Dezant Consulting http://www.dezantconsulting.com/index.asp



**HOME**

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

**Security Providers.**

**Cyber Security Solutions and Services**

**ABOUT US**

**TRAINING**

**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.

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

Governance, Risk and Compliance

The compliance and risk landscape is an increasingly complex world of new mantras, hot topics and flavours of the month. To remain competitive, organisations must have a governance, risk management and compliance (GRC) strategy that tracks legislation, regulatory compliance and stakeholder expectations.

Dezant Consulting’s experience and expertise in both the assessment and management of information risk helps our clients tackle the broad issues of governance, enterprise risk management and effective compliance. We work with our clients to formulate and implement a GRC strategy to:

* Improve strategic business decisions needed to be made.
* Identify critical assets and their associated value.
* Identify threats, threat actors and threat sources for high value assets.
* Measure the likelihood that a threat will exploit a vulnerability.
* Use effective monitoring to minimise potential incidents and reduce risk.
* Increase efficiency to avoid fines, penalties and damage to reputation.
* Have a consistent and clear view on risk and risk appetite.
* Protect brand by capitalising on business models with minimal risk.
* Communicate effectively with stakeholders.
* Become compliant with governance and regulatory requirements.

This helps organisations identify, remediate, monitor, exploit and manage enterprise risks, as well as coordinating the utilisation of people, process and technology to improve GRC effectiveness and manage costs.

Security Architecture & Design Reviews

A well-designed security architecture defines and creates a uniform and consistent set of security processes, information security management systems and ensures that these align with an organisation's core goals and strategic direction.  Put another way, a badly designed or non-existent architecture leads to the famous age old adage of having to fit a square peg into a round hole.



A well designed security architecture takes into consideration several change drivers including:

* Business and technology roadmaps.
* Legislative and legal requirements.
* Threat landscape and threat intelligence.

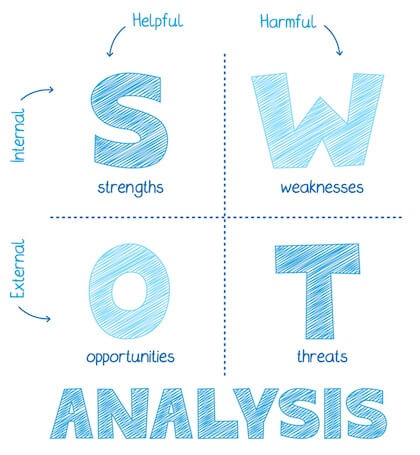
Furthermore, a properly implemented security architecture must achieve certain key objectives including:

* Provide structure, coherence and cohesiveness.
* Enable business-to-security alignment.
* Define a business strategy-driven security architecture and technology implementation.
* Ensure that complicating factors, such as geography and technology, have little impact on the overall architecture.
* Establish a common "language" for information security within the organisation.
* Dezant Consulting will work with organisations to develop a comprehensive and effective security change management program.

Security Strategy and Roadmaps

Dezant Consulting provides cyber security advisory services throughout the security lifecycle, helping with cyber security strategy, planning and ongoing program improvement. Our expert and experienced consultants can support you with the development of comprehensive information security strategies that are effective, manageable and offer maximum return on security investments while addressing emerging threats/risks specific to an organisation's business operations.

We work with organisations to develop a comprehensive risk-based security program, seeking expert oversight to enhance an established program or looking for specific guidance for major elements of their security program.



Dezant Consulting will:

* Develop a comprehensive information security framework for:
  + Information protection and Information Risk Management;
  + Incident prevention and detection;
  + Incident response based on organisation risk and industry best practices.
* Assess current programs to ensure that they meet business objectives.
* Create a strategy to align a security program to business requirements.
* Achieve greater benefits and returns from security budgets.
* Assess how security capabilities facilitate risk and regulatory compliance management.
* Align with industry trends, business dynamics and risk appetite.
* Create detailed project plans with ownership, timelines and resource allocation.
* Develop a roadmap for implementing the required security capabilities to close identified gaps and help reduce risk.
* Communicate the security strategy and roadmap to business executives and stakeholders.
* Define roles and responsibilities needed to develop a more robust security solution.
* Measure your security posture and progress toward security goals.

Security Change Management

Information security processes and controls are often not considered as part of the well-established change and configuration management frameworks. Organisations build secure technological infrastructures and conduct penetration testing to identify vulnerabilities, but there is often no ongoing security maintenance leading to security failures. These failures can be put down to a number of inherent issues:



• Disparate systems with no oversight or joined up management.

• Slow change management leading to processes being circumnavigated, ignored or no joined up decision-making.

• Security not built-in, but bolted on after the event.

• Legacy thinking rather than agile planning.

• Poor succession planning for legacy platforms.

• Lack of security process maintenance.

• Management out of the loop with corporate protection

Increased security concerns have a direct consequence on the number of changes (i.e. patch installations to remediate vulnerabilities, configuration changes to block attacks, etc.) requested. Often these changes are planned, driven by security or compliance requirements, the introduction of advanced technologies or other requirements, but sometimes the changes are driven by urgency when systems/applications/networks are under attack.

We will work with organisations to develop a comprehensive and effective security change management program.

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 organisation 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 organisation 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.

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.

**Our Team**



Anthony Omomia, **MSc. MBA** Cyber Security Architect / Managing Partner

Having worked for big service providers such as DXC, HPE, CSC, Infosys, Capgemini in the Public, Financial, Retail, Pharmaceutical, Manufacturing, Telco, Aviation, Oil & Gas Industries as Technical Security Architect, Cyber Security SME, Infrastructure Consultant / Data / Application & Solution Architect, I have acquired sound Technical and Commercial skill sets in order to effectively perform in a varied and complex environment.

* Over 20 years’ experience designing, implementing and supporting IT projects within a variety of business sectors and scale, public and private sectors (i.e. Retail, Utility, Pharmaceutical, Telco, Manufacturing, Aviation, Oil and Gas, Banking & Finance). Self-motivated with strong knowledge of Technology and Security topics, Architectural, Project management, Team Leadership, Communication and Interpersonal skills.
* Previous Responsibilities includes infrastructure design and scoping projects and deliverables across multiple technical disciplines and recommending technical solutions, and undertaking technical project coordination.
* Also, I’ve been responsible for capturing and analysing customer requirements (Functional & Non-functional), scoping project deliverables & recommending best of breed technologies, including products, vendors and architecture across multiple technical disciplines.
* Architecting & Designing end-to-end security infrastructure - design/management of multi-vendor products including:
* Experience in scoping, estimating and planning infrastructure related initiatives; researching the current and future strategy, market trends and architecture for Platforms, Networks, Storage, and overall data centre Technology including risk assessment.



Banji Oyeniran **MSc., MBA.** (Public Sector Advisor) ICT.

Executive MBA, Imperial College, London UK, MSc. IT Management, London South Bank, UK

Banji’s experience covers ICT management within the public sector, procurement of IT goods and services, contract management and negotiations, tender evaluations, contract reviews, specification writing, user requirement gathering, stakeholder liaison to successful project implementation within budget, scope and timescales.  
  
ICT category analysis, contract monitoring voice and data projects, OJEU tender evaluations, stakeholder relationship and third party vendor management.



Bibian Ogbuji, **PHD**

Data Analytics Consultant

Current research projects focus on interdisciplinary applications of computer science and engineering in the area of flow back and produced water (FPW) characterization, FPW treatment technology, and data analytics in the oil and gas industry. Areas of expertise include machine learning, data analytics, programming, big data, platform implementation/evaluation, digital strategy, database development, data processing, and visualization.

Reuben Ogundeko, BSc ICT (Automation & DevSecOps) SME

Specialized in Software Discovery/ Packaging/Deployment and expertise of Application Virtualization (App-V), MSI technology (Windows Installer), Application Remediation, Wise Package Studio, AdminStudio, SCCM 07/2012/2016 (Package Creation/Deployment and Troubleshooting) Scope, design, development, configuration, implementation & support of SCCM 2012 infrastructure, App-V Infrastructure, Dell Workspace, VMware ThinApp, Symantec Workspace Virtualization, Wise Composer, BMC Marimba Software, Blade Logic, System Administration, Implementation, Testing, Documentation, Production support, End-User support and Requirements gathering