# Third Party Assessment

## ARE YOUR SUPPLIERS THE WEAKEST LINK IN YOUR SECURITY?

However secure your own environment, how can you be sure your data is safe when it is in the hands of others? The rapid growth seen in outsourcing of business processes means third party suppliers and partners are increasingly trusted with access to systems and sensitive information.

Robust policies, procedures and practices may appear to be in place, how can you be sure they are being followed? Even if the suppliers you work with can demonstrate a good level of information security, it may fall short of your own standards.

While outsourcing offers significant business benefits, failing to understand and deal with the risks could leave you open to costly and damaging information security breaches.

## THIRD PARTY INFORMATION ASSURANCE

Many of the most recognised international standards for security and data protection best practice such as ISO 27001:2013, Payment Card Industry Data Security Standard (PCI DSS) and the General Data Protection Regulation (GDPR), have a significant focus on the assurance of security and governance standards for third parties within the supply chain.

The forthcoming PCI DSS changes in January 2018 will increase the need for third party "service providers", with the potential to impact the security of cardholder data, to demonstrate PCI DSS compliance both for themselves and as part of their merchant clients' PCI DSS compliance.

GDPR requirements also add a layer of assurance requirements with the need for accountability to be demonstrable through an organisations' third party suppliers and data processors.

It is clear that organisations should identify third parties and take a prioritised approach to gaining satisfactory assurance for those where there is a risk of data or security breach or non-compliance against standards.

**Information security breaches can lead to serious consequences including:**

- Damage to reputation;
- Loss of current and potential clients;
- Legal liability and litigation;
- Financial penalties;
- Increased vulnerability to hacking;
- Leaking of commercially sensitive information;
- Negative publicity; and
- Regulatory breaches.

The increasingly extensive and complex nature of outsourcing arrangements means a number of different suppliers can be working with your company at any given time, with varying security and data protection implications.

Managing this can be costly and time consuming and in response to a growing need, Gemserv has been delivering a tailored service to help businesses and organisations for the past seven years.

Our Third Party Information Assurance service provides a risk based, robust and independent assessment of your current and future third party suppliers to protect against potential risks.

## WHAT WE OFFER

Our assessments provide complete peace of mind that external organisations comply both with best practice and your specific requirements.

Gemserv's extensive sector experience means we look to ensure a collaborative working partnership rather than becoming a barrier between you and your suppliers. We encourage a proactive, rather than reactive, approach to the secure handling and management of information.

Our services range from one-off third party risk assessments of a particular supplier or project, through to a fully managed service where suppliers are regularly audited based on risk classification. This then enables clients to identify trends and potential issues and maintain their own levels of compliance cost-effectively.

## HOW OUR PROCESS WORKS

As a first step we conduct an assessment of your potential third party information security requirements. This is delivered on your own premises.

We would then conduct an extensive review of the nature of the service provided by each third party supplier within scope, looking at how the relationship works in theory and practice and the extent to which the supplier could affect the security of your information assets. We will also examine any contracts and Service Level Agreements (SLAs) in place.

These assessments are tailored for your suppliers' specific industry sector and the nature of the services provided.

An independent risk assessment will then be conducted by our expert team to confirm that the correct information security requirements are in place and are being implemented to client, contractual and best practice requirements.

We will liaise with the third party supplier for clarification on any points, and if necessary request documented evidence.

If any areas of serious concern are identified we will bring these to your attention and an on-site risk assessment focussing on the key concerns will be recommended.

Where issues are identified, we will highlight these and provide practical advice on how to address them. Our aim throughout this process is to help ensure a continuing relationship between your organisation and the third party.

We also offer ongoing assessment to ensure suppliers maintain best practice, providing peace of mind that they continue to operate to the high standards you expect.

**What we provide:**

- Comprehensive review of potential third party information security needs;
- Bespoke third party supplier security assessments through questionnaires, telephone assessments and on-site assessments;
- Independent and impartial assessments of suppliers;
- Validation of compliance with standards such as ISO 27001 and PCI DSS if required
- On site consultancy if required; and
- Global coverage can extend service to international suppliers.

## CONTACT US

To find out more about third party protection, please contact one of our team on:

E: bd@gemserv.com
T: +44 (0)207 090 1091
W: www.gemserv.com
@gemservinfosec

**London Office**

8 Fenchurch Place
London
EC3M 4AJ

**Ireland Office**

Fitzwilliam Hall Business Centre
Fitzwilliam Place
Dublin 2

Company Reg. No: 4419878