

IT Architecture Consulting

The top-down structuring of infrastructure is the main activity of an architecture consultant. Someone who can ‘tie several silos of expertise together under the constraints of cost effectiveness optimization’.

Extensive experience in a holistic consulting environment, a sound knowledge of methodologies and a broad knowledge of leading technologies are the characteristics of S&T Architecture Consultants.

The outcome of IT architecture consulting is a consistent, structured and appropriate infrastructure platform compliant with SLAs (Service Level Agreements) and derived from business objectives.

These high-level consulting services cover all the major strategy-driven infrastructure taxonomies and interdependencies, such as:

- Availability - covers IT services continuity, including disaster recovery
- Integrity - covers backup/recovery, replication and de-duplication
- Confidentiality - covers comprehensive information security
- Compliance - covers archiving, legal audit ability
- IT Governance - covers performance, scalability and manageability

“**Availability**” means the strategic and operational capability of an organization to plan for and respond to incidents and disruptions in order to continue IT services at an agreed predefined level.

S&T consultants help customers to pursue structured processes that identify potential risks and evaluate their impact on IT operations. The outcome is a documented Services Continuity Plan for building organizational resilience to mitigate IT operation disruption.

Based on such continuity plans, S&T consultants help customers to design and implement an IT Services Continuity Management (SCM) strategy based on the methodologies of BS 25999 and ITIL standards.

“**Integrity**” means a structured and consistent backup/recovery plan, based on agreed recover time objectives (RTO) and recover point objectives (RPO), which are the result of Data Classification.

The S&T consultants support customers to choose the most appropriate technology (continuous data protection, backup to disk, daily full/incremental backup, replication, de-duplication) for meeting



RTO/RPO objectives and adapting recovery operations to fully meet the given business constraints on data integrity.

Confidentiality requires the existence of a security policy and standards that are approved and owned by the company's management. It provides a company-wide, high-level description of the regulations and controls required to protect data and transactions. This policy document is based on the results of a risk assessment.

In order to bring these policies to fruition, S&T consultants help to design and implement an information security management system, which consists of awareness training, adaptations to processes and controls, and auditing standards and technology on the basis of the ISO2700X standard.

“Compliance” related to storage means the audit-proof retention and retrieval of business-relevant data, with a particular focus on e-mail. Data classification specifies the applications affected by compliance regulations and a policy-driven Information Lifecycle Management (ILM) helps to manage the given retention periods and the real-time archiving in an audit-proof storage platform, thus securing a compliant archiving process.

IT Governance includes the appropriate sizing and scalability of capacities, the optimization of infrastructure by means of virtualization and the reduction of complexity by means of consolidation. Furthermore, a suitable management system, with policies for intervention and filtered alerting, and a structured service strategy, helps to manage the infrastructure at optimum cost by applying value based ROI (Return on Investment) models.

S&T consultants streamline such infrastructure tasks, guided by ITIL recommendations, in order to tap into the full potential of standardization and virtualization. But also to put system management and processes in place that achieve a high level of operational transparency and provide efficient procedures to counter possible incidents.