

"During the course of the audit, the Auditor is to obtain sufficient, reliable, relevant and useful evidence to achieve the audit objectives effectively. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence."

ISACA

File interrogation software – enhanced insight into institutional data

Kingston City Group (KCG) has the skills and tools to perform complex data analytic routines for institutions and by doing so unlock some of the value in institutional data. We use IDEA 10.2, which is an advanced audit data analytic system which can accept a wide range of structured and unstructured data inputs and has a range of standard exception reporting, data matching and data analysis routines as well as data visualisation capability. All data, inputs, outputs and working files are stored on a secure partition encrypted to the AES 256 data security standard.

The key stages to delivering a tailored internal audit programme that meets your needs are as follows:

Planning – all data analytics work will be led by a senior member from the KCG team, who will agree the scope, objectives, and timing for the work, and the logistics involved in extracting and securing the data to be interrogated;

Systems understanding – we will gain an understanding of systems and controls in place, and agree with you the most appropriate time period to review;

Data extraction – we will request data to be extracted from key information systems (e.g. electronic data management systems for finance and human resources) and supplied to us in an appropriate format;

Data processing – our auditors conduct a variety of routines using IDEA; data matching, duplicate testing, data integrity, tax compliance and statistical analysis;

Audit processes – our auditors will use the output from the data analytics work to help focus audit effort and to provide the basis for detailed audit procedures to be performed;

Reporting – we report confidentially to our assigned audit sponsors, and provide key executive conclusions along with detailed findings and results.

We develop and use data analytics plans which are tailored to the needs of each institution. Typical tests we have performed include:

- Fuzzy logic matches for duplicate payments using similar amounts, similar due dates and similar invoice numbers
- Statistical analysis of supplier payments (using Benford's law functionality) to identify 'suspicious' patterns, which can be indicative of circumvention of the control environment
- Unusual patterns in input and authorisation
- Identifying potential duplicate suppliers (bank accounts and postcodes)
- Identifying potential duplicate transactions (leading to the recovery of cash)

Contact:



Alan Lees
KCG Managing Director

T: 020 8417 5378

M: 07836 271313

E: a.lees@kcgaudit.co.uk

- Confirming data integrity between the HR/payroll and financial systems (bank details and postcode)
- Identifying unidentified relationships between suppliers and employees (bank accounts and postcodes)
- Determining proportion of purchase invoices that are overdue or delays in payment processing
- Exception reporting of changes to supplier and payroll standing data and investigating any anomalies identified
- Profile credit notes to identify any particular trends and investigate further

Case Studies

Accounts Payable

We assisted one of our medium sized HEI in identifying and reclaiming over claimed staff expenses (recovering more than the cost of the service). Our analysis showed over £100K in duplicate payments (identified using 'soft matching'). Our other checks identified over 100 undetected duplicate suppliers and a number of employees who were set up as suppliers. We also identified the extent of circumvention of segregation of duties and advised on improved control measures.

Space Utilisation

We analysed teaching room usage in 15 minute segments for one of our medium sized HEI across their weekly schedules, and assisted with the installation of a more directive and coordinated approach to timetabling which allowed space utilisation to double. We improved the Audit Committee's understanding with the use of powerful data visualisations.

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

Reference

Information Systems Audit and Control Association (ISACA)	https://algaonline.org/DocumentCenter/View/2847
---	---