Cybersecurity Assurance

A drive to cybersecurity assurance

Cybersecurity is one of the top issues on the minds of management and boards in nearly every company in the world — large and small, public and private. As businesses continue down the path toward more interconnected relationships, their cyber resilience will affect not only their own risk exposure but also that of their entire ecosystem.

An objective measure ·of cybersecurity for all stakeholders will therefore fast become a prerequisite for any partnership, investment, merger, integration, or even just the sharing of vital information.
Assurance reporting on cybersecurity risks gives both internal and external stakeholders a solid understanding of whether a company's risk management program and underlying controls serve as a solid line of defense against potential attacks. An assurance can also enhance reputation and provide transparency to the market, which is critical to maintaining the value of a company's brand.

What is cyber security assurance reporting?

Assurance reporting is an independent assessment of the suitability, design and operational effectiveness of an organisation's cybersecurity risk management programme, governance and controls.

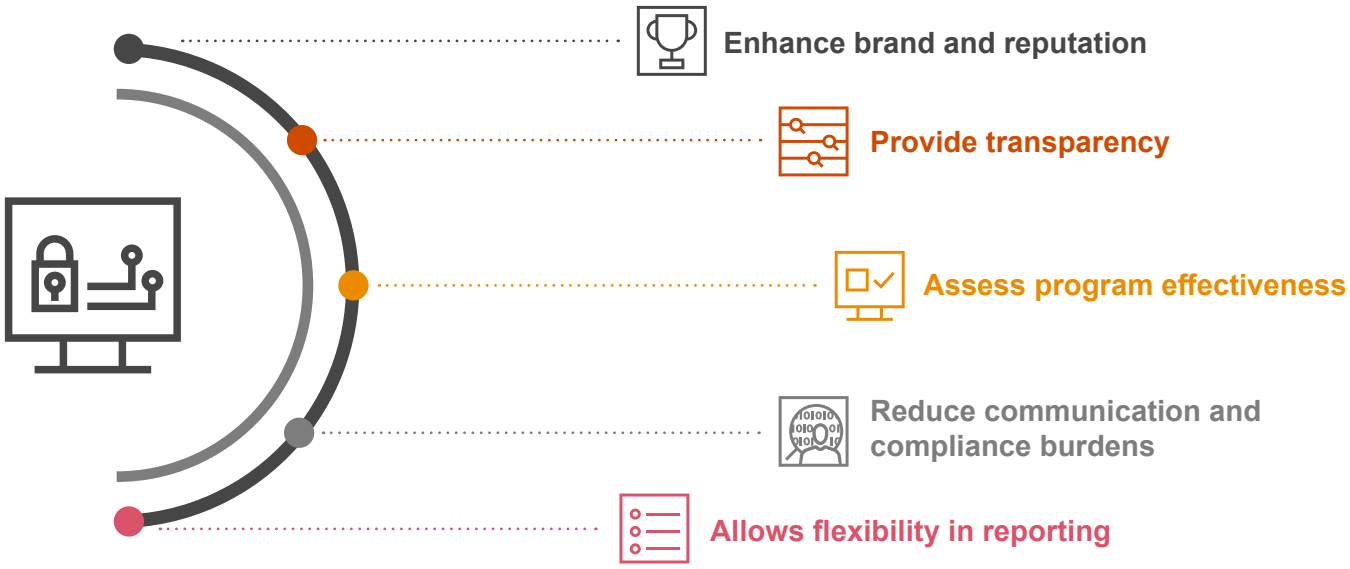
The report can then serve as an input to the decision making process of a broad range of users (both internal and external):

Internal users (e.g., board members, senior management) may need information in order to exercise their fiduciary responsibilities, demonstrate effective governance, and/ or to address questions and concerns from regulators and other parties; and External users {e.g., investors, analysts, vendors and business partners) may require information to help them evaluate management's process for managing cybersecurity risks.

The need for Cybersecurity Assurance

- **Boards** need to effectively perform their fiduciary responsibilities
- Increasing demands from **customers/business partners** due to third party risk management initiatives
- Continued **outsourcing of information technology** (e.g., cloud service providers) and security operations leading to greater complexity in risk management
- Increasing **complexity in regulations, and requirements** (e.g. GDPR, IMO, KYC, NIS), relating to cybersecurity practices, and focus of Regulatory examinations
- Increasing demands from **investors** for a clearer understanding of company risk management practices

Potential benefits of Cybersecurity assurance reporting



Our approach to assurance reporting

Many companies recognize that their cybersecurity assurance challenge is how far they are from assurance readiness. We have outlined the necessary stages of the path to assurance and developed a four-phase cybersecurity assurance solution that aligns with each of these.

Phase 1	Phase 2	Phase 3	Phase 4
Scoping	Readiness	Remediation	Report
Determine the scope of your assurance report We work closely with you to scope a tailored assurance report. We take into account the factors unique to your organisation, what it wants to achieve and its priorities. Our approach includes determining: • the 'users' of the report • stakeholder groups that will be relying on the report.	**Preliminary Assessment** Next, we carry out a readiness assessment for you which serves as a dry run for formal assurance. This would enable Management to identify the "current status" and correct gaps in their cybersecurity risk management program.	**Action Plan** Management develops remediation plans, and takes appropriate steps, to address any gaps identified during the initial assessment phase.	**Undertake formal assurance and reporting (ISAE 3000 / SOC2 / SOC for Cybersecurity)** We will deliver a formal assurance opinion, signed by PwC, demonstrating the robustness and rigour of the reviews undertaken and a means to share the associated comfort over the control framework with both internal and external stakeholders.

If you would like a conversation on this topic, please contact:

Constantinos Taliotis
Partner
Head of Assurance
c.taliotis@pwc.com
T: +357 - 22 555 522

Sophie Solomonidou
Director
Risk Assurance
sophie.solomonidou@pwc.com
T: +357 - 22 555 150

PwC Cyprus

PwC Central, 43 Demostheni Severi Avenue,
CY-1080 Nicosia, Cyprus
P O Box 21612, CY-1591 Nicosia, Cyprus
Tel: +357 - 22 555 000

pwc