European Bank
for Reconstruction and Development

Digital risks

EBRD briefing note

May 2026

Disclaimer

This document contains references to good practices and should be interpreted bearing in mind the Environmental and Social Policy adopted by the EBRD; it is not a compliance document. It does not alter or amend EBRD policies and does not create any new or additional obligations for any person or entity. In case of any inconsistency or conflict between this document and the Environmental and Social Policy adopted by the EBRD as amended from time to time, such policy shall prevail. Questions of interpretation shall be addressed solely in respect of the Environmental and Social Policy. The information and opinions within this document are for information purposes only. No representation, warranty or undertaking expressed or implied is made in respect of any information contained herein or the completeness, accuracy, or currency of the content herein. The EBRD does not assume responsibility or liability with respect to the use of or failure to use or reliance on any information, methods, processes, conclusions, or judgments contained herein, and expressly disclaims any responsibility or liability for any loss, cost, or other damages arising from or relating to the use of or reliance on this document. In making this document available, the EBRD is not suggesting or rendering legal or other professional services for any person or entity. Professional advice of qualified and experienced persons should be sought before acting (or refraining from acting) in accordance with the guidance herein. This document does not constitute or imply a waiver, renunciation or other modification, either express or implied, of any of the privileges, immunities and exemptions granted to the EBRD under the Agreement Establishing the European Bank for Reconstruction and Development, international convention or any applicable law. Certain parts of this document may link to external internet sites and other external internet sites may link to this publication. The EBRD does not accept responsibility for any of the content on these external internet sites.

Contents

1. Introduction: what are digital risks?

Digital risks may have the potential adverse impacts on people and the environment associated with the use of digital products and services.[1]

As an EBRD client — or a consultant supporting an EBRD client — your organisation is expected under the EBRD Environmental and Social Policy (ESP 2024) to identify, assess and manage digital risks associated with EBRD-financed projects in a proportionate and systematic manner. The EBRD therefore expects its clients to consider digital risks as part of broader environmental, social, governance, labour, stakeholder engagement, and community health and safety risk management processes, proportionate to the nature, scale and risk profile of the project.

Almost all EBRD clients – whether public or private, and regardless of sector or size – are exposed to some degree of digital risk, as organisations increasingly rely on digital technologies for internal management, communications, data processing, operational controls, workforce management, monitoring systems, customer engagement and service delivery. The nature and severity of these risks will vary depending on the country context, business model, sector, operational footprint, technological maturity and the type of digital systems and services used by your organisation (see Annex 1 for illustrative examples of digital risks relevant to EBRD clients).

Digital technologies and data systems can create significant opportunities for efficiency, communication, safety, transparency and service improvement. However, if not properly managed, they may also create or exacerbate environmental, social, labour, human rights, security, privacy, misinformation, exclusion, safeguarding, and community health and safety risks. In some contexts, digital systems may also contribute to discrimination, exclusion of vulnerable groups, online harassment, misuse of personal data, surveillance concerns, cyber threats, or barriers to stakeholder access and participation.

This briefing note aims to raise awareness and support you in understanding, identifying and addressing digital risks throughout the project lifecycle, including during project planning, implementation, operations and stakeholder engagement.

[1] See UN Human Rights Office (2024).

2. Why address digital risks?

As well as meeting EBRD requirements, there are important financial and operational reasons why your organisation should manage digital risks. These include avoiding financial losses and penalties, ensuring legal compliance, avoiding reputational risks and meeting investor expectations.

Avoiding financial losses and penalties

A major cyberattack or data breach can result in costly downtime, regulatory fines and expensive remediation efforts. Disruption to operations, including system failures or compromised infrastructure, can halt service delivery, damage supply chains, erode productivity and, in the case of critical infrastructure, even endanger lives. Beyond immediate costs, unmanaged digital risks could reduce a company's ability to attract investment and increase insurance premiums, adding to the long-term financial burden.

Ensuring legal compliance

If your company fails to comply with laws, regulations and standards – such as data protection, cybersecurity and sector-specific digital requirements – it could face substantial fines, legal claims and contractual liabilities. Companies may also face more intense scrutiny from regulators and stakeholders if digital risks are not adequately addressed.

Avoiding reputational risks

Data breaches, misuse of personal information, algorithmic bias or failures in online safety can undermine trust in a company's ability to protect its clients, partners and employees. Customers may switch to competitors, while negative publicity and social media exposure can cause lasting damage to brand value and stakeholder confidence.

Leveraging strategic and competitive advantages

Failure to anticipate and manage digital risks can hinder innovation, slow digital transformation and reduce competitiveness. Companies that neglect these risks may miss opportunities to leverage new technologies safely, leaving them exposed to market disruption or lagging more digitally resilient competitors.

.

Managing environmental and social risks and impacts

Digital technologies can have significant environmental and social risks and impacts. For example, energy-intensive infrastructure, cyberattacks on critical systems or biased artificial intelligence (AI) systems can harm the environment or exacerbate social inequalities. Managing these risks is increasingly linked to environmental, social and governance (ESG) performance, which in turn affects investor confidence, public perception and long-term sustainability.

Complying with human rights frameworks

Digital risks can violate human rights in multiple ways, from privacy breaches and online harms to discriminatory impacts from algorithmic systems. Companies are expected to integrate digital risk management into their existing human rights due diligence frameworks, in line with the UN Guiding Principles on Business and Human Rights (UNGPs). Doing so helps safeguard people, maintain compliance with international norms and strengthen stakeholder trust.

Meeting investor expectations

Investors increasingly recognise that unmanaged digital risks can have material financial, operational and reputational consequences. As a result, they are requiring companies to take concrete steps to identify and manage these risks.

3. EBRD requirements on digital risks

The EBRD's Environmental and Social Requirements (ESRs) include several provisions that set out clients' responsibilities for managing digital risks. These are summarised in Table 1.

Table 1. Client responsibilities for managing digital risks

ESP	• All EBRD clients are required to respect human rights, avoid infringing the human rights of others, and address adverse human rights risks and impacts caused by their business activities in accordance with the EBRD's environmental and social requirements (ESP paragraph 2.5). The ESP explicitly recognises digitalisation and digital risks as a component of this commitment (ESP paragraph 2.13).
ESR 1 – Assessment and management of environmental and social risks	• Clients must identify and assess potential environmental and social risks and impacts associated with a given project, as well as develop and implement an environmental and social management system (ESMS) for mitigating, managing, monitoring and reporting on identified risks and impacts. ESR 1 explicitly recognises the need to consider digital risks as part of this risk-based approach (ESR 1 paragraph 17). • ESR 1 also contains a general requirement that all clients must ensure ongoing compliance with relevant national laws and regulatory requirements, and this should include those relating to digital risks (ESR 1 paragraph 29). See Annex 2 for further detail on national law.
ESR 2 – Labour and working conditions	• Clients must respect the rights of project workers to privacy and data protection (ESR 2 paragraph 14). • Project workers' personal records must be kept confidential and not be disclosed to third parties without the individual's consent (ESR 2 paragraph 14). • Specific requirements relate to workers engaged through digital intermediation platforms (ESR1 paragraph 4(c)).
ESR 4 – Health, safety and security	Digital risks should be addressed as part of broader health, safety and security measures, including in relation to: • continual evaluation of the health and safety risks that digital products or services may pose to consumers throughout their lifecycle • identifying and assessing project security threats (including cybersecurity attacks) to project workers and project-affected communities.
ESR 5 – Land acquisition, restrictions on land use and involuntary resettlement	• Clients must comply with relevant national legislation and data privacy requirements in relation to surveys, censuses, inventories and valuations, consultation records and the management of data associated with them (ESR5 paragraph 25). • Clients must obtain consent to process and store data, whenever required. Consent must be requested formally, and affected persons must be given the right to access and modify data (ESR 5 paragraph 25). • Clients must keep track of measures taken to ensure the privacy and security of personal data (ESR 5 paragraph 25).
ESR 7 – Indigenous Peoples	• If any personal data are collected from Indigenous Peoples during the consultation and participation process, the data must be handled in a way that safeguards privacy and respects individuals' rights.
ESR 8 – Cultural heritage	• If any personal data of individuals associated with cultural heritage sites are collected, they must be protected and handled in accordance with ESP principles on data protection and privacy.
ESR 9 – Financial intermediaries	• Financial intermediaries (FIs) must ensure that human resources (HR) policies, management systems and practices comply with all ESR 2 provisions, including those relating to data protection and privacy. • FIs must comply with the relevant occupational health, safety and security requirements of ESR 4, including those relating to digital risks. FIs must establish a clearly defined ESMS to identify and manage environmental and social risks associated with subprojects and investments. This should include adequate consideration of all potential environmental and social risks, including those relating to digitalisation.
ESR10 – Stakeholder engagement	• Clients must take appropriate measures to ensure data protection and privacy during stakeholder engagement and as part of the grievance mechanism (ESR 10 paragraph 11).

4. Meeting EBRD requirements on digital risks

Meeting EBRD requirements means having in place structured approaches to identifying and managing digital risks, using proportionate systems and controls that are consistent with national laws and good international practice.

4.1 Identifying risks

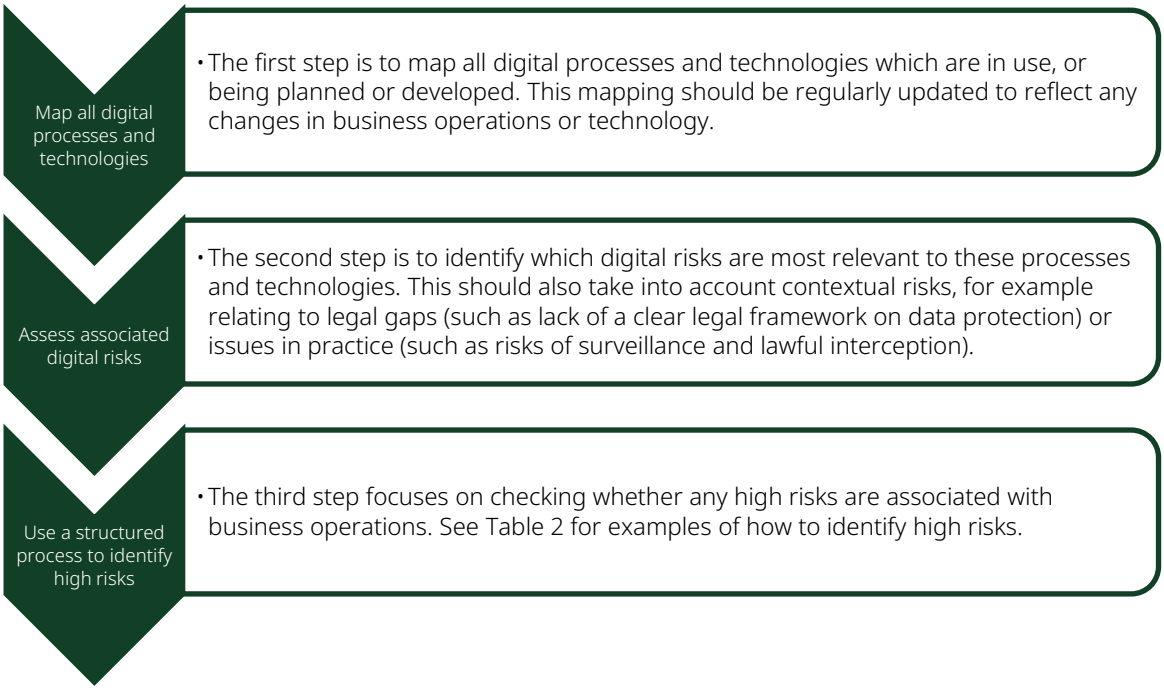

Table 2. How to identify high-risk areas

1. Do your digital systems collect or process large volumes of high-sensitivity personally identifiable information (PII)?	The most significant data protection and privacy risks relate to the collection or processing of high-sensitivity PII (medical records, financial records, biometrics, "special category" data (for example, about health, ethnicity, sexual orientation or religious beliefs)) where unauthorised access or misuse can lead to both immediate and long-term harm for individuals.
2. Do you collect or process any data relating to children (under 18 years), or provide any digital services to children?	Children are especially vulnerable to a wide range of digital risks, including exposure to harmful content and privacy violations. Where any digital services are provided to children, these are specific risks which need to be accounted for.
3. Do you provide telecommunications services or digital infrastructure where there is a risk of misuse of lawful interception, censorship or shutdowns?	Lawful interception is when authorised agencies monitor or intercept specific digital communications or calls, for example as part of crime investigations or national security efforts. Its misuse can create significant human rights risks, particularly where it is used for surveillance and to prosecute activists, journalists or political opponents. Extensive interception creates fear and self-censorship, stifling civil society activities and discouraging legitimate protest or activism.
4. Do you collect large volumes of worker data, or use digital-based management systems?	Digital technologies, such as digital HR systems, are increasingly used to monitor, evaluate and manage the workforce. These can range from sophisticated algorithmic management tools that monitor worker activity and automate task allocations and worker performance evaluations, to digitalisation of worker records, payroll and working-time records. These can generate risks relating to worker surveillance, data protection and privacy. Depending on the form of management system, there may also be risks around the use of algorithmic decision-making, resulting in bias and discrimination.
5. Are digital systems being used, or introduced through digital transformation, to provide critical infrastructure?	When digital systems are introduced into critical infrastructure, such as transport, energy and communications, cybersecurity is essential to ensure the continuous, secure and reliable functioning of these services. Increasing digitalisation and interconnectivity heighten vulnerability, making outages more severe. Cyber threats, including ransomware or nation-state attacks, can disrupt operations, potentially affecting public safety, human rights (such as surveillance risks), economic stability and national security. Such disruptions may also lead to catastrophic safety incidents for workers or service users and significant environmental harm to local communities.
6. Are digital systems being used to provide essential services?	Where digital systems are introduced in relation to essential services, there is a risk of excluding marginalised or vulnerable groups. For example, digital-only access, such as mandatory online accounts, digital payments or platform-based service delivery, can exclude certain groups and disadvantaged users who face skills gaps, language barriers, limited digital literacy or lack of appropriate devices and connectivity.
7. Is there any deployment of "high-risk" AI?	The European Union (EU) AI Act defines certain uses of AI as high risk because they can pose serious risks to health, safety or fundamental rights. These include: • AI safety components in critical infrastructure, the failure of which could put the life and health of citizens at risk • AI tools for employment, worker management and access to self-employment (such as CV-sorting software for recruitment) • certain AI uses to give access to essential private and public services (for example, credit scoring).
8. Are there any services or processes that include user-generated content?	User-generated content (UGC) can facilitate online bullying, the spread of misinformation and other harmful content, exposing users to risks such as harassment, manipulation, age-inappropriate material and hate speech.
9. Is there any engagement of platform workers?	Platform work is an increasingly common work arrangement in many sectors, including transport and logistics, and e-commerce. It can also facilitate non-location-specific "cloud-work" using remote workers, sometimes in other jurisdictions. In many jurisdictions, self-employed platform workers are excluded in part or in whole from protections afforded by labour legislation. The lack of coverage under national labour legislation can have a particularly detrimental effect on vulnerable workers, including in relation to wages, working hours and conditions.
10. Are any digital technologies being developed that are linked to scenarios 1-9?	Where a client is involved in developing digital products and services, rather than just using or deploying digital technologies, this can present significant risks. Companies involved in developing digital products generally have greater liability for compliance failures and system-induced harm in regulation.

4.2 Managing digital risks

To effectively manage digital risks, your company will need to establish robust, well-documented management systems that clearly define how digital risks are identified, owned and controlled. These should comply with national law, reflect good international practice and be proportionate to your organisation's size, sector and risk profile. Technical, organisational and contractual controls should be embedded within this wider management system, and regularly reviewed to reflect evolving technologies, emerging threats and regulatory developments.

Implementing management systems for digital risks

- ✓ Assign clear roles and responsibilities, including designated qualified personnel with clear mandates and reporting lines. Depending on the size of your organisation or the national legislation, this might include a dedicated data protection officer. In large organisations, it might include cybersecurity, privacy committees or working groups that collaborate and coordinate across different organisational functions and areas of expertise (IT, legal, procurement, operations).
- ✓ Ensure staff with digital risk responsibilities have the appropriate expertise, including qualifications or certifications where relevant (for instance, data protection officers or cybersecurity specialists). In smaller organisations, engage appropriate external expertise.
- ✓ Ensure appropriate governance structures, including board-level oversight, or equivalent.
- ✓ Allocate sufficient financial resources for ongoing digital risk management, including staff training, system upgrades and external audits.
- ✓ Put in place ongoing monitoring and reporting of incidents to facilitate continuous development.
- ✓ Regularly review assessments, policies and procedures to adapt to evolving digital threats and organisational needs. Technologies and threats evolve quickly, and it is important for clients to stay ahead of emerging risks.

Table 3 sets out examples of risk management systems that would typically be expected for different digital risk scenarios. Where digital risks are present, the EBRD would expect clients to be able to demonstrate management systems that align with relevant international standards and frameworks, but not necessarily for these to be accredited or certified by a third party. A summary of relevant standards and frameworks is set out in Annex 3.

Table 3. Expected risk management systems for digital risk scenarios

Scenario	Expected risk management system
All clients – fundamentals	• An information security management system (ISMS) that sets out clear principles and responsibilities for protecting information across the organisation. This should incorporate applicable technical controls required for cybersecurity and system integrity such as authentication, encryption, firewalls, endpoint protection and patch management. • A data protection policy that sets out clear principles and responsibilities for protecting personal protection and privacy. It should include the lawful basis for collecting and processing data under applicable laws and regulations, data minimisation practices, a data inventory, and retention or deletion schedules.
Large-scale collection or processing of high-sensitivity PII through digital systems	• A privacy information management system (PIMS) aligned with GDPR, ISO 27701 or any other equivalent non-EU national framework.
Any collection or processing of data relating to children (under 18 years), or provision of any digital service to children	• A management system aligned with the EU Digital Services Act, including governance, risk assessment and mitigation measures for minors, age-appropriate design, and procedures for handling notices, complaints and enforcement requests.
Telecoms services or digital infrastructure where there are risks of misuse of lawful interception, censorship or shutdowns.	• A governance system for lawful interception and network interference, including clear policies, approval and oversight procedures, logging and audit, transparency reporting, and escalation to senior management.

Scenario	Expected risk management system
Large-scale collection of worker data, or use of digital-based management systems	• An HR management system that integrates with the ISMS and data protection framework, including specific policies on worker monitoring and surveillance, with clear purpose limitation and retention rules, and consultation with worker representatives where applicable.
Digital systems/digital transformation for the provision of critical infrastructure	• An ISMS aligned with ISO 27001. • A cybersecurity management system (CSMS) aligned with IEC 62443 (or equivalent sectoral standard), covering asset inventory, network segmentation, secure configuration, incident response and business continuity for operational technology and supporting IT systems.
Digital transformation of essential services	• An ISMS aligned with ISO 27001, extended to cover the continuity and resilience of essential services, and including documented incident response, disaster recovery and business continuity arrangements for the digital components of the service. Where relevant, it should also align with Directive NIS2 on the cybersecurity of critical sectors, or an equivalent national framework. • Operational technology (OT) and physical-digital interfaces – segment OT and IT networks, apply security controls to industrial control systems, and ensure cyber risks are embedded in operational risk frameworks.
Any deployment of high-risk AI	• An AI management system (AIMS) aligned with ISO 42001 and, where applicable, the EU AI Act, including governance roles, risk assessment and mitigation, data and model lifecycle controls, human oversight, robustness and security controls, documentation and post-deployment monitoring.
Services or processes that include user-generated content	• A content governance system aligned with the EU Digital Services Act, including risk assessments, content moderation policies and procedures, notice-and-action mechanisms, complaint handling, transparency reporting and cooperation processes with competent authorities.
Engagement of platform workers	• A platform management system that ensures any use of self-employment complies with national law and that workers receive clear, transparent terms and conditions, including fees and payment arrangements – in line with ESR 2.

Annex 1. Overview of digital risks

	Risk area	Explanation
	Privacy and data protection	• Digital products, services or projects have the potential to infringe on individuals' right to privacy through excessive or unnecessary data collection, misuse of data, insufficient consent, or inadequate transparency and security of personal data. • Privacy and data protection risks typically affect customers and service users. There are also significant risks in relation to workers, for example excessive monitoring of workers' activities through apps and GPS tracking can lead to potential privacy violations. • Risks also arise from lawful interception, which is the interception of electronic communications to gather intelligence or evidence. These risks are heightened in countries with low governance and weak judicial oversight. • Privacy and data protection risks may also arise through insufficient data security protections. These can get exploited through cyber-attacks and may lead to issues such as identity theft or biometric data theft.
	Freedom of expression and association	• Digital surveillance can be used as a tool for suppressing freedom of association and assembly and restriction of civic space, for example through the use of spyware against human rights, environmental or trade union activists. These risks undermine people's ability to access information, share opinions, organise collectively and participate in public life. • In some cases, governments may seek to censor or suppress digital content or shut down the internet or telecommunications to suppress freedom of expression and assembly. This may negatively impact relevant stakeholders, including workers, trade unions, civil society organisations and members of the wider community. • The spread of disinformation or misinformation such as malicious, fabricated, manipulated, misleading or false content can be used to instil fear and suspicion among stakeholders and the wider population.
	Exclusion and the digital divide	• If not designed with accessibility and inclusion in mind, digitalisation can create barriers to essential services for specific groups, for example due to skills gaps (such as digital literacy), language barriers or lack of financial resources. This particularly affects members of low-income households, migrants, refugees, people with disabilities and older people. • The "digital divide" refers to unequal access to digital technologies and the internet, which can lead to marginalised groups being left behind in areas such as education and employment.
	Bias and discrimination (AI)	• AI, algorithms and automated decision-based systems pose significant risks when they rely on biased or limited datasets, as this can lead to discrimination. For example, gendered stereotyping – such as portraying women as weak, incompetent or overly sexualised – further entrenches inequality and undermines female leadership and participation. • Algorithmic decision-making in the workplace – used for recruitment, work allocation and performance assessment – can lead to bias or discrimination. • As decision-making processes of generative AI systems are often difficult to retrace, it is also challenging to assign responsibility for discriminatory or unfair outcomes, as well as accountability for remedial actions. • In general, inaccurate or incomplete data, regardless of whether inaccuracies originate from AI-generated information or not, may lead to flawed assessments or decisions, resulting in unintended negative social or human rights impacts, such as unfairly limiting access to services.
	Physical and psychological harm	• Digital technologies may lead to physical and psychological harm, including through cyberbullying, misinformation and exposure to harmful content (including AI-generated content). For example, digital technology can amplify or facilitate gender-based violence and harassment by enabling online harassment or cyberstalking. • Children face specific risks of psychological and physical harm online, as their limited cognitive development and digital literacy make it harder for them to manage device use and recognise or respond to online dangers. • Online risks can escalate into physical harm when online targeting and identification lead to real-world attacks.

	Risk area	Explanation
		• Cybersecurity incidents can disrupt services and compromise systems, leading to physical, psychological and health risks for consumers, workers and communities.
	Labour rights and violations	• Digital technologies have enabled the growth of platform work – where a digital platform (usually in the form of an app) matches the supply and demand for paid tasks and services. Platform workers are typically not covered by employment law and have very few rights at work, creating risks in relation to wages, access to social security, working hours and conditions.
	Environmental impacts	• Certain digital technologies pose significant environmental risks through their substantial energy and water consumption. For example, certain AI technologies (primarily generative AI models) and internet services consume vast amounts of electricity and require extensive water resources for cooling systems.

Annex 2. National laws on digital risks

National laws and regulations vary significantly between the EBRD's countries of operation but typically address the following areas:

- Privacy and data protection: laws such as the EU General Data Protection Regulation (GDPR) as implemented in EU member states and reflected in equivalent national data protection frameworks in other jurisdictions, set rules for the lawful collection, processing, transfer and storage of personal data.
- Consumer protection: laws and regulations to ensure fair treatment of consumers are relevant to digital services, including in relation to manipulative design (for example, gambling-like features in video games, known as loot boxes or free-to-play mechanics), deceptive or targeted advertising (such as personalised targeting that exploits financial challenges), and security and fairness of digital transactions (for instance, excessive restrictions on unsubscribing from digital services).
- Online safety and content regulation: national frameworks govern the responsibility of online intermediaries for content moderation, the prevention of hate speech, misinformation and harmful digital content.
- Intellectual property and copyright cover the ownership and use of data, software and creative content, including material used in AI model training. Rights compliance has become increasingly relevant for digital platforms and generative AI developers.
- Competition and market fairness: laws regulating dominant digital platforms (for example, app stores, search engines, digital marketplaces) aim to prevent the abuse of market power. The EU's Digital Markets Act and similar emerging laws in large economies set interoperability, transparency and data-access requirements.
- AI and high-risk technologies: the EU Artificial Intelligence Act (Reg. 2024/1689) establishes obligations directly applicable across all EU member states and introduces a risk-based regulatory model for AI. Several EBRD economies are developing or considering legislation modelled on or aligned with the EU AI Act.
- Cybersecurity and data governance laws: national cybersecurity frameworks protect information and communications infrastructure. In the EU, the NIS 2 Directive (2022/2555) and Digital Operational Resilience Act (DORA – Reg. 2022/2554) govern ICT risk management and incident reporting. Similar frameworks are also being developed in non-EU countries.
- Sector-specific regulations are particularly relevant for regulated sectors such as finance, insurance and telecommunications, where they impose additional safeguards.

Annex 3. Standards and regulations on digital risks

- UNGPs set global standards for companies to respect human rights, including those relating to digital privacy, through human rights due diligence, and help to inform responsible business conduct in the technology sector.
- GDPR – the EU's comprehensive privacy law that governs how personal data of individuals in the EU are collected, used, stored and protected, providing strict rules and severe penalties for non-compliance.
- EU AI Act – establishes a risk-based regulatory regime for AI use within the EU, banning unacceptable risk applications and imposing strict requirements on high-risk AI systems, including risk assessment and mitigation.
- ISO 27001 – the international standard for information security management systems, providing a framework for organisations to systematically identify, assess and mitigate risks to protect sensitive data based on robust security controls.
- ISO 27702 – extends ISO 27001 to cover privacy information management, setting requirements for organisations to manage personal data and comply with privacy regulations.
- ISO 42001 – focuses on AI management systems, addresses governance, risk and ethical challenges around AI technologies to ensure that AI systems are designed, deployed and monitored responsibly.
- ISO 8183 – the international standard that defines a comprehensive data lifecycle framework for AI systems and provides guidelines for managing data processing throughout the AI system's lifecycle to ensure quality, security, compliance and effective governance.

1979 Digital risks – EBRD briefing note, May 2026

Five Bank Street
London E14 4BG
United Kingdom

ebrd.com