TRUSTMARQUE

GRC Consultancy Services

trustmarque.com

GRC consultancy

Our Governance, Risk, and Compliance (GRC) Consultancy team provides top-tier strategic solutions tailored towards the unique regulatory, operational, and cybersecurity challenges of your organisation.

Our team of seasoned experts have extensive experience in GRC frameworks, offering a holistic approach to managing your organisation's governance structures, risk management practices, and compliance obligations.

We start by understanding our client's business environment, objectives, and the specific regulatory landscape they operate in. This enables us to deliver personalised, actionable strategies which ensures compliance, promotes operational efficiency and assists with strategic decision-making.

Our services range from risk assessments and compliance audits to the development of comprehensive GRC programs, all designed to protect your assets, mitigate risks, and foster a culture of informed, proactive governance.

With our GRC Consultancy team, you can navigate the complexities of today's regulatory environment with confidence, ensuring your business is resilient, compliant, and primed for sustainable growth.

Key stats:

There have been numerous global data breaches affecting UK entities with over 8 billion records being exposed in 2023 alone, leading to the loss of sensitive information.

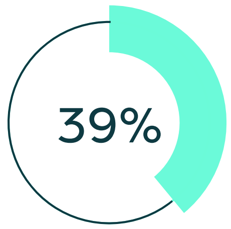
These incidents highlight the importance of UK cybersecurity and adhering to recognised cybersecurity standards, the need for improved board engagement and governance, and the increasing cost of cyber crime

Cyber essentials certification

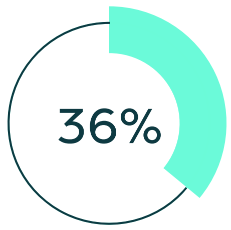
Our Cyber Essentials Certification Service is designed to help organisations protect themselves against common cyber threats and vulnerabilities.

This service offers a comprehensive approach to achieving Cyber Essentials certification, a UK government-backed scheme that encourages organisations to adopt basic cybersecurity practices.

By obtaining Cyber Essentials certification, businesses demonstrate their commitment to safeguarding sensitive information, reducing the risk of cyberattacks, and enhancing customer trust.



As of 2023, 39% of businesses and 31% of charities in the UK have an external cyber security provider, indicating a significant reliance on external expertise to strengthen cyber security postures.



Approximately 36% of businesses and 35% of charities have formal cyber security policies in place, highlighting the growing recognition of the importance of structured cyber security measures.

Cyber essentials plus certification

Our Cyber Essentials Plus Certification Service goes a step beyond the basic Cyber Essentials certification by providing a more rigorous assessment of your organisation's cybersecurity defences.

This service is designed to help your business, government agency, or other organisation enhance its security posture and demonstrate a higher level of protection against cyber threats. It is based on the UK government's Cyber Essentials scheme and includes a detailed assessment of your IT systems and networks.

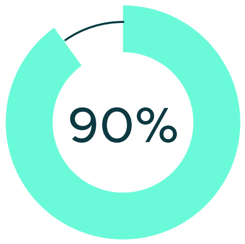
The average cost of a data breach within the UK has increased by 8.1%. This results in a total cost of £4.56 million, emphasising the financial benefits of enhanced security measures.

According to statistics, around 70% of charities and 66% of businesses examine a cyber threat after an incident takes place, highlighting the need for proactive defence strategies like Cyber Essentials Plus.

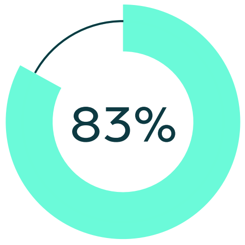
Cyber essentials advisor

Our Cyber Essentials Advisor service is a professional consulting service designed to help organisations understand, prepare for, and achieve Cyber Essentials certification.

The service guides businesses through the necessary security controls required for certification, offering expert advice on improving IT security posture, ensuring that the scheme's five key control requirements: secure configuration, boundary firewalls, access controls, patch management, and malware protection are met.



Around 90% of UK organisations have encountered a greater risk of exposure to cyber security threats due to the rise of digital use over the past two years, indicating a crucial need for expert advice and guidance on managing these risks.



Approximately 83% of businesses that encountered a cyber threat were targeted by a phishing attack, showing the importance of advisory services in educating and protecting against common cyber threats.

Virtual chief information security officer (VCISO)

Our VCISO service provides your organisation with expert cybersecurity leadership and strategic guidance on a virtual basis.

We understand not all organisations can afford a full-time, in-house Chief Information Security Officer. This is where our experienced professionals' step in to help you navigate the complex world of information security.

vCISOs can fill temporary knowledge gaps, ensure compliance, and provide rapid response during cybersecurity incidents.

ISO270001 Information security management system (ISMS) implementation

Our ISO 27001 Implementation Service helps organisations establish a robust information security management system (ISMS) to safeguard their data and ensure compliance with international security standards.

This service guides you through the entire ISO 27001 implementation process, from initial assessment to certification, with a focus on tailoring the ISMS to your specific requirements.

I

Cybersecurity maturity assessment

Our Cybersecurity Maturity Assessment service enables organisations to gauge and enhance their cybersecurity posture.

With this comprehensive service, we provide a thorough evaluation of your current cybersecurity practices, identifying potential vulnerabilities and assessing the maturity level of your security measures against industry standards and best practices.

Our experts deliver actionable insights tailored to your unique business context, enabling you to prioritise investments, strengthen defences, and reduce your risk exposure.

Whether you're looking to comply with regulatory requirements, safeguard sensitive data, or simply build a more resilient IT environment, our Cybersecurity Maturity Assessment service offers the strategic guidance necessary to elevate your cybersecurity maturity and safeguard your assets.

Information security risk assessment and management

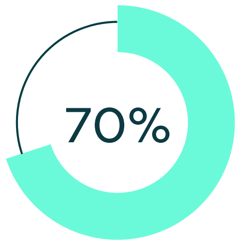
Our Information Security Risk Assessment Service helps organisations identify and evaluate potential vulnerabilities, threats, and risks to their information systems and data.

In an increasingly digital world, understanding and managing these risks is vital to protect sensitive information and maintain operational continuity.

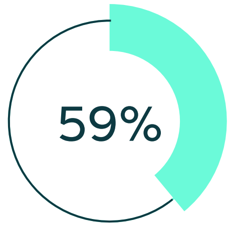
Cybersecurity strategy development

Our Cyber Security Strategy Development Service assists organisations in creating a robust and customised cybersecurity strategy tailored to their unique business needs and risk profile.

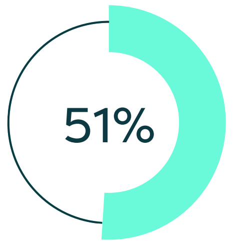
In today's digital landscape, a well-defined and proactive cybersecurity strategy is critical to protect sensitive data, maintain operational continuity, and safeguard the reputation of your organisation.



Board engagement and governance in cybersecurity reveal that 70% of businesses and 69% of charities do not have board members or trustees explicitly responsible for cyber security within their job role



This percentage drops to 59% for medium businesses and 47% for large businesses.



Furthermore, 51% of medium businesses and 32% of large businesses do not have a formal cyber security strategy in place.

Cybersecurity gap analysis

Our rapid Cybersecurity Gap Analysis service efficiently assesses and improves an organisation's cybersecurity posture within a condensed 10-day timeline.

We combine industry-leading frameworks and in-depth analysis to deliver actionable insights and recommendations for immediate and long-term cybersecurity enhancements.

Penetration testing remediation consultancy

Our Penetration Testing Remediation Consultancy Service provides targeted, expert guidance to address vulnerabilities exposed during penetration testing.

Following a thorough analysis of the penetration test results, our skilled consultants collaborate with your team to develop and implement effective remediation strategies. These are tailored to your specific business needs and security requirements.

We prioritise identified vulnerabilities based on their severity and potential impact on your business, ensuring critical issues are immediately addressed.

Our service extends beyond simple fixes by offering strategic recommendations to strengthen your overall security posture. This prevents future breaches and ensures you comply with the relevant cybersecurity regulations.

With our consultancy, you can enhance your defences and safeguard yourself against cyber threats. As a result, you will be able to maintain the trust of your clients and stakeholders.

trustmarque.com
info@trustmarque.com