What is DORA?

Overview

Before we can appreciate how as a business, we can assist our customers being compliant with this new regulation, we first need to understand what it is and why it has been introduced.

The **Digital Operational Resilience Act (DORA)** is a regulatory framework established by the European Union to enhance the resilience of financial entities against digital and cyber threats. It aims to ensure that financial institutions can withstand, respond to, and recover from ICT-related incidents and operational disruptions, with an ever-growing cyber threat landscape and the interconnected nature of the financial sector.

The financial sector is a prime target for cyber attackers, with a single breach possibly spreading across the broader supply chain, affecting critical infrastructure and eroding trust in financial systems.

Key Requirements

The key requirements of DORA are:

1. **ICT Risk Management**: Financial entities must implement robust policies and controls to mitigate risks associated with information and communication technologies.
2. **Third-Party Risk Management**: Rigorous assessments and continuous monitoring of ICT third-party service providers are required to ensure they meet resilience standards.
3. **Incident Reporting and Response**: Entities must have processes in place for timely detection, classification, and reporting of ICT-related incidents.
4. **Operational Resilience Testing**: Regular stress tests and simulations to validate preparedness and identify vulnerabilities.
5. **Information Sharing**: Collaboration and transparency between entities to share insights on emerging threats and best practices.

Compliance Deadline

Organizations must comply with DORA by **January 17, 2025** and non-compliance can result in significant penalties, increased regulatory scrutiny, and reputational risk.

Best Practices for Compliance

To be compliant with the legislation, an organization should:

- Establish comprehensive ICT risk management policies.
- Conduct regular assessments of third-party service providers.
- Implement a robust incident reporting and response framework.
- Perform regular operational resilience testing.
- Foster a culture of information sharing and collaboration.

DORA is not just about compliance; it's about embedding resilience into the DNA of financial entities to ensure they can continue to operate even in the face of cyber threats.

Who's affected by DORA?

DORA applies to a wide range of financial entities, including and not limited to:

- Banks and credit institutions.
- Insurance companies and reinsurance undertakings.
- Payment institutions and electronic money institutions.
- Investment firms, alternative investment funds, and management companies.
- Third-party ICT providers servicing financial entities.

The regulation also indirectly impacts ICT service providers outside the financial sector if they supply critical ICT-related services to regulated entities, such as Bluesource and where we can assist our customers on their compliance.

Bluesource and DORA

We are here to help!

Bluesource recognises the importance of this new regulation and aims to assist customers on their compliance journey wherever we can, and so we can be easily identified, rather than just relying on our company's registration number in the UK, we also have also registered a globally recognised **Legal Entity Identifier (LEI)** number.

We see that our ISO27001:2022 certified Information Security Management System ("ISMS"), built around ISO27002 controls and best practice, provides a solid framework for our processes, procedures and services to be in line with DORA's requirements, and the need for them to continuously be reviewed and here's how:

ICT Risk Management:

Bluesource has implemented robust policies and controls as part of its ISMS to mitigate risks associated with information technology. These are regularly reviewed both internally and externally, at least annually. We have achieved certification against the internationally recognised ISO27001 standard for information security and are early adopters of the latest 2022 version, ahead of the October 2025 deadline for compliance, to ensure we are ahead of our customer's requirements and that they can continue to put their trust in our services.

Third-Party Risk Management:

Ours ISMS requirements extend to our key service providers and subcontractors, with whom we contract and have close working relationships. We regularly undergo service reviews, conduct risk assessments, perform security assessments, cascade our information security and data processing requirements and where applicable, have conducted transfer risk assessments and put Standard Contractual Clauses in place.

Where applicable and largely dependent on the type of service being provided to a customer, we will conduct regular service reviews with them and where contracted to do so, or required by legislation, reasonably assist with any annual security questionnaire/assessment they require for their own monitoring requirements and compliance.

We also perform regular Pen Tests on our environment using specialist third-party providers.

Incident Reporting and Response:

As part of the requirements for Bluesource's ISMS and its continued compliance and certification to ISO27001, it has systems and processes in place for timely detection, classification and reporting of ICT-related incidents.

As with the requirements for the DPA 2018 and GDPR, as well as its own ISMS, Bluesource will engage customers in a timely manner, typically within 24 hours, to advise them of a potential or actual incident, or treat. This timely approach ensures that the customer can meet their own obligations, typically as the Data Controller, with their reporting requirements to relevant parties and regulatory bodies, such as the ICO.

Operational Resilience Testing:

As part of our ISMS, we perform regular disaster recovery and business continuity testing and simulations, typically 6 monthly, and have a DR and BCP Policy in place, which is also regularly reviewed.

Our internal systems are also monitored to ensure capacity, resilience and availability of service, and having invested in virtual systems such as IaaS and SaaS, we are able to provide a wide range of remote service offerings, which are not necessarily dependant on a physical location, ensuring our robustness and continuity, with scenarios like loss of access and pandemics.

With our expertise in the use of IaaS, SaaS solutions, backup services, and system monitoring, we can provide a range of services to our customers, to meet their own requirements for DORA, in terms of resiliency and being prepared for the unknown.

Information Sharing:

Where applicable, Bluesource will collaborate and be transparent between entities to share insights on emerging threats and best practices. We have put in place an internal Threat Policy and utilise information from various sources to look at the emerging threat landscape to ensure we put necessary measures in place to mitigate any risks and warn any relevant parties.

DORA's Article 30 requirements

Article 30 of DORA (Digital Operational Resilience Act) outlines key contractual provisions between financial entities and ICT third-party service providers. These provisions allocate and set out the rights and obligations of both parties in writing.

The key requirements outlined are:

- **The rights and obligations of the financial entity and of the ICT third-party service provider** - Contracts with Bluesource are usually in form of placing orders for goods and/or services against our general terms and conditions, applicable service schedules and any terms agreed at order level, such as the applicability of a statement of work (SOW), or any agreed variance.

- **A clear and complete description of all functions and ICT services to be provided** – These are agreed as part of the contract for the relevant service(s) and are typically set out in the "Agreement" between the parties (i.e., within the General Terms and Conditions, service schedule, statement of work, or work order).

- **The locations, namely the regions or countries, where the contracted or subcontracted functions and ICT services are to be provided and where data is to be processed** – This is usually specific to a service and detailed in the Agreement.

- **Provisions on availability, authenticity, integrity, and confidentiality in relation to the protection of data, including personal data** – Unless otherwise agreed within an Agreement, Bluesource's data processing and confidentiality is compliant with relevant legislation and its published Data Processing and Privacy policies on its website (https://bluesource.co.uk/privacy-and-governance).

- **Provisions on ensuring access, recovery and return in an easily accessible format of personal and non-personal data processed by the financial entity in the event of the insolvency, resolution, or discontinuation of the business operations of the ICT third-party service provider, or in the event of the termination of the contractual arrangements** – If this is applicable it will be detailed within the relevant Agreement and also aligned with the requirement for return or destruction of personal data under GDPR and DPA.

- **Service level descriptions, including updates and revisions thereof** – Detailed within the Agreement and any contract variations agreed between the Parties.

- **The obligation of the ICT third-party service provider to provide assistance to the financial entity at no additional cost, or at a cost that is determined ex-ante, when an ICT incident that is related to the ICT service provided to the financial entity occurs** – If applicable for a particular contracted service, this would be detailed within the Agreement. We are obliged to provide a contracted service, so an incident affecting that service would be our responsibility and cost to rectify, unless it was caused by the customer.

- **The obligation of the ICT third-party service provider to fully cooperate with the competent authorities and the resolution authorities of the financial entity, including persons appointed by them** – This is very similar to the requirements of a "data processor" under the DPA2018 and GDPR. Bluesource shall reasonably assist within the scope of the contracted service/s.

- **Termination rights and related minimum notice periods for the termination of the contractual arrangements** – Agreements will detail the initial and any renewal terms relevant to the contractual arrangements.

- **The conditions for the participation of ICT third-party service providers in the financial entities' ICT security awareness programmes and digital operational resilience training in accordance with Article 13(6)** – As part of our ISMS and ISO27001 certification, our workers are regularly trained and assessed on information security (ISO27001) and GDPR at least annually. Any specific requirements relating to a customer's own training and awareness programme, would be agreed and detailed in the relevant Agreement.

The contractual arrangements on the use of ICT services supporting critical or important functions shall include, in addition to the elements referred to above:

- **Full-service level descriptions, including updates and revisions thereof with precise quantitative and qualitative performance targets within the agreed service levels** - Depending on the service(s) being contracted, any quantitative and qualitative performance metrics, such as service levels, shall be detailed in the relevant Agreement.

- **Notice periods and reporting obligations of the ICT third-party service provider to the financial entity** - Covered in the relevant Agreement.

- **Requirements for the ICT third-party service provider to implement and test business contingency plans and to have in place ICT security measures, tools and policies that provide an appropriate level of security for the provision of services** – Covered by our ISO27001 certification and ISMS requirements.

- **The obligation of the ICT third-party service provider to participate and fully cooperate in the financial entity's TLPT** – This is a similar requirement for processors under data protection and Bluesource would assist by providing reasonable information relevant to the service, usually through completing an annual questionnaire, proving copies of its certifications and policies on request, participating in service reviews and conducting our own security assessments and annual Pen Test. Where a service is procured on behalf of the customer, such as a vendor's subscription service, Bluesource shall have no obligation in this respect other than to request relevant information from the vendor on the customer's behalf. The customer must ensure that it has risk assessed the relevant service and is happy with the security provided by the vendor.

- **The right to monitor, on an ongoing basis, the ICT third-party service provider's performance** – Any monitoring requirements shall be agreed between the Parties and detailed in the relevant Agreements, such as SLAs, targets, service reviews, reporting, etc.

- **The obligation of the ICT third-party service provider to fully cooperate during the onsite inspections and audits performed by the competent authorities, the Lead Overseer, financial entity or an appointed third party** – Where applicable the requirements are detailed within the relevant Agreement(s), such as the obligations of a Data Processor under DPA 2018 and GDPR.

- **The obligation to provide details on the scope, procedures to be followed and frequency of such inspections and audits** Where applicable the requirements are detailed within the relevant Agreement(s), such as the obligations of a Data Processor under DPA 2018 and GDPR.

- **Exit strategy** – If applicable to a service, any exit strategy requirements need to be agreed and detailed within the relevant Agreement.

- **When negotiating contractual arrangements, financial entities and ICT third-party service providers shall consider the use of standard contractual clauses** – For consistency and risk mitigation, and unless otherwise agreed, Bluesource has put in place a General Terms and Conditions document which its service schedules and orders relate to.

If you require any further information on how we can help you with DORA and our services, please let us know.