PORTFOLIO

BDO Cyber security

Continuous Security

New
Perspectives

BDO's vision on Cybersecurity

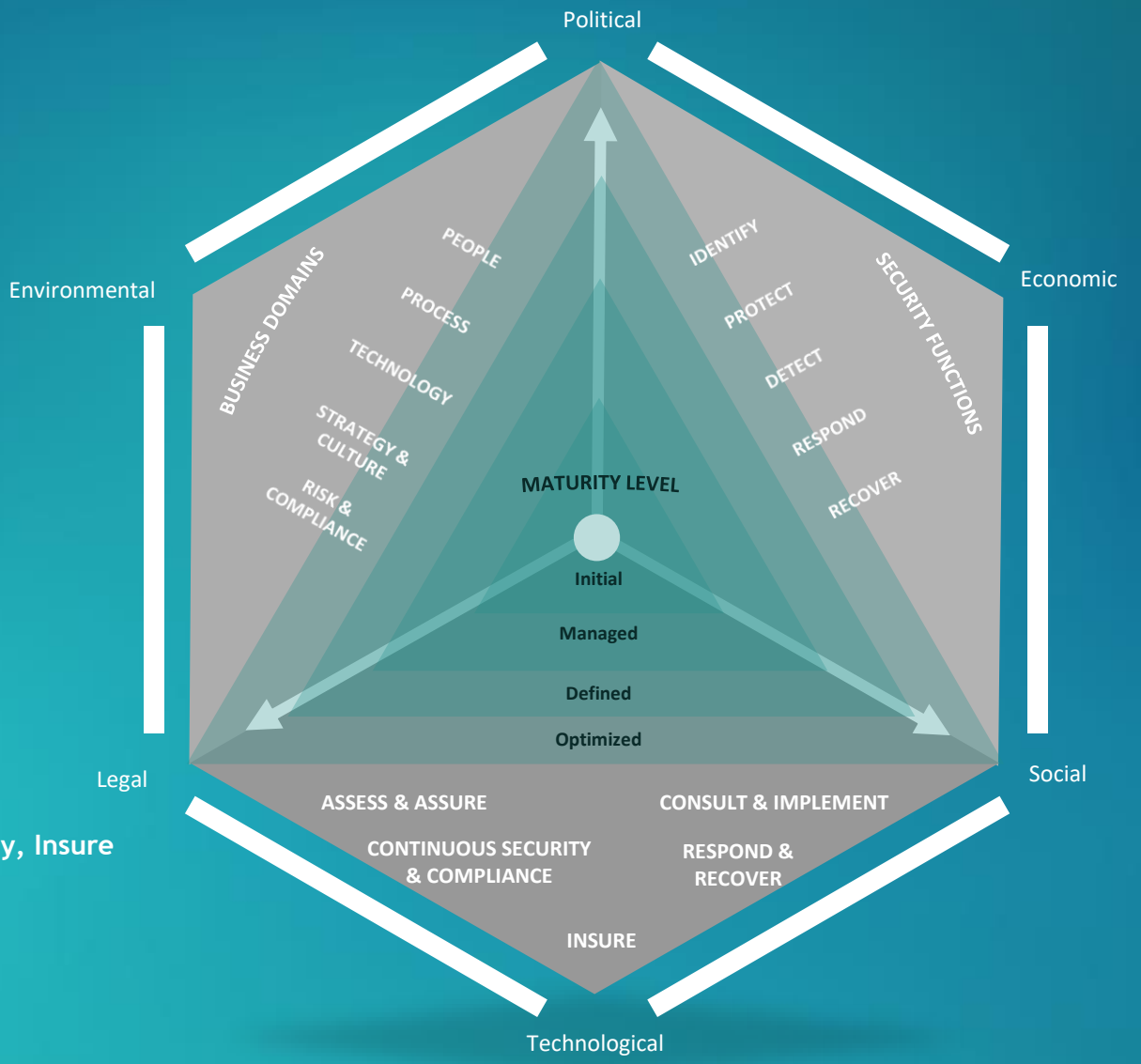
Cybersecurity is a broad domain that touches all elements of the orgamozation and can quickly become large, elusive, and overwhelming. New digital opportunities and threats demand attention, and in BDO's view, above all a pragmatic approach and an efficient set of measures.

BDO, with its company-wide expertise, helps to get information security clear and in order across all domains, especially where the risks have the greatest impact on your business. We call this risk-based. These can be technical risks, but certainly also organizational or compliance risks.

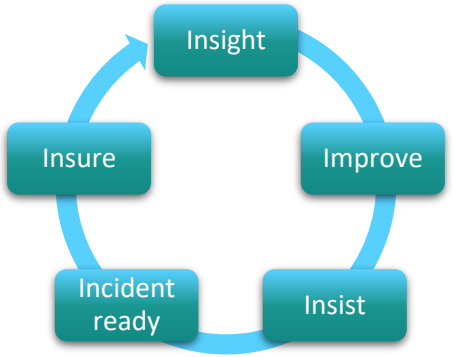
From a clear insight, with a focus on people and an understanding of the company's objectives, market conditions, and the right organization structure, we jointly determine the right measures and services to optimize the resilience of our customers.

A holistic approach based on 5 principles:

Insight, Improve, Insist, Incident Ready, Insure



5 Cybersecurity pilars



Cybersecurity is present in all aspects of the organization and only a complementary set of measures ensures a robust security level. Therefore, we group security services into a holistic approach: **Assess & Assure**, **Consult & Implement**, **Continuous Security & Compliance**, **Respond & Recover** and **Cyber insurance**. A solid implementation of these domains provides a strong foundation for Cybersecurity.

Insight - Assess & Assure

Gain a clear starting point in terms of insight into risks, obligations, and the need for certainty. Analyzing risks within the organization in the areas of IT, information, cybersecurity, and privacy answers questions such as: What threats and vulnerabilities exist? What consequences can these have for business operations? Additionally, an independent and in-depth insight assesses the extent to which the organization has arranged information security and privacy.

Services

- Risk & threat assessment
- Business impact assessment
- Reviewing policies & authorization assessments
- Technical, organizational, and compliance assessments through Baseline, Maturity & Gap analyses, CSAT, based on applicable frameworks ISO27001, BIO, NEN7510, CIS, NIST, NIS2, etc.
- Red teaming, Ethical hacking, OSINT assessments, social engineering, and Phishing
- DigiD ICT security assessments
- Cloud security, implementation & compliance assessments
- Privacy, e.g. in accordance with the GDPR, NOREA Privacy Quality Framework, ISO27701

Improve - Consult & Implement

From an unbiased perspective and experience, we provide clear and tailored recommendations for enhancing your cyber resilience. This involves the implementation of adequately scaled measures, including policies and procedures in business operations, technical (IT and OT) environments, and behavioral adjustments to mitigate unacceptable risks identified in the assessment. We provide comprehensive organization-wide support, and, where needed, specific assistance to the CISO, DPO, and executive team.

Services

- Developing and implementing effective cybersecurity policies
- Implementing specific components as well as comprehensive Information Security Management Systems, in line with ISO27001, BIO, NEN7510, CIS, NIST, NIS2, etc.
- Ensuring cybersecurity for operational technology (OT) as per IEC 62443
- Implementing Cloud security measures
- Establishing Privacy measures, for instance, in compliance with the GDPR, the NOREA Privacy Quality Framework, and ISO27701
- Conducting and monitoring a Privacy Impact Assessment
- Providing CISO or Data Protection Officer as a Service
- Designing and implementing a business continuity plan

5 Cybersecurity pilars

Insist - Continuous Security & Compliance

Once cybersecurity has been brought to the desired level, it is important to maintain that level. From this perspective, it is essential to be able to quickly detect threats and ward off attacks. In addition to periodic testing by ethical hackers, BDO also provides continuous insight through security sensors that detect weaknesses and intruders in the IT infrastructure. With BDO Security Monitoring (SIEM), it is even possible to create a complete company-wide cybersecurity picture and, through an internal audit, assess the governance structure as well as the maturity level relative to standards such as ISO 27001.

Services

- Vulnerability scanning as a service
- Ethical hacking/Penetration testing as a service
- Social engineering (phishing, vishing, mystery guesting) as a service
- Security Incident & Event Monitoring
- Security Operations Center (SOC) services
- Gap analyses, or maturity measurement/maturity level assessment
- Internal audit
- Monitoring PDCA measures

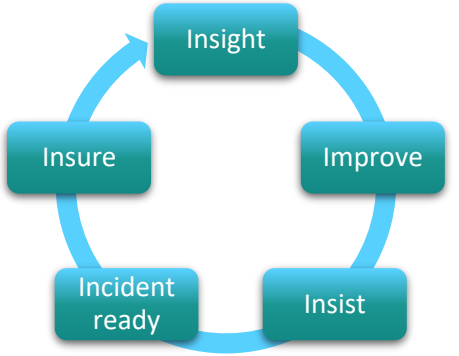
Incident ready - Business continuity, resilience, respond & recover

Robust cyber resilience requires a solid safety net for unforeseen incidents. The ability to act immediately during a cyber incident and to respond swiftly and adequately according to a crisis plan is crucial. You can rely on us to guide your organization through the critical phases after an incident. By doing so, we reduce the risk of reputational and financial damage, improve business continuity, and ensure that business operations comply with laws and regulations simultaneously.

Services

- Management of business continuity, testing, determining, developing, and implementing
- Incident Readiness Assessment
- Forensic Readiness Assessment
- SOC/SIEM monitoring & alerting
- Logging and performance indicators
- First responder training
- Digital Forensic Investigation

5 Cybersecurity pilars



Insure - Cyber insurance

The potential for unforeseen events or successful cyberattacks always exists. When such incidents occur, it's crucial to have immediate access to specialized assistance for resolution. However, skilled cyber security experts are not only scarce but also not readily available and expensive to hire on an ad hoc basis. In these situations, having cyber insurance can be a lifesaver. It not only covers the unexpected high costs but also ensures that there's a predetermined plan for incident response. A crucial consideration is whether the insurance costs justify the potential damage. Additionally, it's important to carefully evaluate which aspects are covered by the insurance, how they are covered, and any obligations related to preparation.

Cyber insurance can significantly reduce the financial impact of cybersecurity incidents. events. It typically covers costs related to responding to a cyber incident, including forensic investigation, data recovery, legal costs, public relations efforts, and often also the costs of informing customers and providing identity protection services after a data breach. The importance of cyber insurance is only increasing as cyber threats evolve and refine. While this insurance cannot prevent the attacks themselves, it can help mitigate their impact on operations. However, it is also essential to remember that cyber insurance complements, and does not replace, effective cyber security practices and procedures.

BDO Approach

First and foremost, BDO specialists conduct a thorough cyber security investigation to identify potential weaknesses, the attack surface, and cyber risk. This results in clear advice that, after implementation, leads to a positive recommendation regarding cyber insurance. By doing this jointly with BDO specialists, it also ensures extensive coverage and significant discount on the cyber security premium. If a cyber incident does occur, incident response specialists from BDO can be engaged. They will assist in the event of an incident, stop the problem, determine the cause in a forensically sound manner, and restore the business as quickly as possible.

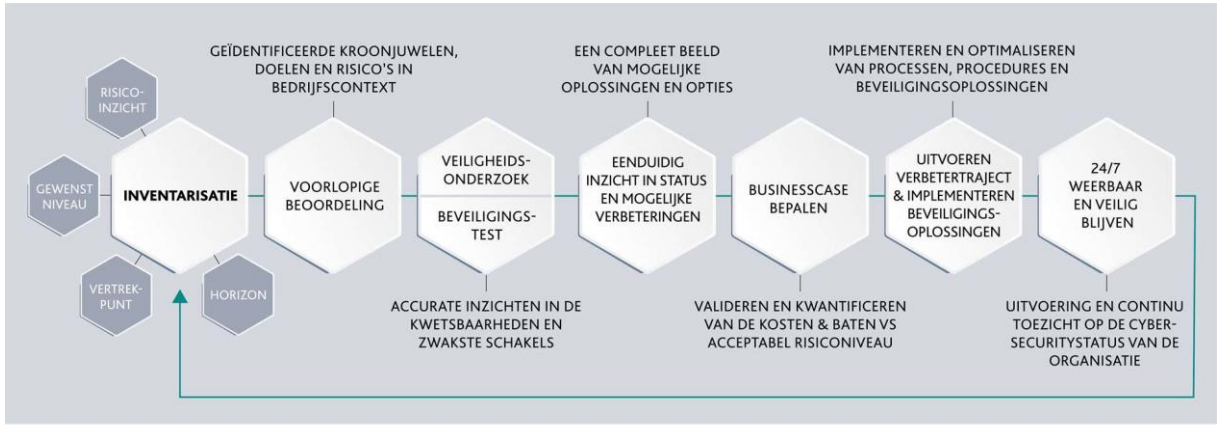
Services

- Thorough assessment & Improvement advice
- Incident readiness preparation and plan
- Incident Respond contract
- Cyber insurance

A pragmatic approach

Effective cybersecurity requires a comprehensive understanding of the present situation, goals, and the necessary security measures aligned with them. These measures must always be current to defend against the most recent threats and be consistent with pertinent developments. Cybersecurity is more than just a technical fix; it is not solely about a product. Adequate protection against cyber threats also encompasses people and processes.

Our strategy entails outlining a distinct roadmap that initiates with generating insights as the foundation for informed recommendations and a business case. This is succeeded by the implementation and organization, and ultimately, the execution and operational accountability. Our Incident Response team ensures the maintenance of continuity & resilience, both proactively and reactively. A crucial element is the ISO 27001, serving as the groundwork for the inventory and the starting point for subsequent steps in our approach.



Insist

Continuous security & compliance

To maintain your Cyber Security at the right level, from both a security and compliance perspective, BDO provides support in the implementation and execution of various operational and auditing activities. This way, we can also ensure that you are prepared for certification, or 'certification ready'. We do this from both a defensive and offensive perspective with the Blue team SOC/SIEM specialists and the ethical hackers from the Red team. This way, we continuously monitor your digital environment; cloud-, IT-, information- and cyber security of your organization and the external environment, and respond immediately to possible incidents and malicious events.

Services

BDO can assist you with various technical measures, including those emerging from the revised ISO 27002, related to preventing and detecting information security incidents.

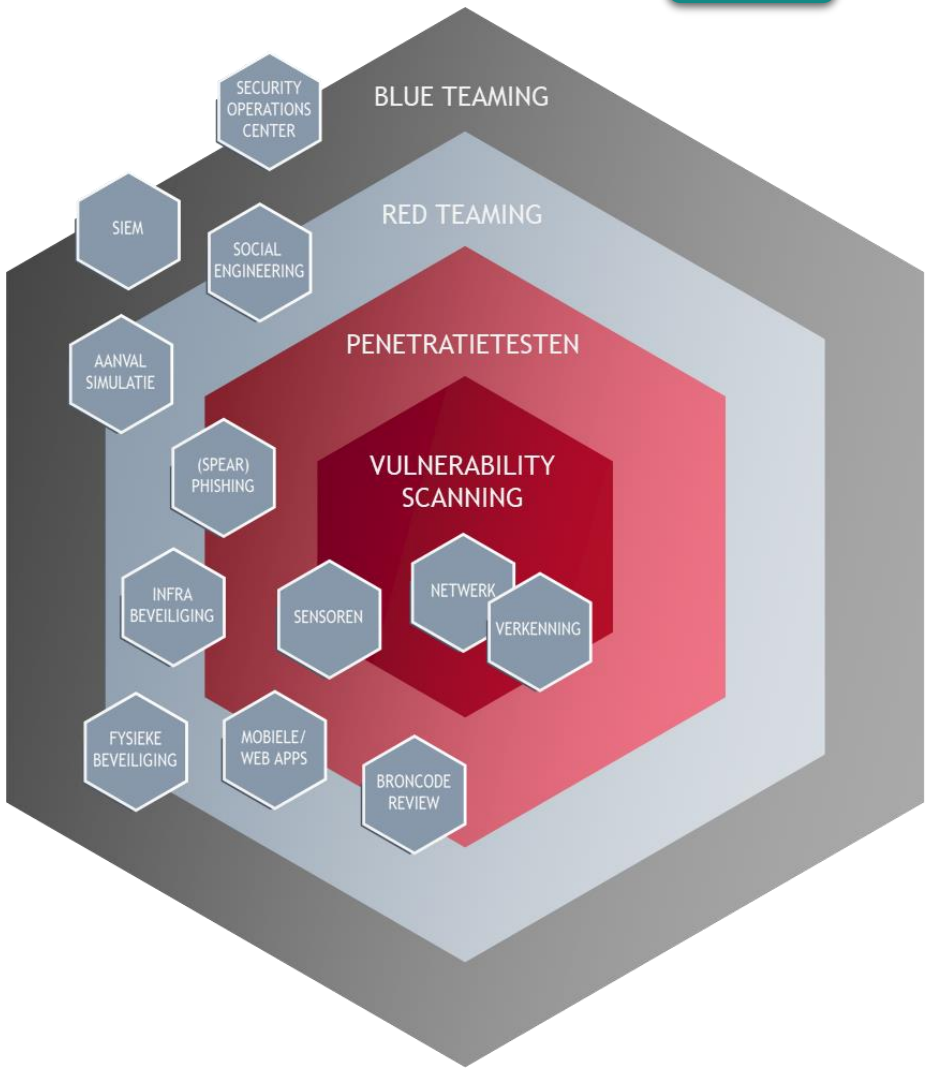
Vulnerability Management: This is a continuous process involving the identification, assessment, resolution, and documentation of vulnerabilities in computer systems and the software they run.

IDS/IPS: These are the Intrusion Detection System and Intrusion Prevention System, network sensors that continuously monitor traffic and obstruct any suspicious network activities.

SOC: This is the Security Operation Center located in Utrecht, where our team of security analysts perform monitoring activities.

SIEM: This stands for Security Information and Event Management, a system that gathers, analyzes, and correlates log information to detect and address suspicious computer system activities.

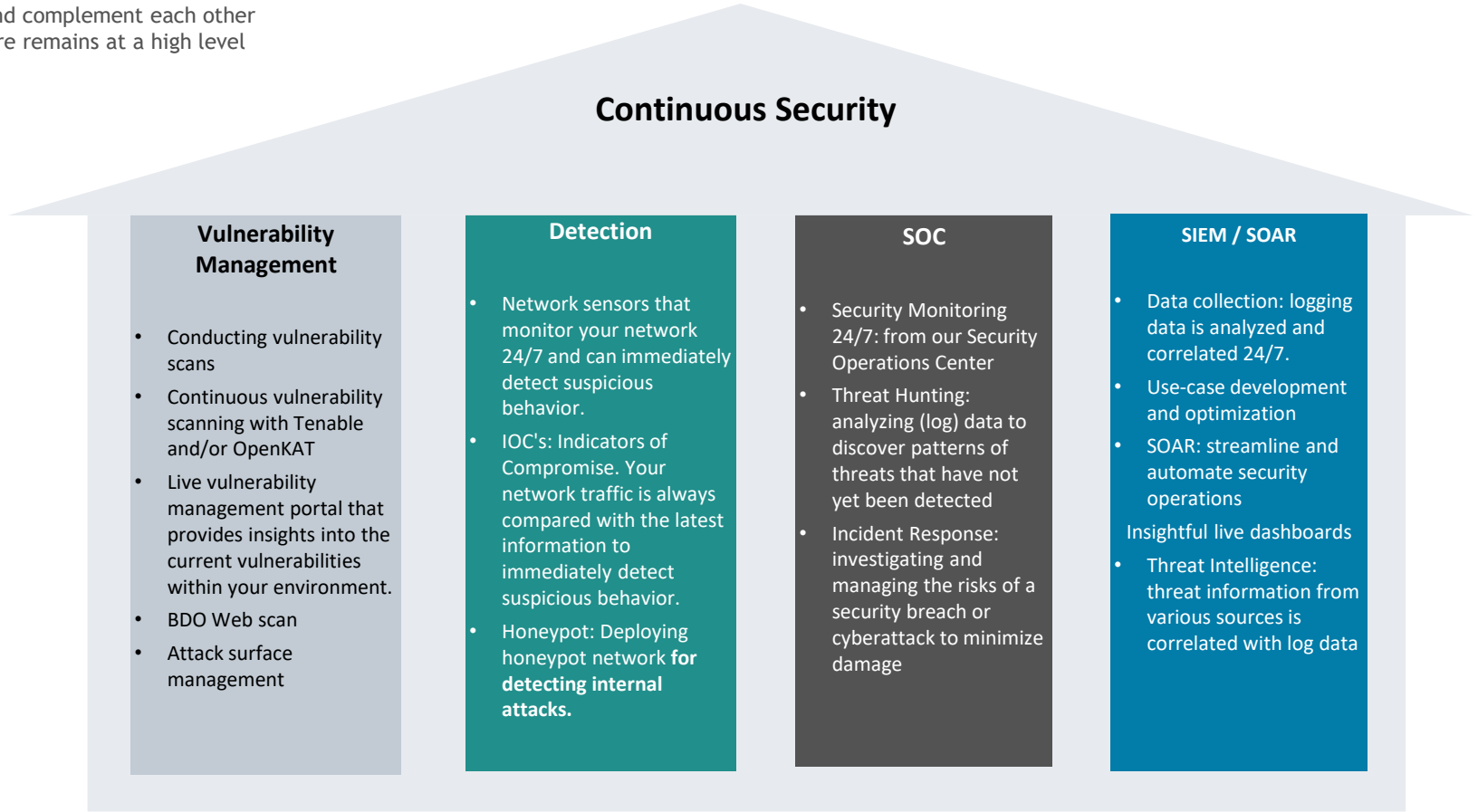
Compliance: This involves translating the aforementioned technical activities into various compliance directives and standards, and then consistently implementing them.



Insist

Overview

The various services strengthen and complement each other ensuring your cybersecurity posture remains at a high level



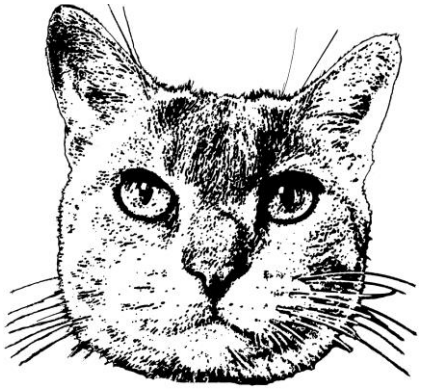
Solutions

SIEM/SOAR
- Microsoft Sentinel

Vulnerability Management
- Tenable
    - Tenable.io
    - Tenable WAS (Web App Scanning)
    - Tenable Lumin (Visualise Risk)
- OpenKat
- Discovery Scans
    - BDO tooling
- Vulnerability scanning
    - Nessus Professional

Detection
- Defender
- FortiGate
- FortiAnalyser
- Forti EMS (Endpoint Management Server)

Microsoft



nessus Professional

tenable

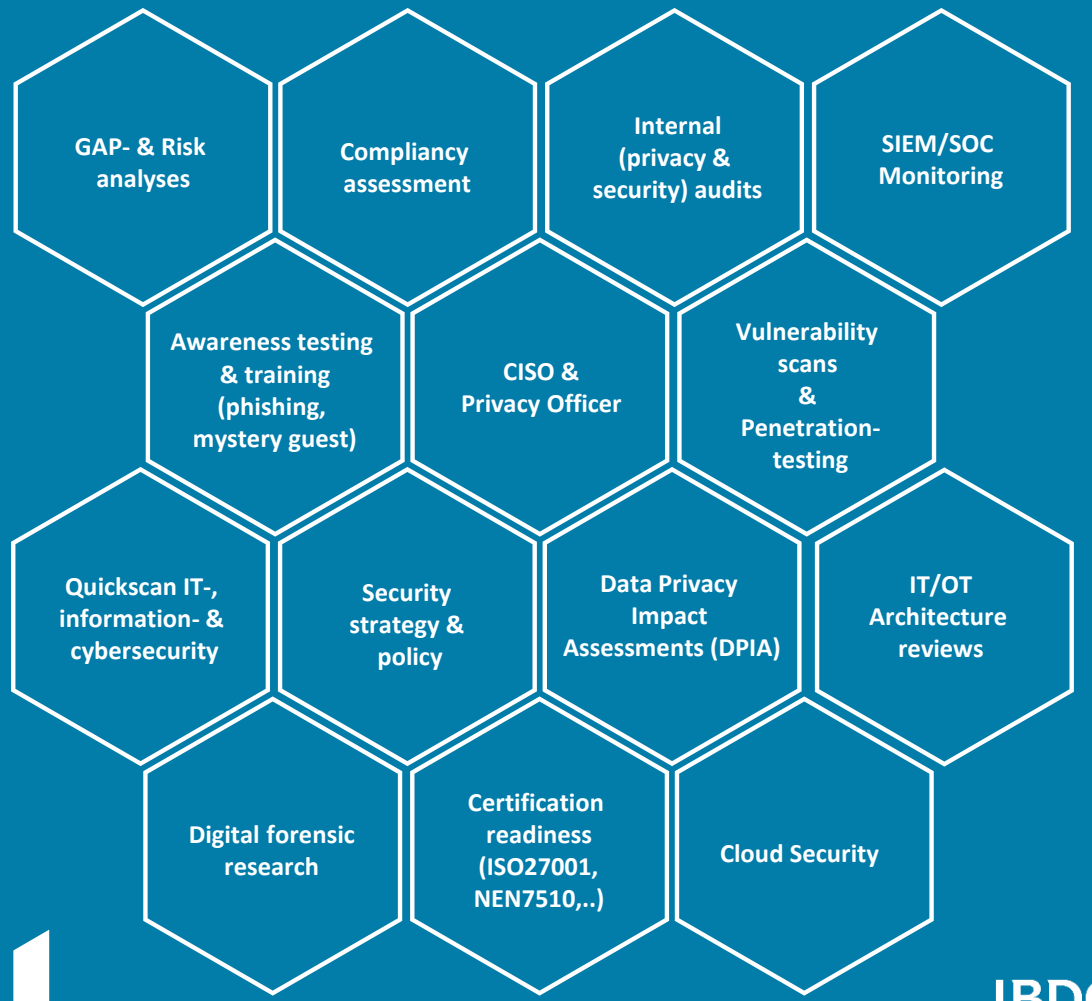
FORTINET

New Perspectives

In the new economy, opportunities arise faster than ever. New rules of the game boost the way we do business. And a new generation is ready to do things differently. Better, smarter, more innovative. To be successful in business, you must also innovate. Be open to change. And look openly at the opportunities ahead.

New perspectives, that's what BDO wants to offer you. And can offer, thanks to our unique combination of local market knowledge and an international network. Personal service and a professional approach. BDO is happy to help you look at your business from a different angle. So you can make the right decisions to make your organization stronger, more agile, and more successful. Whether you are an SME, family business, public organization, or international company.

BDO is happy to look ahead with you. Together we come to new insights and new opportunities in your market. Together we create new perspectives.



BDO