A checklist to help identify potential fraud when conducting an audit

The Procurement and Contract Audit Forum were privileged to have Chris Clement, Partner with Grant Thornton, give a talk at the 2011 PACAF Annual Conference on Forensic Auditing. Chris highlighted many traits which a good auditor could identify during an audit which could mean that a fraud may be taking place. The key areas are:

Behavioural

Behavioural red flags, whilst often subjective, can give a good indication that something might be amiss with a particular employee. Typical ones that might be encountered are:

- *Employee lifestyle changes* - such as signs of excessive spending or wealth that do not accord with the employee's known level of remuneration;

- *An habitual disregard for organizational processes and procedures* – incorrigible behaviour of this kind can often be linked to more malevolent misconduct;

- *Working excessive hours and/or failure to take leave* - discovery is one of the fraudster's greatest fears. The less absence, the less chance of discovery;

- *Abnormal social behaviour* - could indicate problems with drink, drugs or gambling, which might motivate fraudulent behaviour or other organizational abuse;

- *Resistance to questioning of personal working practices and/or providing implausible or misleading answers to questioning* - this is often an indicator of someone with something to hide and demonstrates an inclination to deliberately misrepresent facts;

- *Tendency to* go *sick shortly before crucial meetings involving personal performance and accountability* - avoiding such meetings forestalls the day when the fraudster might have to explain themselves, the hope being that events might have moved on in their absence;

- *Repeated complaints of workplace discrimination and harassment that appear groundless or vexatious* - this sort of diversionary tactic creates an understandable reluctance on the part of those who might ordinarily challenge suspicious or questionable behaviour, which allows the fraudster to operate almost with impunity, or buys them time.

Transactional

Transactional red flags can be the most difficult to identify as they vary widely from one organisation to another and can be overwhelming in their frequency. The blizzard of electronic data created by high-speed, multiple transactions can appear daunting, which is why sophisticated electronic detection and data-processing tools are often employed to help identify red flags.

Examples of transactional red flags are:

- *Excessive number of year end transactions* - while this could merely be part of the normal year-end rush, it might also indicate an attempt artificially to hit yearend performance targets or an attempt to conceal fraudulent transactions among the flurry of others;

- *Excessive issuing of credit notes* - this might possibly indicate deliberately inaccurate billing or the fraudulent provision of inventory or services;

- *Clustering of transactions below payment authority levels* - this might suggest an attempt to avoid supervisory scrutiny of suspicious transactions;

- *Payments to offshore tax-haven jurisdictions* - this is not necessarily suspicious but worthy of enquiry, particularly if there is little or no track-record of such payments having occurred in the past.

System

While there is no doubt that modern technology has enabled fraud to proliferate, it is also true that technology can be used to counter the fraudsters. Given that fraud reveals itself through the inconsistent or aberrant, IT programs are ideally suited to routinely monitor large electronic communication systems for suspicious activity.

Typical system red flags are:

- Login and system usage at odd times of the day;

- Multiple failed logins;

- Use or attempted use of ex-employees' logins;

- Use of non-corporate e-mail accounts, such as Hotma.il;

- Attempts to access data without the necessary permission(s);

- Introduction of unauthorised software or hardware into the system;

- Insistence on using personally owned hardware, such as a laptops or mobile telephones;

- Excessive levels of non-work related traffic;

- Exporting of data to non-corporate e-mail accounts.

Unlike behavioural or transactional red flags, system red flags should not be widely disclosed and are best kept within the knowledge of the relevant departmental staff, though advertising to others that some form of monitoring is taking place will have a deterrent effect.

Chris Clements *I* Les Dobie
Grant Thornton UK LLP
30 Finsbury Square
LONDON
EC2P 2YU
M +44 (0) 7968 338 895
E chris.m.clements@gtuk.com

June 2012