What's in your data?

Traditional computerised audit techniques can be used to analyse procurement spend for suspicious amounts or to identify a fraudster using the same bank account for a fictitious supplier as they gave to payroll. However, modern organisations collect a lot of other data relevant to identifying unauthorised transactions. For example, if a manager who is on holiday abroad logs on to a desktop PC in the office to authorise payments then it likely indicates that something untoward might be taking place with stolen or misused credentials.

A device logged on to a corporate network regularly sends authentication requests to the network's domain controller servers and these records can be obtained to establish a baseline of 'normal' activity for approving managers.

Leave records and potentially time clocking gaps can be obtained from your HR systems, transaction approvals from finance and other business applications, and these dates and times compared for anomalies. Internal policies should unambiguously prohibit sharing of system credentials. You should also make sure that processes to disable network and system accounts when people leave are effective, to avoid these passing into other hands. Many systems also permit password self-reset, and managers delegating access to inboxes may not stop and consider that by doing so they are granting access to far more than the emails.

There are opportunities to block or uncover wrong-doing after the fact but without effective separation built into processes or careful scrutiny of budgets additional payments amongst high volume and high value spend could go unchallenged.

There is also scope for other cross-system uses of data in an organisation such as a council. Data warehousing can help to identify fraud or error and protect public funds. A regular check of additions to the electoral register against council tax discounts, for instance, can be straightforward when information is brought together. This could take the form of a formal database with an interface for users to query, but could alternatively be regular extracts of key data from various systems into a secure folder for use with analysis tools.