

“The assignment planning was collaborative and excellent. The (security analysis) tool was helpful and added insight.”

IT Director, mid-sized university in London

IT audit – reduce risk, add value and improve security

Kingston City Group (KCG) provides bespoke IT assurance and advisory services to each member organisation which reflects the high rate of change within the IT and information environments and because at any point in time each member has a unique combination of organisational structure, technology, operational processes and project priorities driving their audit requirements.

Specialised KCG IT audit services are principally provided by the KCG Assistant Director of IT Audit and supported by other Director level staff experienced in IT audit, management and data analytics. Our Assistant Director is a fully certified IT auditor possessing CISSP, ITIL and PRINCE-2 qualifications, and has undertaken a wide range of technology training.

Key IT audit services which deliver a tailored internal audit programme that meets the needs of Board Executives, CIOs and Heads of IT Services include:

IT Governance and risk management – providing expertise in developing effective governance systems and managing IT and information risks and considers arrangements to ensure the effective direction of IT by the organisation and provision by IT of appropriate decision making information. An effective governance framework provides the right strategy and the appropriate management of data and information.

IT operations (ITIL framework) – supporting IT Directors to maximise the effectiveness and value of available IT resources through review tailored to the size of the organisation. Techniques include gap analysis and identification of quick wins for service level management, configuration management, change control and release management, incident and problem management, availability and capacity management and functional integration. Developing continual service improvement processes ensures IT talent is demonstrably focussed on refinement and innovation.

Contact:



Alan Lees
KCG Managing Director

T: 020 8417 5378

M: 07836 271313

E: a.lees@kcgaudit.co.uk

Cyber security – protecting organisations against compromise of information through staff error or by the deliberate actions of an outsider. A ‘cyber attack’ could have a permanent or long-term impact such as loss of reputational standing, of intellectual property and research data and material financial loss. In the short term there is loss of productivity, potential downtime, recovery costs and investigation time to consider. Audit ensures that security activities or the Information Security Management System are proportionate to the risks faced through comparison with recognised frameworks such as the ‘ten steps’ published by the UK government’s National Technical Authority for Information Assurance (CESG) and the Centre for the Protection of National Infrastructure (CPNI) and the ISO 27000 security standard.

Project management – delivering successful projects through implementing controls to increase the probability that organisations complete projects which are customer focused and satisfy users, which are on time and on budget, provide increasing ROI, and effect positive business change.

Networks and telecommunications – building secure IT systems processing capability, increasing resilience through fault tolerant planning and generating value for money benefits by reducing significant recurring telecommunications costs.

"The auditor is very thorough....he does an excellent job and is well respected by the department."

CIO, large university

Case Studies

Project management

We are assisting several of our larger HEIs to implement major back office systems. We've advised one HEI on how to carry out parallel testing on the new systems which helped enable them to develop protocols to confirm successful data migration and testing. Another engagement entails regular progress reviews for the Project Steering Group and has flagged the need to implement security controls for extracted data being migrated between systems.

Networks

Assistance was provided to a medium sized HEI using a network security analysis tool (SekChek). The tool identified a large number of accounts provided with administrator and excessive operating system privileges. Management was then able to reduce the risk of successful cyber attack by enabling the correct privileges for these powerful accounts.

Data Security at KCG

KCG has comprehensive information security policies which all staff follow, and which ensures we comply with all relevant legislation, including the Data Protection Act. All audit data, including that used for data analytics, is securely stored with strong access controls in place. KCG has detailed data retention and destruction/deletion policies so that we do not hold on to your data once we no longer need it.

What you can expect

The KCG team is highly experienced in working in collaboration with member institutions to implement good practice audit solutions. We tailor our approach to the specific needs of our members, ensuring they receive optimum value from their investment in internal audit.