**Phone numbers**

+44 7448147604

+44 7459657995

E-mail: [info@dezantconsulting.com](mailto:info@dezantconsulting.com)

**Services**

**Cloud Security Services**

**“**When it comes to the subject of cloud security, cloud providers and cloud users must uncompromisingly pull together and work with one another. After all, both have a goal and each has an awful lot to lose: for the cloud users it is their likely critical data, and for the cloud providers it's their reputation and, ultimately, their business”

**Cloud Monitor 2019, KPMG and bitkom research**

Our architects have expert knowledge of Cloud security architecture, strategies and standards to determine, develop and deliver comprehensive security requirements as an advisor for potential cloud solutions. Our security architects can use industry toolkits designed for peeling back and revealing those layers of accountability and responsibility between Cloud Service Providers and their Tenants, applying measurable risk-based decision making for both assessing and attesting to governance, risk and compliance best practices.

**Selecting the appropriate cloud model**

Whether private, public, community, or hybrid; and hosting scenarios: internal, external, or combined, whatever cloud model you are considering adopting, we can help you importance of what you are considering moving to the cloud and which of the models (IaaS, PaaS, SaaS) can work for your own risk tolerance

**Aligning cloud security to your information security program**

We can assist aligning your information security program using best practice tools with emerging cloud security requirements such as CAMM (Common Assurance Maturity Model).

**Public Cloud Services**

Hosted by third-party cloud service providers (eg. Amazon Web Services (AWS), Microsoft Azure, Google Cloud) and generally accessible through web browsers, so identity management, authentication, and access control are essential.

**Private Clouds**

Usually dedicated and accessible to only a single organization. However, they are still vulnerable to access breaches, social engineering, and other exploits.

**Hybrid Clouds**

Combine aspects of public and private clouds, allowing organizations to wield more control over their data and resources than in a public cloud environment, yet still be able to tap into the scalability and other benefits of the public cloud when needed.

**Improving your security posture, with cloud**

While much has been said for the potential risks of using cloud services, the reality is, many businesses can actually improve their security posture by adopting cloud services where the security controls and internal governance imposed are actually far beyond what they are actually doing in house. We shine the light not only on the risks, but on the tangible benefits of improving your current on-premise services, by moving in to the cloud.

**What Cloud Security Brings to You**

* Guidance to define an effective security strategy to protect cloud environments and data in the cloud.
* Assistance to deploy new technologies like Cloud Access Security Broker and Security Posture Management, as well as ongoing tuning and optimization.
* Protection to stop threats from penetrating cloud environments and executing malicious actions.
* Detection of malicious activity throughout all phases of the attack kill chain, with the goal of minimizing dwell time.
* People, processes, and technologies to help prevent or minimize the damage cyber threats can cause.
* Specialized training to help reduce risk and equip staff with knowledge and tools.

**Clients and Partners**

UK Public and Private sectors

Partners: **Delta3**





**Goldwyns is a Firm of Chartered Accountants**

CISSP Certification Course Overview

The CISSP certification training develops your expertise in defining the IT architecture and in designing, building, and maintaining a secure business environment using globally approved information security standards. The course covers industry best practices and prepares you for the CISSP certification exam held by (ISC)².

CISSP Training Key Features

* 67 hours of in-depth learning
* 5 simulation test papers to prepare you for CISSP certification
* Offers the requisite 30 CPEs for taking the CISSP examination

**Accelerated CISSP training**

Developed by (ISC)2, the world’s leading cyber-security membership association, this international information systems security certification is key for professionals aiming for senior roles in the field. With Firebrand, you’ll build the expert knowledge needed to implement and manage an enterprise security programme.

On this accelerated course, you’ll study the eight domains of the CISSP Common Body of Knowledge (CBK):

* Security and Risk Management
* Asset Security
* Security Architecture and Engineering
* Communication and Network Security
* Identity and Access Management (IAM)
* Security Assessment and Testing
* Security Operations
* Software Development Security



**Workshop & Seminar**











Reuben’s picture