

# Executive summary

The digitalisation of businesses has continued apace in recent years. Across sectors, firms of all sizes are increasingly equipping their staff with digital tools, although smaller firms do so more slowly, and some sectors do so more quickly. Digitalisation is multi-faceted as it involves the use of different technologies, serving different purposes, and requires a recombination of different strategic assets. Not all SMEs have the capacity to undertake this transformation. The smaller the firms, the less likely they are to adopt new digital practices, and the more likely they are to limit uptake to basic services. Overall, SME digitalisation is strongly related to the way value is created within the firm and the sector in which it operates.

SMEs tend to digitalise general administration or marketing functions first. Business surveys on ICT use show that the digital gap is smaller between SMEs and large firms in their online interactions with the government, in electronic invoicing or in using social media or selling online. SME gaps in adoption increase, however, when technologies become more sophisticated (e.g. data analytics) or mass matters for implementation (e.g. enterprise resource planning for process integration). There are also striking differences across firms in their use of cloud computing (CC), despite the potential of “pay-as-you-go” CC services to raise IT capacity.

Cross-industry differences in digitalisation are significant. In knowledge-intensive sectors, firms make a more intensive use of all types of technologies and some aspects of the digital transformation are almost fully completed, e.g. the OECD median share of employees with access to connected devices is around 90%, compared to 50% across all sectors. Diffusion rates in other sectors are much lower. The uptake of a couple of key technologies, which mix differs across industries, can explain the gaps. For example, in the accommodation and food services, high-speed broadband connection, a website and CC to store files are the main technologies associated with higher gaps in uptake and higher sectoral value added. In the wholesale sector, there are e-sales, CC to host databases and the training of ICT specialists; in retail trade, e-sales and CC to manage customer relationships.

When SMEs digitalise their business functions, they tend to outsource solutions, partly to compensate for weak internal capabilities but also on cost-grounds. For example, digital platforms (e.g. social networks, e-commerce marketplaces, etc.) serve for optimising certain functions at very low cost (e.g. business intelligence and data analytics services). Similarly, for managing digital security risks, SMEs tend to rely on external consultants or the security-by-design features of the products and services they use. They also source artificial intelligence (AI) solutions from knowledge markets, and leapfrog to new AI systems with CC-based Software as a Service.

The COVID-19 crisis has heightened the importance of SME digitalisation, and served as an accelerator. Firms have moved operations online and implemented smart working solutions to remain in business during lockdowns and overcome disruptions in supply chains, with online platforms playing an instrumental role in connecting users to new markets, suppliers or resources. Early evidence from business surveys worldwide point to up to 70% of SMEs having intensified their use of digital technologies due to COVID-19. Most of these changes are poised to last since some investments are irreversible and the efficiency gains have now been demonstrated.

However, the COVID-19 context has also provided an opportunity for hackers to intensify attacks, exploiting SME lack of preparedness and ability to face increasingly sophisticated threats. Indeed, SMEs have lower investment in digital security, and, often, a limited understanding of the consequences of those threats. In fact, SMEs have smaller ‘attack surfaces’, due to lower digital intensities (exposure) and smaller volumes (and value) of data or intellectual property to hack. When they are affected though, costs can be disproportionate, amounting to months of revenue, well beyond their average available cash reserves. As they go digital, their degree of exposure is likely to increase dramatically. And the impacts of attacks may permeate beyond targeted SMEs, either because of potential supply-chain disruption costs or because hackers use these SME as a back-door entry point to the larger firm.

Pre-COVID risks related to digital (non) adoption remain. At the firm level, digital gaps are strongly associated with gaps in productivity, scaling up, innovation and growth. At the market level, concerns remain about technology lock-ins, SME data protection, or distortions in competition. At the aggregate level, the SME digital gap contributes to increased inequalities among people, places and firms. First-mover advantage on digital markets, strong network effects and complementarities in digital diffusion, especially as the firm grows in size and scale, could exacerbate digital divides. The COVID-19 crisis has already exacerbated the impact of existing divides.

Pre-COVID barriers to SME digital adoption remain too: access to infrastructure; low interoperability of systems; a lack of data culture and digital awareness; internal skills gaps; financing gaps for covering high sunk costs to transform; uncertainty about liabilities and responsibilities when engaging in new digital activities; risks of reputation damage, etc.

Policy makers have a key role to play in helping SMEs adapt their culture and processes to the digital world. SME digitalisation is high on the policy agenda across OECD countries and beyond, but there is a large mix of approaches and, in some areas, diverging viewpoints on how to do so. The heterogeneity of the SME population and the diversity of their business ecosystems add to the complexity in designing effective policy. Some countries seek to mainstream SME policy considerations in other policy agendas, others target SMEs, with often instruments tailored to specific places or sectors.

Policy intervention spans across a broad range of areas, including: awareness campaigns; training and technology assistance; access to finance; support for the development of SME-tailored digital solutions; data centres, experimentation platforms and networking programmes; regulatory reforms (e.g. data protection); e-government and one-stop-shops; and investment in infrastructure.

These findings raise several policy considerations and point to a number of future research avenues. First is the role of governments in removing regulatory barriers and market distortions, and enabling greater SME uptake, e.g. through the digitalisation of public services. Second is how policies should be adapted to the specific industries SMEs operate in, as well as the business functions that are subject to transformation, as challenges and changes vary by sector/function. Third, are more evidence, comparable data, sectoral studies and business cases (successful or not) to inform all relevant actors, i.e. SMEs themselves of course (those that are lagging and those at the frontier), investors, insurers, service providers, business associations, business partners, such as large firms, and last but not least, online platforms, which are major enablers of digitalisation and potentially key source of data and evidence on the SME digital transformation.



**From:**  
**The Digital Transformation of SMEs**

**Access the complete publication at:**

<https://doi.org/10.1787/bdb9256a-en>

**Please cite this chapter as:**

OECD (2021), "Executive summary", in *The Digital Transformation of SMEs*, OECD Publishing, Paris.

DOI: <https://doi.org/10.1787/71cb507b-en>

This work is published under the responsibility of the Secretary-General of the OECD. The opinions expressed and arguments employed herein do not necessarily reflect the official views of OECD member countries.

This document, as well as any data and map included herein, are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area. Extracts from publications may be subject to additional disclaimers, which are set out in the complete version of the publication, available at the link provided.

The use of this work, whether digital or print, is governed by the Terms and Conditions to be found at <http://www.oecd.org/termsandconditions>.