The Digital World – risk, vulnerabilities and the use of technology in corruption prevention

Corruption Prevention and Integrity Conference

3 – 4 October 2017

Susan Fraser, CA
Assistant Auditor-General, Technical Audit

VAGO

Common areas where fraud can occur

- Procurement/expenditure – suppliers, employees
- Payroll
- Asset management
- Contract management

Some vulnerabilities seen in our clients – payroll cycle

Limited or lack of governance and controls over:

- segregation of duties and access to data
- creation, updating and review of employee accounts, bank details and standing data
- review and approval of payroll variations/adjustments
- employment screening (limited or lack of)
- sub-ledger reconciliations (timely?)

How can technology contribute to increased fraud and corruption risks?

- Ease of access to cheap technology tools & skills
- Huge amounts of data collected by agencies – has to be stored and secured
- Use of online services being provided to public – knowledge of data stored
- Sharing of data electronically between agencies – data not ‘contained’
- Outsourcing of data to third-party vendors to manage
- Legacy I.T systems (outdated, incompatible)

How can technology contribute to increased fraud and corruption risks? (cont'd)

- Size of data held in many different systems – data inventory?
- Data stored digitally can be more easily accessed particularly if in the cloud – remote access
- Wide variety of attacks possible – cyberattacks - steal, alter, delete or hold ransom data, DoS attacks, malware, identify theft, phishing emails etc..

Key I.T internal controls to help prevent, detect fraud

- Automated system controls wherever possible – e.g. workflows, approval processes per financial delegations
- Access security – controlling physical, system and data access; password management; super user access; timely monitoring & response
- System acquisition, development and maintenance – I.T project management, backup processes, systems fully supported by vendors, critical system updates (patches) kept up to date; log files/audit trails
- Program change management – policies in place to govern key system changes
- Disaster recovery and business continuity plans
- Security software up to date – firewalls in place, continuous updating, monitoring, threat assessments, pen testing, malware & intrusion detection

Key internal controls to help prevent, detect fraud

- ‘Tone at the top’ – governance, oversight/monitoring and reporting
- Segregation of duties
- Active financial delegations – monitored, enforced, reviewed
- Data matching wherever possible
- Active monitoring and reconciliations of transactions by appropriate staff
- Vulnerabilities (pen) testing - ability to identify and test for any system vulnerabilities
- Staff awareness and training in key fraud policies, controls
- Internal audit function – program coverage, use of data analytics/mining

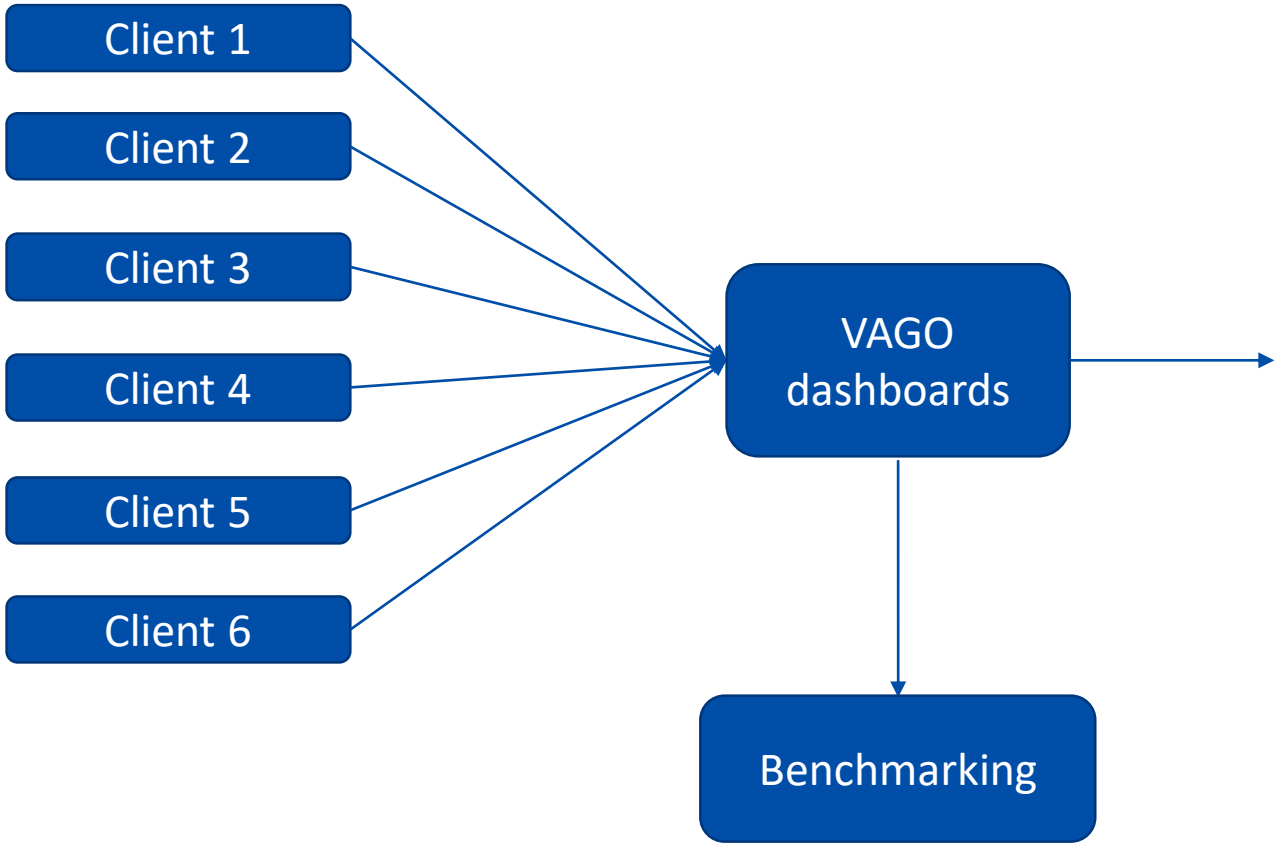
VAGO's investment in technology in audits – data analytics

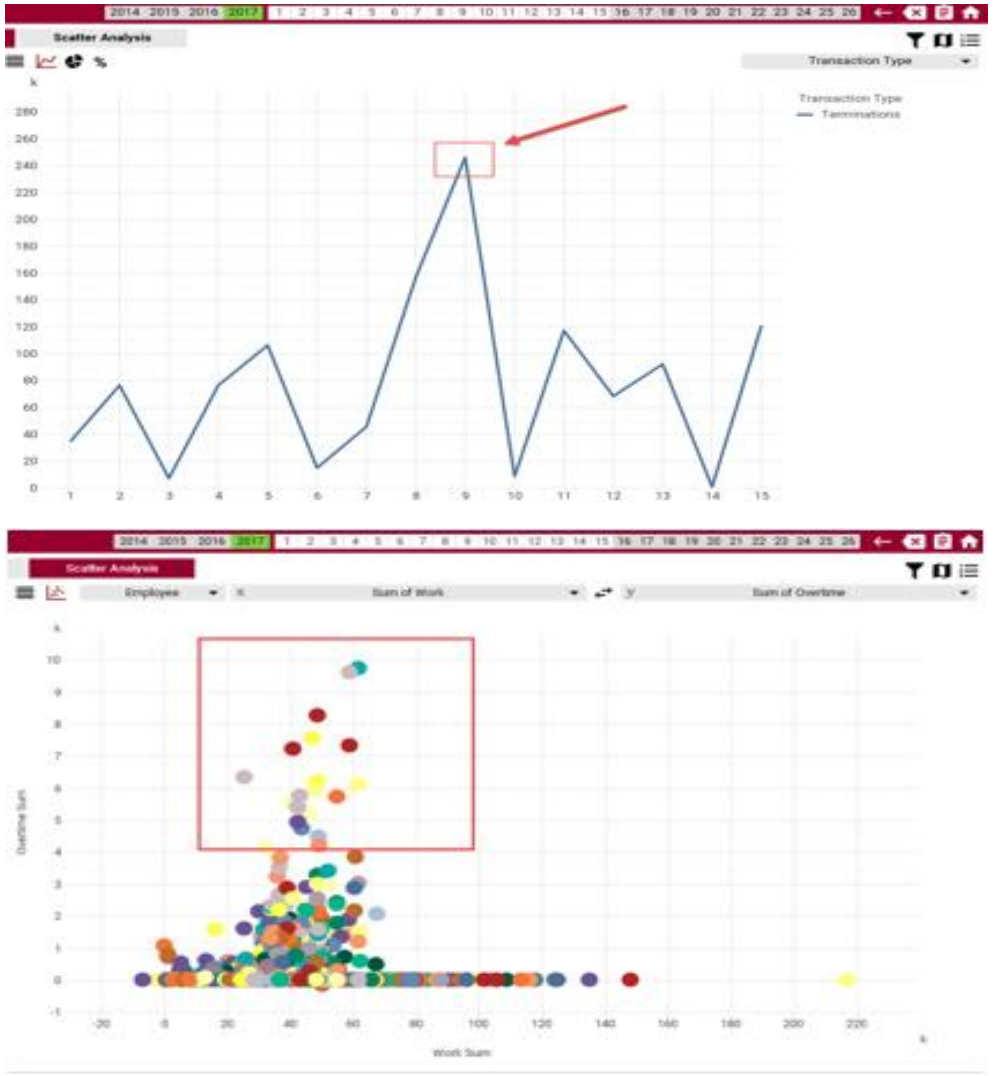
The power of data analytics – a more targeted, efficient audit

- Ability to collect entire data populations from key financial and other I.T systems (within agency, multiple agencies, and from other sources) – numerical/non-numerical
- Better analyse total data population through pre-set tests (including statistical methods) to identify expected/unexpected trends, fraud risks, data matching, compliance with approval limits, unusual relationships review etc..
- Results of audit tests are visualised on a interactive digital dashboard to help identify specific audit items for follow up testing
- Sentiment analysis, data mining, benchmarking on a particular subject matter

Using data analytics – the future of audit

Where we see technology assisting us as **auditors** in identifying fraud?





Any questions?

For further information contact:

Victorian Auditor-General's Office
[p] 8601 7000
[e] enquiries@audit.vic.gov.au