BDO ADVISORY | RISK ADVISORY | THIRD PARTY ASSURANCE

CYBERSECURITY COMPLIANCE

AS CYBERSECURITY THREATS INCREASE IN NUMBER AND COMPLEXITY, IS YOUR ORGANISATION DOING EVERYTHING IT CAN TO PROTECT ITSELF AND TO REASSURE YOUR PARTNERS AND CLIENTS ON YOUR CYBERSECURITY JOURNEY?

CYBERSECURITY RISK IS AT THE TOP OF THE CORPORATE AGENDA IN 2022

Cybersecurity threats are increasing around the globe, growing more complex and affecting organisations of all sizes and industries. Cybersecurity issues can result in financial losses, operational disruption, legal consequences, and reputational damage. Yet many organizations around the world report that they remain unprepared for this critical area of risk.

Twenty percent of global C-suite executives surveyed in our **2021 Global Risk Landscape** listed cybercrimes as the area of risk that they are least prepared for. The numbers are even more concerning for middle market businesses: Nearly half of middle market executives believe that cybersecurity and data privacy risks are their top IT resilience challenge, and 34% say cyberattacks or privacy breaches are their top digital threats, according to BDO's 2021 **Middle Market Digital Transformation Survey**.

HOW PREPARED IS YOUR ORGANISATION — AND YOUR VENDORS — FOR CYBER ISSUES?

Cybersecurity risk is a critical focus area for C-suite executives and board members globally. But it is crucial to remember that this risk needs to be managed not only for a company's *owned* IT infrastructure, but also when IT infrastructure and services are *outsourced* — which is more and more common today.

Outsourcing (parts of) IT — or any critical business function for that matter — brings an additional layer of risks. Even when IT or other services are outsourced, it is still your organisation's business data and your reputation on the line if your vendor experiences a data breach or fails to provide the expected service. If you are a service organisation or vendor yourself, it needs no further explanation that it is essential that you are able to provide transparency on (cyber) controls in place with the objective of putting your customer's minds at rest.

> “YOU CAN OUTSOURCE YOUR ORGANIZATION'S PROCESSES AND INFRASTRUCTURE.
> BUT YOU CAN'T OUTSOURCE RISK.

DEMONSTRATING CYBERSECURITY COMPLIANCE

There are a number of options available to you which allows your organization to create (typically as a service provider or vendor) or obtain (as a customer) more trust and transparency on Cybersecurity across your supply chain. Two of the most commonly applied and established standards are

- **ISO/IEC 27001:2013:** Information Security Management and related standard ISO/IEC 27002:2022 recently revised; and
- **SOC 2:** Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy.

While there are distinct differences between both standards on the level of approach, they achieve similar objectives and can go hand-in-hand in supporting you on your Cybersecurity Compliance journey.

FACT SHEET

SOC 2

1. Attestation report provided by Chartered Public Accountant firms
2. Topics: 5 potential Trust Services Criteria and related illustrative Points of Focus
3. Focus on Service Organisations and the service provided
4. Main deliverables: long form audit report
5. Flexible framework allowing you to focus on the relevant Trust Services Criteria and identified controls specific to your organization
6. Yearly renewal of the attestation

ISO27001

1. Certification provided by an accredited Certification Body
2. Topics: 7 clauses on defining and maintaining your ISMS (Information Security Management System) and Annex A with reference to control objectives and controls
3. Any organization can apply and focus on the whole or part(s) of the organization
4. Main deliverables: detailed ISMS and certificate
5. Rigid framework detailing how an ISMS needs to be designed and operated. All control areas of Annex A need to be addressed unless specified otherwise in your SoA (Statement of Applicability)
6. Yearly surveillance audit and three-yearly recertification audit

HOW BDO CAN HELP

BDO strongly believes in the complementary nature of both frameworks, allowing both service providers or any organisation to progress in their Information Security Compliance journey at their own pace

SOC 2 ATTESTATION

Starting off with the SOC 2 Trust Services Criteria, the framework allows you to define and implement controls (also known as the System Description) that are relevant to your organisation's context. Having the System Description assessed by BDO enables you to demonstrate compliance to key Information Security principles and respond to assurance needs of internal and external stakeholders in a relatively short time.

ISO 27001 IMPLEMENTATION

Designing and implementing an ISO 27001 ISMS requires more time and resources. Leveraging a strong baseline of controls from the SOC 2 attestation, we can support your organization in building on that experience and formalising your way of working in a set of Information Security Policies and procedures detailing the continuous maintenance of your Information Security programme.

SOC 2+ ISO27001 ATTESTATION

Having implemented the corner stones of ISO 27001, your existing SOC 2 report can be extended to a SOC 2+. This allows you to report on the state of your ISO 27001 programme without formally having gone through a certification by a Certification Body.

ISO27001 CERTIFICATION

As a final step in your compliance journey, we can assist you in obtaining the ISO 27001 certification through one of our partners as an official Certification Body.

For a tailored approach on how you can improve your organization's approach to cybersecurity, please contact us today.

CHRISTOPHE DAEMS
Senior Manager

E-mail: christophe.daems@bdo.be
Tel.: +32 474 90 78 51

FRANCIS OOSTVOGELS
Senior Manager

E-mail: francis.oostvogels@bdo.be
Tel.: +32 474 92 08 00

NICK HUYSMANS
Advisor

E-mail: nick.huysmans@bdo.be
Tel.: +32 486 31 90 45

▶ Follow us

▶ www.bdo.be

BDO Advisory BV/SRL, a company under Belgian law in the form of a cooperative company with limited liability, is a member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms.