Overview of frequently asked questions about the application of the IDRS

What is the IDRS?

IDRS stands for International Digital Reporting Standards. It is a reporting standard developed by NOREA that enables organisations to account annually for how they manage their digital processes and IT risks. Similar to a financial annual report, IDRS provides a structured overview of Digital Innovation and Transformation; Data & AI; Third Party Management; Cybersecurity; IT Continuity Management and Privacy. The aim is to provide transparency to stakeholders, directors and regulators about an organisation's digital resilience.

Is the use of the IDRS mandatory?

No, the use of the IDRS is not (yet) legally mandatory. It is a standard that organisations can use voluntarily to demonstrate their digital control. However, the IDRS is in line with existing and emerging legislation such as NIS2, DORA, and GDPR, making it a valuable tool for meeting compliance requirements. Its use is expected to be more widely encouraged in the future, including by regulators.

Why was the IDRS developed?

The IDRS was developed to gain control over digital risks and to replace fragmented IT accountability with a single, integrated report. In a world where IT is at the heart of virtually all business processes, transparency about digital security and compliance is crucial. The use of the IDRS helps organisations inform stakeholders, strengthen trust, and substantiate strategic choices. It also provides a basis for assurance by auditors.

What is the IDRS not intended for?

The IDRS is not a standards framework for IT control or regulatory compliance. The IDRS prescribes which control aspects must be reported on, but not how these controls should be organised or implemented.

Does the IDRS improve IT control?

Yes, the IDRS offers a holistic framework that integrates IT governance, risk management, and compliance. By reporting annually according to the PDCA cycle (Plan–Do–Check–Act), organisations gain better insight into their digital vulnerabilities, areas

for improvement, and strategic IT goals. This leads to better control over IT processes, better decision-making, and fewer surprises in the event of incidents or audits.

Does the IDRS improve digital security?

Absolutely. The application of the IDRS forces organisations to think structurally about cybersecurity, IT continuity, and privacy. By identifying risks and documenting measures, a culture of digital responsibility is created. The report highlights vulnerabilities and encourages improvement actions, thereby increasing digital resilience.

Does the IDRS reduce costs?

Indirectly, certainly. By bundling all digital accountability into a single report, the application of the IDRS saves time and resources that would otherwise be spent on separate accountability reports. It prevents duplication of work and speeds up internal and external communication. In addition, it provides supervisors (including the Supervisory Board and the Supervisory Committee) with reliable information about IT control, as well as any gaps in that control.

Are there any costs associated with using the IDRS?

The use of the IDRS itself is free of charge, but drawing up a report requires time and the involvement of internal and sometimes external experts. These costs depend on the complexity of the organisation, the degree of digitisation, and whether external support is required. In the long term, however, it will result in savings through more efficient compliance and risk management. Better IT management also leads to fewer outages and better quality of services and products, which also results in savings and competitive advantage.

Do I need an auditor?

An auditor is not required to apply the IDRS. However, IT auditors can assist in preparing, assessing, and validating the report. This increases reliability and makes it possible to provide assurance to stakeholders.

Does applying the IDRS help directors fulfill their duty of care?

Yes. Directors have a legal duty of care to manage risks and be accountable (for example, under the Cybersecurity Act and the Corporate Governance Code). The IDRS offers a structured way to demonstrate that the organisation takes digital risks seriously and takes appropriate measures. This strengthens their position vis-à-vis regulators, shareholders, and society.

How does the IDRS help regulators?

The IDRS provides regulators with a single, clear document that brings together all relevant IT risks, measures, and compliance information. This facilitates supervision, prevents fragmented reporting, and increases transparency. It helps regulators assess risks more quickly and ask more targeted questions, making their work more efficient.

Can I use the IDRS internationally?

Yes. The IDRS is designed as an international standard and complies with European regulations such as NIS2, DORA, and GDPR. The IDRS can be applied in various sectors and countries. Discussions are underway to anchor the IDRS at the European level as well, making it a valuable tool for internationally operating organisations.

Which laws does the IDRS cover?

There are more than 100 EU laws in development and partially already implemented that address IT, and a number of these laws require accountability. The application of the IDRS helps organisations comply with a number of IT-related laws and regulations, including:

- NIS2 (network and information security)
- DORA (digital operational resilience in the financial sector)
- GDPR (privacy)

Not all laws specify exactly how accountability should be achieved, but by combining all requirements in a single report, a clear and coherent accountability is created. An organisation, the IDRS platform, is currently being set up to maintain the IDRS, including embedding more laws in the IDRS.

Which functions do I need to involve internally in order to apply the IDRS?

Several departments are needed for good IDRS reporting, but in any case the owners of the following components:

1. Digital Innovation and Transformation
2. Data & AI
3. Third Party Management
4. Cybersecurity
5. IT Continuity Management
6. Privacy

Consider the following individuals:

1. CIO, CTO, CITO
2. CISO
3. Compliance and Legal Affairs
4. Risk management
5. Privacy officers
6. Data governance
7. Management and internal audit

Together, they provide a complete picture of digital processes, risks, and control measures.

How much time does it take to prepare the IDRS report?

Organisations can start by developing a number of chapters of a report based on the IDRS. The first complete report takes an average of 200-300 hours, depending on the maturity of IT processes and available data. After that, annual updates become easier. Organisations that already work with ISO, NIST, or other frameworks can switch more quickly. Periodic updates make it a dynamic and manageable process. Incidentally, in many cases, some of the content included in the report will already be available within the organisation but will not end up on the boardroom table, or at least not in a structured and coherent report.

What does the IDRS platform do?

The final version of the IDRS was delivered in May 2025. The purpose of the IDRS platform is to maintain the IDRS from the following perspectives:

- New laws may give rise to amendments to the IDRS.
- New IT developments (e.g. quantum) may give rise to amendments to the IDRS.
- Drawing up sector standards. Examples include an addendum to the IDRS for the financial sector (to report on DORA), critical infrastructure (to report on NIS2) or local government, whereby current accountability requirements could be replaced by a single report based on the IDRS.
- Providing solicited and unsolicited advice.

A group of experts will then amend the IDRS if necessary.

How can I participate in the IDRS platform?

On this page, you will find more information about the activities of the IDRS platform. If you are interested in joining the IDRS platform, please contact Lisanne van Helten at idrsplatform@ecp.nl.