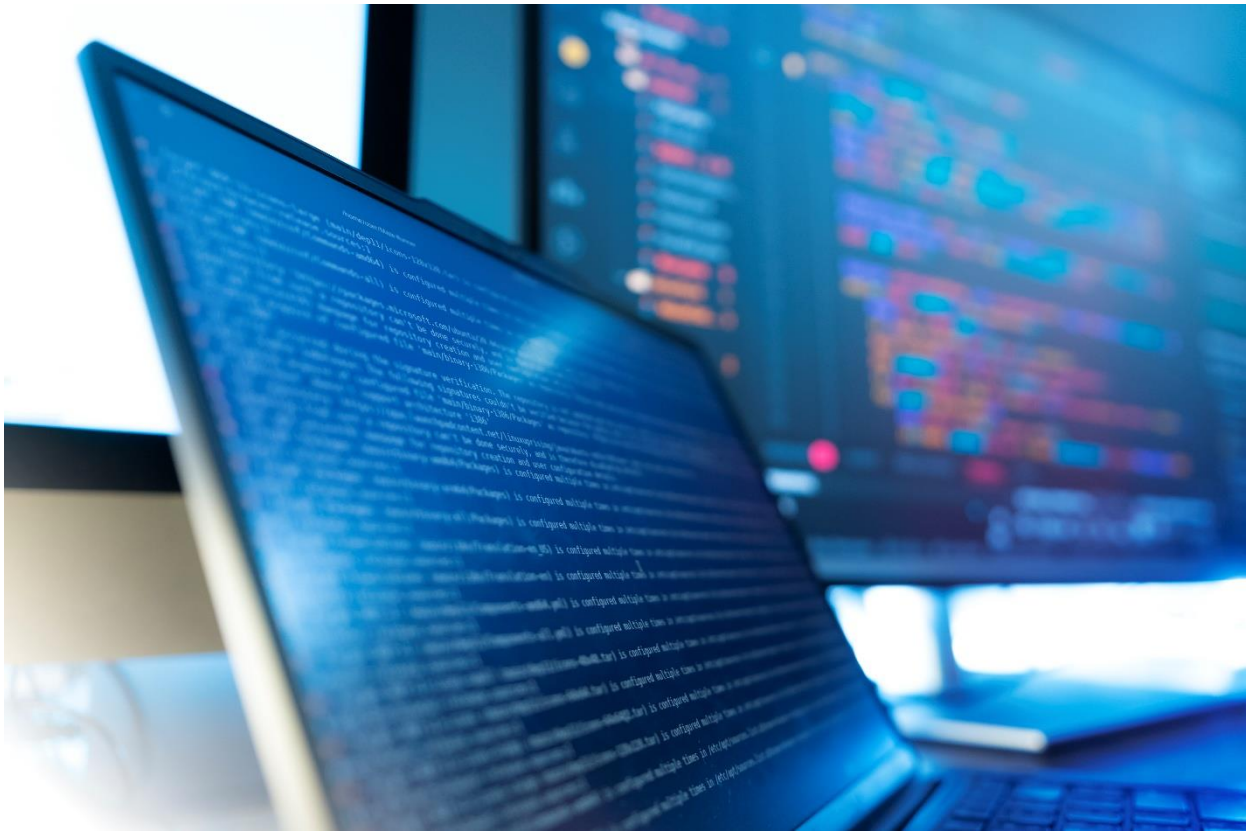
Due diligence essentials for responsible software

Software such as online platforms, social media, distributed ledger technology (blockchain and cryptocurrency), software as a service (SaaS), data analytics and artificial intelligence (AI) have driven monumental shifts in human and business behaviour. Its rapid growth and evolving nature present unique challenges and opportunities, particularly in relation to responsible business conduct (RBC). Software tools can help companies address pressing issues in supply chain due diligence such as establishing traceability, sharing accurate risk information, and improving the transparency of supply chain actors. The reliance of the software sector on data, online platforms, and digital infrastructure can also create diverse and novel environmental, social, and governance risks, from high energy use to labour risks in outsourced digital work, privacy and security harms, discrimination, free speech, and information integrity challenges. This case study explores significant impacts related to the development and use of software and challenges and opportunities in addressing them in line with international standards on RBC.[1] It is targeted at companies involved in the software sector who are seeking to understand their exposure to related risks, and also for policymakers and stakeholders seeking to better understand opportunities for promoting effective due diligence in the sector.



Key characteristics of the sector and its value chain

Software refers to the collection of data and instructions that guide a computer to perform specific tasks. It is created from source code, which consists of sequences of statements written in programming languages. Unlike hardware, the physical device that executes these instructions, software is intangible.

The software sector has become an integral part of the global economy, not only by driving technological innovation but also by shaping the way individuals, organisations and industries interact with each other. As one of the most rapidly evolving sectors, software companies are leading the transformation of the global economy through advancements in automation, communication, artificial intelligence (AI) and data analytics. Software is one of the main catalysts for innovation and productivity gains in many other sectors such as healthcare, finance, education, logistics, energy, public administration and media.

Market landscape

The software sector is characterised by its reliance on cutting-edge technology and fast-paced innovation cycles, allowing companies to rapidly adapt to evolving market demands and technological advancements. In recent years, the adoption of software solutions has surged, fuelled by the expansion of e-commerce, advancements in AI and data analytics, and the proliferation of connected devices.

Unlike physical goods with long lifespans, software products have a relatively short innovation cycle, requiring frequent updates and new versions to keep pace with user needs and emerging technologies. The rise of cloud computing and high-speed digital networks has transformed software delivery, shifting from traditional installations to cloud-based access models like Software-as-a-Service (SaaS). In the past, software was typically distributed through physical media (e.g. CDs or floppy discs), the customer would install software locally, and the customer would manually handle updates and maintenance. SaaS

represents a shift in how software is accessed and maintained, as software is now hosted on remote servers powered by external data centres; updates are now handled by the service provider; and customers access the software through a continuous subscription model rather than one-off payment. This shift enables greater scalability, cost efficiency, and remote accessibility, eliminating the need for on-premises infrastructure.

While the software sector has evolved significantly, research published before the AI boom classified the sector into three broad categories that still roughly hold (Lippoldt and Stryszowski, 2009[1]):

- **Applications**: Programs designed to perform specific tasks for end-users. They may be locally installed or accessed remotely. Common examples include word processors, spreadsheets, email, desktop publishing tools, and web browsers.
- **Operating Systems**: These serve as the interface between hardware and software applications, providing essential services such as file management, printing, and device control.
- **Middleware**: A category of software that enables communication and data management between applications and operating systems, regardless of their programming languages. It acts as a bridge, ensuring system interoperability.

AI does not fit neatly into any single category and cuts across all three. Unlike conventional software, whose category is determined by its function, AI's category is determined by its deployment context: the same underlying model may function simultaneously as application, middleware, or system component. This has direct implications for how risks are assessed and attributed across the software supply chain. At the application layer, AI products such as large language models (LLMs) deployed as standalone tools or embedded features perform specific tasks for end-users and are typically accessed remotely, placing them squarely within the applications category. Many AI systems, however, operate at the middleware layer, where foundation models serve as infrastructure upon which other applications are built, managing data flows and enabling interoperability across systems. This is often invisible to the end-user, but may be consequential from a risk management perspective. AI is also integrated into operating systems directly, further blurring categorical boundaries.

Beyond these core classifications, embedded software represents a distinct segment. Permanently integrated into hardware systems, it is essential for the functionality of medical devices, consumer electronics, automobiles, mobile phones, robotics, and telecommunication systems. This rapidly growing market operates largely outside the traditional software sector but plays an important role in AI-driven devices.

As software becomes increasingly integrated with diverse industries, the sector has expanded into several key segments, each catering to different business and consumer needs:

- **Enterprise and business software solutions:** Tailored applications that optimise operations in areas such as finance, human resources, supply chain management, and customer relations where users pay upfront for the license.[2] Unlike SaaS, users typically pay upfront for a license and manage their own infrastructure.
- **Cloud computing and Software-as-a-Service:** Cloud-based applications providing subscription-based access to software, eliminating upfront infrastructure costs. This model enhances flexibility, collaboration across teams and geographies while enabling businesses to scale efficiently across global markets.
- **Mobile apps and platforms:** Essential tools for smartphones and tablets, covering industries from social networking and gaming to digital banking and e-commerce.
- **Cybersecurity and privacy software:** Solutions designed to protect the confidentiality, integrity and availability of digital systems, networks, and data from threats, ensuring operational security and compliance with data protection laws.

AI cuts across all four segments rather than occupying any one of them. It is embedded as a feature in enterprise platforms, delivered primarily via cloud and SaaS models, increasingly integrated into mobile operating systems and applications, and plays a dual role in cybersecurity both as a tool for threat detection and as a source of novel risks. This cross-cutting character means AI simultaneously functions as a product delivered through these segments and as a transformative input into each of them.

By continuously evolving and integrating with other industries, the software sector remains a key driver of digital transformation, innovation, and global economic growth.

According to the World Intellectual Property Organisation (WIPO), "In 2024, global software spending reached USD 675 billion, up nearly 50% nominally from 2020's level of USD 454 billion. These figures - not adjusted for inflation - reflect a significant post-pandemic push to invest in improved software. This surge aligns with the rise in e-commerce and the maturation of artificial intelligence (AI) technologies" (WIPO, 2025[2]). Its expansion is primarily driven by the adoption of cloud computing and AI-driven applications, reliance on software solutions to streamline business applications and the expansion of mobile and SaaS-based platforms across industries. While advanced economies benefit from well-established software ecosystems, emerging markets are also undergoing rapid digitalisation, creating new opportunities for software development and deployment.

Software companies generate revenue through various channels beyond direct sales, including advertising, bundled services and complementary offerings.[3] Business models in the sector include *proprietary models*, which rely on patents, copyrights and licensing fees for financial sustainability; and *open-source models*, that encourage multi-party collaboration, allowing companies to benefit from collective contribution and flexible licensing agreements (Lippoldt and Stryszowski, 2009[1]).

The software sector is primarily driven by multinational enterprises (MNEs), with limited involvement from state-owned enterprises (SOEs). A significant number of mid-sized companies specialise in niche software solutions, while startups play a crucial role in fostering innovation, particularly in emerging fields such as AI, fintech, digital health and automation. A select number of companies with strong ties to government entities in specific geographies continue to shape the landscape.

The ongoing shift toward cloud-based services has catalysed a monumental transformation in the software sector, driving a surge in demand for scalable, flexible, and highly accessible software solutions. By migrating to the cloud, businesses and organisations gain the ability to store, process and share vast amounts of data with far greater flexibility than traditional on-premise infrastructure allows. This shift enables companies to scale operations quickly in response to fluctuating demands while optimising operational costs. These services eliminate the need for significant investments in hardware, allowing businesses to instead pay for the resources they use on a subscription basis. A relevant example is SaaS[4] which has been the dominant delivery model in the software sector over the last decade.

Artificial Intelligence is reshaping the software sector by unlocking new capabilities for software. Software applications incorporating AI technologies can process and analyse large datasets, potentially offering insights through predictive analytics and machine learning algorithms (Soral, 2024[3]). These technologies have demonstrated utility in various operational contexts, including customer service interfaces, where automated response systems can handle routine enquiries. Similarly, AI-assisted tools are being explored for back-office functions like supply chain management, financial reporting, and human resource processes, with potential implications for operational efficiency.

The intersection of software and Information and Communication Technology (ICT) is gradually transforming how businesses approach digital service delivery. As the software sector interfaces with broader technological advancements, including big data[5] and the Internet of Things (IoT),[6] organisations are exploring more nuanced digital service models. The integration of big data analytics into software solutions offers potential for more informed decision making processes. However, this technological evolution also presents complex considerations, particularly regarding environmental implications such as

the energy consumption associated with data centres and cloud service infrastructure (Lippoldt and Stryszowski, 2009[1]).

Overview of the value chain structure

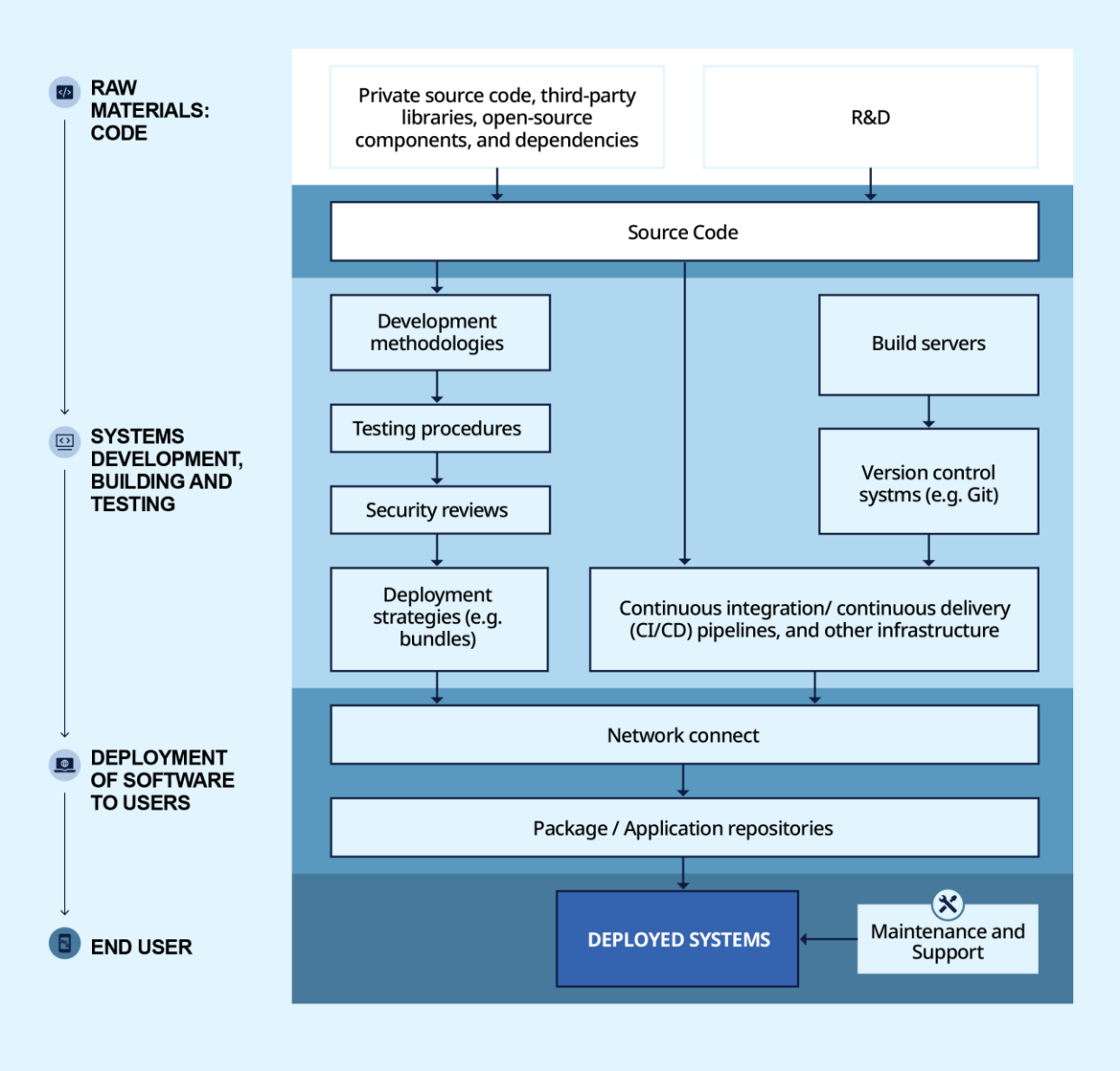
As software is integrated into different industries and services in today's economy, precisely defining the software sector has become more complex (Lippoldt and Stryszowski, 2009[1]). Many companies outside the traditional software sector are now incorporating software development to complement their non-software offerings, broadening the scope of contributors in the sector.

The software sector described here consists of several stages that encompass the entire lifecycle of a software product, from its initial development to ongoing maintenance and support. These stages include research and innovation (which covers planning, designing, coding and testing), deployment, distribution, and maintenance, with each phase playing a critical role in ensuring the software's functionality, security, and viability (Clark, 2025[4]). Also discussed are intermediary actors and other key players outside of the lifecycle of a software product but that facilitate the development and use of software.

- **Development stage:** The value chain begins with research and innovation, where companies invest in research and development (R&D) to identify customer needs or market solutions. The next step is coding, where developers use various programming languages to build the software, according to specified functionality, security standards, and performance requirements. Following development, the software undergoes testing and quality assurance to identify and resolve any bugs, security vulnerabilities, or performance issues before its release. Cloud services and hosting platforms play a vital role here and in the deployment stage, providing global accessibility, scalability, and some level of security, though it also presents security risks.
- **Deployment and distribution stage:** Once the software is developed, it enters the deployment and distribution phase. Cloud service platforms are essential for distributing software across different geographies. Software platforms, app stores and marketplaces enable product distribution, allowing companies to reach a broad audience. Additionally, SaaS and licensing/subscription models are increasingly used to distribute software, providing users with ongoing access to the software and companies with recurring revenue streams.
- **Maintenance and support stage:** After deployment, ongoing maintenance and support ensure that the software remains functional and secure. Regular updates and upgrades are released to enhance performance, improve security, and introduce new features. Cybersecurity and data protection are increasing priorities, with companies investing in security patches, and compliance with data protection and cybersecurity regulations. To support users, software providers offer technical assistance and managed services, including help desks, AI-powered support and IT management services, ensuring that users can resolve issues quickly and continue using the software with minimal disruption. Gathering user feedback and market data to inform new features and improvements is an essential activity of this stage.

Each stage of the software value chain plays a role in ensuring that the software remains functional, secure, and aligned with user needs throughout its lifecycle.

Figure 1. Simplified software value chain



Role of intermediary actors and key players

Key stakeholders in the sector include software developers, investors, service providers, platform operators, and end-users, all of whom collaborate to ensure the success and growth of software products and services in the marketplace.

Investors are essential stakeholders in the software sector, providing the capital necessary for innovation and growth. They fund software development projects, startups, and technology companies, helping to drive research and development in emerging areas, seeking to generate long-term returns while supporting technological advancements.

Data providers represent a critical and increasingly strategic component of contemporary software development ecosystems, functioning as essential infrastructure suppliers that enable technological innovation, product development, and competitive differentiation. These entities supply raw and processed

data that serve as fundamental inputs for software development across multiple domains, including AI, business intelligence, and specialised application development.

Service providers play a crucial role in ensuring that software products are not only accessible but also functional and scalable. They provide the infrastructure, management, support, and ongoing services needed to make software applications operational. Key players in this segment deliver the hosting, storage, and computational power necessary for software to run efficiently in the cloud. Additionally, IT support firms and SaaS providers also contribute significantly by offering continuous software management, regular updates, and customer service (Monga, n.d.[5]).

Platform operators are another vital component of the software value chain. These large technology companies manage and control platforms that facilitate the distribution and accessibility of software. They provide the environment for software distribution. Marketplaces serve as primary channels through which both businesses and consumers discover, download, and use software. By managing these platforms, they create an ecosystem where developers, service providers, and end-users can interact, while ensuring that software products meet specific platform requirements for security, compliance, and performance (Microsoft, n.d.[6]).

End-users are the ultimate consumers of software products, ranging from individuals to businesses and governments. These users rely on software solutions for various applications, including communication, commerce, data management, customer service, and operational efficiency. Their needs drive the demand for innovation and usability, making them a crucial factor in the software development lifecycle.

Salient impacts associated with the sector

The rapid digital expansion has significantly driven up energy consumption, as data centres and transmission networks, essential for supporting digitalisation, continue to grow in scale and demand. Historically, the software sector has been seen as less environmentally impactful when compared to resource-heavy sectors like manufacturing or mining. However, the increasing demand for energy in data centres, the rapid rise of electronic waste (e-waste), and the growing social implications around privacy, digital security, mis/dis-information and labour rights in software development, among other impacts outlined below, underscore the urgent need for a stronger focus on responsible business conduct (Shah, 2023[7]) and implementation of related OECD Recommendations on this policy area, including the Recommendation on AI (OECD, 2025[8]), the Recommendation on Children in the Digital Environment (OECD, 2012[9]), the Recommendation on the Digital Security of Products and Services (OECD, 2022[10]); the Recommendation on Digital Technologies and the Environment (OECD, 2010[11]) and the Recommendation on Information Integrity (OECD, 2024[12]), among others.

Environmental impacts

GHG emissions and water and energy consumption associated with data centres and cloud computing

The reliance on digital services is driving higher energy and water consumption and increasing greenhouse gas (GHG) emissions. Data centres, which form the backbone of the software sector, are massive buildings filled with hundreds of thousands of connected central processing units (CPUs) that manage the necessary computing tasks to run operating systems and applications (OECD, 2022[13]). Data centres are responsible for storing, processing, and delivering digital services globally. They require vast amounts of electricity to run and water for cooling. According to the IEA, they account for approximately 1.5% of global electricity demand (IEA, 2025[14]). Looking forward, “[d]ata centre electricity consumption is set to more than double to around 945 TWh by 2030. This is slightly more than Japan’s total electricity consumption today. AI is

the most important driver of this growth, alongside growing demand for other digital services." A newer trend in the industry is the shift toward what is called software-defined infrastructure (SDI) (i.e. using software to control and manage equipment that used to require physical hardware changes). This approach makes systems more flexible and automated. However, it also means that more tasks are handled by software running continuously in the background, which increases the amount of computing power needed (Marsh and Robinson, 2021[15]). This extra digital workload can raise energy use, sometimes cancelling out the efficiency benefits that SDI is meant to deliver.

The deployment and training of AI systems have intensified energy and water consumption, particularly when these systems run on specialised computing hardware. Many large AI models rely on graphical processing units (GPUs), which are designed to handle complex, parallel mathematical operations more efficiently than traditional CPUs. Although GPUs were originally developed for graphics rendering, their design makes them well-suited for training and operating AI systems, and they can consume up to 1 000 watts compared to roughly 250-500 watts for a typical CPU. However, GPUs are not the only hardware used: application-specific integrated circuits (ASICs), such as Google's Tensor Processing Units (TPUs), have been developed specifically for machine learning workloads, and can further accelerate computation while also drawing substantial power (Metz et al., 2025[16]). While energy use varies widely depending on the system design, even relatively smaller AI models can demand significant electricity (CFA Institute, 2024[17]).

Not all AI workloads run in large data centres. Some AI applications can operate "on device" or at the network edge (e.g. on smartphones, laptops, or small servers), which can reduce the need for continuous cloud-based computation. However, as AI capabilities expand and models grow in size, overall demand for computing power continues to rise. In addition, frequent software updates and digital redundancy across services contribute to increased energy consumption, as they require additional storage, processing, and infrastructure capacity. In response, software and cloud service providers are pursuing different strategies to meet these energy needs, ranging from investments in low-carbon or alternative energy sources, such as nuclear power, to continued reliance on fossil fuels and natural gas.

Social impacts

Labour impacts related to the development of software

Workers, especially in outsourcing destinations, may be subjected to insecure contracts, low wages, and extended working hours (ILO/ISSA/OECD, 2023[18]). These conditions foster an environment of vulnerability, undermining labour rights in the sector. Data enrichment and content moderation services present a particular risk of adverse labour impacts. Data enrichment services involve human workers manually labelling, categorising, and enriching data (such as images, text, or audio) to make it understandable for machine learning algorithms. These services are critical for developing AI systems, as they convert raw data into structured, contextual information that computers can learn from. As part of this process, and also for content moderation, workers may be exposed to graphic, sexually explicit, and violent images. The labour involved is often outsourced to workers in lower-income countries or through crowdsourcing and gig-economy platforms, raising questions about fair compensation and working conditions (Jindal, 2021[19]).

Labour impacts related to the use of software

Deployment of certain software in the workplace to support with company operations can also present labour risks, including undermining freedom of association and collective bargaining rights. AI powered tools can enable practices such as invasive monitoring or surveillance of workers, productivity scoring, and predictive algorithms that track or intervene in efforts to organise workers. More broadly, deployment of software, particularly AI systems, without appropriate stakeholder engagement, can result in systemic

impacts on labour (e.g. job losses/redundancies, labour displacement, lack of appropriate re-skilling measures and associated well-being threats) (Lane, Williams and Broecke, 2023[20]).

Human rights impacts related to the collection and processing of data

Data collection forms the foundation upon which software builds intelligence and functionality, particularly for AI systems. Comprehensive datasets allow developers to train algorithms that can recognise patterns, make predictions, and simulate human-like understanding across diverse contexts and languages. Privacy risks occur for example when personal data is harvested without legal justification or beyond stated purposes, undermining individuals' right to control information about themselves.[7] Discrimination and bias risks also emerge when collected data reflects or amplifies existing societal biases, leading to algorithmic systems that disadvantage certain groups in areas like hiring, loan approvals, or criminal justice. Additionally, this could also mean that these groups are systematically excluded from datasets or misrepresented, which could impact decision making about those groups.

This data is often used to target advertisements, improve services, or develop new features, but it also raises significant concerns related to surveillance, censorship, and the potential for data breaches. As the volume of data grows, so does the potential for misuse.

Human rights impacts related to the use of software

Human rights impacts related to the use of software are mostly linked to violations of privacy and surveillance, bias and discrimination and mis/dis-information.

Privacy and surveillance

Certain software known as spyware can be used to enable unauthorised data access and surveillance of personal devices. While spyware is used by governments for legitimate national security and law enforcement purposes, it is also reportedly used to target political dissidents and civil society (United Nations, 2022[21]). In many jurisdictions, spyware is also available for purchase by individuals, often marketed for purposes like parental control or employee monitoring. More sophisticated spyware tools can be acquired through less regulated channels, including online marketplaces or forums. Similar software like facial recognition have sparked concerns about privacy and surveillance. While facial recognition can serve security and authentication purposes, its use by governments and private entities to track individuals without consent has raised alarms about the erosion of personal freedoms (Civil Liberties Union for Europe, 2022[22]).

Mis/dis-information

Software such as search engines, social media feeds, and chatbots plays a central role in shaping how information is produced, recommended, and consumed online (OECD, 2024[23]; 2024[24]). These systems rely on algorithms designed to maximise user engagement, which can inadvertently amplify sensational, misleading, or false content. The OECD's Disentangling Untruths Online analysis highlights that untruths often spread faster and reach wider audiences than accurate information because digital platforms privilege highly engaging material and reinforce users' pre-existing beliefs through personalised recommendation systems, echo chambers, and filter bubbles. The OECD's typology shows that mis- and disinformation circulate differently but thrive under the same design incentives that reward virality over quality. The OECD Truth Quest Survey further demonstrates that although most people believe they can recognise false or misleading content, their actual ability to identify untruths online is significantly lower, revealing a persistent gap between confidence and accuracy in digital information environments. This mismatch not only reinforces vulnerability to untruths but also helps explain why low-quality or misleading content continues to circulate widely. While software companies have developed content moderation

systems aimed at detecting and removing harmful or deceptive content from feeds, their effectiveness remains inconsistent, allowing mis/dis-information to persist and influence public discourse.

Generative AI tools add further complexity to this evolving landscape. While AI systems can assist with information access and content summarisation, they can also inadvertently produce or amplify misleading or low-quality information when trained on unverified datasets. The same structural features that enable fast and widespread diffusion of false content apply to AI-generated material, increasing the risk that inaccurate information is replicated across platforms. At the same time, malicious actors can leverage AI to automate and scale the creation of persuasive false content, including deepfakes and synthetic media. While deepfakes have legitimate applications in entertainment and gaming, their misuse in political campaigns, fraud, sexual harassment and disinformation campaigns poses significant human rights and societal risks (Chauhan, 2024[25]).

Bias and discrimination

Software trained on biased or low-quality data sets risk amplifying biases and discrimination. As AI-driven decision making systems become more prevalent in areas such as hiring, lending, law enforcement, government administration, and healthcare, they introduce new risks of bias and discrimination. For example, studies have shown that facial recognition systems are significantly less accurate in identifying people with darker skin tones, especially women, which has led to concerns it can have negative effects in applications related to healthcare and law enforcement (Amnesty International, 2023[26]; Johnson, 2023[27]). Likewise, certain AI-based hiring algorithms have been found to favour male candidates over female candidates for certain positions, reinforcing gender disparities in the workplace. Similarly, biased lending algorithms may result in unfair credit denials for minority groups, exacerbating financial inequalities and restricting economic opportunities (Amnesty International, 2023[26]; Johnson, 2023[27]).

Governance impacts

Competition and power concentration

Large software companies are facing growing scrutiny for engaging in monopolistic practices and misleading advertising. Regulatory bodies and watchdog organisations have initiated antitrust investigations, accusing the largest companies of leveraging their dominant market positions to suppress competition, limit consumer choice, and impose unfair terms on smaller businesses and developers (Medium, 2024[28]). These companies have pioneered advancements in cloud computing, and AI, yet they simultaneously build integrated ecosystems, such as cloud services, data centres, and app stores, that solidify their control over vast markets. By creating proprietary platforms that lock users and developers into their services (Medium, 2024[28]).

Cybersecurity and privacy-related risks

As digital technologies become increasingly embedded in everyday life, cybersecurity threats pose significant risks to businesses, governments, and individuals. Cyberattacks, data breaches, and software vulnerabilities can lead to financial losses, operational disruptions, safety risks and compromised personal information, making cybersecurity a high priority for the software sector (Jain, 2025[29]).

One of the most critical issues is the growing threat of supply chain vulnerabilities. Over 54% of large organisations identify supply chain challenges as the most significant obstacle to achieving cyber resilience (Jain, 2025[29]).

While AI enhances threat detection and provides defence mechanisms, it can also be exploited by cybercriminals to launch sophisticated attacks (e.g. cyber and phishing attacks, exploitation of software vulnerabilities, generation of deep-fake social engineering threats, and development of advanced

malware). AI is also creating ethical dilemmas and privacy-related concerns (OECD, 2024[30]; Marr, 2023[31]). This rapid advancement of AI has often outpaced regulatory frameworks, leaving gaps in governance and increasing the risk of misuse.

Intellectual property (IP) protection

Software companies invest heavily in developing innovative technologies, designs, and brands, making intellectual property (IP) essential to sustaining competitive advantage; however, the rise of generative AI has introduced new and significant IP challenges (OECD, 2025[32]). Developing these models often relies on large datasets collected through data scraping, a process the OECD identifies as a core method for assembling AI training data but one that frequently captures copyrighted, licensed, or otherwise protected content without clear permissions, creating uncertainty around the lawful use of such material and exposing developers to growing global litigation. Scraped datasets are also difficult to audit, as creators, licences, and rights are often not clearly identifiable at scale, which complicates compliance with diverse copyright, database, and privacy regimes across jurisdictions. At the same time, generative AI blurs traditional concepts of authorship and ownership because many AI-generated outputs lack a clear human creator, and major legal systems still require human authors or inventors for copyright and patent protection. These unresolved issues, from training data rights to authorship, ownership, and enforceability, pose substantial risks for software companies seeking to protect their assets, while highlighting that overly restrictive approaches could also hinder innovation, competition, and responsible AI development.

Key considerations for due diligence

Due diligence in the software sector has become increasingly complex as software value chains grow more global, interconnected, and diverse. Various and sometimes overlapping regulatory approaches to address specific software related impacts has added to this complexity. However, these challenges also create opportunities for innovation and improvement in risk management strategies to understand the high-level linkages between different issues (e.g. data governance and addressing bias) and support adherence to multiple risk management frameworks across different jurisdictions.

Challenges

Technological advancement outpacing policy

The software sector operates within a complex and evolving regulatory landscape, where laws and policies governing due diligence, data protection, product safety, intellectual property, and anti-competitive practices are continuously adapting to technological advancements. Emerging technologies such as AI further complicate this environment, introducing new legal and ethical challenges that companies and policymakers must navigate. These advancements are outpacing the ability of legal and voluntary frameworks to comprehensively address emerging RBC concerns. The complexity is further compounded by the global and often borderless nature of technological development, where technological breakthroughs can rapidly proliferate across jurisdictions before policymakers can effectively analyse their potential societal implications and human rights impacts. The dynamism of technological disruption means that regulatory frameworks and other standards are perpetually reactive rather than proactive, constantly playing catch-up with innovations that fundamentally reshape human interaction, privacy, autonomy, and human rights.

Divergent regulatory approaches

The lack of uniformity in regulatory frameworks is becoming an increasingly significant hurdle to carrying out due diligence for businesses operating globally. At the 2024 World Economic Forum's Annual Meeting on Cybersecurity, 76% of Chief Information Security Officers (CISOs) highlighted concerns over fragmented regulations, which not only complicate compliance efforts but also hinder effective cybersecurity risk management on a global scale. (Jain, 2025[29]).

Responsibility and accountability

Data management practices are a key component of responsible product development. Widely used operating systems and platforms facilitate vast ecosystems of third-party applications, each with varying levels of digital security and privacy protections. This creates challenges in determining the extent of responsibility that platform providers should bear for third-party software and user behaviour. While app stores have strict guidelines for app developers, ensuring compliance across millions of applications is an ongoing challenge. Incidents such as data breaches, unauthorised tracking, and misuse of user information raise questions about whether responsibility lies solely with the app developers or if platform providers should play a more active role in enforcing digital security measures.

While platform providers clearly enforce policies against specific applications, such as removing spyware from app stores, the question becomes more complex when the issue stems from broader operating system functionalities or underlying digital infrastructure. This ambiguity raises critical concerns about the role of platform providers in mitigating potential misuse and in implementing more proactive safeguards, such as restricting access to sensitive APIs, enforcing stricter developer guidelines, or integrating stronger privacy protections by design. While such measures could enhance user security, they must also be balanced against innovation, user autonomy, and concerns over overreach.

These accountability challenges are compounded by the high degree of market concentration in the software sector. A small number of firms control the dominant operating systems, app distribution channels, cloud infrastructure, and the foundation models that underpin AI-enabled products and services. This concentration has implications for applying leverage to encourage positive change as part of the process to prevent and mitigate risk, or disengagement where necessary. It limits the practical options available to businesses and consumers seeking to disengage from providers whose practices may fall short of RBC standards. Where a platform or underlying technology is effectively essential infrastructure switching costs are prohibitive and alternatives may not exist at comparable scale, which may make disengagement more difficult or practically impossible.

Opportunities

International coherence and alignment towards risk-based due diligence

There is growing policy momentum to address these challenges through the increasing development of voluntary and mandatory frameworks. A notable feature of this emerging policy landscape is the degree of convergence around a risk-based approach to due diligence. Despite differences in scope and sector focus, these frameworks broadly share a common approach, based on core RBC principles, that firms are expected to identify, assess, prevent, mitigate, and remediate adverse impacts proportionate to their severity and likelihood. This convergence is significant. It suggests that the due diligence infrastructure that responsible businesses already have experience building is consistent with emerging requirements, reducing the compliance burden for early movers and reinforcing the business case for proactive adoption of RBC standards in the software sector. The publication of the OECD Due Diligence Guidance for Responsible AI and endorsement by OECD Members and partner governments exemplifies the

opportunity for companies in the software sector to strengthen coherence across their risk-management practices (OECD, 2026[33]).

Identification of control points for undertaking due diligence

The most advanced software (e.g. AI systems) depends on high-quality digital infrastructure (OECD, 2024[34]). This includes broadband access networks, core Internet backbone transmission networks, such as subsea fibre cables, Internet Exchange points, data centres, content delivery networks (CDNs), compute (including cloud infrastructure and semiconductors), and the logical infrastructures of the Internet (routing, domain name servers, etc). Digital Infrastructure is the foundation for all transformative digital technologies, including AI. Parts of the AI value chain, such as data centre providers, cloud service providers and advanced semiconductor manufacturers, are controlled by a small number of large technology firms (OECD, 2025[35]). Those firms' activities are often subject to significant regulatory and geopolitical constraints. Focusing due diligence efforts on control points can support efficiency of due diligence efforts more broadly across the supply chain.

Traceability

Traceability in the software sector refers to the ability to track and document every stage of the software development lifecycle; from the initial design to the ongoing maintenance. This process ensures that every decision is recorded and can be traced back, promoting transparency, accountability, and compliance with relevant standards, security protocols, and regulatory requirements (OECD, 2022[10]).

Key aspects of traceability in the software sector include:

- Version control and code traceability: enables tracking of all modifications to the software, ensuring every change is accounted for (IN-COM, 2024[36]).
- Issue management: monitors and resolves software defects, providing a clear history of identified problems and their resolutions.
- Track software components helps identify and manage vulnerabilities, reducing risks related to cybersecurity.
- Compliance and auditability: ensures the software meets sector standards and regulatory requirements, supporting thorough audits and reviews (Mubarkoot et al., 2023[37]).

A "software bill of materials" (SBOM) has emerged as a key building block in software security and software supply chain risk management. An SBOM is a formal record containing the details and supply chain relationships of various components (including third-party libraries, artifacts, licenses, scripts, and package versions, as well as dependencies) used in building software. These components, including libraries and modules, can be open source or proprietary, free or paid, and the data can be widely available or restricted access.[8]

Related OECD resources

The OECD has developed various resources to support businesses carrying out due diligence for responsible software, notably through a specific Due Diligence Guidance for Responsible AI, which can help inform business efforts on other software and digital technology beyond AI. The OECD also has developed other broader cross-sectoral resources on RBC, as well as topical research on specific software related risk issues.

- OECD Due Diligence Guidance for AI
- OECD Privacy Guidelines

- AI Incidents and Hazards Monitor
- G7 reporting framework – Hiroshima AI Process (HAIP) international code of conduct for organizations developing advanced AI systems
- The OECD Truth Quest Survey
- Measuring the environmental impacts of artificial intelligence compute and applications
- Transparency reporting on terrorist and violent extremist content online
- Companion document to the OECD Recommendation on Children in the Digital Environment
- Recommendation of the Council on Digital Security Risk Management

Cross-sectoral resources:

- OECD Due Diligence Guidance for Responsible Business Conduct
- OECD Guidelines for Multinational Enterprises on Responsible Business Conduct
- OECD e-learning Academy on Responsible Business Conduct

References

Amnesty International (2023), *Racial bias in facial recognition algorithms*, https://amnesty.ca/features/racial-bias-in-facial-recognition-algorithms (accessed on 11 March 2026). [26]

CFA Institute (2024), *The Hidden Environmental Costs of Tech Giants' AI Investments*, https://blogs.cfainstitute.org/investor/2024/10/31/the-hidden-environmental-costs-of-tech-giants-ai-investments/?preview_id=110519&_thumbnail_id=110525#_ftn19 (accessed on 11 March 2026). [17]

Chauhan, P. (2024), "Deepfake: Risks and Opportunities", *Computer*, Vol. 57/6, pp. 141-144, https://doi.org/10.1109/MC.2024.3392992. [25]

Civil Liberties Union for Europe (2022), *7 Biggest Privacy Concerns Around Facial Recognition Technology*, https://www.liberties.eu/en/stories/facial-recognition-privacy-concerns/44518 (accessed on 17 March 2026). [22]

Clark, H. (2025), "What is the Software Development Life Cycle (SDLC)?", *The CPO Club*, https://cpoclub.com/product-development/software-development-life-cycle/ (accessed on 11 March 2026). [4]

IEA (2025), *Energy and AI*, https://www.iea.org/reports/energy-and-ai. [14]

ILO/ISSA/OECD (2023), *Providing adequate and and sustainable social protection for workers in the gig and platform economy*, https://www.ilo.org/publications/providing-adequate-and-sustainable-social-protection-workers-gig-and-0. [18]

IN-COM (2024), *Code Traceability for Predicting Change Impact Before Deployment*, https://www.in-com.com/blog/code-traceability (accessed on 17 March 2026). [36]

Jain, S. (2025), "Cybersecurity in 2025: Geopolitical Tensions, AI, and Cybercrime Shape the Future", *The Cyber Express*, https://thecyberexpress.com/cybersecurity-outlook-2025/ (accessed on 11 March 2026). [29]

Jindal, S. (2021), "Responsible Sourcing of Data Enrichment Services", *Partnership on AI*, https://partnershiponai.org/responsible-sourcing-considerations (accessed on [19]

11 March 2026).

Johnson, A. (2023), “Racism And AI: Here’s How It’s Been Criticized For Amplifying Bias”, *Forbes*, https://www.forbes.com/sites/ariannajohnson/2023/05/25/racism-and-ai-heres-how-its-been-criticized-for-amplifying-bias/ (accessed on 11 March 2026). [27]

Lane, M., M. Williams and S. Broecke (2023), “The impact of AI on the workplace: Main findings from the OECD AI surveys of employers and worker”, *OECD Social, Employment and Migration Working Papers*, No. 288, OECD Publishing, Paris, https://doi.org/10.1787/ea0a0fe1-en. [20]

Lippoldt, D. and P. Stryszowski (2009), *Innovation in the Software Sector*, OECD Publishing, Paris, https://doi.org/10.1787/9789264076761-en. [1]

Marr, B. (2023), “The 15 Biggest Risks Of Artificial Intelligence”, *Forbes*, http://www.forbes.com/sites/bernardmarr/2023/06/02/the-15-biggest-risks-of-artificial-intelligence (accessed on 11 March 2026). [31]

Marsh, C. and S. Robinson (2021), *ESG & Technology: Impacts and Implications*, S&P Global Market Intelligence, https://www.spglobal.com/content/dam/spglobal/mi/en/documents/general/451-esg-and-tech-dckb-report.pdf. [15]

Medium (2024), *Tech Giants’ Battle for Dominance: The Latest Developments in the Tech Industry*, https://medium.com/lampshade-of-illumination/tech-giants-battle-for-dominance-the-latest-developments-in-the-tech-industry-899607a4c4c0. [28]

Metz, C. et al. (2025), “How A.I. is Changing the Way the World Builds Computers”, *The New York Times*, https://www.nytimes.com/interactive/2025/03/16/technology/ai-data-centers.html?searchResultPosition=1 (accessed on 11 March 2026). [16]

Microsoft (n.d.), *Understanding cloud operator access*, https://learn.microsoft.com/en-us/compliance/assurance/assurance-sovereignty-cloud-operator-access (accessed on 11 March 2026). [6]

Monga, S. (n.d.), “Service Provider: Meaning, Types, Key Roles, Challenges & More”, *Plutus Education*, https://plutuseducation.com/blog/service-provider/ (accessed on 17 March 2026). [5]

Mubarkoot, M. et al. (2023), “Software Compliance Requirements, Factors, and Policies: A Systematic Literature Review”, *Computers & Security*, Vol. 124/102985, https://doi.org/10.1016/j.cose.2022.102985. [37]

OECD (2026), *OECD Due Diligence Guidance for Responsible AI*, OECD Publishing, Paris, https://doi.org/10.1787/41671712-en. [33]

OECD (2025), “Intellectual property issues in artificial intelligence trained on scraped data”, *OECD Artificial Intelligence Papers*, No. 33, OECD Publishing, Paris, https://doi.org/10.1787/d5241a23-en. [32]

OECD (2025), *Recommendation of the Council on Artificial Intelligence*, OECD/LEGAL/0449, https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449. [8]

OECD (2025), “The chip landscape: Geographical distribution of wafer fabrication capacity”, [35]

OECD Science, Technology and Industry Policy Papers, No. 188, OECD Publishing, Paris, https://doi.org/10.1787/02dbd028-en.

OECD (2024), "AI, data governance and privacy: Synergies and areas of international co-operation", *OECD Artificial Intelligence Papers*, No. 22, OECD Publishing, Paris, https://doi.org/10.1787/2476b1a4-en. [30]

OECD (2024), *Facts not Fakes: Tackling Disinformation, Strengthening Information Integrity*, OECD Publishing, Paris, https://doi.org/10.1787/d909ff7a-en. [24]

OECD (2024), "Financing broadband networks of the future", *OECD Digital Economy Papers*, No. 365, OECD Publishing, Paris, https://doi.org/10.1787/eafc728b-en. [34]

OECD (2024), *Recommendation of the Council on Information Integrity*, OECD/LEGAL/0505, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0505. [12]

OECD (2024), "The OECD Truth Quest Survey: Methodology and findings", *OECD Digital Economy Papers*, No. 369, OECD Publishing, Paris, https://doi.org/10.1787/92a94c0f-en. [23]

OECD (2022), "Measuring the environmental impacts of artificial intelligence compute and applications: The AI footprint", *OECD Digital Economy Papers*, No. 341, OECD Publishing, Paris, https://doi.org/10.1787/7babf571-en. [13]

OECD (2022), *Recommendation of the Council on the Digital Security of Products and Services*, OECD/LEGAL/0481, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0481. [10]

OECD (2012), *Recommendation of the Council on Children in the Digital Environment*, OECD/LEGAL/0389, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0389. [9]

OECD (2010), *Recommendation of the Council on Digital Technologies and the Environment*, OECD/LEGAL/0380, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0380. [11]

Shah, A. (2023), "Navigating ESG Risk in the Software and Technology Sector", *Grant Thornton Stax*, https://www.stax.com/insights/navigating-esg-risk-in-the-software-and-technology-sector (accessed on 11 March 2026). [7]

Soral, S. (2024), "Chief AI Officer Blog - The future of coding is here: How AI is reshaping software development", *Deloitte*, https://www.deloitte.com/uk/en/Industries/technology/blogs/2024/the-future-of-coding-is-here-how-ai-is-reshaping-software-development.html (accessed on 17 March 2026). [3]

United Nations (2022), *The right to privacy in the digital age. Report of the Office of the United Nations High Commissioner for Human Rights*, https://docs.un.org/en/A/HRC/51/17. [21]

WIPO (2025), *Global Software Spending Surges to Close to USD 700 Billion in 2024, up 50% From 2020; the United States Extends its Lead*, https://www.wipo.int/en/web/global-innovation-index/w/blogs/2025/global-software-spending. [2]

Notes

[1] The sector was chosen for a case study based on a previous study by the OECD to identify and synthesise insights from key resources on the prevalence of issues covered by the OECD Guidelines for

Multinational Enterprises (the OECD Guidelines) across industry sectors. To complement this analysis, the OECD further conducted an expert survey to attain a broad picture of the perceived association with Responsible Business Conduct (RBC) issues across sectors.

[2] The programming services sector has historically been the largest within the software sector, encompassing major companies which have played a pivotal role in developing innovative solutions to meet business needs, including data analysis, storage and organisation, and software programmes that power machinery and automated processes (https://www.investopedia.com/articles/markets/050416/industry-handbook-software-industry.asp).

[3] In some cases software is offered for free or at little direct cost, creating challenges to accurately measure and value the industry (Lippoldt and Stryszowski, 2009[1]).

[4] Examples of SaaS include Google Workspace (Docs, Sheets), Microsoft 365, Dropbox, etc.

[5] Big data refers to large, complex datasets that traditional data processing software cannot adequately manage. These datasets are characterised by high volume, velocity, and variety, requiring advanced analytical methods to extract meaningful insights.

[6] IoT refers to a network of physical devices, vehicles, home appliances, and other items embedded with electronics, software, sensors, and network connectivity, enabling these objects to collect and exchange data.

[7] There is ongoing debate across different jurisdictions about whether personal data for AI training can be collected without consent, for example under other legal basis such as legitimate business interest.

[8] Adapted from the United States Cybersecurity and Infrastructure Security Agency (2024), Software Bill of Materials (SBOM) (https://www.cisa.gov/sbom).
