commissum
INFORMATION ASSURANCE

# Consultancy and Advisory Services

**With over 20 years of experience, Commissum is adept at offering pragmatic advice and recommending cost-effective solutions that are tailored to your organisation's needs, to manage Information Security risk in a coordinated, cohesive and consistent manner across numerous business units and functions. Whether you require a traditional approach of measuring your Information Security Management controls against the international benchmark of ISO 27001, an assessment against governmental frameworks, a Payment Card Industry Data Security Standards (PCI DSS) assessment, or a review focused on cost optimisation, Commissum has the experience, capability and track record that holds its own with the best.**

### GOVERNANCE, RISK AND COMPLIANCE (GRC)

In today's heightened business and financial regulatory environment, organisations need to ensure compliance with new and evolving global laws and regulations such as financial services regulations and various international data protection laws (e.g. GDPR). Strategic planning is critical to setting the course for your organisation. GRC refers to an organisation's strategy for managing enterprise risk, compliance and corporate governance in the context of legal, regulatory requirements, and industry best practice. Spanning the entire organisation, designing and implementing an effective enterprise-wide GRC strategy can be onerous and costly. This is where our consultants' years of experience and pragmatic, focused approach yields value.

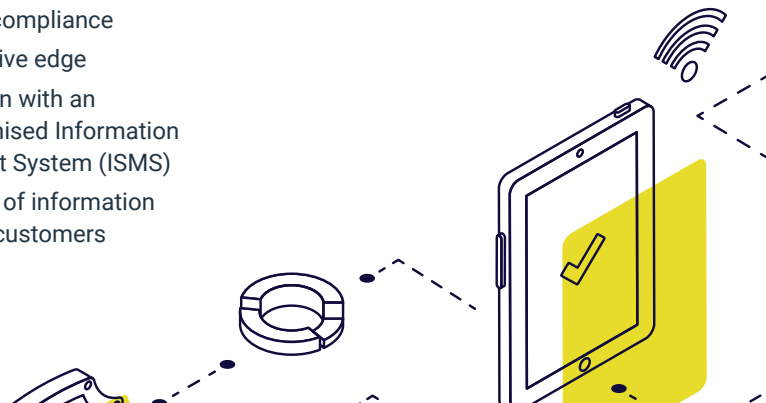
### ISO 27001 AND SECURITY MANAGEMENT

Increasingly, regulators, legislators, customers and business partners demand effective information assurance and cite ISO 27001 as the benchmark for compliance. By implementing ISO 27001 your organisation can:

- Effectively manage business and regulatory risks and compliance
- Increase its competitive edge
- Enhance its reputation with an internationally recognised Information Security Management System (ISMS)
- Reduce the workload of information assurance audits by customers

### OUR SERVICES:

- Governance, Risk and Compliance (GRC)
- ISO 27001 and Security Management
- Data Protection and GDPR
- PCI DSS
- Business Continuity Consulting
- Technology Assessment and Advisory
- Supply Chain Security Assessment
- UK HMG Security Policy Framework (SPF)
- NCSC 10 Steps to Cyber Security
- Cyber Essentials
- Training
- Outsourced CISO, DPO and ISO



### ISO 27001/2 GAP ANALYSIS

A gap analysis identifies areas where you are not compliant with the ISO 27001/2 standards. Commissum will deliver an independent assessment of your information security policies and practices, and a pragmatic, prioritised roadmap to remediate identified gaps in order to establish a compliant ISMS.

### ISO 27001/2 TRANSITION MANAGEMENT

Establishing an ISMS to certify to ISO 27001 standards can be a daunting task. Commissum's ISO 27001/2 Transition Management services build upon the roadmap established during the gap analysis, minimising the burden of implementation, business disruption, and the cost to your organisation.

### DATA PROTECTION AND GDPR (GDPR)

A comprehensive update to Data Protection Directive 95/46/EC in May 2018, the GDPR increases rights of data subjects while exponentially increasing the burden of compliance for organisations that gather and use personal data. This has initiated a global trend with other countries also strengthening data protection legislation.

The stakes are high for non-compliance, with heavy fines applying and business reputation at risk (e.g. fines of up to 4% of global turnover for GDPR non-compliance). Regulators have made it clear that they intend to fully flex their powers to enforce regulation.

Complying with GDPR or other legislation can be a significant burden:

- Compliance requires a comprehensive understanding of all your business processes and IT systems in the context of handling and collecting personal data
- Compliance affects all parts of the organisation
- The success of compliance strategies depends on a coherent and consistent application
- The need for compliance extends beyond your organisation into your supply chain

Commissum's Data Protection advisory service will help your organisation continue its operations with minimal disruption while capitalising on the valuable data you hold. We take time to understand your business priorities and risks, correlated with the storage and processing of personal data and applicable legislative requirements, before laying out the steps you need to take to comply.

### PCI DSS

PCI DSS is a multifaceted security standard introduced by the Payment Card Industry (PCI) Security Standards Council, founded by the major credit card brands. The aim was to address security and reduce fraud by mandating an industry-wide standard for all organisations that store, process or transmit cardholder data. Such organisations are required to address security management, policies, procedures, network architecture, software design and other critical protective measures related to handling payment card data. Non-compliance with this standard can attract heavy fines or even withdrawal of the payment card facility altogether.

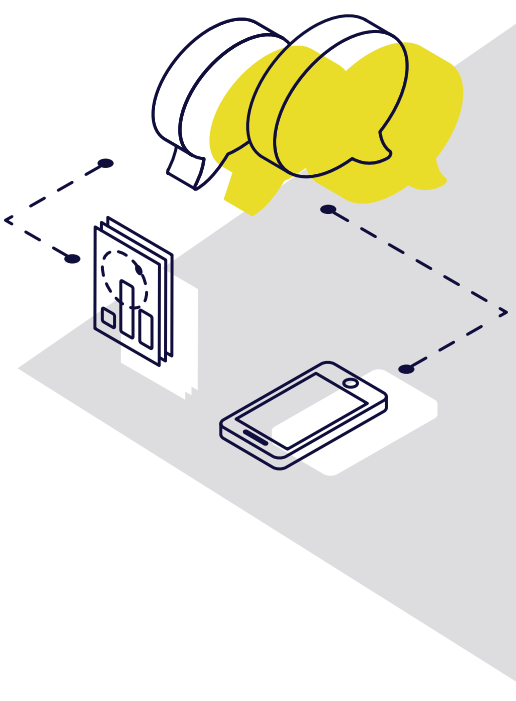
The main issue for most organisations is appropriate, but also sensible and pragmatic, interpretation and application of the standard. This requires expertise and experience, especially in the early, critical stages of planning and preparing for compliance. By leveraging Commissum's PCI DSS services, your organisation can identify the improvements that need to be made to comply with the PCI DSS standards with optimal investment and minimal business interruption.

### BUSINESS CONTINUITY

Commissum will help you prepare for the worst. Our business continuity consulting can make sure you have a plan to minimise the impact of disaster to your business. We assist you with formulating appropriate plans to prepare, regularly exercising these plans, and in the event of an incident, support you in restoring business operations and critical systems.

# Get in touch.


**EMEA:**
**+44 330 223 0709**
**APAC :**
**+60 328 583 601**
**commissum.com**

CHECK IT Health Check Service · CREST · CYBER ESSENTIALS PLUS · Assured Service Provider in association with National Cyber Security Centre · ISOQAR REGISTERED ISO 27001: 2013 0026 · ISOQAR REGISTERED ISO 9001: 2015 0026 · Crown Commercial Service Supplier