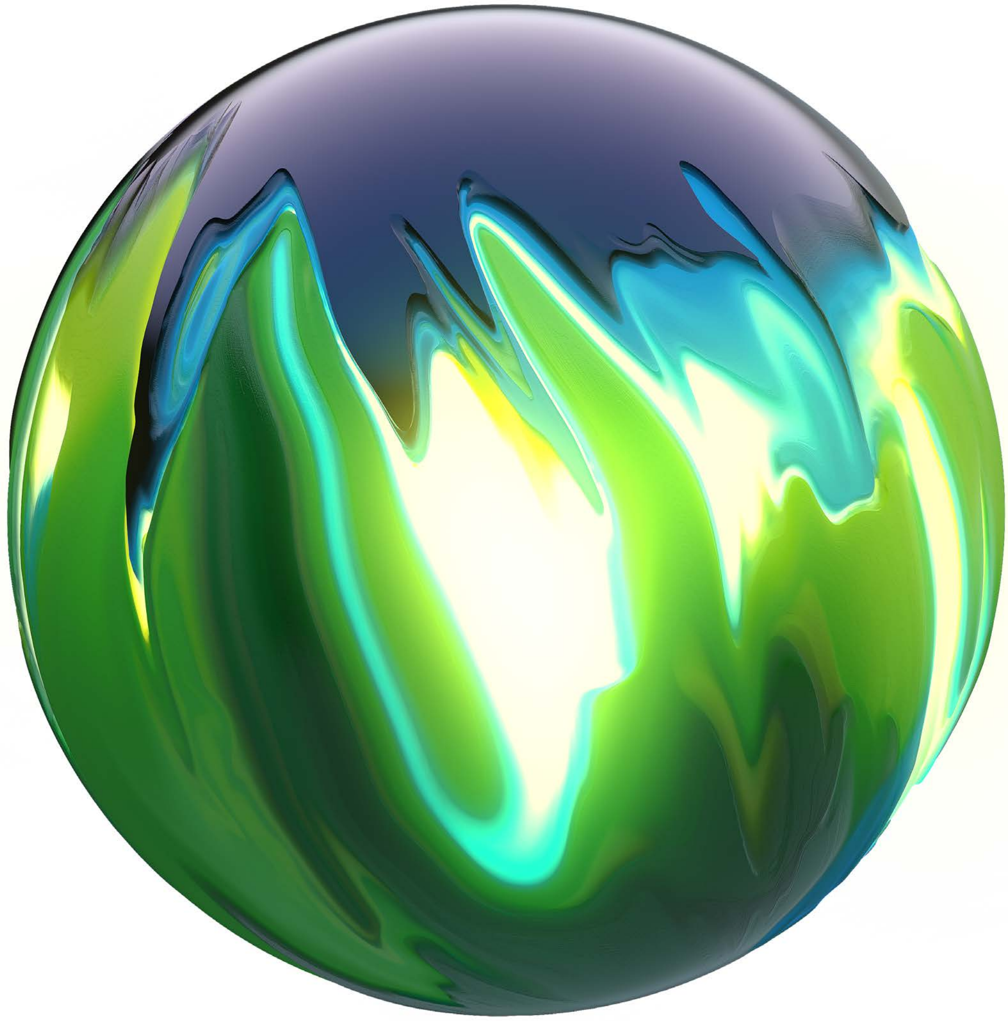
Deloitte.



Cybersecurity@Scale
IoT and Healthcare Cybersecurity Services

A smart, affordable way to strengthen cybersecurity for your medical devices
In the medical device market, growing security concerns add to the challenges of complex medical ecosystems and a stricter regulatory framework. Having better cybersecurity infrastructure reduces business risk and opens the door to additional services as well as use cases. Deloitte is here to support you on your journey. We provide all of the resources and tools you need to strengthen your cybersecurity infrastructure and keep up with the threats of tomorrow.

MAKING AN IMPACT THAT MATTERS since 1845

Today's healthcare market

The demand for smart, connected medical devices is growing in modern healthcare, with new product launches often featuring connectivity to the internet, hospital networks and/or other medical devices. There are a host of new use cases emerging around sharing patient or machine data, while central data storage has opened a window of opportunity for healthcare professionals with new services and new treatments.

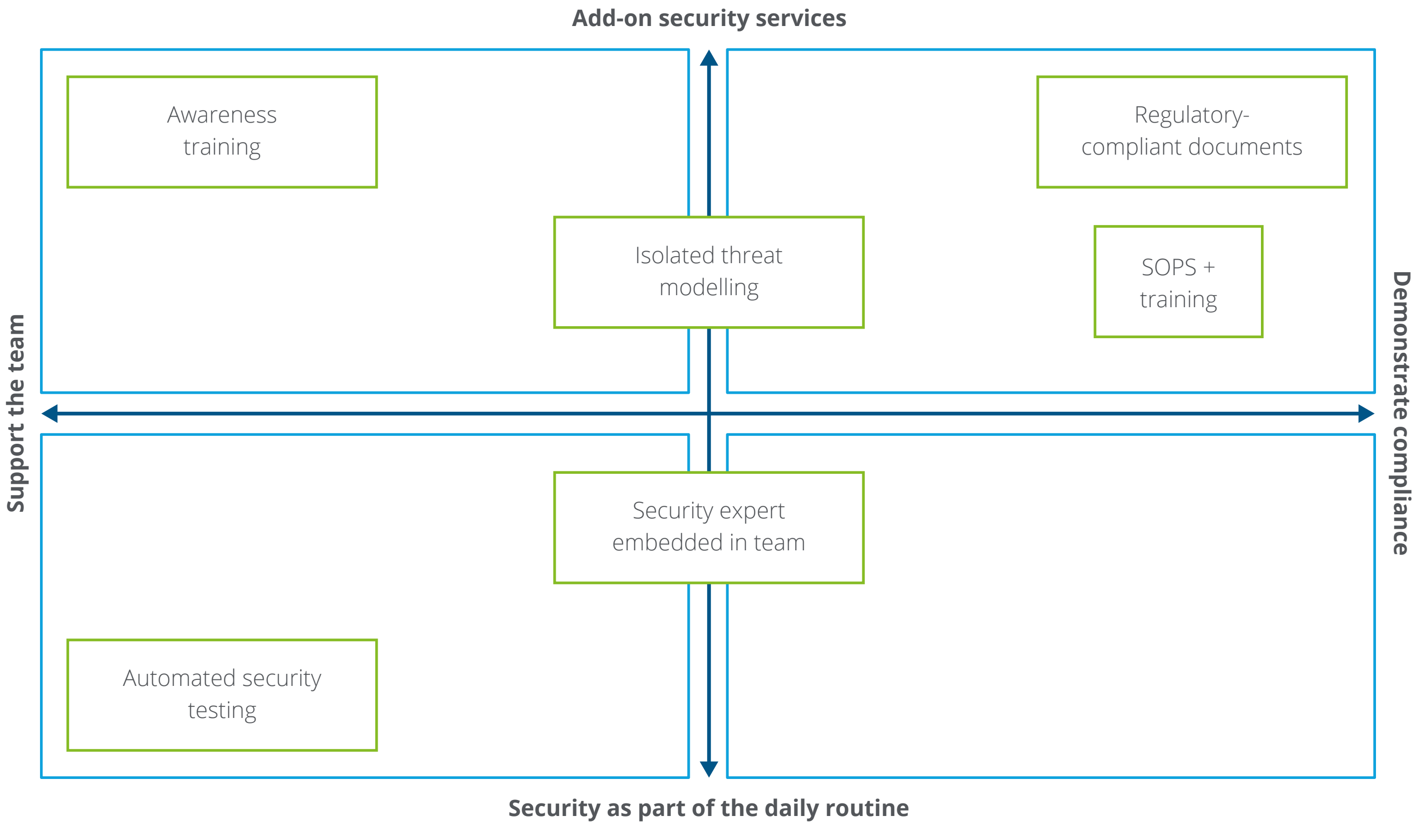
Unfortunately, these same features also introduce risk. Medical devices, like other computer systems, can be vulnerable to security breaches, potentially impacting the safety and effectiveness of the underlying device.

How to strengthen cybersecurity

Over the past few years, we have heard many media reports about hospitals being hacked – with malicious actors targeting the IT infrastructure – but also about medical devices being vulnerable to attack. Regulatory bodies worldwide have responded to these risks by issuing new, stricter and more detailed regulations along with better enforcement of the rules. Hospitals have identified their cybersecurity needs and started adding security specifications to tenders and purchase orders. We have also seen engineers make cybersecurity a key part of the product development process.

Now it is up to medical device manufacturers to find their sweet spot between meeting the bare regulatory minimum and adopting a high-end, integrated approach to cybersecurity. They need to decide whether to focus on adding cybersecurity-related compliance tasks to existing product development lifecycles or to move to a new, state-of-the-art, more automated approach designed to appeal not only to regulators but also to their own engineers. In the end, the choice facing senior management is whether to pursue the regulatory route on its own or strengthen their engineering teams with modern security development practices and tools as well.

Fig. 1 – Map of exemplary services

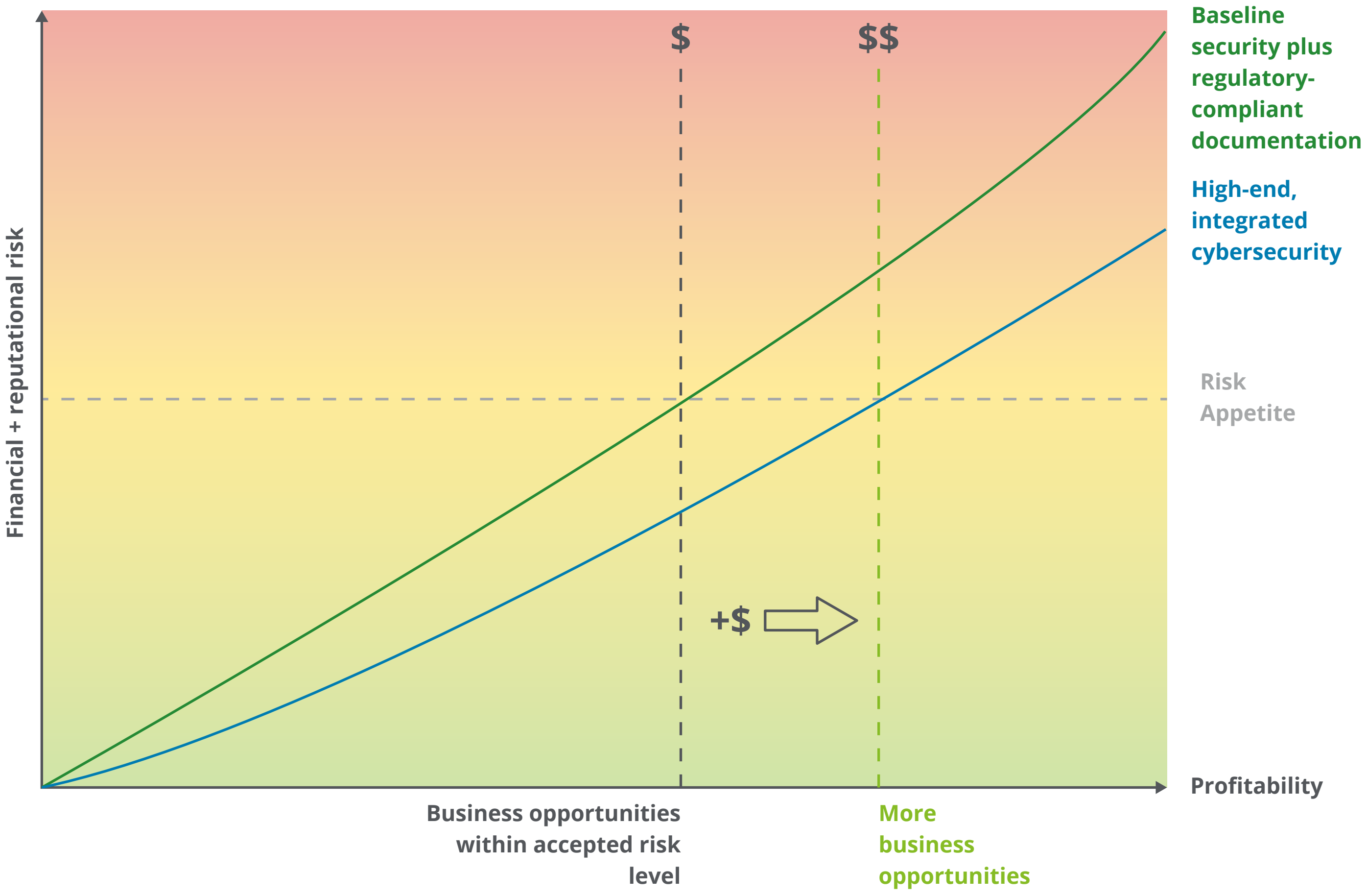

Add-on security services
Awareness training
Regulatory-compliant documents
Isolated threat modelling
SOPS + training
Support the team
Demonstrate compliance
Security expert embedded in team
Automated security testing
Security as part of the daily routine

Why more cybersecurity pays off

Meeting the pure regulatory minimum may sound attractive at first. After all, it allows for low-cost outsourcing (e.g., to "pentest factories"), helps you better manage the cybersecurity talent shortage on the German market and can simply be added to existing development lifecycles. Plus, you can still guarantee secure development and sufficient documentation.

If you opt for a high-end integrated security focus instead, your cybersecurity processes will be seamlessly integrated into the product development process, your engineers will benefit from more security guidance and your security-related tasks will be automated. As a result, the PDLC becomes a lot more agile, the overall medical ecosystem has better connectivity and your business is fit for the future.

Fig. 2 – Business benefit of sound cybersecurity



How to implement high-end security at scale

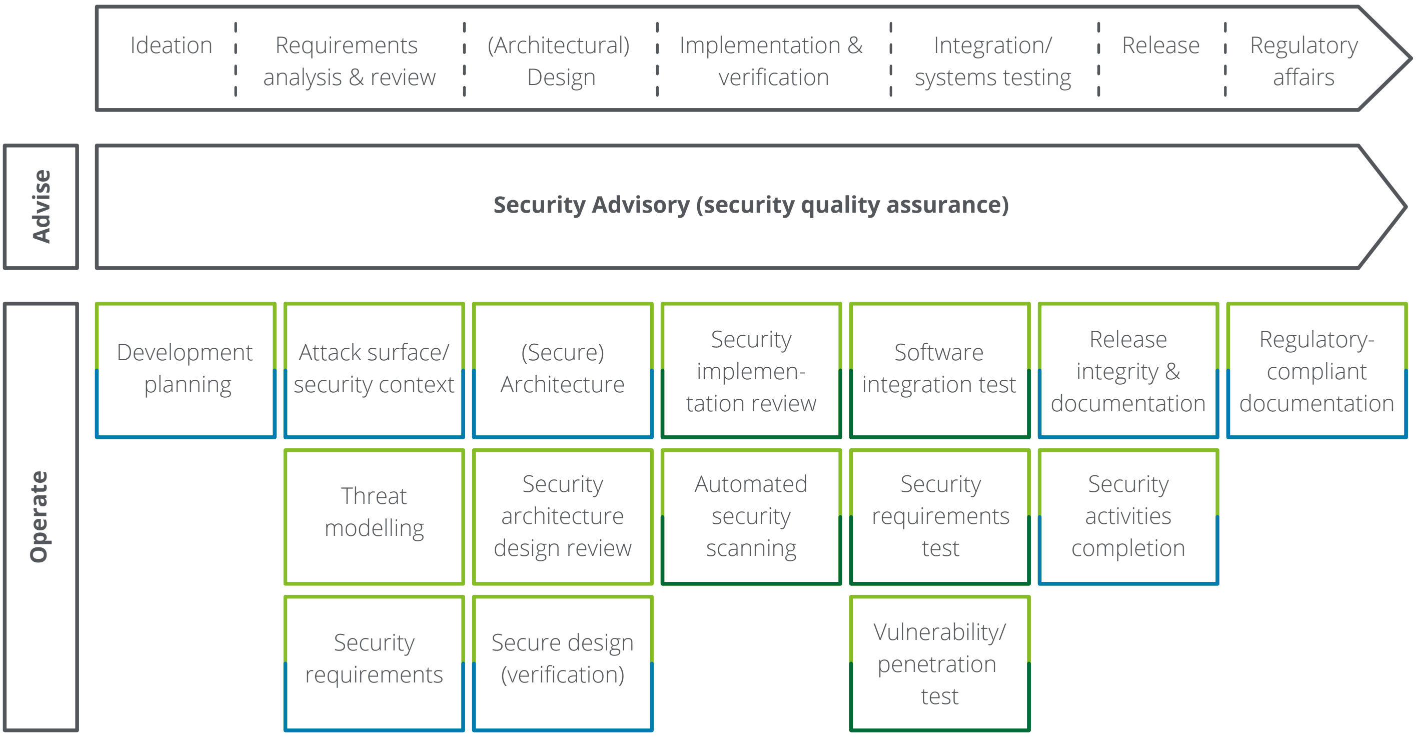
Deloitte offers a large variety of both on-site and near-shore services in cybersecurity. While you can obtain some of these services as isolated add-ons (including the formal documentation required by your Quality Management System), we also offer an end-to-end Security Advisory Service that guides your engineering teams from the very beginning of product development through the maintenance phase. Our security advisors oversee the entire development process, taking on threat modelling and other critical tasks as well as acting as a sparring partner for your project manager, requirements engineer or test manager. For co-located teams, we can offer this either as an on-site or as a semi-virtual service.

The diagram below provides an example of how our on-site security advisors share responsibility with the engineering teams from Deloitte's Cybersecurity Centers and your engineers and cybersecurity experts.

This solution leverages Deloitte's expertise to address any knowledge gaps as well as the high scalable services at our near-shore service centers. You may opt for a straightforward regulatory baseline designed to get your medical device ready for market launch, or we can provide the support you need to achieve state-of-the-art, integrated cybersecurity for your development processes, tools and the product itself.

Whatever you decide, we will adapt to your strategy and deliver the high-end security services you need for your medical devices or healthcare applications. Get in touch with us to find out more.

Fig. 3 – Exemplary cybersecurity services along the life cycle



	Ideation	Requirements analysis & review	(Architectural) Design	Implementation & verification	Integration/ systems testing	Release	Regulatory affairs
Advise	**Security Advisory (security quality assurance)**						
Operate	Development planning	Attack surface/ security context	(Secure) Architecture	Security implemen-tation review	Software integration test	Release integrity & documentation	Regulatory-compliant documentation
		Threat modelling	Security architecture design review	Automated security scanning	Security requirements test	Security activities completion	
		Security requirements	Secure design (verification)		Vulnerability/ penetration test		

🟩 Performed by Deloitte Security Advisor on request
🟦 We recommend keeping this in-house with the client engineering team
■ Performed by the Deloitte Security Center as a near-shore service or by the client

Contacts

Ingo Dassow
Partner
Global Automotive Cyber Lead
Tel: +49 30 2546 8451
idassow@deloitte.de

Carsten Heil
Director
Risk Advisory
Tel: +49 69 75695 7339
cheil@deloitte.de

More information about Engineering Excellence can be found here:
https://www2.deloitte.com/de/de/pages/risk/articles/engineering-excellence-medtech.html

Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities (collectively, the "Deloitte organization"). DTTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/de/UeberUns to learn more.

Deloitte provides industry-leading audit and assurance, tax and legal, consulting, financial advisory, and risk advisory services to nearly 90% of the Fortune Global 500® and thousands of private companies. Legal advisory services in Germany are provided by Deloitte Legal. Our professionals deliver measurable and lasting results that help reinforce public trust in capital markets, enable clients to transform and thrive, and lead the way toward a stronger economy, a more equitable society and a sustainable world. Building on its 175-plus year history, Deloitte spans more than 150 countries and territories. Learn how Deloitte's approximately 415,000 people worldwide make an impact that matters at www.deloitte.com/de.

This communication contains general information only, and none of Deloitte GmbH Wirtschaftsprüfungsgesellschaft or Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms or their related entities (collectively, the "Deloitte organization") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.

Issue 12/2022