

Organisations commonly aggregate the focus on GRC (Governance, Risk and Compliance) at both corporate and cybersecurity levels to achieve governance objectives, risk management and regulatory compliance, aiming at improving business performance and enhancing decision-making.

Our GRC advisory services provide organisations with the guidance necessary to develop a comprehensive GRC strategy and approach. Our advisory team will work with your organisation to identify and assess risks, as well as develop modern frameworks and control systems to ensure compliance with applicable regulations and industry standards. Our team will also provide guidance on the implementation of policies and procedures that will help ensure that your organisation is meeting its objectives and obligations under applicable laws and regulations.

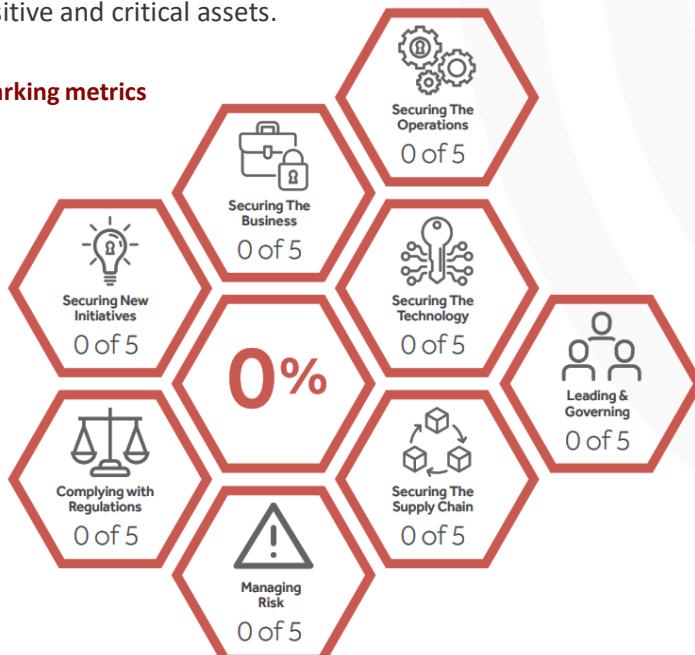
Our value proposition

Security benchmark assessment & roadmap

One-day Benchmark: We conduct a one-day cybersecurity benchmark assessment which consists of evaluating your high-level cybersecurity posture and guiding your companies' overall security strategy and risk priorities.

In-Depth Benchmark: We also provide an in-depth assessment, identifying key gaps within your technology landscape and control environment and helping you develop a prioritised strategic improvement plan. We leverage an adaptive approach for cybersecurity by shifting the mind-set from incident response to continuous response, resulting in a security program that satisfies stakeholder and regulatory scrutiny and meets the organisation's responsibilities for protection of sensitive and critical assets.

Security benchmarking metrics



Highlights

Security benchmarks

As companies embrace new technologies to drive their digital transformation initiatives, cyber risks remain a top priority concern for business leaders. Relying only on internal efforts and programs has proved to be insufficient against modern cyberattacks. Conducting regular security benchmarks provides important insight of where the company stands in terms of best practice, within the industry, and its performance over time.

ISO 27001 framework

ISO 27001, part of the ISO 27000 set of information security standards, is a worldwide guiding standard for establishing, implementing, operating, monitoring, and continuously improving the information security management system (ISMS). As part of ISO 27001 compliance, organisations must evaluate the effectiveness and sustainability of their ISMS and its response to emerging security threats.

NIST Cybersecurity framework

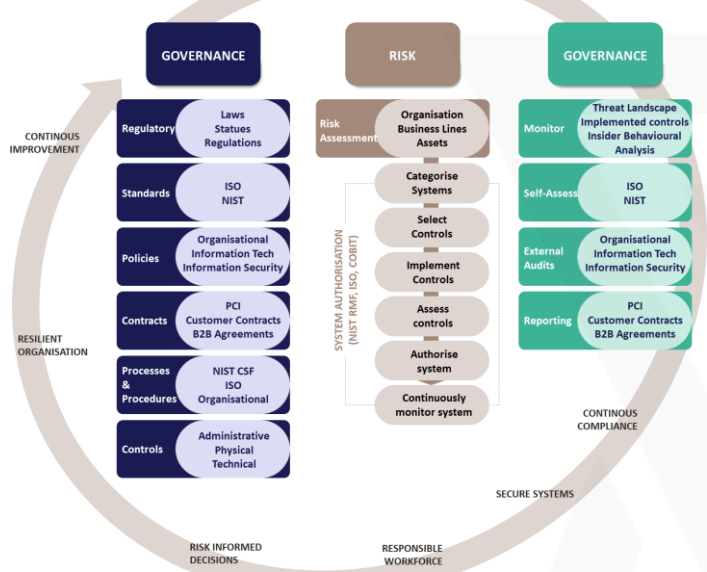
NIST is one of the most popular cybersecurity frameworks which provides guiding principles and standards to organisations, irrespective of industry, to implement or strengthen their cybersecurity programs. An adapted NIST-based security framework will help in improving threat detection, mitigate risks and enhance the response modern cyber incidents.

Security risk analysis & framework development

We assess your organisation’s unique security risks, identify vulnerabilities and evaluate controls. We also define risk mitigation strategies and design customised internal and third-party supplier risk frameworks aligned to business objectives, risk tolerance and compliance requirements.

Security governance assessment & framework development

We assess your current security governance and management practices to identify areas of improvement. We design tailored enterprise security governance frameworks, including setting up of forums, defining policies, define a control environment and conducting organisational structuring.



ISO 27001 assessment and certification

We assist from the initial pre-assessment to certification and beyond. We walk you through each step of the process to define your Information Security Management System (ISMS) and prepare for the external certification audit.

Cybersecurity framework & program implementation

We adapt, define and implement your cybersecurity framework and program based on NIST, ISO 27001 or other standard. We conduct multi-year program management initiatives to help define and implement the security processes, controls and technologies needed to mature your cybersecurity function over the long-term.

Key benefits

Enhanced security posture
Minimise vulnerabilities and protect against modern security threats.

Stakeholder trust
Demonstrate your commitment to data protection and security assurance from the board to suppliers and partners.

Regulatory compliance
Meet legal, contractual, and regulatory requirements.

Operational excellence
Streamline security processes and improve efficiency.

Competitive advantage
Differentiate your business in the marketplace through enabling cybersecurity practices and customer confidence.



ABOUT US

Founded in 2015, VoxExcel Cyber are a leading consulting led cyber security company focused on providing best-in-class, strategic advisory services and innovative technology solutions. We specialise in assisting C-level executives in navigating the complexity of security governance, risk management and regulatory compliance requirements, while bridging the gap between management objectives and the requirements of technical teams.

Our team of consultants and engineers are focused problem solvers with deep technical knowledge and broad industry experience, across many and industry sectors including banking, financial services, retail, airline, government, telco, oil and gas, mining and manufacturing.

Acquired by DVGA in 2022, the company also provides data privacy, supply chain audit, and ISO implementation software solutions, to many major clients. The company operates across Europe, USA, Africa and Middle East.

