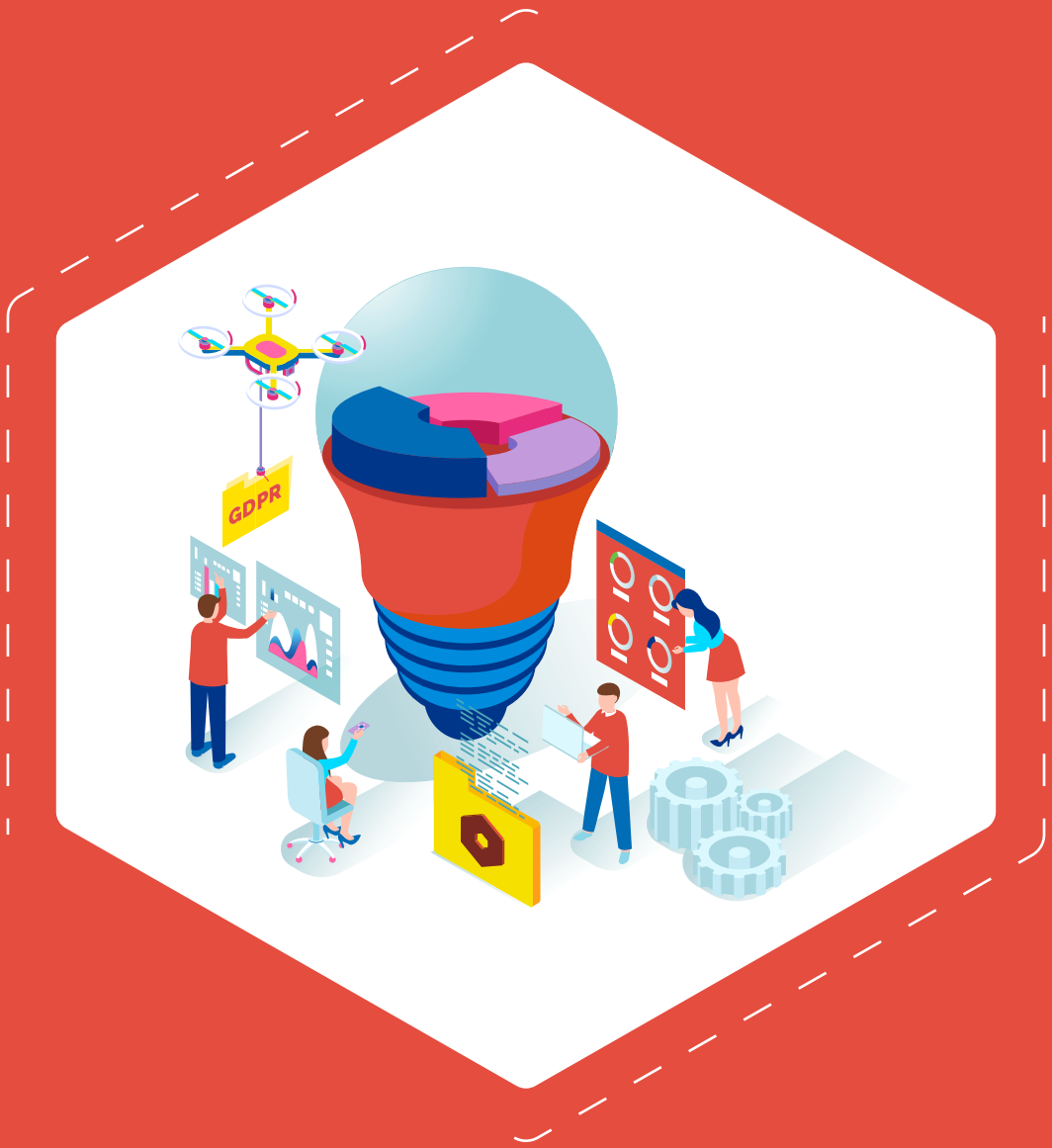
turremgroup



smartcomply

- GDPR
- Cyber Essentials
- Penetration Testing
- Security Audits

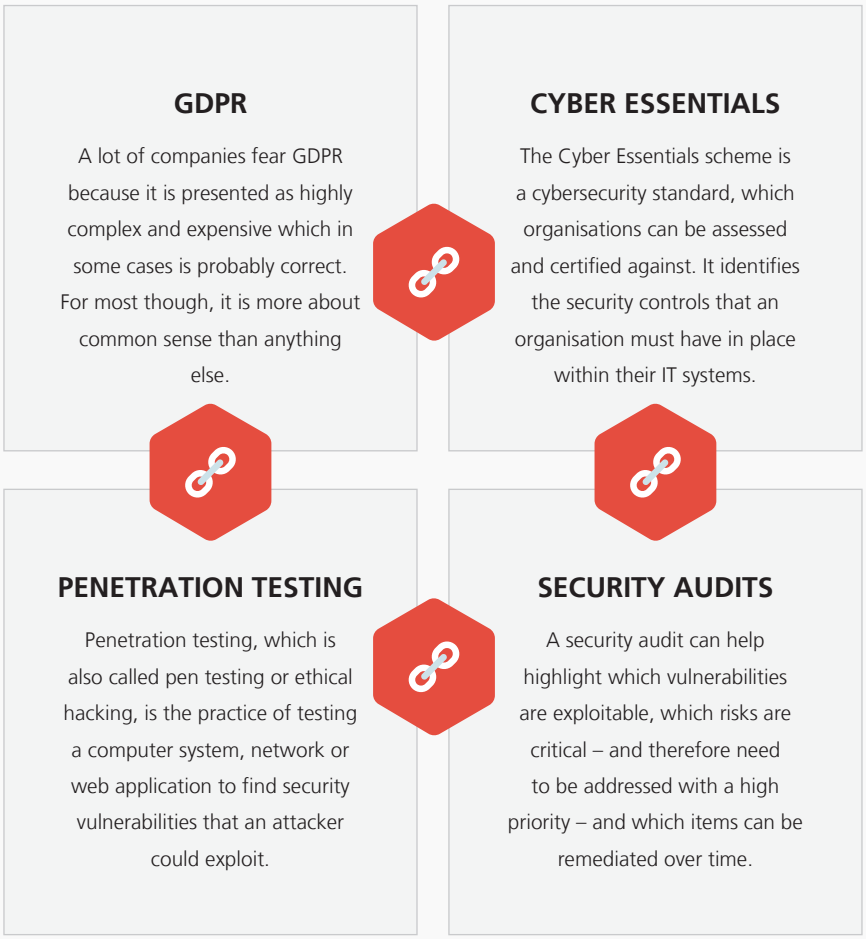
BECOME CYBER COMPLIANT THE EASY WAY

So how do you build and manage an information security program that will demonstrate compliance to management and outside parties? Today, organisations must either adopt expensive, complex software systems that take months to deploy or piece together disjointed tools from a variety of suppliers.

If you add GDPR requirements to this as well, it means that for many businesses compliance starts to become a major headache for all concerned.

Our **smart**comply suite provides an easy and flexible way for your organisation to become "cyber compliant". The services offer a "mix & match" toolset that allows our clients to select the specific set of services they need, rather than paying for items that are not needed but are supplied as part of an overall package.

All the services are provided based on a managed service, so, in a nutshell we do all the work for you and work alongside your staff from beginning to end.



GDPR

Yes it's a nightmare, but unfortunately it is also the law – Brexit or no Brexit. Organisations in the UK must comply; from one-man bands all the way up.

A lot of companies fear GDPR because it is presented as highly complex and expensive which in some cases is probably correct. For most though, it is more about common sense than anything else.

What a lot of people also forget is that as an organisation you can only do so much, because budgets, skills, and time restraints have to be taken into account.

The other factor that a lot of people forget is that GDPR is an ongoing set of laws, so carrying out a GDPR compliance exercise once and then forgetting about it simply does not work.

Don't ignore GDPR!

Fines of £17.5 million or 4% of global turnover could easily bankrupt an organisation.

What makes your business an exception?

WHAT'S ON OFFER?

The most important side of GDPR is what is known as Personally Identifiable Information (PII). This is information that can identify someone, or at least partly identify someone, with data such as name, address, bank account, credit card number and the list goes on and on.

Critically there is a requirement to identify this PII and to know where it is located within the IT infrastructure, no small task right!

Fortunately, our data mapping tool takes care of all of this for you. It scans for unsecured data across a network – even in persistent storage – and provides an estimated financial figure for an organisation's potential liability in the event of a data breach. This allows us to discover areas that need attention and to prioritise the next steps to get you GDPR compliant as quickly as possible.

Once the data mapping has taken place, you are presented with "actionable" information that clearly shows which file the PII data is in and what the PII data actually is, such as a credit card or bank account number.

Contact us today for more information **0330 043 1723**

CYBER ESSENTIALS

The Cyber Essentials scheme is a cybersecurity standard, which organisations can be assessed and certified against. It identifies the security controls that an organisation must have in place within their IT systems in order to show that they are addressing cybersecurity effectively and mitigating the risk from Internet-based threats.

There are two types of certification: Cyber Essentials and Cyber Essentials Plus. The first is the basic standard focusing on:

- Boundary Firewalls and Internet Gateways
- Secure Configuration
- Access Control
- Malware Protection
- Patch Management

What does it do?

Cyber Essentials helps you to guard against the most common cyber threats and demonstrate your commitment to cyber security

If you choose to go for Cyber Essentials Plus, the key differentiator is the inclusion of a technical review of the organisation's workstations and this additional phase of testing increases the validity of certification considerably, by providing evidence of compliance against the following scenarios:

- Can malicious files enter the organisation from the Internet through either web traffic or email messages?
- Should malicious content enter the organisation, how effective are the anti-virus and malware protection mechanisms?
- Should the organisation's protection mechanisms fail, how likely is it that the organisation will be compromised due to failings in the patching of the organisation's workstations?

Cyber Essentials Plus is a more thorough assessment of the organisation and, as a result, may provide greater security assurance. However, it does come at an additional cost, which will factor in the decision-making process. Ultimately the decision on which level to certify against will be influenced by an organisation's cybersecurity stance and those of its business partners, suppliers, and stakeholders.

Once an organisation has been assessed against the Cyber Essentials security criteria and passes, it will receive the relevant Cyber Essentials award (badge) based on the level of certification achieved, which demonstrates it has achieved a fundamental level of cybersecurity.

Contact us today for more information **0330 043 1723**

PENETRATION TESTING

Penetration testing, which is also called pen testing or ethical hacking, is the practice of testing a computer system, network or web application to find security vulnerabilities that an attacker could exploit. Penetration testing can be automated with software applications or performed manually. Either way, the process involves gathering information about the target before the test, identifying possible entry points, attempting to break in – either virtually or for real – and reporting back the findings.

How secure is your network?
20% of all vulnerabilities discovered are High or Critical Risk
What measures have you taken to be secure?

SECURITY AUDITS

Are you prepared for today's security threats?

Today's complex security landscape can be difficult to navigate on your own. Cyberattacks are an ever-increasing threat, users demand greater mobility, and the amount of data you must protect continues to grow year after year. In today's IT world, it's no longer a matter of 'if' a security breach will occur; it's a matter of when.

In order to be prepared, you must fully understand your risk. You need an accurate picture of the security risk profile for the assets, applications, and services that you are managing at all times. You need a partner who understands how to help you protect your organisation effectively and efficiently. Our experts can address your most critical security needs, stringent compliance requirements, and complex technology challenges – with a deep understanding of your unique environment, needs, and goals.

How well do you know your security procedures?
Have your own digital security partner highlight your vulnerabilities and work with you to ensure you do not fall a victim to cyber threats.

A security audit can help highlight which vulnerabilities are exploitable, which risks are critical – and therefore need to be addressed with a high priority – and which items can be remediated over time.

An audit generally takes the form of internal technical testing, penetration testing, or ethical hacking from the outside. The goal is to determine whether or not any of the services that your organisation is operating have any types of flaws in them – and, more importantly, whether or not those flaws can be exploited by somebody with the right skill set and motivation.

Contact us today for more information **0330 043 1723**

turremgroup

turremgroup
Watchoak Business Centre
5 Chain Lane
Battle
East Sussex
TN0 33GB

www.turremgroup.com