Portfolio Fraud and Corruption Risk Assessment

Organisational Context	
Topic of the Risk Assessment	Portfolio Fraud and Corruption Risk Assessment
Risk Activity / Context Statement	The Environment, Planning and Sustainable Development Directorate (EPSDD), the City Renewal Authority (the Authority) and the Suburban Land Agency (the Agency) make up the Portfolio and is part of the ACT Public Service (ACTPS) and as such is accountable for the efficient and effective use of public resources. The Portfolio recognises the responsibility and the need to develop, encourage and implement sound financial, legal and ethical decision-making processes and the development and implementation of tools to identify, manage and ultimately reduce the risk of the occurrence of fraudulent and/or corrupt conduct.

Directorate Contact Details			
Directorate	EPSDD Portfolio	**Division / Business Unit** *(If applicable)*	Governance, Compliance and Legal Services, Legal Services and Integrity
Name of Contact:	Clinton Dengate	**Contact Details (phone):**	X55001
EPSDD Decision Maker	Chief Operating Officer/SERBIR	**Contact Details (phone):**	X76322
City Renewal Authority Decision Maker	TBD	**Contact Details (phone):**	
Suburban Land Agency Decision Maker	Agency Secretary and Governance Manager	**Contact Details (phone):**	X59980

Risk reference	Risk Description	Current Level of Risk	Is a risk treatment action plan in place?	Date risk and/or risk Treatment action plan to be reviewed.	Risk Owner	Comments
Reference 1	Fraudulent or corrupt conduct occurs when procuring goods or services	**HIGH**	Yes	October 2019	SERBIR/CEOs	
Reference 2	Failure to protect personal and corporate information	**HIGH**	Yes	October 2019	SERBIR/CEOs	
Reference 3	Misuse of public property and money	**MEDIUM**	Yes	December 2019	SERBIR/CEOs	
Reference 4	Misuse of delegations, position and/or workplace entitlements	**MEDIUM**	Yes	December 2019	SERBIR/CEOs	

RISK REFERENCE	1

RISK DESCRIPTION/RISK EVENT	Fraudulent or corrupt conduct occurs when procuring goods or services

SOURCE: How can this happen, the drivers of the risk event	IMPACT/OUTCOME: If what can happen does happen what is the most likely consequence	RISK CONTROLS CURRENTLY IN PLACE: Actions Taken
Quote and tender processes • Collusive practices resulting in the purchasing process not being sufficiently competitive. • Staff involved in decision making or monitoring may have a personal interest in the contract. • Appointing contractors/consultants or purchasing goods and/or services not supported by proper process. • Goods and/or services purchased from an organisation with a previous fraud history. • Goods and/or services purchased from a fictitious vendor created by an employee, who then submits false invoices for payment. • Goods and/or services are procured for personal benefit (money, family employment or other gratuities). **Payment** • Payments to contractors/consultants when work is not performed or not performed satisfactorily. • Splitting procurement activity to avoid obtaining quotes or to get around delegation limits. **Gifts and hospitality** • Gifts, benefits and/or bribes accepted from current or potential contractors, consultants or other service providers.	**Failure to deliver fit for purpose product** • Final product not completed to the task specification. • Final product not completed to regulated standards. • Opportunity is lost to procure efficient, effective, streamlined business solutions to improve the directorate's service offering **Loss of reputation** • Loss of reputation in business community due to biased tender and contract evaluation practices, resulting in less entities willing to do business with the Portfolio • Loss of reputation and confidence in the Portfolio. • Adverse media attention. **Financial** • Increased cost of service delivery/purchase of goods - Not achieving the best value for money. • Legal claims against the Portfolio by alternative suppliers who claim unfair advantage in contract negotiations. • Breach of panel and whole of government contracts already in place. • Additional costs incurred to rectify faulty work. • Increased public liability claims as a result of poor construction of public structures. • Additional audit expenditure required to conduct investigations. **People** • Negative impact on staff morale and culture	Director-General/Chief Executive Officer Financial Instructions in place and accessible to all staff Human Resources Delegations in place and accessible to all staff **Quote and tender processes** • Procurement policies and processes are in place and are accessible by all staff • Under procurement policies, where a single select procurement at the value of $25,000 (inclusive of GST) and over is recommended for approval by the Director-General/CEO, significant demonstration to support the recommendation is required • Panel contracts and whole of government contracts are in place for regularly procured items and services • A whole of government cloud request for quote service is being rolled out across a number of panel contracts • EPSDD Audit Committee and the Audit and Risk Committees of the Authority and Agency undertake regular reviews/audits of procurement processes as required • All procurements with a value of $25,000 (including GST) and over must be registered on the whole of government contract register within 21 days of execution • The Directorate is developing a procedure to review samples of procurement and contract management activities across the Directorate to ensure the correct processes, financial delegation approvals, and records management requirements are met **Payment** • The Financial Delegate, who may also be the Project Sponsor if the procurement is part of a project, is responsible for: - ensuring that the proposed purchase is for a legitimate business purpose - is efficient, economical and ethical; and - complies with relevant legislation, regulations, guidelines and circulars The Financial Delegate is also responsible for ensuring all procurement activities are adequately documented, from identifying the need, through the quotation/tender process, and the contract management phase. • The Contract Manager, who is often the Purchasing Officer, and may also be the Project Manager is responsible for ensuring that the supplier has delivered the goods, services or works in a satisfactory manner, and within the scope of the original request • Segregation of responsibility between recommending invoices be paid and the decision to pay an invoice

				Gifts and hospitality • EPSDD, Agency and Authority Gift policies in place and accessible by all staff. • All gift and benefits declarations are reviewed and approved by the relevant business unit head, the SERBIR and where necessary, the Director-General/CEO. • EPSDD, the Agency and the Authority Gifts Register in place and regularly updated **Conflict of interest** • Conflict of Interest Factsheets are in place and accessible by all staff • Conflict of Interest Register in place and updated as required • Portfolio employees and any parties advising the Portfolio must disclose any conflicts of interest arising during the procurement process. Potential service providers should also be required to divulge all potential conflicts of interest with their tender • Ability to restrict a staff member's accessible to information in Objective or other Portfolio systems **Training** • Integrity training provided as part of the Learning and Development Framework • Fraud, Corruption and Ethics Training as part of Learning Essentials Framework	

Consequence Rating	Likelihood Rating	Current Level of Risk	Control Effectiveness Rating	Risk Owner	Treatment Action Plan Required
Major	**Possible**	**High**	**Room for Improvement**	**SERBIR/CEOs**	**Yes**

RISK REFERENCE	2
RISK DESCRIPTION/RISK EVENT	Failure to protect personal and corporate information

SOURCE: How can this happen, the drivers of the risk event	IMPACT/OUTCOME: If what can happen does happen what is the most likely consequence	RISK CONTROLS CURRENTLY IN PLACE: Actions Taken
External • External party gains unauthorised access to Portfolio buildings and accesses hardcopy files, Objective or the ACT Government network • External party gains unauthorised access to Portfolio information or data via by external unauthorised entities • External entities eavesdrop on Portfolio activities through phishing and exploitation of software vulnerabilities or other external intrusion • External parties with authorised access to Portfolio systems misuse access provisions • Privacy breaches, ransomware attacks, encryption and deliberate destruction of Portfolio information by external parties **Internal** • Misuse, disclosure or destruction of information by a Portfolio officer or contractor for personal gain • Information in Portfolio systems is maliciously/fraudulently tampered with for personal gain • Unauthorised release of sensitive or confidential information • Portfolio officers purposely fail to capture records of decisions in approved recordkeeping systems • Portfolio officer, without a legitimate business need, views records e.g. ACT residents' personal information, development applications before they are publicly released • Inadequate management of authorised physical and system access (e.g. Authorised access maintained after staff member changes role, moves agency or resigns from the ACT Public Service or commences long term leave) • Sensitive hardcopy records are not stored securely • Customer credit card details held in electronic or hardcopy format are accessed for personal gain • Inadequate physical security for handling records / information • Incorrect classification of information records • Non-compliance with requirements of Cabinet Handbook • Staff sharing or not changing passwords • Hard drives or portable storage devices such as CDs, DVDs and USB thumb drives, not encrypted or properly disposed of • Staff log onto EPSDD systems remotely enabling members of the public to	**Loss of reputation** • Loss of reputation, trust and confidence in the Portfolio • Adverse media attention **People** • Failure to engage staff and / or loss of staff morale • Vulnerable people are put at risk • Negative impact on staff morale and culture **Financial** • Additional audit expenditure required to conduct investigations. **Business operational** • Litigation and compliance actions	**Policies and Procedures** Policies in place and accessible by all staff: • WhoG ICT Security Policy (2016) • ACT Government Protective Security Policy Framework • Cabinet Handbook • Permissions Policy and Business IT Systems Permission Plans (under development) • Portfolio Information Privacy Policy **Training** • The Learning Essentials Framework includes units on fraud, corruption and ethics, and records management. **Access controls** • Appropriate level of computer access provided to staff upon commencement • Staff required to lock or log out of workstations before extended periods away from computer, to prevent unauthorised use • Automatic lock on computers when extended period away from computer • Staff reminded of responsibilities, for example not to share passwords • Dissemination limiting markers applied to all emails • Permissions Policy and Business IT Systems Permission Plans (in development) • Physical security access controls on all Portfolio buildings **Records management** • Appropriate and timely storage or disposal of sensitive or confidential information. • Acceptable Use of ICT Resources Policy and declaration signed on commencement for all staff and contractors • Access to Portfolio IT systems is closed as staff conclude employment. There is a separation checklist available on the intranet. • Auditing ICT security controls for business systems on request • Use of Objective Connect to transfer large documents to external stakeholders

view sensitive ACT Government records **Loss of data** • Loss of data following a business interruption event resulting in staff taking unfair advantage of the situation (e.g. stealing assets not recorded, demanding inappropriate payments etc.)		**Audit** • The ACT Audit Office reviews some system audit logs and access controls as part of the end of financial year audit • Shared Services ICT Security undertakes regular review and reporting of generic user accounts and access **Shared Services** • Administrator access to the ACTGov network is limited • User-ids protected by a secure password which must be changed at regular intervals • External access is audited and ongoing access requirements are questioned with inactive users removed • Staff separation/exit process initiates the removal from systems access • Electronic devices are restored to factory settings when returned

Consequence Rating	Likelihood Rating	Current Level of Risk	Control Effectiveness Rating	Risk Owner	Treatment Action Plan Required
Major	**Possible**	**High**	**Room for improvement**	**SERBIR/CEOs**	**Yes**

RISK REFERENCE	3

RISK DESCRIPTION/RISK EVENT	Misuse of public property and money

SOURCE: How can this happen, the drivers of the risk event	IMPACT/OUTCOME: If what can happen does happen what is the most likely consequence	RISK CONTROLS CURRENTLY IN PLACE: Actions Taken
Assets • Assets stolen or borrowed without permission, including portable and attractive items. • Unauthorised or unlawful access to Portfolio premises resulting in theft or damage to assets and/or loss of information. • Excessive private use of office resources and equipment (phones, internet, photocopiers). • Unauthorised use of government vehicles, petrol cards and petrol. • Unauthorised use of Cab charge vouchers/MyWay Cards/Uber and GoGet. **Cash handling (where applicable) and credit cards** • Theft or borrowing of petty cash. • Submission of false petty cash claims. • Receipts not issued for money received. • False travel/expense claims made by staff. • Misuse or unauthorised use of credit card/fuel card/MyWay card. • Late acquittal of credit card transactions. • Inappropriate or non-existent management of records. **Payment of invoices** • False invoices accepted resulting in payment for goods not received or not ordered for work purposes. • Collusive practice between supplier and purchasing officer resulting in invoice price higher than approved on ordering. • System is manipulated resulting in EFT payments to non-existent supplier. **Staff** • Fraudulent claims for leave (including not submitting leave applications) and attendance records.	**Financial** • Additional expenditure on replacement assets • Additional expenditure on petrol, vehicle wear and tear and Cab charge vouchers/MyWay Cards. • Reimbursement required for money missing from petty cash advances. • Additional audit expenditure required to conduct investigations. **Loss of reputation** • Loss of reputation, trust and confidence in the Portfolio • Adverse media attention. • Difficult to justify future requests for assets **People** • Loss of productive staff time due to misuse of resources during working hours, resulting in increased workload pressures for other staff members in the team • Negative impact on staff morale and culture **Business operational** • Litigation and compliance actions	• Director-General/CEO Financial Instructions in place and accessible by all staff • Human Resource Delegations, under the Public Sector Management Act and Enterprise Agreements **Assets** • Adequate building security and authorised issue and use of access passes • Centralised authorisation for purchase/lease of ICT assets • Portable and Attractive Asset Database and annual returns to CMTEDD • Assets given a number and recorded in a Fixed Assets Register that is maintained and regularly updated • Digital Solutions undertakes audits of ICT assets as time allows • All Cab charge vouchers are signed out by the staff member and the stub and receipt must be returned to the office manager/relevant finance officer for processing • Petty cash reimbursement processes for Uber and GoGet • Regular review/audit of usage of government vehicles, travel and assets • Staff are required to fill in the vehicle log book or electronic log book before operating a government vehicle • Staff are required to fill in a Vehicle Use Form before operating a government vehicle • Acceptable Use of ICT Resources Policy and declaration signed on commencement for all staff and contractors • Uber and GoGet used in accordance with relevant policies. • MyWay Card Register for bus and light rail travel. **Cash handling** • Copies of travel/expense receipts and reimbursements kept on file alongside management approvals • Security Operating Procedures – Cash, Cheque, EFTPOS Security • Reviews of cash handling practices are regularly undertaken **Credit Cards** • Some credit card usage has been audited and recommendations have been made in relation to card limits • Credit card holders are reminded of outstanding acquittals by Shared Services/relevant finance officer • Shared Services Finance/relevant finance officer contacts credit card

			holders with outstanding acquittals to remind them to process acquittals in a timely manner. **Payment of invoices** • Appropriately delegated staff member approves expenditure. • Centralised authorisation for purchase/lease of ICT assets • Segregation of responsibility between recommending invoices be paid and the decision to pay an invoice • All payments authorised and made on the basis of valid supporting documentation. **Staffing** • Staff submit attendance records regularly and managers process these and leave applications in a timely manner, ensuring these records are up to date and accurate in accordance with Enterprise Agreements. • Managers remind staff of their obligations on a regular basis and address any issues in a timely manner, including seeking assistance from People and Capability should concerns arise.		
Consequence Rating	**Likelihood Rating**	**Current Level of Risk**	**Control Effectiveness Rating**	**Risk Owner**	**Treatment Action Plan Required**
Moderate	**Possible**	**Medium**	**Room for improvement**	**SERBIR/CEOs**	**Yes**

RISK REFERENCE	4
RISK DESCRIPTION/RISK EVENT	Misuse of delegations, position and/or workplace entitlements

SOURCE: How can this happen, the drivers of the risk event	IMPACT/OUTCOME: If what can happen does happen what is the most likely consequence	RISK CONTROLS CURRENTLY IN PLACE: Actions Taken
Delegations and decision-making • Staff involved in decision making or monitoring may have a personal or financial interest in the decision • Staff member approving expenditure or making a decision without the relevant delegation • Staff member making decision, including in relation to expenditure, without appropriate authorisation/delegation • Staff member using delegated position to order goods and services for personal use • Fraud committed through negligence as a result of manager/supervisor not checking claims for payment before approval **Recruitment** • Unauthorised staff appointments • Appointments made other than on merit • Falsification of qualifications • Applicants not providing full information, including in relation to having been subject to misconduct proceedings • Conflict of interest due to a relationship between a member of a recruitment panel and an applicant **Position** • Abuse of position and power for personal gain, including seeking and obtaining bribes in exchange for favourable treatment, creating 'ghost' employees profiles to receive payment • Making decisions which benefit the decision-maker in breach of conflict of interest processes • Bribery influencing decision-making **Workplace entitlements** • Overtime claimed without authorisation • Timesheets altered to increase hours worked • Favourable roster to benefit specific staff • Leave taken exceeds entitlement • Collusion between staff to cover unauthorised absenteeism • Conducting personal business during working hours	**People** • Failure to engage or retain staff • Negative impact on culture and staff morale **Business operational** • Litigation and compliance actions **Financial** • Misuse of government funds • Additional audit expenditure and resources required to conduct investigations **Reputation and Image** • Loss of reputation, trust and confidence in the Portfolio • Adverse media attention	**Delegations and decision-making** • The EPSDD, the Agency and the Authority's delegations register and/or delegations matrix is accessible to all staff on the intranet in relation to legislation administered by EPSDD, the Agency and the Authority • Director-General/CEO Financial Instructions in place and accessible by all staff • Human Resources Delegations are in place and accessible by all staff • Delegations and appointment instruments and register reviewed regularly (every 12 months, or otherwise on a needs basis) to ensure accuracy and currency for delegations and appointment • Good Administrative Decision-Making training provided as part of the Learning and Development Framework • Conflict of interest factsheet in place and accessible by staff **Recruitment** • Recruitment and Staff Selection training is currently being delivered to senior managers across the Portfolio. This training provides information regarding obligations, including conflict of interest processes and unconscious bias, and will form part of the essential training package for all staff in the future • Staff are required to conduct all recruitment in line with the ACTPS Recruitment Guidelines • A delegate that is independent to the recruitment panel must sign off on all documents relating to a selection recommendation. Delegates should attend Recruitment and Staff Selection training and ensure they are familiar with the ACTPS Recruitment Guidelines. • Certified copies of original documentation are required to verify personal and professional details of new staff **Workplace entitlements** • All leave is requested and approved in accordance with the Enterprise Agreements • Objective electronic approval tracking records completion and approval of timesheets • Manager approval of salary reports • Staff submit attendance records regularly and managers process these and leave applications in a timely manner, ensuring these records are up to date and accurate in accordance with Enterprise Agreements.

				• Managers remind staff of their obligations on a regular basis and address any issues in a timely manner, including seeking assistance from People and Capability should concerns arise.	
Consequence Rating	**Likelihood Rating**	**Current Level of Risk**	**Control Effectiveness Rating**	**Risk Owner**	**Treatment Action Plan Required**
Moderate	**Possible**	**Medium**	**Room for Improvement**	**SERBIR/CEOs**	**Yes**

Risk Treatment Action Plan

A risk treatment action plan is required for all risks rated as **"Extreme"** or **"High"** or where the control effectiveness rating is **"room for improvement"** or **"inadequate."**

Risk Ref No.	**Risk Description/Risk Event** What can happen?	**Additional Actions (treatments) to be taken to manage the risk**	Consequence	Likelihood	Residual Risk Rating	Control Effectiveness	**Implementation and Review**		
							Responsible Officer *(Officer responsible for implementation and review)*	**Implementation Date** *(Date to be completed by)*	**Progress Review Date** *(Review the progress of implementation of the risk treatment)*
1	Fraudulent or corrupt conduct occurs when procuring goods or services	EPSDD will provide fraud, corruption and integrity training, including details of the role and responsibilities of the SERBIR, Disclosure Officers and managers. Specific training is being provided to senior managers as part of the Learning Framework, including on Integrity and Procurement. An eLearning course on Fraud, Corruption and Ethics as part of the Learning Essentials Framework is available to all Portfolio staff. Rolling procurement audits have been included on the EPSDD Internal Audit Program. The City Renewal Authority has advised a procurement audit has recently been undertaken and will be covered again in the next financial year. The Suburban Land Agency has advised a procurement audit has recently been undertaken and that procurement will be included in future audits.	**Moderate**	**Possible**	**Medium**	**Adequate**	Executive Branch Manager, Governance, Compliance and Legal Services Executive Branch Manager, People and Capability Senior Director, Legal Services and Integrity EPSDD - Audit and Risk and Audit Committee City Renewal Authority - Chief Operating Officer and Audit and Risk Committee Suburban Land Agency -Agency Secretary and Governance Manager and Board Audit and Risk Committee	March 2020	December 2019

Risk Ref No.	**Risk Description/Risk Event** What can happen?	**Additional Actions (treatments) to be taken to manage the risk**	Consequence	Likelihood	Residual Risk Rating	Control Effectiveness	**Implementation and Review**		
							Responsible Officer *(Officer responsible for implementation and review)*	**Implementation Date** *(Date to be completed by)*	**Progress Review Date** *(Review the progress of implementation of the risk treatment)*
2	Failure to protect personal and corporate information	EPSDD will provide fraud, corruption and integrity training, including details of the role and responsibilities of the SERBIR, Disclosure Officers and managers. Specific training is being provided to senior managers as part of the Learning and Development Framework, including on Integrity. An eLearning course on Fraud, Corruption and Ethics and Records Management, as part of the Learning Essentials Framework, is available to all Portfolio staff. Review and update of the Information Privacy Policy Provide advice to staff on the use of Objective Connect to share large volume of documents with people outside of the Portfolio	**Major**	**Possible**	**High**	**Adequate**	Executive Branch Manager, Governance, Compliance and Legal Services Executive Branch Manager, People and Capability Senior Director, Legal Services and Integrity Information and Knowledge Management Digital Solutions	March 2020	December 2019
3	Misuse of public property and money	EPSDD will provide fraud, corruption and integrity training, including details of the role and responsibilities of the SERBIR, Disclosure Officers and managers. Specific training is being provided to senior managers as part of the Learning Framework, including on Integrity. Audit of asset registers EPSDD Strategic Finance team to review and revise/develop and implement guidance of cash handling procedures	**Moderate**	**Possible**	**Medium**	**Adequate**	Executive Branch Manager, Governance, Compliance and Legal Services Senior Director, Legal Services and Integrity EPSDD - Audit and Risk City Renewal Authority – Chief	March 2020	December 2019

Risk Ref No.	Risk Description/Risk Event What can happen?	Additional Actions (treatments) to be taken to manage the risk	Consequence	Likelihood	Residual Risk Rating	Control Effectiveness	Implementation and Review		
							Responsible Officer *(Officer responsible for implementation and review)*	**Implementation Date** *(Date to be completed by)*	**Progress Review Date** *(Review the progress of implementation of the risk treatment)*
							Operating Officer Suburban Land Agency - Secretary and Governance Manager Chief Financial Officers		
4	Misuse of delegations, position and/or workplace entitlements	EPSDD will provide fraud, corruption and integrity training, on the role and responsibilities of the SERBIR, Disclosure Officers and managers EPSDD Legal Services and Integrity to coordinate the review of appointments and delegations under legislation administered by EPSDD at least annually People and Capability to review Human Resource Delegations at least annually Finance Units to review DG/CEO Financial Instructions at least annually EPSDD providing Good Administrative Decision-Making training as part of the Learning and Development Framework Employees and managers to apply and approve staff entitlements in accordance with the Enterprise Agreements and relevant policies. People and Capability to review, develop and promote policy guidance and the role and responsibilities of employees and managers periodically	**Moderate**	**Possible**	**Medium**	**Adequate**	Executive Branch Manager, Governance and Legal Services Executive Branch Manager, People and Capability Senior Director, Legal Services and Integrity Finance Units	March 2020	December 2019

			Consequence				
			Insignificant	Minor	Moderate	Major	Catastrophic
		Assets	Loss or destruction of assets up to $2,000	Loss or destruction of assets $2,000 to $10,000	Loss or destruction of assets $10,000 to $100,000	Loss or destruction of assets $100,000 to $5M	Loss or destruction of assets greater than $5M
		Compliance/ regulation	Non-compliance with work policy and standard operating procedures which are not legislated or regulated	Numerous instances of non-compliance with work policy and standard operating procedures which are not legislated or regulated	Non-compliance with work policy and standard operating procedures which require self reporting to the appropriate regulator and immediate rectification.	Restriction of business operations by regulator due to non-compliance with relevant guidelines and / or significant non-compliance with policy and procedures which threaten business delivery.	Operations shut down by regulator for failing to comply with relevant guidelines and /or significant non-compliance with internal procedures could result in failure to provide business outcomes and service delivery.
		People	Injuries or ailments not requiring medical treatment.	Minor injury or First Aid Treatment Case.	Serious injury causing hospitalisation or multiple medical treatment cases.	Life threatening injury or multiple serious injuries causing hospitalisation.	Death or multiple life threatening injuries.
		Environment	Limited effect to something of low significance	Transient, minor effects	Moderate, short-term environmental harm	Significant, medium-term environmental harm	Long term environmental harm
		Financial	1% of Budget or <$5K	2.5% of Budget or <$50K	> 5% of Budget or <$500K	> 10% of Budget or <$5M	>25% of Budget or >$5M
		Products and Services	No disruption to services	Minor disruption to services for up to 1 month	Total cessation of service for up to 1 days and subsequent disruption of 1 to 2 months	Total cessation of service for up to 7 days and subsequent disruption of 2 to 3 months	Total cessation of service for more than 1 week and disruption over subsequent months involving a major facility
		Technology	Interruption to electronic records and data access less than ½ day.	Interruption to electronic records and data access ½ to 1day	Significant interruption (but not permanent loss) to data and electronic records access, lasting 1 day to 1 week	Complete, permanent loss of some electronic records and/or data, or loss of access for more than one week	Complete, permanent loss of all electronic records and data
		Reputation & Image	Internal Review	Scrutiny required by internal committees or internal audit to prevent escalation.	Scrutiny required by external committees or ACT Auditor General's Office, or inquest, etc.	Intense public, political and media scrutiny. E.g.: front page headlines, TV, etc.	Assembly inquiry or Commission of inquiry or adverse national media.
		Cultural & Heritage	Low-level repairable damage to commonplace structures	Mostly repairable damage	Permanent damage to items of cultural significance	Significant damage to structures or items of cultural significance	Irreparable damage to highly valued items of cultural significance
		Business Process & Systems	Minor errors in systems or processes requiring corrective action, or minor delay without impact on overall schedule.	Policy procedural rule occasionally not met or services do not fully meet needs.	One or more key accountability requirements not met. Inconvenient but not client welfare threatening.	Strategies not consistent with Government's agenda. Trends show service is degraded.	Critical system failure, bad policy advice or ongoing non-compliance. Business severely affected.
Likelihood	Frequency		Matrix	1	2	3	4	5
	Almost Certain	Is expected to occur in most circumstances	>1 in 10	5	Medium	High	High	Extreme	Extreme
	Likely	Will probably occur	1 in 10 - 100	4	Medium	Medium	High	High	Extreme
	Possible	Might occur at some time in the future	1 in 100 – 1,000	3	Low	Medium	Medium	High	Extreme
	Unlikely	Could occur but doubtful	1 in 1,000 – 10,000	2	Low	Medium	Medium	High	High *
	Rare	May occur but only in exceptional circumstances	1 in 10,000 – 100,000	1	Low	Low	Medium	Medium	High *

Priority for Attention / Action		
Priority	Suggested Timing of Treatment	Authority for continued tolerance of risk
Extreme	Short term – normally within one month * Detailed action plan required	Director- General
High	Medium term – normally within three months Needs senior management attention	Senior Executive
Medium	Normally within 1 year Specify management responsibility	Managers
Low	Ongoing control as part of a management system Manage by routine procedures	All staff

Risk Control Effectiveness	
Control Effectiveness	Guide
Adequate	Nothing more to be done except review and monitor the existing controls. Controls are well designed for the risk, are largely preventative and address the root causes and Management believes that they are effective and reliable at all times. Reactive controls only support preventative controls.
Room for Improvement	Most controls are designed correctly and are in place and effective however there are some controls that are either not correctly designed or are not very effective. There may be an over-reliance on reactive controls. Some more work to be done to improve operating effectiveness or Management has doubts about operational effectiveness and reliability.
Inadequate	Significant control gaps or no credible control. Either controls do not treat root causes or they do not operate at all effectively. Controls, if they exist are just reactive. Management has no confidence that any degree of control is being achieved due to poor control design and/or very limited operational effectiveness.