

Alfa Laval and CRA

EU Cyber Resilience Act (CRA): Impact and response at Alfa Laval

The EU Cyber Resilience Act (CRA) establishes mandatory cybersecurity requirements for products with digital elements, aiming to ensure a high common level of cyber resilience across the European market. The CRA impacts manufacturers, importers, and distributors by requiring them to address vulnerabilities throughout the product lifecycle, from design to end-of-life.

How Alfa Laval is affected

As a leading provider of industrial equipment and solutions, Alfa Laval integrates digital technologies into many of its products and services. The CRA directly affects Alfa Laval by mandating robust cybersecurity measures for connected devices and software, ensuring that products are secure by design and by default. Compliance is essential to maintain market access, customer trust, and regulatory alignment.

Alfa Laval's approach to CRA compliance

Alfa Laval addresses CRA requirements by:

- Embedding cybersecurity into product development processes, from risk assessment to secure coding and testing.
- Maintaining a coordinated vulnerability disclosure policy and rapid incident response mechanisms.
- Training staff and partners on CRA obligations and best practices.
- Continuously monitoring regulatory updates and adapting internal policies to ensure ongoing compliance.

Through these actions, Alfa Laval demonstrates its commitment to delivering secure, resilient solutions and supporting customers in a rapidly evolving digital landscape.