www.pwc.de

Cyber Managed Services in practice

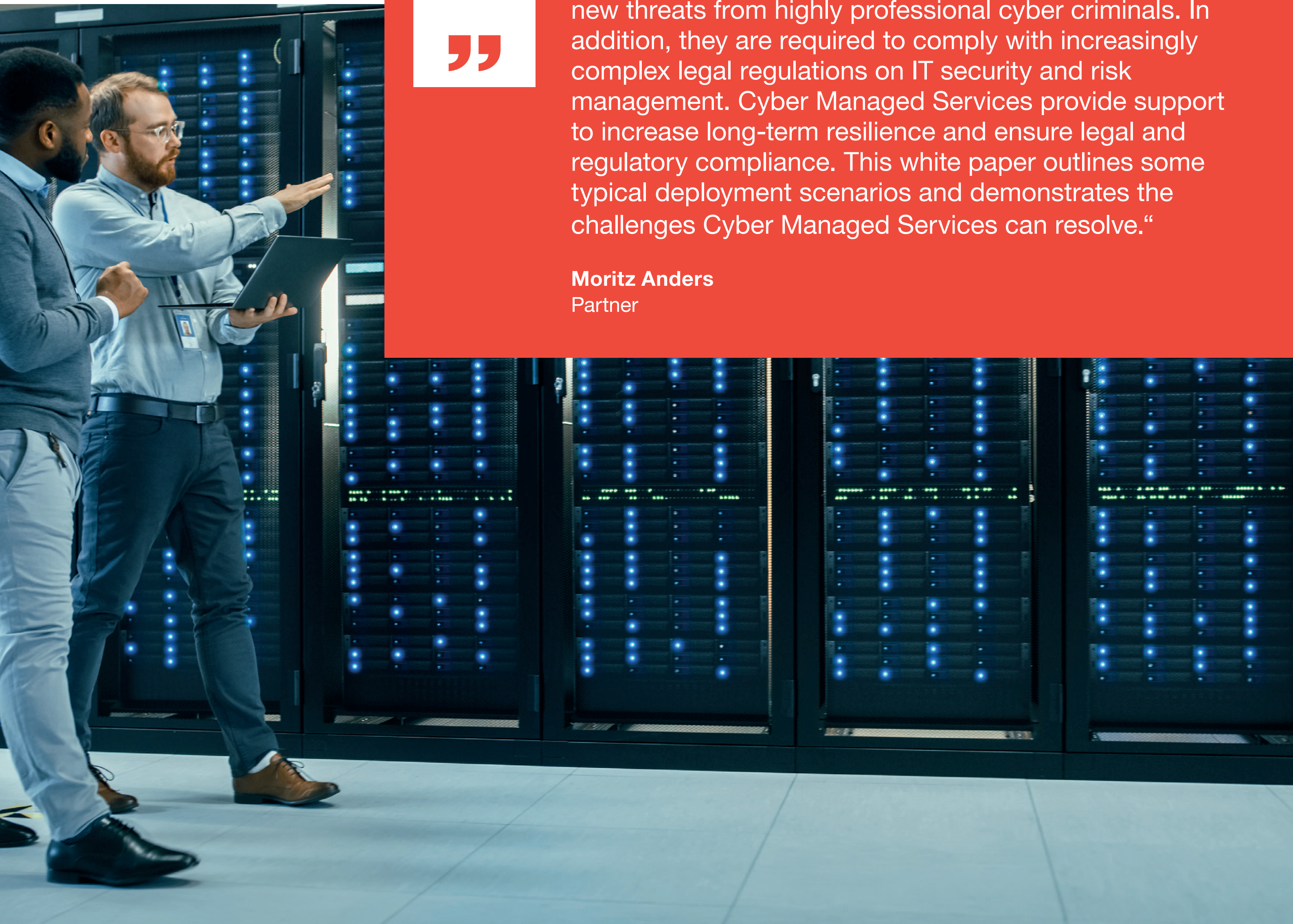
How and when organisations benefit from managed IT security

pwc

Contents

„Companies are constantly facing challenges caused by new threats from highly professional cyber criminals. In addition, they are required to comply with increasingly complex legal regulations on IT security and risk management. Cyber Managed Services provide support to increase long-term resilience and ensure legal and regulatory compliance. This white paper outlines some typical deployment scenarios and demonstrates the challenges Cyber Managed Services can resolve.“

Moritz Anders
Partner



Introduction

Ongoing digital transformation is impacting and reshaping more and more areas of our lives. This transformation is enabling companies to innovate with their products and services. It is also enabling them to make processes more efficient, whether through networked devices on the growing Internet of Things or new ways of managing information. This can also involve content enabled by evolving generative AI.
However, digital transformation is also opening new possibilities for cybercriminal groups. Without adequate IT security, it's not just the digital dividend that will hang in the balance. Successful cyberattacks can disrupt your operations, cause immense costs, and damage your company's reputation. Ultimately, these attacks can threaten your company's very existence.

Digital transformation and IT security need to go hand in hand

According to a report on the state of IT security in Germany in 2023 by the German Federal Office for Information Security (BSI), the threat level in cyberspace is higher today than ever before.
The number of vulnerabilities registered daily in software products during the report's observation period increased by 24% compared to the previous year. An average of 250,000 new malware variants are discovered every day.

In addition to the ongoing danger of ransomware attacks, the situation is also rapidly escalating due to geopolitical conflicts. Russian 'hacktivism' attacks and cyber espionage have long been commonplace in Germany. It's understandable why 89% of decision-makers identify resilience as a strategic priority, according to PwC's Global Crisis and Resilience Survey 2023.

Stricter regulations are ratcheting up the pressure for compliance

The fact that the threat situation has been worsening over the years has not gone unnoticed by governments. Companies are facing increasingly stricter requirements, with heavy fines for non-compliance breaches. These regulations include data protection provisions and cross-industry rules such as the NIS2 Directive, which is intended to increase the overall level of cybersecurity in the EU. There are also industry-specific requirements such as the Digital Operational Resilience Act (DORA), which establishes new cybersecurity regulations for the financial sector.

Cyber Managed Services allow you to outsource certain security functions

To adequately address the increased demands made on cybersecurity, it's important to professionalise your cyber defence. However, it's not always feasible or sensible to obtain or develop all the necessary resources yourself and handle every task internally. In many cases, outsourcing certain functions is cost-effective, safer, and provides more reliable protection.

Collaboration with service providers is becoming increasingly important, which is where the managed services model comes in. In this model, a Managed Services Provider (MSP) takes over selected security functions or processes.

Key questions to consider include: Which use cases is this model particularly suitable for? What does the collaboration between you and the MSP look like in practice? What are the advantages of outsourcing? The following chapters provide answers to these questions and offer insights into specific deployment scenarios.

What are Cyber Managed Services?

Cyber Managed Services customise the Managed Services framework to address specific needs in IT security. A Managed Services Provider (MSP) assumes responsibility for security-related functions or processes within a company – whether it's identity and access management, risk assessment, or detecting and responding to threats.

PwC relies on combining current technologies and interdisciplinary expertise. Going beyond simply running contracted tasks to continuously improve performance is a core tenet of this approach.

A Rebuilding IT after restructuring – asset management organisation sets up IT organisation faster

The use case at a glance

Initial situation:

- New IT departments and capabilities had to be created and implemented for a new subsidiary of a financial service provider, which had more than 3,000 employees.

Challenges:

- Tight time constraints for a seamless, uninterrupted transition to operations.
- Providing security in a dynamic threat landscape.
- Ensuring compliance with complex financial industry regulations.
- Limited resources and expertise for sustainable operations.

Implemented Cyber Managed Services:

- Digital Identity
- Cyber Defence
- Cyber Risk

Benefits:

- Supporting the resolution of audit findings.
- Proactively assuring operational resilience and compliance.
- Enhanced resilience thanks to highly qualified cyber experts and strategic alliances.
- Standardised and efficient approach thanks to the use of best practices and exploring automation potential.

Developing essential new IT services and capabilities. This decision ultimately had a knock-on effect on IT operations which impacted 3,000 employees.

Establishing a new IT services / organisation under time constraints

Establishing new IT services of this size usually takes one to three years, but these systems had to be operational in a matter of months.
Although it is sometimes possible to use certain organisational aspects of the parent organisation as a model, in practice they often provide little more than a few ideas. Implementation can be complex for the new department(s), ranging from drafting a data governance and data protection policy to configuring access controls.

In this specific case, the operations were made even difficult as the organisation had to comply with strict financial industry regulations. These include requirements imposed by the German Federal Financial Supervisory Authority (BaFin), such as the Banking Supervisory Requirements for IT (BAIT) and Minimum Requirements for Risk Management (MaRisk), as well as European Banking Authority (EBA) regulations. Additionally, the new regulation "DORA" added further challenges.

Outsourcing cybersecurity tasks with three Managed Services

It quickly became apparent that the organisation would be unable to ensure adequate security on its own. Finding appropriate security specialists in such a short time would be almost impossible. At the same time, however, the organisation did not want to give up all control over the operations.

A balance was agreed upon. The organisation would operate the essential infrastructure itself but would use three Managed Services from PwC to ensure security and compliance. The Digital Identity service covers identity and access management (IAM) and privileged access management (PAM) – essential components for an organisation's cybersecurity strategy. The former manages access for normal users and their daily activities. The latter regulates privileged accounts which administer sensitive systems and data.

Cyber Defence monitors potential incidents, analyses vulnerabilities and takes appropriate countermeasures to strengthen cyber defence. Cyber Risk helps to continuously analyse and mitigate cyber threats and associated risks.

The Managed Services were introduced gradually. One major challenge was that the underlying environments were at different stages of the organisation. Some had already been fully implemented, while others were still under construction. The various efforts between the client and the MSP required careful coordination and close collaboration between the client teams and PwC teams, ultimately ensuring smooth operations.

Protected against cyberattacks and better positioned for audits

After the successful handover, PwC assumed full responsibility for running the contracted functions. In addition to handling operations, continuous consulting was provided at a strategic and tactical level. For example, continuous monitoring verifies whether best practices are in place and utilised.

Processes are continuously developed in close coordination with the client to effectively support the prevention of cyberattacks, increasing operational resilience while supporting the compliance of the requirements – against the backdrop of constant changes to the threat situation and legislation. The organisation now benefits from round-the-clock security service without the need to set up its own team to create an equivalent in-house security operations centre.

Our assessment of this deployment scenario

IT faces huge challenges during restructuring. Confusion is at times inevitable, especially during transition periods, and this is precisely what hackers love and deliberately exploit. When resources are limited and deadlines are tight, Cyber Managed Services offer solutions. They help to minimise cyber risks, support the resilience of the new organisation and ensure regulatory compliance.

The operations of the services can vary greatly. In this case, the client is responsible for the infrastructure, which is more typical for large companies. In medium-sized companies, it is often advisable to outsource the infrastructure if operations cannot be guaranteed using the company’s own resources. Different requirements can be mapped using individual service contracts with clearly defined service level agreements (SLAs) and key performance indicators (KPIs).

B Professionalising IT security – engineering company recovered hacked IT environment

The use case at a glance

Initial situation:

- A ransomware attack forced an engineering company to shut down its IT infrastructure.
- Legacy systems in a heterogeneous global IT landscape meant that the IT environment could not be recovered within a reasonable timeframe.
- The IT infrastructure needed to be restored gradually, with appropriate security measures and controls in place.
- Rapid restoration of the IT environment was business critical.

Challenges:

- Further cyber incidents needed to be effectively prevented.
- Limited in-house IT resources.
- No asset management – there was no configuration management database.

Implemented Cyber Managed Services:

- Cyber Defence

Benefits:

- 24/7 monitoring by the security operations centre during and after restoration of the attacked environment.
- Analysing security alerts and identifying potential incidents.
- 100% automated triage with integrated threat analysis to ensure rapid response.
- Recommendations for improvements in cyber hygiene.

The IT department of a medium-sized international engineering company realised that a ransomware Trojan had infiltrated the company's systems. They shut down the company's entire IT landscape just in time to prevent the systems from being encrypted and to stop the leak of sensitive data.

Nevertheless, the entire network was down, which had a significant impact on operations. Production was restricted, and employees resorted to using pen and paper, limiting their ability to carry out day-to-day business or operational activities. All communication had to be conducted through alternative means.

Step-by-step recovery together with PwC

It was initially assumed that a completely new build-out would be needed to provide an operational and secure IT landscape. It was not known which parts of the network had been compromised, and it was also unclear whether the backups contained affected data. However, when it was realised that a new-build would take months and that some legacy systems could not be re-started, a new plan was formulated.

In collaboration with PwC's Incident Response Team, an approach was developed that enabled individual systems to be restarted and checked, step-by-step. The IT landscape was restarted so that the individual systems could be systematically analysed and quarantined if problems or threats were identified.

A security solutions agent was installed on the endpoints to enable the monitoring of systems within the network environment. The data was collected (read-only) in a central software solution and evaluated through specific rules to identify anomalies.

Security operations centre with 24/7 monitoring

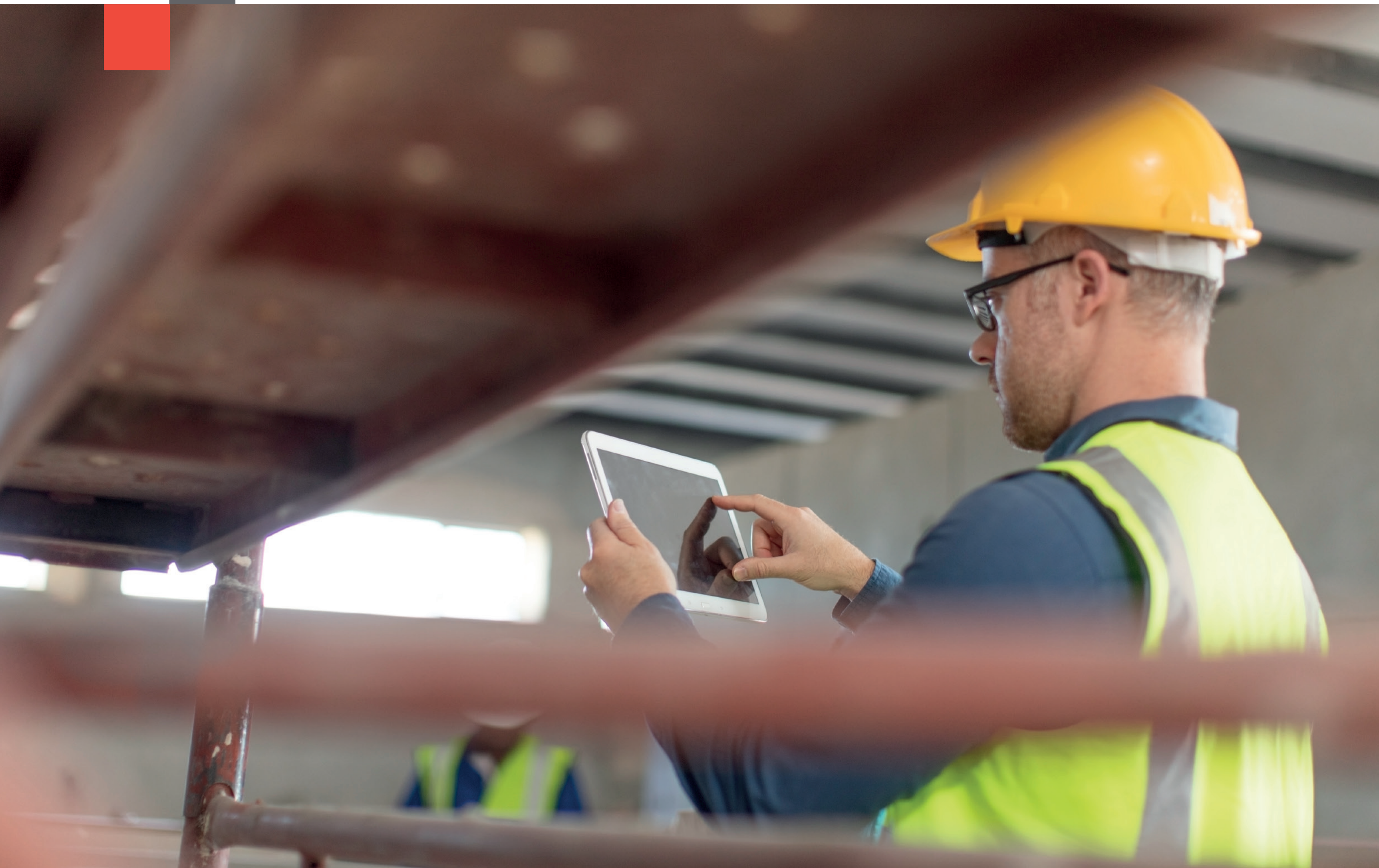
The company chose PwC's Cyber Defence Managed Services to enable IT security monitoring during the recovery phase and beyond. A security operations centre (SOC) staffed around the clock has been continuously monitoring the environment ever since the recovery stage. Between three and five hundred alerts are triggered every week, and these alerts are then analysed and classified according to their criticality. If action is required, the company is notified by the SOC immediately, as operational measures can only be conducted by the company.

During the recovery and continuous monitoring, it became apparent that the company had not implemented important security solutions. For example, there was a lack of asset management, with no systematic overview of which devices and systems were in use (asset lifecycle) within the company. This resulted in an urgent need for coordination and action, but it also presented an opportunity for the company to close the identified gaps and improve its security posture.

Our assessment of this deployment scenario

Even with the best security precautions, the risk of a cyber incident cannot be 100% ruled out but the impact can be minimised. In practice, however, incidents are often the result of oversights – whether due to incorrect configurations, outdated software, or a lack of security solutions. Hackers typically take the path of least resistance. Cybercriminal groups are highly professional, making it increasingly difficult, particularly for medium-sized companies, to protect themselves adequately.

Managed Services offer opportunities and advantages to strengthen cyber defences. To reduce the risks, this should ideally happen before an incident. However, external support is also highly beneficial in the aftermath of an incident when setting up a new security organisation. Managed Services offer companies a cost-effective path to more mature security precautions without having to set up an in-house security operations centre.



C Compliance with regulations – insurance group addresses DORA compliance

The use case at a glance

Initial situation:

- An insurance group comes under the scope of the EU's Digital Operational Resilience Act (DORA).
- This required the implementation of new cybersecurity and operational resilience measures.

Challenges:

- Internal teams were tied up with important digital transformation projects without specific regulatory focus.
- The group lacked the expertise to securely implement and test the measures mandated by DORA.
- Time constraints – ensuring compliance prior to the set effective date of the regulation.

Implemented Cyber Managed Services:

- Cyber Defence
- Cyber Risk

Benefits:

- Taking pressure off the internal IT organisation, allowing it to focus on strategic digital projects.
- Clearly documented and audit-compliant processes to support DORA compliance.
- Demonstrable compliance with regulations to prevent the imposition of penalties.
- Best practices for increased resilience and protection against cyberattacks.

New legal requirements rarely come as a surprise. Anyone following the regulatory process can anticipate new developments at an early stage. Nevertheless, a lack of resources can prevent the necessary measures from being implemented effectively before a regulation comes into force. This is exactly what happened to an insurance group regarding the DORA financial regulation.

DORA tightens requirements for cybersecurity and operational resilience

The Digital Operational Resilience Act is a new legal framework intended to strengthen the operational resilience of the financial sector in the EU. It targets a wide range of organisations in the financial industry and requires them to implement various measures related to cybersecurity and operational resilience to effectively prevent cyberattacks and manage disruptions.

In Germany, more than 3,600 companies must adhere to DORA, including banks, payment service providers, investment firms, trading platforms, insurance and reinsurance companies, credit rating agencies and IT service providers. The DORA policy was adopted by the European Parliament and European Council on December 14, 2022. The regulation came into force on January 17, 2024 and will be applicable from January 17, 2025. In Germany, DORA (also known as Regulation (EU) 2022/2554) is being transposed into national law by the Financial Market Digitalisation Act (FinmadiG).

Analysis of the requirements reveals a need for action

Shortly after DORA came into force, the insurance group formed an internal task force to understand the new requirements and plan how to implement the necessary measures.

The good news was that not all of the requirements were completely new. For example, some risk management requirements were already mandated by BaFin's insurance supervisory requirements for IT (BAiT), so the group's starting point was strong. Nevertheless, numerous additional measures had to be implemented or enhanced – in risk management, handling cyber incidents, and mandatory threat intelligence and reporting.

The IT department was under immense pressure and tied up with important strategic digital transformation projects. Refocusing activities to be compliant with DORA would have led to massive delays and gaps in other operational areas. At the same time, there were limited resources available with the necessary expertise in IT security.

Cyber Managed Services supports compliance with regulations

The insurance group decided to cover the gap in adhering to the requirements set by DORA by engaging external support in the form of PwC's Cyber Risk and Cyber Defence Managed Services. This enabled the implementation of measures to ensure compliance with the regulator. The foundation was the policy level and the operational regulatory implementation of standards, along with guidelines that clarify how DORA should be applied. These guidelines are set by the European Securities and Markets Authority, the European Banking Authority, and the European Insurance and Occupational Pensions Authority.

As a result of PwC's Cyber Managed Services, the insurance group was able to meet its obligations, manage IT incidents, and closely examine the information and communication technologies used. For example, the company receives an overview of incidents as part of the Cyber Defence Service, categorised using the criteria set out in DORA. This allows the company to know exactly which incidents need to be reported to its supervisory authority (e.g. BaFin), enabling it to fulfil its reporting obligations.

Our assessment of this deployment scenario

Many companies still have serious gaps when it comes to implementing cybersecurity and risk management measures required by regulations and even best practices. In many cases, necessary management systems are in place, but the implementation of the actual measures is inadequate. This creates gaps or risks, as the level of security that these measures are intended to ensure is not realised. There are risks of penalties and fines if the authorities judge the company's procedures to be insufficient.

Cyber Managed Services offer opportunities and benefits to ensure that measures are implemented in accordance with regulatory requirements and laws, providing proven operational measures to increase long-term resilience.

How we can help you

PwC is one of the leading cybersecurity consulting firms in Europe. Our extensive portfolio of services in the field also enables us to offer much of our range as Managed Services.

Our Managed Security Services can helb you in achieve your goals more quickly by offering much more than just outsourcing. We bring the skills, expertise, and passion of our professionals to manage your business functions from end to end, working in partnership with you and your teams.

We leverage a network of over 30 technology partners and integrate proven industry-specific solutions. Most importantly, our expertise ensures the seamless integration of your employees and operations with our services, allowing your company to quickly realise the benefits.

All Cyber Managed Services at a glance

Our approach is driven by results and best practices, offering compliance, effective control, and optimised processes.

Managed Digital Identity

These services focus on designing and implementing a governance framework that monitors and manages digital identities within an organisation.

- Identity Governance
- Privileged Access

Managed Cyber Defence

These services will help identify and respond to security data, alerts and incidents through continuous assessment, analytics and automation.

- Threat Detection & Response
- Vulnerability Management
- High-Volume Testing
- Threat Intelligence
- Forensics and Analytics

Managed Cyber Risk

These services focus on identifying, analysing and assessing potential cyber threats and risks.

- Risk Assessment
- Risk Reporting
- Data-Trust-as-a-Service

Managed Cloud Security

Services which help manage risks related to cloud engineering and operations through continual monitoring and remediation.

- Cloud Security Posture
- Cloud Identity Entitlement Management
- Attack Surface Management

Managed Digital Identity

Identity Governance
Designing and implementing a governance framework that oversees and manages digital identities within your organisation.

Privileged Access
Securing, controlling, managing and monitoring privileged access to critical systems, helping your organisation to minimise data breaches and protect sensitive data.

Managed Cyber Defence

Detection & Response
This service manages monitoring, detection, and response – both for potential and ongoing incidents.

Vulnerability Management
Managing vulnerabilities by identifying gaps in security and applying countermeasures.

High-Volume Testing
Assessing and analysing the impact of vulnerabilities.

Forensics & Analytics
Compiling data for forensic analysis and collecting evidence.

Managed Cyber Risk

Risk Assessment
Identifying, analysing, and assessing potential cyber threats and risks.

Risk Reporting
Systematic analysis and provision of essential data for managing and mitigating risks.

Data-Trust-as-a-Service
This service implements various protective measures to ensure that your company's data is secure, reliable, and compliant.

Managed Cloud Security

Cloud Security Posture
Measures such as access controls, data encryption, and network security.

Cloud Identity Entitlement Management
Managing identities and authorisations in cloud environments.

Attack Surface Management
Analysing and reducing your attack surface and the potential impact.

Contact us

Moritz Anders
Partner
Tel.: +49 1515 5455621
moritz.anders@pwc.com

Joshua Khosa
Senior Manager
Tel.: +49 1514 4254179
joshua.khosa@pwc.com

About us

Our clients face diverse challenges, strive to put new ideas into practice and seek expert advice. They turn to us for comprehensive support and practical solutions that deliver maximum value. Whether for global players, family businesses or public institutions, we leverage all of our assets: experience, industry knowledge, high quality standards, a commitment to innovation and the resources of our expert network in 151 countries. Building a trusting and cooperative relationship with our clients is particularly important to us – the better we know and understand our clients' needs, the more effectively we can support them.

PwC Germany. More than 14,000 dedicated people at 20 locations. €2.93 billion in turnover. The leading auditing and consulting firm in Germany.

www.pwc.de