

Technology Risk and Business Continuity Management



A simple philosophy. Helping clients succeed.

Kingston Smith Consulting LLP is the leading business protection consultancy providing proven solutions to the real threats and challenges faced by your business. Major losses can take the form of a single incident or a prolonged leakage of value, Kingston Smith Consulting has a range of services focused on preventing those losses or minimising their consequences. Avoiding the negative outcome means taking control of risk management, technology, key third parties, execution of change, legal and regulatory compliance and basic business controls. With solutions to address these challenges, Kingston Smith Consulting will help you protect your business for the long term.

Our experience. Your development.

Working with our clients, often at the heart of their critical business initiatives, the success of each engagement is built on our strong service values:

- We **deliver solutions**, defining and agreeing the outcome you require and charging the price which achieves that end, so that you will always understand the cost and benefit of our services.
- We focus on achieving **return on investment**; we measure our success on the value you realise. This means solutions delivered to your specific needs and not someone else's template.
- We **bring expertise** and experience to every engagement. Every consultant in our team has a record of successful delivery in their field of expertise.

- We **build capability** in our clients, through training, coaching and mentoring, through open access to our methodologies and intellectual property; on every engagement we aim to move our clients closer to self-sufficiency.

Technology

Technology can be transformational in helping to deliver significant business improvements and yet it brings with it some of the greatest and fastest changing threats. With technology taking an ever growing proportion of corporate spending it now represents the major concentration of risk and reward for many businesses. Kingston Smith Consulting's technology solutions are based on two principles: the need for high levels of technical skill to address technical threats, and awareness that many of the greatest losses come from 'routine' risks which are not addressed effectively.

Business continuity

Every organisation needs to ensure that the impact of the unexpected is minimised. Those who are least prepared are the most likely to be unable to survive a disaster. Kingston Smith Consulting can help you to fully understand how business continuity management and its related disciplines apply to your organisation and complement a broader risk management framework. We can provide guidance and assistance with your continuity requirements and help you mitigate the risks impacting critical business functions, technology, resources and infrastructure. This will put you in the best position possible should the worst happen, and assist in preserving your profitability, competitive advantage and reputation.

IT Governance and Risk

IT Policies, Standards and Procedures Development –

Evaluation and/or creation of documentation used to establish a governing framework around IT or related controls. Kingston Smith Consulting can create the documents through facilitated sessions and interviews whilst incorporating best practice.

IT Risk Management – Create or assess the IT control framework. A risk assessment will identify redundancies, inefficiencies, weak controls. Risk mitigation plans would then be designed and implemented.

Monitor/Manage IT Controls – Monitoring helps ensure that internal controls continue to operate effectively. Kingston Smith Consulting can assess the effectiveness of current monitoring methods and suggest solutions and tools to enable more efficient monitoring.

Process Improvement – We bring a systematic approach to identify and analyse IT process improvement opportunities using a variety of methods such as benchmarking, continuous quality improvement, Six Sigma, CMMI (Capability Maturity Model Integration) or Lean. We can facilitate full process re-engineering – a process improvement involving multiple processes across an organisation and requiring a great deal of change.

IT Value Management – Evaluation and selection of IT investments, benefit realisation, delivery of value (Val IT). Kingston Smith Consulting can assess the current procedures in the investment decisions and recommend widely accepted methods to implement metrics, measure the value obtained, and establish decision points.

IT Cost Management – Kingston Smith Consulting can assist you in measuring and optimising IT costs. Our approach follows five distinct but related work streams:

- Financial Baseline – Linking costs to services, providing management with an organisational budget mapped to service lines.
- Benchmarking – Comparing IT expenditure against industry benchmarks, identifying key areas of cost over or under-utilisation in order to determine whether the IT budget is considered low or high by industry standards.
- Assets – This determines how efficiently items are being used in the organisation and identifies the degree of standardisation and duplication. This assists in identifying potential asset candidates for retirement or consolidation.
- Project – Assesses all IT-related projects against their contribution to business objectives. This allows projects to be categorised as essential or discretionary, which in turn provides management with a prioritised list of all projects, detailing the deliverables and financial return on project investment.
- IT Management – Deliverables are based on COBIT (Control Objectives for Information Technology), which enables the development of clear policy and best practice for technology control. It importantly assesses the alignment with the corporate strategic objectives using proven methodologies (eg Balanced Scorecard). It allows the development of the appropriate technology change management and governance programmes.

Programme Assurance

IT Programme Management – Integrated processes, tools and templates to plan, manage, control and execute change. Based on size and complexity, services can be delivered at either a project or programme level.

Project Support Office – Provision of technology professionals with specialised skills on a temporary or a whole project basis. Kingston Smith Consulting will typically augment your own staff.

Technology Requirements Specification – Identify the specific user requirements, functions, and business rules for the system and then broadly analyse these to identify appropriate technical solutions and options.

Project/Application Pre- and Post-Implementation Review

– Pre-assess project preparedness to enter the execute phase using an accepted methodology such as PRINCE2. Post-implementation review is conducted some months after implementation to evaluate the achievement of the project objectives and identify any lessons to be learned.

Off-Shoring, Outsourcing, Call Centres and Shared Services

– Explore efficiencies across the enterprise and identify support delivery more focused on customer needs. Shared services are more than just centralisation of consolidation of similar activities on one location; to be most cost-effective, this means running these service activities like a business. We can provide input to the relevant contracts and service level agreements to maximise results and ensure that the requirements of the client are not compromised. The following are services we can provide:

- Offshoring and Outsourcing
 - Governance and Risk Management
 - Internal Audit and Best Practice
 - Application Development and Maintenance
 - Call Centre Thought Leadership
- Vendor
 - Selection & Proposal Evaluation
 - Due Diligence
 - Pre- and Post-Contract Review
 - Governance Framework
 - Self-Assessment
 - Service Level Management
 - Contract Management Review
- Call Centres
 - Internal Audit and Best Practice Reviews
 - Onshore/Offshore Governance
 - Technology - Service Delivery Enablers
 - IT Cost Reduction
 - Benchmarking
 - Effectiveness Measuring
- Business Continuity Management (BCM)
- Business Process Outsourcing (BPO) and Shared Service reviews
- Compliance with Legal and Regulatory Requirements
- Sourcing – Supplier Risk Management/Service Management
- Supplier Performance Management, Monitoring Delivery of Services
- Third Party Supplier IT Security Management/Assessment
- Exit Strategy developing and Exit Plan (Managing geopolitical risk/supplier failure/service level failure)

Information Security Governance (ISO 27001) – We can advise on a security governance framework and strategy appropriate to any organisation; produce suitable policies, procedures and security infrastructure; and design and implement a relevant information security awareness programme for all staff.

Security Risk Management – Kingston Smith Consulting can create and maintain a risk management framework relevant to the organisation. The framework documents a common and agreed level of IT risks, mitigation strategies and agreed-upon residual risks.

Vulnerability Analysis – A process that defines, identifies, and classifies the security vulnerabilities in a computer, network, or communications infrastructure.

Web Application Security Review (OWASP) – We can perform a specialised vulnerability analysis on internet facing applications to assess potential security exposures in their implementation.

Penetration Testing – The perimeter of a network where it connects to external sources (eg the internet, or a third-party's own network) is a potentially weak area of defence, and should be regularly tested to provide assurance over its integrity. Kingston Smith Consulting has staff with appropriate specific skills to perform this work using a range of tools.

Incident and Response Management – Timely and effective response to IT user queries and problems requires a well designed and well-executed service desk and incident management process. Kingston Smith Consulting can assess the process, technology and organisation using a relevant maturity model.

Identity Management – All users (internal, external and temporary) and their activity on IT systems (business application, system operation, development and maintenance) should be uniquely identifiable. We can ensure that cost-effective technical and procedural measures are designed and deployed.

Data Encryption – Encryption is one of the mechanisms used to protect the most sensitive data, but needs to be implemented carefully to be cost-effective, manageable and legal. We can devise and implement the most appropriate encryption architecture for any organisation.

Security Awareness Training – The design, implementation and roll-out of a programme of regular training to ensure that all staff in an organisation are aware of their security role and responsibilities.

Security Architecture Design – Implementation of a framework covering personnel, hardware and software to protect an organisation's assets most cost-effectively. This may also include the assessment or specification of appropriate physical security and environmental controls.

CLAS – The Public Sector including the UK government requires work to be performed by CLAS certified consultants who have appropriate technical skills, understand government methodologies and techniques; and have appropriate security clearances to ensure security. We can provide CLAS consultants certified up to level 3 to provide the Public Sector and UK government with Information Security and Assurance related services.

Service Delivery and Support – The IT Infrastructure Library (ITIL) comprises recognised best-practice in areas such as incident management, problem management, change management, release management, configuration management (see below) and the service desk; also service level management, capacity management, availability management and IT continuity management. We can assist in the implementation of an ITIL-compliant function, or perform reviews in each of these areas.

Configuration Management – Physical and logical architecture of internal networks, platforms, hardware, software, security components, source code management or revision control, test environments, test documentation, databases, and applications.

Application Audit – Perform a specific audit of a single application. Application audits can also pertain to a business process that relies on multiple IT systems. We typically examine controls in administration, inputs, processing, outputs, etc.

IT Infrastructure Audit (operating systems, databases and network) – Assessment of logical access, data protection, interfaces, data transmission etc.

IT Audit – Kingston Smith Consulting can perform the entire process of collecting and evaluating evidence of an organisation's information systems, practices, and operations; or supplement an existing function. We use COBIT as recognised best practice control objectives.

Regulatory Audits – We work with the client organisation to define the scope of the survey, then we assist you to evaluate a programme fairly against relevant legal and regulatory requirements. We have staff experienced in Sarbanes Oxley, Data Protection Act, Basel II, MiFID, HIPAA, amongst others.

SAS70 Assessment – Reviewing of contracts, procedures, controls regarding the transaction processing of a service organisation. If you need to prepare a SAS70 we can develop the document, identify control gaps and help you remediate them. For an existing SAS70 we can act as the independent auditor performing the required testing and issuing the audit report.

PCI – Evaluation of compliance with the Payment Card Industry Data Security Standard (PCI-DSS). Such compliance is designed to assist organisations handling credit card data to protect themselves against the threat of security breaches. As a fully accredited Qualified Security Assessor firm we are able to certify that your security controls satisfy the Standard, advise on where remediation is necessary, and complete the necessary reports. We can assist with PCI scoping to help limit the amount of work needed to be performed and provide assistance with the completion of Self Assessment Questionnaires for smaller organisations.

ERP – We work with industry-standard enterprise resource planning packages eg SAP, Oracle, etc and can provide consulting and audits related to these ERP packages.

End-User Computing – Reviewing the controls associated with technology outside the traditional IT environment, especially assurance over critical spreadsheets etc

Data Management

Data Architecture Review – Data architecture defines how data is stored, managed, and used in a system. It establishes common guidelines for data operations that make it possible to predict, model, gauge, and control the flow of data in the system. We can review the architecture to ensure that it best fits business requirements.

Data Privacy – This offering covers collection, storage, processing, retention and disposal of sensitive personal data. Our provision encompasses a review of existing policies, standards and procedures in place to achieve compliance. Where appropriate we would structure our work around relevant legislation.

Data Analytics and Forensics – These processes are employed to identify data errors (which may in turn identify system bugs) or fraud. We have skills and experience in data analytics tools such as ACL, IDEA, etc.

Storage Architecture – This relates to the physical nature of the infrastructure that stores corporate data, and the relationships between the various components. We can design and implement a cost-effective solution.

Data Warehousing – A data warehouse is the main repository of an organisation's historical data. It contains the raw material for management's decision support system. The critical factor leading to the use of a data warehouse is that a data analyst can perform complex queries and analysis on the information, such as data mining, without slowing down the operational systems. We offer the design and implementation of such a solution, including optimisation according to business requirements.

Business Continuity Management

Operational Resilience Review – The overall assessment of business continuity, disaster recovery, and emergency operations. Kingston Smith Consulting can identify potential impacts that threaten an organisation, and provide a framework for building resilience and the capability for an effective response. We can assist with an organisation's accreditation with BS25999.

We can also perform or review the following individual components of the BCM programme:

Business Impact Analysis – Identifying the business processes deemed critical to the client's ongoing success in the event of a disaster or long-term business interruption and highlighting the impacts the business would face.

Risk Analysis – Used in conjunction with the business impact analysis, this allows an organisation to arrive at an informed business continuity strategy.

Business Continuity Strategy – As a result of the business impact and risk analyses, the various continuity options are considered and an overall strategy defined.

Business Continuity Planning – The design of a detailed plan or set of plans for invocation in the event of a disaster.

Continuity Testing – Regular testing of continuity plans, using a variety of methods, as an essential component of business continuity management. Kingston Smith Consulting can draw up a testing strategy, or provide an independent view on the effectiveness of a single test or entire programme of testing.

Continuity Training – Training of relevant personnel in their roles. This can also be tailored to form part of security awareness training for all staff.

Data Storage and Backup Architecture – Development of a plan and/or testing the adequacy of the data backup and storage architecture. We can determine if the plan/architecture will meet the recovery expectations of the business. If not, Kingston Smith Consulting can recommend a backup frequency, method, storage devices, and locations of the backup media.

Manage External Dependencies – Assessment of the contractual agreements (eg service level agreements) with internal and external parties on whom critical processes depend.

About Kingston Smith Consulting LLP

Kingston Smith Consulting is the specialist consulting practice associated with the top 20 accountancy firm Kingston Smith LLP. Kingston Smith was originally formed in 1923 and the firm has grown to its current position through organic growth and mergers. Kingston Smith is a member of KS International which is an association of independent accounting firms in over 50 countries around the world.

Kingston Smith Consulting LLP

Devonshire House, 60 Goswell Road, London EC1M 7AD, UK Telephone +44 (0)20 7566 4000 Fax +44 (0)20 7566 4010
info@kscllp.co.uk www.kscllp.co.uk

A list of partners is available for inspection at the above address.

Registered in England and Wales as a Limited Liability Partnership: No OC341786 Registered office: Devonshire House, 60 Goswell Road, London EC1M 7AD