trade and Development, and the IFRS Foundation points toward a clear conclusion: the next generation of successful businesses will not simply be more digital. They will be more capable of integrating digital systems with management quality, human capability, trust, sustainability, and strategy. AI adoption is rising, but adoption alone is not enough. The foundations of digital maturity—connectivity, data context, competency, governance, cybersecurity, and purpose—will determine whether firms derive durable value or simply accumulate more complexity. (OECD)

For that reason, the future belongs not to firms that chase every emerging tool, but to those that understand how to make technology serve a coherent business philosophy. Such firms will use AI not as a spectacle, but as a decision aid. They will use data not as a slogan, but as disciplined evidence. They will treat cybersecurity not as a technical afterthought, but as a core element of resilience. They will understand that workforce capability is not secondary to digital investment, but one of its preconditions. And they will recognize that sustainability is not separate from digital transformation, but part of what makes digital transformation worth pursuing in the first place. In that fuller sense, smart technology in action is the craft of building businesses that can move quickly, think clearly, and endure wisely. (World Economic Forum)

Glossary

1. Smart technology
Digital tools and systems that collect data, process information, support decisions, and often interact dynamically with operational environments. In business, this commonly includes AI, analytics, cloud systems, connected devices, and automation. (OECD)

2. Business agility
The organizational ability to detect changes quickly and reconfigure actions, processes, or resources in response. In a digital context, agility depends heavily on data access, connectivity, and coordination. This is an inference based on OECD's treatment of digital foundations and drivers of transformation. (OECD)

3. Intelligent business
A business that can convert data into timely, context-sensitive, and strategically useful decisions. Intelligence in this sense is not mere data accumulation; it depends on governance, interpretation, and action. This is an inference supported by OECD and NIST materials on AI use and trustworthy AI. (NIST)

4. Business resilience
The capacity of a firm to withstand shocks, adapt to disruption, and continue functioning under adverse conditions. In digitally intensive firms, resilience includes operational continuity, cyber preparedness, and robust decision systems. (NIST)

5. Data governance
The policies, roles, standards, and controls used to ensure that data is accurate, secure, usable, and properly managed. It is essential because AI and analytics only create dependable value when the underlying data and oversight structures are reliable. This is an inference from NIST, OECD, and IFRS guidance. (NIST)

6. Trustworthy AI
AI that is developed and used with attention to validity, reliability, safety, security, accountability, transparency, explainability, privacy, and managed bias. (NIST)

7. Cyber resilience
The ability of an organization not only to defend against cyber threats, but also to prepare for, respond to, recover from, and adapt after cyber incidents. (NIST)

8. AI foundations
The World Bank's framework of connectivity, compute, context, and competency as the core conditions needed for effective and inclusive AI adoption. (World Bank)

9. Sustainability-related risks and opportunities
Under IFRS S1, these are sustainability-related matters that could reasonably be expected to affect an entity's cash flows, access to finance, or cost of capital over the short, medium, or long term. (IFRS Foundation)

10. Skills gap
The mismatch between the capabilities workers currently have and the capabilities businesses need. The World Economic Forum identifies skills gaps as a major barrier to business transformation. (World Economic Forum)

11. Digital paradox
The tension that digital technologies can improve productivity, innovation, and sustainability performance while also increasing electricity demand, material use, cyber exposure, and governance complexity. (UN Trade and Development (UNCTAD))

12. Purposeful digital transformation
A form of transformation in which technology adoption is guided by

strategic goals, governance, workforce capability, and long-term value creation rather than by novelty alone. This is an inference from the combined logic of OECD, NIST, and World Bank sources. (OECD)

APA 7 References

The reference list below is formatted in APA 7 style and draws on the official institutional publications used in the essay. (OECD)

IFRS Foundation. (2023). *IFRS S1 general requirements for disclosure of sustainability-related financial information*. IFRS Foundation.

International Energy Agency. (2025). *Energy and AI*. IEA.

National Institute of Standards and Technology. (2023). *Artificial intelligence risk management framework (AI RMF 1.0)* (NIST AI 100-1). U.S. Department of Commerce.

National Institute of Standards and Technology. (2024). *The NIST cybersecurity framework (CSF) 2.0* (NIST CSWP 29). U.S. Department of Commerce.

OECD. (2024). *Fostering an inclusive digital transformation as AI spreads among firms*. OECD Publishing.

OECD. (2024). *OECD digital economy outlook 2024* (Vol. 2). OECD Publishing.

UN Trade and Development. (2024). *Digital economy report 2024: Shaping an environmentally sustainable and inclusive digital future*. United Nations.

World Bank. (2025). *Digital progress and trends report 2025: Strengthening AI foundations*. World Bank.

World Economic Forum. (2025). *The future of jobs report 2025*. World Economic Forum.

World Economic Forum. (2025). *Global cybersecurity outlook 2025*. World Economic Forum.

Copilot for this article: ChatGPT 5.2. Thinking (2025). Access date: 22 March 2026. Author's account

https://chatgpt.com/c/69bf5e8b-e174-8399-90ba-20f651be6a0b