European Data Centre Association

EUDCA Reply to EBA's Consultation on ICT and security risk management

The European Data Centre Association (EUDCA), the organisation representing the voice of data centres in Europe, is committed to offering highly secure and reliable ICT service support for financial institutions. It is essential that financial actors consider not just cloud but also underlying data centre infrastructure security, which is an essential part of the digital ecosystem. Therefore, we welcome the intention of the EBA's guidelines and, in reference to mentions of data centres on pages 16 and 21 of the Consultation document (sections '4.2.3. Use of third party providers' and '4.4.4. Physical security'), recommend defining data centre security requirements in more detail.

In general, data centres supporting financial institution operations should possess or adhere to internationally recognised certifications, controlled by independent auditors. The following standards greatly contribute to data centre security:

- Minimum **Tier 3 level** of redundancy of the data centre infrastructure to ensure continuity of operations. This amounts to an availability of at least 99.98% of data centre services annually, with all systems being present in double (electricity, cooling, maintenance and capacity). Back-up installations allow data centres to continue operating during maintenance or power outage.
- The **ISO 27001** standard certifies the quality of an information security management system, guaranteeing the confidentiality and availability of data. Strict procedures protect information and ensure effective incident management.
- The **ISO 14001** standard specifies requirements for an effective environmental management system. This implies a commitment to reducing unnecessary energy consumption and continuously striving to achieve greater efficiency in all parts of operations.
- The **ISO 9001** standard ensures effective quality management, providing a systematic approach to maintaining and improving customer experience.
- **ISAE 3000, Type 2** and **ISAE 3402, Type 2 reports** ensure adequate risk management, quality and reliability of internal processes. ISAE 3000 focuses on operational management, while ISAE 3402 on financial reporting. Type 2 reporting means the security measures are periodically tested and verified.

Furthermore, we recommend applying the following criteria to enhance the physical security of data centres:

- Location should be safe, avoiding risks such as natural hazards (extreme weather, e.g. floods, fire and earthquakes), nearby threats, such as chemical plants, and political risks (e.g. unrest and lock-out risks in areas frequently restricted by police).
- Large and systemically important financial institutions should use a minimum of two data centres, connected to different power grids to diversify risks.
- Financial institution data servers must be stored separately from any other customers.
- Controlled access system to the data centre needs to be in force with identity verification.

Please contact us at policy@eudca.org for further information. We remain at your disposal to assist your work and contribute to the security and proper functioning of Europe's financial ICT systems.