Corporate Integrity Group Action Plan – updated 07 November 2018

Aims:
1. reduce organisational vulnerability to fraud, crime and corruption across departments through a preventative approach
2. consider areas where it would be possible to enhance existing systems and controls

1	2	3	4	5		6	7
Identify risk/ Vulnerability	Potential for risk to arise/ frequency of occurrence 1. low 3. medium 5. high	Consequences of occurrence: Reputational risk/financial loss 1. low 3. medium 5. high	Combined risk of 2 & 3	What mitigation measures are in place?	Residual risk	What further mitigation measures are needed?	Action by
Vetting of Staff							
New Employees. Opportunity for misrepresentation Financial impropriety	2	4	8	PVG GSX Work permit check Check referees Code of conduct/induction Check Professional Qualifications	2x2=4	Consider open source checks for higher risk posts Nb resource implications and proportionality. How do we identify high risk posts ? how do we evaluate data ?	HR
Existing employees Risks: Conflict of interest, financial impropriety, Qualifications eg driving licence.	3	4	12	Code of conduct Register of Interest and Register of Gifts ERDP's GSX accreditation	2x2=4	Consider regular reminders about Code of conduct .	group

				PVG Line management Team brief reminder on integrity issues			
Information Security							
Risk of loss of data. Opens up further risks of financial vulnerability, Data protection breach,	4	4	16	Close links to the risks managed by the Information Assurance group. ICT policies Continuity Plans	3x3=9	Further actions with Information assurance group	
Procurement							
Contracts over £50k risk of fraud and non-compliance	4	4	16	Financial regulations Procurement procedures Procurement legislation PCS Payment section compliance checks	3x3=9	Stress the need for departments to comply with procurement procedures, contract management and financial management	Head of finance
Contracts under £50k	4	3	12	Payment section compliance checks	4x2=8	Stress the need for departments to comply with procurement procedures, contract management and financial management Check appropriate measures are in place for self-directed support?	Head of finance
General risks Contractor involved in	3	3	9	Regular liason with police keep intelligence	3x3=9		

organised crime Contractor personnel aren't security checked				levels up. National fraud intelligence service (NAFN) The Council shares data on its supplier database with Police Scotland			
Conflicts of Interest and staff discipline							
Potential in Moray for conflicts and abuse of processes including: -Award of contracts -Permissions and consents -discretionary fines/payments	4	3	12	Staff Code of conduct Councillors Code of Conduct Register of Interest and Register of Gifts Supervision and management processes	3x3=9	Categorise and audit all processes to minimise risk Suggest promotion of code of conduct obligations through: 1. ERDP 2. Induction 3. PC log in tick screen 4. Team brief.	For next CIG meeting
Gifts and hospitality which are designed to get favourable treatment.	3	3	9	Staff code of conduct Management and peer oversight Regsiter of Interest and Register of Gifts	2x3=6	Highlight this aspect when promoting code of conduct Can we link register of gifts to the new staff database ?	
Having staff policies in place but not properly publicising/enforcing them.	2	2		A number of staff policies in place. Eg periodic mandatory computer policy acceptance to staff via	2x2=4	How do we identify policies which are observed more in breach than observance ?	

				a pop-up		Easyfind. Use interchange to bring all the different policies together in one place.	
Finance							
Risk of fraud/theft	4	4	16	Forensic accounting system to pick up • duplicate payments • unusual patterns Finance systems and protocols National Fraud initiative and data matching Publication of the staff Code of Conduct Whistleblowers anonymity guaranteed.	2x2=4	Fraud theft and corruption policy to be updated and publicised (SOC checklist) Fraud response plan on HR website. Links to information assurance group:make sure ransomware systems and staff awareness of risks. Opportunity to analyse complaints to identify and mitigate risks in several areas in this register.	
Misuse/personal use of council vehicles	4	1		Fuel consumption and speed monitored plus GPS tracking. Info stays with fleet services Ctrack being	3x1=3	Should service managers receive regular reports ? If ctack successful consider roll out across council.	

				introduced to DLO vehicles. Provides further information for managers to monitor			
Physical security of buildings							
Access to buildings	3	2	6	Buildings manual for each building **ID card buildings** -standard users access during normal hours -special users get extended hours -time limited visitors badges **Key/Keypad buildings** -numbers regularly changed. -key safes **Building responsibility**: Single service=that service Multiple service=building user group: shared responsibilities.	2x2=4	Note links to information assurance group and emergency planning. **Council Depots** Consider installing CCTV and intruder alarms. Consider security audit Need to improve staff awareness and tighten up on procedures so everyone knows their responsibilities. Cultural change needed. Use of security badges, awareness of policy,	
Peripherals issued to staff	3	2	6	Some departments use inventory checklists and leaving checklists.	3x2=6	Consider extending use of this across Council and	AM

				These can be extended to include access to other resources		increased publicity. Example given by Dianne. Raise with CMT	
Staff awareness							
Risk of uninformed staff increasing the risk in other areas on this action plan.	4	2		Already actions above in relation to individual areas eg code of conduct and conflict of interest.	3x2=6	Consider use of CLIVE for online training	
Make staff aware of risk of cyber crime (from SOC survey)	3	3	9	NAFN briefings and computer use policy.	3x3=9	Briefing	
Internal and External Communication							
Reputational risk from ill-considered use of social media	3	2		Employee code of conduct	3x2=6	Need for a policy and training	
Reputational risk from ill-considered press releases	2	2		Media protocol in place governing contact with the press	2x2=4		
Risk of deliberate leaking of confidential material to the press. *Would these be better on the Corporate Risk register ? Are they fraud/corruption risks*.	2	3		Ad hoc. Often hard to find who is responsible.	2x3=6		
Have we disseminated our understanding of SOC risks to our community partners	3	3	9	Public protection partnership, business gateway, leader funding ?	3x3=9	Needs further thought and ownership	

Notes:

1. This plan needs to be viewed as part of a wider Council risk management strategy. Links need to be identified to the Corporate risk register and service specific issues in individual registers.
2. Consider timescale for SOC checklist (Falkirk model checklist) review.