Joint Audit and Governance Committee

Report of Corporate Fraud Officer

Author: Fergus Nugent

Telephone: 01235 422506

Textphone: 18001 01235 422510

E-mail: fergus.nugent@southandvale.gov.uk

SODC Cabinet member responsible: Councillor David Dodds

Tel: **01844 212891**

E-mail: david.dodds@southoxon.gov.uk

VWHDC Cabinet member responsible: Councillor Robert Sharp

Tel: **07771 760549**

E-mail: robert.sharp@whitehorsedc.gov.uk

To: Joint Audit and Governance Committee

DATE: 25 March 2019

Corporate Fraud and Cyber Security Risk Review

Recommendation
That members note the content of the report

Purpose of report

1. The purpose of this report is:

   - to provide an update on the corporate fraud and cyber security risk review, commissioned by strategic management team (SMT); and
   - to summarise current progress and initial findings.

2. The contact officer for this report is Fergus Nugent, Corporate Fraud Officer (fixed term contract) for South Oxfordshire District Council (SODC) and Vale of White Horse District Council (VWHDC), telephone 01235 422506.

Strategic objectives

3. Delivery of a corporate fraud and cyber security risk assessment will support the councils in meeting their strategic objectives.

Background

4. The Chartered Institute of Public Finance and Accounting (CIPFA) fraud and corruption report (2018) reported that 80,000 frauds totalling £302 million were detected or prevented by local authorities in 2017/2018. Cybercrime has also become more prevalent, with targeted attacks at commercial and government levels, requiring a dynamic and proactive approach to IT security, particularly as SODC and VWHDC increase the amount of online self service offerings.

5. SMT recognise the potential for additional risk that this move to online delivery of services may bring to SODC and VWHDC and have agreed to an independent review of corporate fraud and cyber security risks that may impact both councils. The purpose of this assessment is to identify the key fraud and cyber security risks across SODC and VWHDC and to validate the effectiveness of any mitigating controls.

6. The councils' approach to fraud is documented in the joint anti-fraud, bribery and corruption policy. This review will evaluate how operational behaviours align to this policy.

   This activity is undertaken in addition to the existing activities to manage fraud risk, including our annual pro-active anti-fraud audit, and the work carried out by our in-house fraud management team specifically focused on benefit and council tax fraud.

Approach

7. The following steps will be undertaken during the review:

   7.1. Compile a list of corporate fraud and cyber security risks for SODC and VWHDC based on benchmarking against other similar councils, key outputs from the recent Local Government Association (LGA) cyber security risk survey, and input from heads of service on key risks for each service area.

   7.2. Conduct interviews with service managers and staff officers to identify mitigating controls for each risk area.

   7.3. Evaluate the operating effectiveness of mitigating controls through control testing.

   7.4. Assign a post-mitigation risk score for each individual fraud and cyber security risk and assess any residual risk.

7.5. Develop corporate fraud and cyber security summary risk matrices.

7.6. Evaluate the content of relevant corporate policies.

7.7. Create a corporate fraud and cyber security risk training pack, summarising key learnings from the assessment.

Progress update

8. Interviews to identify key risks across service areas have now been held with heads of service and staff officers. Risk tracking spreadsheet for corporate fraud and cyber security risks have been created and non-mitigated risk scores have been assigned (Appendix 1). The risk tracking spreadsheet currently has 39 corporate fraud and 27 cyber security risks

9. As at 3 March 2019, 29 out of 39 of fraud and 22 out of 29 cyber security risks have been reviewed and tested. Testing of the remaining controls is in progress, once completed the risk matrices will be populated.

10. It should be noted for the cyber security review many of the controls are performed by Capita and in the absence of third party testing we are dependent on Capita to provide assurance that the controls are in place and operating effectively.

11. Preparation of a fraud awareness training pack is in progress.

12. A final report together with documentation outcomes will be reported to the July 2019 joint Audit and Governance Committee. Recommendations will be considered for incorporation into the 2019/2020 internal audit plan.

Documentation outcomes

13. The corporate fraud officer will produce a summary of findings and recommendations for each area reviewed. In support of this, the review will document the following:

- Corporate fraud and cyber security risk summary matrices, highlighting key risk areas.
- The review will include an assessment of applicable council policies to determine if they are accessible, up to date, relevant, and whether they have been communicated to staff officers.
- The review will document a fraud awareness training pack focused on risks specific to SODC and VWHDC.
- The corporate fraud officer will provide input into the councils' cyber security training.
- The corporate fraud officer will produce a summary of findings and recommendations for each area reviewed.

Financial implications

14. The review is likely to identify a range of potential financial implications to SODC and VWHDC resulting from corporate fraud risks that are not mitigated. In addition to any financial loss the reputation of the councils may be impacted if a cyber security incident impacted the councils' ability to deliver services, or if sensitive data was compromised.

Legal implications

15. Within the annual governance statements, the councils set out the financial and risk governance frameworks. This review may identify areas where the councils are failing to deliver against their commitments, which could have legal implications. The following regulations and standards relate to the management of corporate fraud and cyber security risks:

- GDPR (General Data Protection Regulation 2018) – the councils are required to secure sensitive data and restrict its use to that agreed by the customer.

- PCI DSS – (Payment Card Industry - Data Security Standards), the councils have an obligation to comply with payment card industry standards. Non-compliance may result in the councils losing their ability to process credit card payments.

- Cyber security standards – the councils should, wherever possible, align to the guidance issued by the National Cyber Security Centre (NCSC) to help protect against cyber security issues.

Risks implications

16. This review will provide an assessment of the key corporate fraud and cyber security risks facing both SODC and VWHDC. Based on the outcomes from this review, additional mitigation actions may be required.

17. It should be noted that this review is still in progress, which may result in further risks being identified.

Other Implications

18. None.

Conclusion

19. None.

Appendices

- **Appendix 1** - 3X3 Risk Score Matrix
- **Appendix 2** - Exemplification of Fraud Risk Summary Matrix
- **Appendix 3** – Exemplification of Fraud Risk tracker

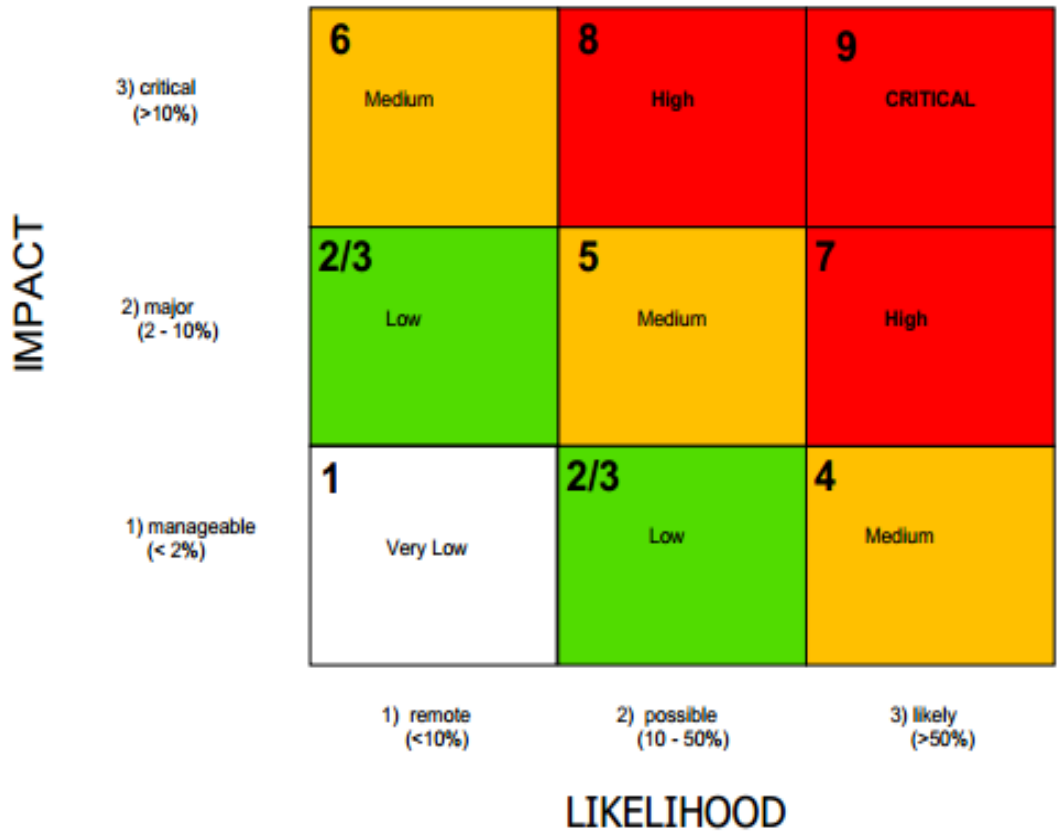
- **Appendix 4** - Exemplification of Cyber Risk tracker

FERGUS NUGENT

CORPORATE FRAUD OFFICER

Appendix 1 - 3X3 Risk Score Matrix

3X3 Risk Score Matrix



South Oxfordshire District Council and Vale of White Horse District Council Risk Management Policy and Guidance 2017 -2019

Fraud Risk Summary - March 2019

Fraud Risk profile

Net evaluation

Risks:

(ranked by priority band, numbering is for referencing purposes only) reviewing the top risks

Critical:

2F Procurement-supplier selection, suppliers are selected outside the agreed process resulting in preferential treatment for some suppliers, potential for bribery and poor quality goods/services. *Risk owner name*

High:

8F. Overtime payments/TOIL abuse, overtime and TOIL claims are submitted and authorised when there is no entitlement. *Risk owner name*

3F. Fraud risk name, further details on the actual risk. *Risk owner name*
15F. Fraud risk name, further details on the actual risk. *Risk owner name*
22F. Fraud risk name, further details on the actual risk. *Risk owner name*
11F. Fraud risk name, further details on the actual risk. *Risk owner name*
12F. Fraud risk name, further details on the actual risk. *Risk owner name*
20F. Fraud risk name, further details on the actual risk. *Risk owner name*