Compliance: the connected product's *best friend*

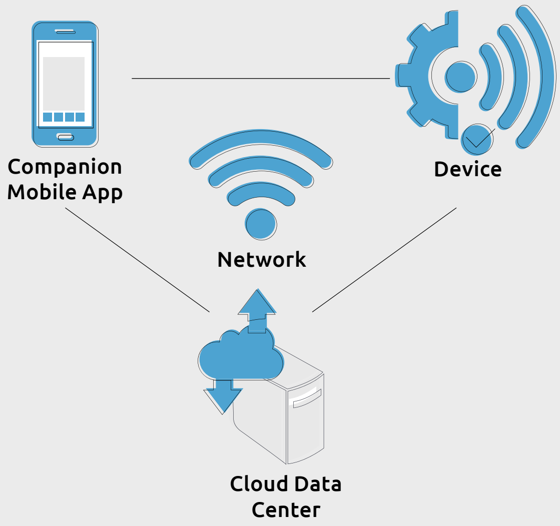
Capgemini

On the right side of *connected product compliance*

A growing wave of regulations is impacting connected products, driven by concerns over numerous risks. These regulations aim to protect users, ensure environmental responsibility, safeguard personal data, and bolster cybersecurity. This affects the whole product lifecycle, from development and operation to decommissioning. They can apply to both the physical and digital components of connected products, with further geographic and industry-specific requirements.

While the path to compliance is not always easy, companies can unlock broader benefits. These include improved customer and partner trust, market differentiation through transparency, and avoiding financial penalties.

Connected Product



A connected product is typically defined as a connected device **and** any additional product components that are necessary to use the device beyond basic operational features: companion mobile applications, network components, backend computing cloud/datacenter.

Before the Internet explosion of the '90s, most products affected by compliance were either not connected, or were not complex, either electronically or in their software. The omnipresence of the internet and connectivity has caused an explosion of complex, ubiquitously connected devices and systems, spreading further with the growth of the Internet of Things (IoT). Regulations have evolved to govern privacy and cybersecurity as software integration in connected products components has progressed.

More recently, a greater sense of urgency about climate change, awareness of environmental damage, and the adoption of artificial intelligence (AI) has led to new regulations for sustainability and safeguarding respectively.

The growing cybersecurity threat

The menace of cybercrime is growing enormously and rapidly. As a proxy for cybercrimes generally, the Federal Bureau of Investigation recorded 880,418 complaints in 2023 in the US alone, a 10% increase from the previous year.[1] Kaspersky, a technology provider, detected 1.5 billion attacks on smart devices through its global monitoring network in the first half of 2021. This represented a doubling of cyberattacks on IoT devices over a single quarter.[2]

Connectivity adds a new way to access devices, sometimes from anywhere in the world, which also increases the risk of unauthorized access. Connected devices offer additional attack surfaces, making mundane devices potential gateways for attackers. Examples include connected grocery store fridges that could lead to point-of-sale credit card theft; attacks on water treatment plant controllers that compromise water safety; and botnets[3] infecting IoT devices to launch denial-of-service attacks.

The ease of flow of data to and from connected products is, if not designed with it in mind, in competition with maximum cybersecurity. Both should be in harmony. Achieving this balance requires advanced integrated cybersecurity from the very beginning of product development.

Greater sustainability awareness

Legislators have raised their expectations of manufacturers' responsibility for their products' impact on the environment throughout the lifecycle, from production to disposal. Recent and anticipated regulations significantly impact the connected products industry. Key themes in these regulations include:

1. **The right to repair:** these laws are gaining momentum globally and require manufacturers to provide documentation and support for repair, promoting repairability and the extension of consumer electronic products' lifespans. California's Right to Repair Act (SB 244) takes effect in July 2024, the third such state law in the US.[4] The EU announced its proposals for rules to reduce waste and prioritize repair over replacement in May 2023.

[1] "FBI: Critical infrastructure suffers spike in ransomware attacks", The Register, March 6, 2024
[2] "IoT attacks skyrocket, doubling in six months", Threatpost, September 6, 2021
[3] A group of computers connected in a coordinated fashion for malicious purposes. Techopedia, October 4, 2023
[4] "California Becomes Third U.S. State to Join the Right-to-Repair Movement", Sidley, October 24, 2023

2. **Single-use plastics:** for example, the EU's Single Use Plastics Directive (2019), which restricts the sale of certain single-use plastics. While not specific to consumer electronics, it requires manufacturers to adopt sustainable packaging.

3. **Extended producer responsibility programs:** these have expanded significantly worldwide. These programs assign responsibility for managing end-of-life products to manufacturers. They require companies to consider their products' fate after obsolescence. In the US, since 2004, 25 states and the District of Columbia have implemented electronics recycling laws.[5] The EU's Waste Electrical and Electronic Equipment (WEEE) Directive (2005) is anticipated for amendment in 2025. It is likely to have revisions relating to Li-ion battery disposal and rare earth minerals recycling, affecting supply chain practices and systems.

Increasing artificial intelligence concerns

The rapid rise of AI in daily life has been accompanied by greater concern about its associated risks. These include its application in creating disinformation, invading privacy, threatening security, reinforcing bias, and IP infringements. A survey of 120 chief product officers identified human oversight of AI for control and credibility as a key to success.[6]

The European Union, United States, and other entities are drafting corresponding regulations. In its AI Act, the EU has taken a risk-based approach, addressing the development, deployment, and use of AI, along with ethical and transparency considerations. Once finalized, provisions of this act could apply as soon as the end of 2024.

Consequently, connected product developers will need to define their approach to classifying generative AI risks to ensure non-discrimination, transparency, explainability, data protection and privacy, and ongoing human oversight.

A wide regulatory landscape

Different industries have their respective regulatory domains, such as automotive, medical devices in life sciences, aviation, or consumer products. Regulations for privacy, cybersecurity and the environment can span all these industry-specific domains. At a high level, these regulations can be split into five pillars:

- **Mechanical:** physical aspects, such as materials, safety, and physical operation procedures
- **Electrical:** electrical safety and conformity compliance
- **Radio frequency:** electromagnetic and wireless compatibility aspects
- **Digital:** data, software, and infrastructure technologies related to privacy, cybersecurity, and artificial intelligence
- **Sustainability:** covering energy, material, waste management, and environmental protection

As an example of regulations affecting connected consumer products, Figure 2 depicts how regulations within each of the five pillars could affect a connected product. This may include medical, artificial intelligence, and credit card processing, should they be in scope. For instance, a smartwatch with electrocardiogram functionality, classified as a Class II device and equipped with an AI anomaly detection model, would be subject to medical and AI regulations.

[5] NCSL, Extended Producer Responsibility, October 24, 2023
[6] CPO Insights, "2023 CPO Insights Report #2: Into the AI Era", October 18, 2023

How regulations affect a consumer connected product

(Regulations in gray apply, dependent on product features)

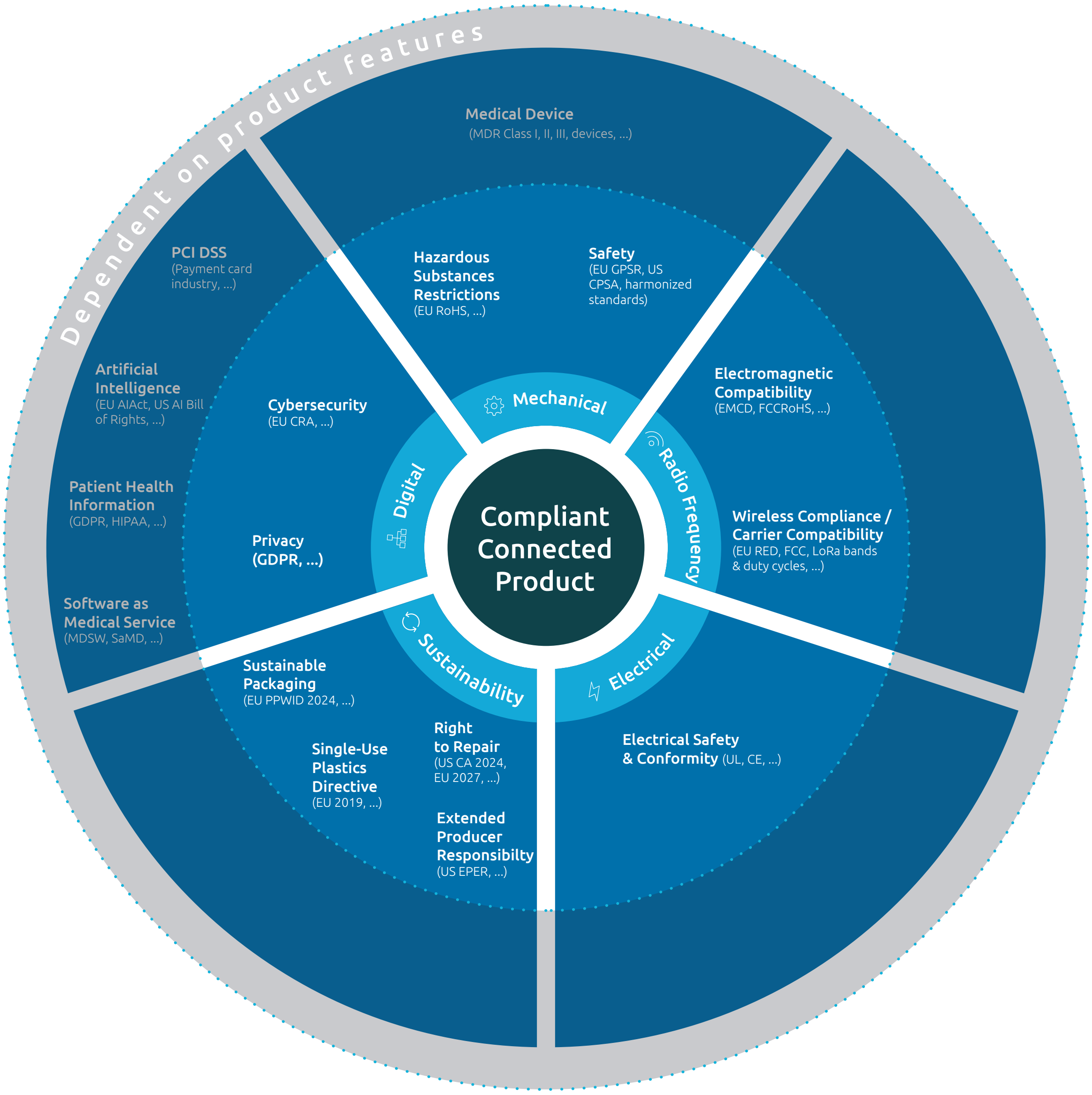

Dependent on product features
Medical Device
(MDR Class I, II, III, devices, ...)
PCI DSS
(Payment card industry, ...)
Artificial Intelligence
(EU AIAct, US AI Bill of Rights, ...)
Patient Health Information
(GDPR, HIPAA, ...)
Software as Medical Service
(MDSW, SaMD, ...)
Hazardous Substances Restrictions
(EU RoHS, ...)
Safety
(EU GPSR, US CPSA, harmonized standards)
Electromagnetic Compatibility
(EMCD, FCCRoHS, ...)
Wireless Compliance / Carrier Compatibility
(EU RED, FCC, LoRa bands & duty cycles, ...)
Cybersecurity
(EU CRA, ...)
Privacy
(GDPR, ...)
Sustainable Packaging
(EU PPWID 2024, ...)
Single-Use Plastics Directive
(EU 2019, ...)
Right to Repair
(US CA 2024, EU 2027, ...)
Extended Producer Responsibilty
(US EPER, ...)
Electrical Safety & Conformity (UL, CE, ...)
Mechanical
Radio Frequency
Electrical
Sustainability
Digital
Compliant Connected Product

Figure 2.
Source: Capgemini

What does this matrix of regulations imply for manufacturers? Failure to comply with any of the pillars risks legal and financial sanctions, potentially jeopardizing its commercial future and viability.

Reactive compliance is a gamble; proactively seizing a compliance advantage is a more far-sighted strategy to set a connected product on its path to commercial success.

Additionally, product features and their corresponding compliance requirements should be aligned with the target market positioning and chosen business and monetization models. Since regulations are continually advancing, this creates an ongoing burden for many connected product developers. This is often better suited as a service outsourced to regulatory specialists.

Geography-specific regulations can also impact product design and operations to varying degrees. For example, long range (LoRa) WAN products use different ISM radio bands with regulations covering transmission power, duty cycle, and channel usage. These differ between Europe, North America, and Asia-Pacific. Similarly, gaining the US FDA's approval, or the EU's CE mark, is essential for legal product marketing and distribution in each of those jurisdictions.

Compliance is typically achieved by aligning with industry standards since most regulations have their origins in standards well-known to engineering teams. However, adherence to an industry standard alone is not sufficient to demonstrate full regulatory compliance of the whole product. For example, the mobile application cybersecurity framework OWASP-MASVS provides a solid foundation for a mobile application component with the EU Cybersecurity Resilience Act, but not for the whole connected product.

Discipline and defined processes on the route to compliance

Compliance is related to regulation and quality management but is a distinct process. For clarification, we define each of these domains as follows:

Regulatory – the function that monitors applicable regulations for new iterations and assesses the regulatory environment of potential new markets to inform regulatory strategies. This involves identifying changes and verifying implementation. It is also a company's primary contact point with the authorities and notified bodies[7] that assess product conformity. Regulatory communication and activities come in the form of audits, submissions, vigilance reporting, and adverse event reporting.

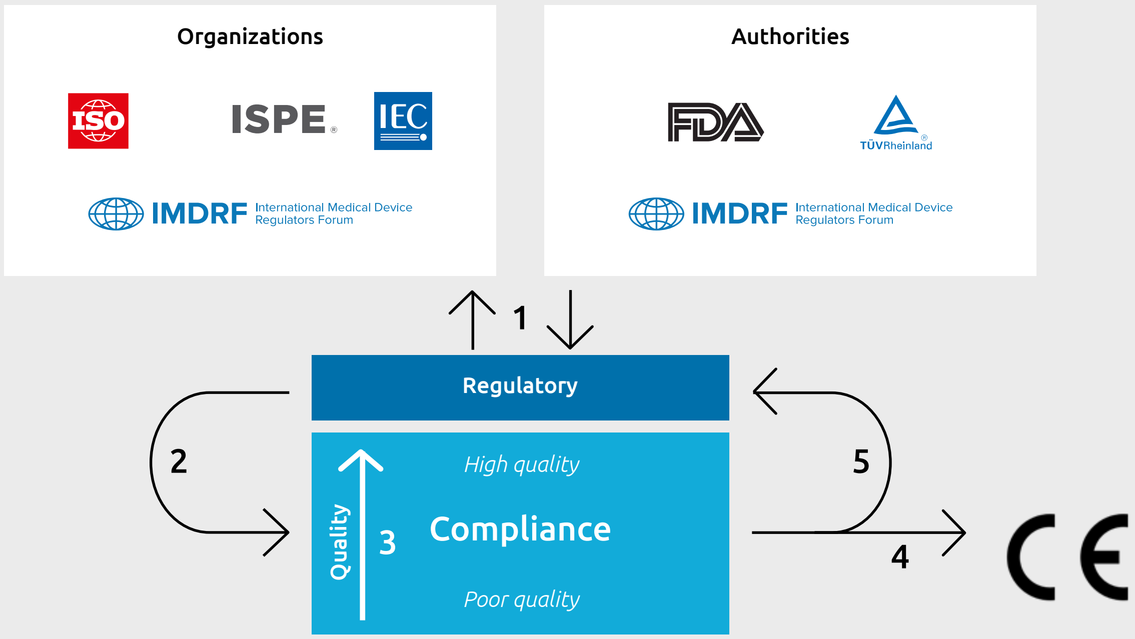
Quality – this is an organization's mindset, expressed through the Quality Management System. To increase quality in an organization requires clear processes across development, manufacturing, testing, and quality assurance. To establish them effectively requires well-defined responsibilities, recurring training, continuous process improvement, consistent handling of defects, monitoring of KPIs, and more.

Compliance – the necessary quality filter level that products need to pass through to achieve compliance with relevant regulations and standards.

Ensuring compliance with relevant regulations and adhering to standards and guidelines is paramount for companies developing connected products. By following quality standards such as ISO 13485, manufacturers guarantee that medical devices undergo rigorous manufacturing, testing, and monitoring processes within established quality management systems.

Regulatory standards not only establish performance benchmarks, but they also safeguard end-users and promote public health. Consequently, a commitment to safety and efficacy fosters trust among medical device manufacturers, regulatory bodies, society, and device users.

[7] European Commission, "An organisation designated by an EU country to assess the conformity of certain products before being placed on the market."



1. **Regulatory domain** - managing regulatory affairs, including communication, reporting requirements, contributing to industry consultations
2. **Compliance domain:** processing the output of regulation
3. **An organization's quality**, set by its QMS, is a contributor to its standard of compliance
4. **Quality and Compliance** lead to product approval, continuously overseen by Regulatory

The rewards of trust and cost of non-compliance

Trust is difficult to earn and easy to break. According to the Harvard Business Review, 88% of customers say they're more likely to buy from a trusted brand again, and 62% will buy almost exclusively from that brand.[8]

A stark example of how trust can be lost was that of a large American pharma company, to which the FDA sent a Form 483 observation. This notified management of objectionable conditions in one of its medical device products. Since no specific person felt responsible to act, the company provided an inadequate response, which resulted in escalation to an FDA warning letter. Resolving the warning caused the effective blocking of all new product development while resources were switched to remediate the findings. This process led to direct costs of $10 million in unplanned work, damage to the company's reputation for quality, and delays to several new product launches.

Any lack of customer confidence in a product often leads to low levels of satisfaction and reduced customer adoption, causing loss of revenue. A Capgemini Research Institute consumer survey found that only 42% of respondents were satisfied with connected products' cybersecurity; 62% had privacy concerns.[9]

A device's physical safety is also a major concern. This becomes abundantly clear when product recall is necessary. An extreme example was that of a global electronics manufacturer forced to withdraw 2.5 million cell phones because of batteries at risk of explosion. It incurred a cost estimated to be billions of dollars.[10]

Financial penalties for non-compliance are also a powerful motivator, especially with the possibility of cumulative fines. In the European Union, GDPR data privacy penalties can be up to €20 million or 4% of global turnover.[11] In the imminent Cyber Resilience Act (CRA), penalties are set for up to €15 million or 2.5% of global turnover. Additionally, the EU's AI Act includes penalties of €35 million or 7% of global turnover. Hence, a negligent approach to a connected product's digital compliance could add up to €70 million or 13.5% of global turnover. Along with formal financial penalties, there are potential costs of re-complying and reputational damage – enough to make many executives seriously reconsider their approach.

[8] Ashley Reichheld and Amelia Dunlop, "4 Questions to Measure — and Boost — Customer Trust", Harvard Business Review, November 1, 2022

[9] Capgemini Research Institute, Connected Products survey, November 2023

[10] "Samsung to Recall 2.5 Million Galaxy Note 7s Over Battery Fires", The New York Times, September 2, 2016

[11] "Europe, a laggard in AI, seizes the lead in its regulation", The Economist, December 10, 2023

Smoothing the path to compliance

Building compliant connected products requires proactive planning and foresight – as does quality. The process must begin at the initial product definition and design stages, encompassing all the pillars identified above. Considering a two-to three–year development timeframe, an integrated, forward-looking compliance strategy that anticipates regulations is a prerequisite for later success.

This is where *compliance by design* comes in. By involving skilled personnel, defined processes, and the right tools, organizations can establish the optimal approach for connected product compliance. This frees them to focus on innovation, rather than regulatory hurdles. Capgemini can help companies navigate the ever-evolving regulatory landscape through each compliance step, allowing them to efficiently unlock connected products full potential and value. Capgemini has the expertise and experience to define comprehensive compliance approaches for connected products across many industries, resulting in customer trust and profitable outcomes.

Contact our experts

Paul Ganichot
Principal IoT Architect
paul.ganichot@capgemini.com

Mark Hersey
Solution Director & Business Development Lead Life Sciences
mark.hersey@capgemini.com

Teja Chatty
Managing Consultant - Sustainability Engineering
teja.chatty@synapse.com

Brian Piquette
Director of Electrical Engineering, Synapse
brian@synapse.com

Ola Olsson
Solution Manager
ola.olsson@capgemini.com

Ian Carvalho
CTO Intelligent Devices
ian.carvalho@capgemini.com

About Capgemini

Capgemini is a global business and technology transformation partner, helping organizations to accelerate their dual transition to a digital and sustainable world, while creating tangible impact for enterprises and society. It is a responsible and diverse group of 340,000 team members in more than 50 countries. With its strong over 55-year heritage, Capgemini is trusted by its clients to unlock the value of technology to address the entire breadth of their business needs. It delivers end-to-end services and solutions leveraging strengths from strategy and design to engineering, all fueled by its market leading capabilities in AI, cloud and data, combined with its deep industry expertise and partner ecosystem. The Group reported 2023 global revenues of €22.5 billion.

Get the future you want | www.capgemini.com

MACS 3690_04-2024