//Security Gap Analysis

Non-compliance with data protection regulations can be costly

In a constantly shifting risk landscape, the need to demonstrate ongoing compliance and a high standard of data security has never been more important. With an ever-increasing number of data breaches and evolving threats, how do you reduce the chances of becoming the subject of the next new headline, or yet another statistic?

The first step is knowing where your business stands in relation to data protection and cyber security. Once you know where you are on your compliance journey, you can start moving forward.

Compliance can be complicated, and the standards that govern data vary in complexity and scope. What you need is someone who can make sense of what is required and how it applies to you.
We start by understanding your business and security needs. By getting to know your business inside-out, we can work with you to determine the level of assurance that you need.
Depending on your security needs, we can assess you against standards including:

- ISO 2700l:2013- Information Security Management
- PCI DSS- Payment Card Industry Data Security Standard (PCI DSS)
- ISO 2230l:2012- Business Continuity Management
- Cyber Essentials (and Cyber Essentials+)

We can also review your data protection processes so that you understand any changes that you need to make to become or remain compliant with the General Data Protection Regulation (GDPR).

We have decades of compliance expertise and experience in working closely with our customers to ensure that you understand your current level of compliance. At every stage, we will offer pragmatic and clear advice on how to close the gaps to ensure that you get to where you want to be.

Reviewing your practices

No matter what your current level of security capability is, having an external review of your people, premises and processes will give you peace of mind that any issues have been identified and resolved.

For organisations just starting out on the journey to putting robust data protection practices in place, implementing a Gap Analysis based on security standard like ISO 27001 will give you a clear indication of where you are most at risk.

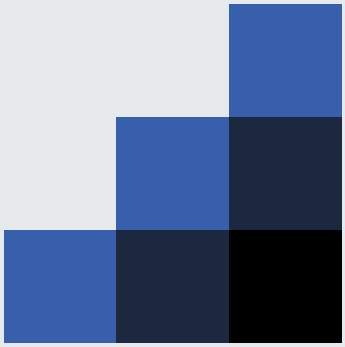
Businesses that have already undertaken the steps to achieve full certification against one of the above standards can also benefit from having an external party of highly-experienced consultants review current practices and ensure that data protection measures are comprehensive enough to ensure continued protection.

Understanding your compliance needs

Both PCI DSS and ISO 27001 standards are organised in sets of controls or requirements, but vary in terms of the areas of data protection that they focus on.

The journey to compliance can be complex, but by analysing your current approach to security in a structured way, we can give you a clear understanding of what lies ahead.

- PCI DSS has 12 requirements with 255 controls based on securing cardholder data. We can help you understand this technical standard to establish your current levels of compliance, and any changes you might need to make.
- ISO 27001 consists of 114 control requirements spanning 14 areas, and we can help you get to grips with this risk-based standard, enabling you to focus on planning, implementing, running, monitoring, and improving an information security management System (ISMS).



A comprehensive approach to understanding your security

- Complete review of risk management and security policies and procedures.
- Bespoke recommendations and opportunities for continual improvement
- A clear action plan to ensure peace of mind and continuing data protection