Australian Government

Australian Commission for
Law Enforcement Integrity

DEVELOPING FRAUD AND CORRUPTION RISK CONTROL PLANS

DEVELOPING FRAUD AND CORRUPTION RISK CONTROL PLANS

ACLEI November 2015

aclei.gov.au

Developing fraud and corruption risk control plans—a primer

ACLEI has developed the following tips for strengthening the value and effectiveness of risk control planning.

More insights about how to manage corruption risk can be found at ACLEI's website www.aclei.gov.au under Corruption Prevention.

Tips	Tricks
Gather expertise around you	• Form an inter-agency reference group comprising agencies with similar risks or shared environments (brains trust and sounding board; leverage common issues and solutions; join-up risk treatments; innovate) • Have an external consultant involved in assessment of risk (help avoid subconscious bias; import skills you may not have in-house; assist with executive buy-in; contribute process and business improvement knowledge)
The journey is as important as the destination	• Communicate to staff that: ○ They administer public **assets** (resources, information, decision-making and public sector integrity/reputation) on behalf of the government and the community ○ Opponents (including trusted insiders) may conspire to steal or misuse those assets • Assist stakeholders (business owners) to understand the risks they are managing for the organisation • Fraud and corruption vulnerability assessment gives managers another window on organisational capability, maturity and systems • Use the risk assessment and planning process as part of the mitigation and stakeholder engagement strategy

Tips	Tricks
Ways to describe the task	• Protecting core business o Use ACLEI's asset protection model (see *key concepts* webpage)—what assets are critical to your core business? o Protect assets + from improper use + by someone + through theft or deceit • Fraud (theft or misuse of resources) is the crime o When an "insider" is involved, then "corruption" (misuse of public office for a perceived gain by self or others) is the method by which the crime occurs
Ways to understand the risk	• Develop a detailed typology of how fraud or corruption could occur. Use the typology as the basis for the risk assessment and to design your control measures • Use ACLEI's five approaches for assessing corruption risk, (see *corruption prevention toolkit* webpage): o Commodity o Location o Corruptor o Susceptibility (staff) o Vulnerability (systems) • Workshop challenges: Ask staff, contractors and customers: "If you were corrupt, o What would you want to steal/ misuse? o How would you do it? o How could you cover it up? o Why would you do it? o Who would you work with? o Why wouldn't you be caught?"

Tips	Tricks
Ways to understand the risk	- P(C)=ExS (the Probability of Corruption depends on Exposure to the environment (including deterrence measures) and the Susceptibility of individuals (see *corruption resistance* on the key concepts webpage). ○ Assess what factors in your operating environment that might increase your risk (eg. targeting by organised crime; defences are low; likelihood of whistleblowing is weak) ○ Examine how well your organisation finds and looks after people who may be vulnerable to compromise (they may need support, moving, or close supervision) - What does your underlying culture (workplace norms about behaviours and whistleblowing) tell you about your risk? - If you strengthen one area, where could the risk move—will there be a counter-productive “displacement” effect in another area?
Explain the risk clearly	- Let senior managers know what the inherent risk is (what will happen if control measures are not effective) as well as the residual risk (with effective measures). They need to have skin in the game—they need to know what will happen if control measures aren’t as effective as planned. - Tell staff what the risks are, and what the stakes are. They need to know what fraud and corruption look like to be able to report it.

Tips	Tricks
Direct resources to control the highest harms	• Plans should identify and drive resource allocation towards risk mitigation, including detecting fraud or corruption • Don't build a system around people who are already compliant (locks only keep honest people out). Build most controls in the high-risk spaces, use detection as well as control measures. • Detection measures recognise that not everyone has the same values as you • Look for **risk aggregations** (hot spots of assets and vulnerabilities) and target those aspects the most • "Crown jewel" strategy—give priority to protecting your most important assets or processes
Use innovation to understand and control risk	• Identify and manage the temporal aspect: how is environmental risk—or other emerging issues, including changes in business—expected to change the risk picture in the next two to five years? • Do a control plan for an entire operating environment (eg, a Port Fraud Plan might involve a number of public sector agencies and private sector partners) • Map out your hot issues: eg: ○ "Hard to detect" corruption points (where you have low control) ○ ICT superusers ○ Shift in employee values over time ○ Trigger events ○ Managing "reach-back" from former staff ○ Secondary employment ○ Cyber-crime

Tips	Tricks
Make the product useable and useful	• How deep should a plan go? o The plan needs to inform managers what corruption and fraud looks like in the space they administer—not phrased as a generic rating • How do you make it meaningful? o Simplify the message: link actions to desirable outcomes—for instance: ▪ We are protecting the integrity of our people by… ▪ To deliver [our core business], we must ensure we …(.. protect the supply chain, fight corruption, protect our information…)
How to keep the plan "live"?	• Executive reporting and governance against key indicators • Senior Executive talking points (key messages for staff) • "Lessons learnt" products • Build linkages to other corporate messaging. Integrity messaging and risk management is part of: o Personnel Security o Public Interest Disclosure/ Whistleblower o Code of Conduct/ Ethics o Fraud and Corruption Control training o Business improvement o Culture building

Traps	Dodges
Behavioural science tells us that people typically under-estimate risk and over-estimate their ability to manage risk, and that we make judgements based on our own biases and values. These factors can lead to complacency and risk-denial.	• Get a “second pair of eyes”; gather expertise around you; base the risk assessment on objective measures
High risk operations should expect corruption or fraud to occur. The purpose of the fraud plan is not to prevent every instance.	• You need to be confident that your agency is dealing with your most serious risks to an acceptable tolerance level. Check that risk tolerance with the ultimate risk owner—usually the head of agency
Don’t assume you know every aspect of your business.	• A good plan acknowledges unanticipated things will happen and has a response strategy ready
Be careful not to describe the risk too generally or at too abstract a level to be meaningful—be concrete.	• Fraud and corruption will actually only occur in a handful of reasonably predictable ways—your description of the risk should be quite granular. Something is wrong if you didn’t predict with some accuracy how a fraud might occur
Don’t hide risks from staff.	• Tell staff about the risks that concern you most. It is not generally the case that people will use the plan as a “How To” guide. Telling staff makes them part of the detection and deterrence regime
Don’t “cry wolf”—agencies need to be able to simultaneously: ○ Deliver results ○ Cut red tape, and ○ Manage risk	• Act proportionately to the risk; link controls to protecting core business • Controls can slow down business delivery. Make an assessment about whether it is worth it. Get approval! • Use detection as well as control mechanisms