**We are I.T Architects and Cyber**

**Security Providers.**

**Cyber Security Solutions and Services**



Dezant Consulting

**About Us**

Delta Consulting is a UK listed expert in I.T Solution Architecture, Cyber security and Risk mitigation, working with governments and businesses in US, Europe and Africa to protect their brand, value and reputation against the ever-evolving threat landscape. As the cyber arms race continues to outpace the ability of organisations to cope with security, performance and availability issues, we are best placed to help organisations identify, assess, mitigate & respond to the risks they face.

When it comes to cyber security, business continuity and other I.T & Telecom services, working with Dezant Consulting is one of the only ways to ensure your back is covered and you can focus on your core business.

**We offer Specialist expertise, Access to a worldwide network of technical specialists,**

**A trusted partner in the event of a cyber-attack, and we give on-going advice & briefing**

* We deliver to clients with love which reinforce our commitment and diligence.
* We uphold trust key in our area of delivery acknowledge that no organisation can thrive without being trustworthy.
* We resolve with our clients on the need to manage cost without compromising productivity and quality.

Services

**SERVICES**

Security GAP Assessment

Most organisations continue to invest in technology and services to reduce their risk exposure. However, it is common for businesses to direct investment and select controls that have little or no material impact on reducing the threats posed by cyber attackers. Often, these “next generation” technologies are procured as a result of media scare mongering or vendor misdirection, and over emphasis on their specific technologies.

Dezant Consulting unique GAP assessments, also often called maturity assessments, carried out by our leading team of experts, can help you swiftly:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

• Summarise your investments to date.

• Identify areas of strength and qualified domain practices, and vulnerable or weak controls.

• Identify weaknesses in your compliance against standards such as PCI-DSS, ISO 27001:2013, GDPR, TOGAF-SABSA and other HMRC frameworks.

After the analysis, we publish a report that details the findings of our gap analysis and ensures that our findings are easy to understand for the business executive.

Areas of a Security GAP Assessment

We can carry out a GAP assessment in the following security and compliance domains:

• GDPR.

• ISO 27001:2013.

• PCI-DSS.

• Cyber Essentials & Plus.

• SANS TOP 20.

• SOX (IT related).

• Cyber Incident Response.

• Cyber Crisis Management.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Data Security & Governance

A critical path to information governance involves putting in place correct data definitions that the organization

as a whole can use to better understand information. While a full understanding of business context and meaning resolves ambiguity and leads to more accurate decisions, users often require more detail behind their data. Understanding where the data is coming from—and who modified it and

when—significantly affects its value, authenticity and accuracy.

Under the GDPR, ‘personal data’ means any information relating to an identified or identifiable natural person; an identifiable

natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an

identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental,

economic, cultural or social identity of that natural person.

For example, information that you might immediately think of as Personal Data (e.g. Name, Email Address, Medical History,

etc.), any other information which can be linked to an individual (which might include, for example, IP Address, IMEI, IMSI, Location,

etc.) is also within the scope of the GDPR as Personal Data.

Non-compliance with GDPR can result in heavy fines and increased regulatory actions. More importantly, however, significant breaches can damage an organisation’s brand, value, and reputation. Protecting the brand requires that an organization that collects personal data must be able to prove it consistently and reliably complies with the GDPR privacy and security principles.

The path towards GDPR compliance includes a coordinated strategy involving different organisational entities including legal, human resources, marketing, security, IT, and others.

Dezant Consulting can help Organisations to have a clear strategy and action plan to address the GDPR requirements with an eye towards the 25 May 2018 deadline and beyond.

Third Party Security Assessments & Audits

Third parties remain responsible for a large number of high profile cyber-attacks including Private and public organisations, amongst others.



With the ever-increasing dependency on outsourcing, it is imperative for businesses to manage risks posed by third parties. Leaving the backdoor unlocked is simply not an option.

Some third parties that could pose a risk to your organisations are:

* Web hosting providers.
* Data centres.
* Web and application development companies.
* Payment providers and gateways.
* Call centres.
* Customer service centres.
* IT service outsourcers.
* Managed service providers.
* Auditors.
* HR outsourcers.

All of the above can be high valuable targets as they may hold customer/employee data, intellectual property or credit card data, the theft or distraction of which can cause an organisations significant pain both financially and to the reputation of the business.

Dezant Consulting can support your organisation to establish and implement processes to reduce your supply chain risk by:

* Reviewing and improving supplier risk management processes and frameworks.
* Reviewing and improving operational information security controls.
* Assessing a supplier's baseline security posture.
* Reviewing and improving response in depth controls.