CITY OF BELMONT ACTION PLAN
as required s7.12A(4)

AUDIT DETAILS	MANAGEMENT RESPONSE	ACTION	TIMEFRAME
Information Systems Audit Report 2020- Local Government Entities **Office of the Auditor General's Performance Report 27: 2019-20 25 June 2020** Part One: Security Gap Analysis Recommendations 1. understand and assess the risks unique to their business activities and environment to inform their strategy for information security management. 2. assess their controls against good practice standards to identify gaps and develop plans to improve information security. 3. implement processes to continuously monitor and improve information security controls to ensure that they meet entity needs.	**Responsible Officer: Director Corporate & Governance** **Comments:** City will review the OAG recommendations and undertake risk assessment to understand and identify gaps in security controls, practices and processes.	1. Review OAG recommendations 2. Carry out risk assessment to understand and identify gaps in security controls, practices and processes 3. Update and inform relevant strategies, policies and plans 4. Implement processes to continuously monitor and improve information security controls	June 2021
Information Systems Audit Report 2020- Local Government Entities **Office of the Auditor General's Performance Report 27: 2019-20 25 June 2020** Part 2 General Controls **Recommendations** 1. Information security To ensure security strategies align with, and support, business objectives senior executives should implement appropriate frameworks and management structures. Management should ensure good security practices and controls are implemented and continuously monitored. 2. Business continuity Local government entities should have an appropriate business continuity plan, disaster recovery plan and incident response plan to protect critical services and systems from disruptive events. These plans should be tested on a periodic basis to ensure unexpected events do not affect business operations. 3. Management of IT risks Local government entities need to identify threats and risks to their operations arising from information technology. These should be	**Responsible Officer: Director Corporate & Governance** **Comments:** City will review the OAG recommendations and undertake risk assessment to identify opportunities to further strengthen and manage information security general controls and practices.	1. Review OAG recommendations. 2. Carry out risk assessment to identify opportunities to further strengthen and manage information security general controls and practices 3. Update and inform relevant strategies, policies and plans 4. Implement processes to continuously monitor and improve information security, business continuity, IT risks, IT operations, change management and physical security of IT infrastructure and assets	1. Completed 11/2019 2. Completed 11/2019 3. Completed 4. Progressing– substantial progress towards implementation of required changes.

AUDIT DETAILS	MANAGEMENT RESPONSE	ACTION	TIMEFRAME
assessed and treated within appropriate timeframes. These practices should become a core part of business activities and have executive oversight. 4. IT operations Local government entities should use good practice standards and frameworks as a reference to implement good controls for IT operations. Entities should have appropriate policies and procedures in place to manage incidents, IT risks, information security and business continuity. Additionally, entities should ensure IT strategic plans and objectives support their overall business strategies and objectives. 5. Change control Change control processes should be well developed and consistently followed when applying patches, updating or changing computer systems. All changes should be subject to thorough planning and impact assessment to minimise the occurrence of problems. Change control documentation should be current, and approved changes formally tracked. 6. Physical security Local government entities should develop and implement physical and environmental control mechanisms to prevent unauthorised access or accidental or environmental damage to computing infrastructure and systems.			