CALGARY MUNICIPAL LAND CORPORATION – CONTROL ENVIRONMENT ASSESSMENT
June 2024

COMPONENTS OF INTERNAL CONTROL		DESCRIPTION (EXAMPLES)	CURRENT ASSESSMENT	FURTHER ACTIONS PLANNED
1	CONTROL ENVIRONMENT	The overall control environment at CMLC is critical in ensuring that the Internal Controls Over Financial Reporting (ICFR) operates efficiently and effectively.	CMLC has a strong control environment. CMLC's governance structure is set by Council through a Unanimous Shareholder Agreement and includes a Board of Directors which in turn has appointed an Audit and Finance Committee. As part of its terms of reference, CMLC's Audit and Finance Committee oversees the integrity of CMLC's financial statements and the system of disclosure and internal controls. The President & CEO and CFO / VP, Corporate Services meet and provide representations to the External Auditor describing how their responsibilities are discharged.	Ongoing review and active application of control policies and procedures and documentation. Keeping current on new accountability requirements and industry standards to ensure control policies and procedures remain appropriate.
		City Council sets the overall tone for internal controls for all business units. The CMLC Board and management contribute to this tone through its operating practices, integrity, and adherence to core values.	There is a culture and operating practices at CMLC that deliberately and emphatically produce an environment of strong financial control. CMLC has a conservative and careful approach to financial management. CMLC follows industry best practices for the acquisition of goods and services required to fulfill its mandates. CMLC has a code of conduct in place for its staff, and for its Board members.	CMLC will continue to stress the importance of a strong control environment by remaining aware of City initiatives in this regard.

CALGARY MUNICIPAL LAND CORPORATION – CONTROL ENVIRONMENT ASSESSMENT
June 2024

COMPONENTS OF INTERNAL CONTROL		DESCRIPTION (EXAMPLES)	CURRENT ASSESSMENT	FURTHER ACTIONS PLANNED
2	RISK ASSESSMENT	An overall risk assessment should help determine the highest risk areas at CMLC that could impair the achievement of objectives.	• The Audit and Finance Committee reviews Risk Management on a regular basis. The last update was completed in 2023.	• The Audit and Finance Committee update the overall risk assessment for CMLC on an annual basis in addition to a mid year review.
3	CONTROL ACTIVITIES	Control activities include policies, procedures, documented approvals, reconciliations, verifications, reviews, physical security, segregation of duties, and so on.	• Controls are monitored and updated on a regular basis as the dynamics of the organization changes. The Audit and Finance Committee is informed of the changes at Board committee meetings by management. All the process and control procedures are posted on the CMLC intranet site for staff to review. • These controls include: clear delegation of signing authority which requires dual signatures on all purchases according to specified limits. Dual signatures are also required on all cheques. • In addition, the CICA Handbook requires external auditors to be more proactive in assessing control activities and the risk of fraud. This provides more independent feedback on CMLC's existing controls.	• Management reviews and updates policies and control procedures on an on-going basis. The Audit and Finance Committee reviews the policies and control procedures for CMLC on an annual.
4	INFORMATION AND COMMUNICATION	There should be a continuous flow of financial reporting and information throughout CMLC to support the strong control environment.	• Monthly financial reports are used as a foundation for control activity. • Cash flows are monitored on a weekly basis. • Relevant information is disseminated through staff, management, and Board meetings.	• CMLC continues to meet with City of Calgary Finance representatives (Treasury) on a quarterly basis. • CMLC also meets with Council twice a year and provides a financial update during those meetings. • Staff will be apprised as new or revised policies, procedures, and controls are developed.

CALGARY MUNICIPAL LAND CORPORATION – CONTROL ENVIRONMENT ASSESSMENT
June 2024

COMPONENTS OF INTERNAL CONTROL		DESCRIPTION (EXAMPLES)	CURRENT ASSESSMENT	FURTHER ACTIONS PLANNED
5	MONITORING	Ongoing monitoring occurs in the normal course of operations and includes regular management and supervisory activities and other actions by personnel as part of the assessment of internal controls.	• The Business Plan and Budget is monitored to ensure objectives are achieved. • CMLC reviews its financial policies on a regular basis to ensure compliance. • Financial reconciliations are performed on a monthly basis to ensure accuracy and completeness of accounts payable. • Monthly financial statements are prepared for review by management. • Quarterly financial statements are prepared for review by management and Audit and Finance Committee. • Infrastructure project budgets are reviewed on a monthly basis and any variances are immediately followed up. • Change orders are required for all changes to contracts.	• Continued monitoring and enforcing compliance with policies and procedures. The Board and Management emphasize a control conscious environment that supports the business processes.
6	INFORMATION TECHNOLOGY – DISASTER RECOVERY	CMLC's business needs require business continuity and high availability. In order to accomplish this, disaster recovery infrastructure and methods have been implemented.	• Real time data replication (5-minute delay maximum) to an off-site datacenter. This system is tested with management oversight annually. • The Disaster Recovery Point Objective (maximum amount of potential data loss due to a disaster situation) is less than 10 minutes. • The Recovery Time Objective (time from disaster status until data and services are operating on the off-site datacenter servers) is under 4 hours. • A disaster recovery plan is available to all staff on the shared office network drive, and is reviewed annually. • Internal IT audits of the Disaster Recovery infrastructure are done periodically to ensure all hardware and methods are up to date and functioning properly. • Co-located Exchange/Email servers provide redundancy and high availability. In the case of a disaster situation, email roles are taken over by the standby server in the off-site datacenter.	• Continued monitoring and annual testing of the systems to ensure business continuity by Management. Audit and Finance Committee updated on IT activities on a quarterly basis.

CALGARY MUNICIPAL LAND CORPORATION – CONTROL ENVIRONMENT ASSESSMENT
June 2024

	OTHER INFORMATION TECHNOLOGY SECURITY MEASURES	We have implemented procedures to protect CMLC from cyber attacks.	• Office365 Multi-Factor Authentication (MFA) - Account logins utilize random-generated security codes as additional layer of authentication – can eliminate up to 95% or more of account compromises. • Exchange upgrade - Exchange Online - Microsoft is pushing for customers to get off of on premises Exchange servers and move to the cloud. Exchange Online is better protected against attacks like the recent HAFNIUM attack. Includes user mailboxes under MFA protection for logins. Evolution of disaster recovery and business continuity for Exchange. • Bitlocker on CMLC laptops - Encryption of laptop hard drives – if a laptop is stolen, it's data can be protected if the thief were to remove the hard drive to extract data. • Immutable backups - Specialty disk storage that can only be read, but not altered. New standard in protection against would-be ransomware attackers – protects backups from being encrypted or deleted. • Cloud backups - Move away from tape backups, offsite backups to the 'cloud', housed securely at Ci2 datacenters. Offsite, but local (YYC), for quick restores in case of emergencies. • Hardware - Industry leading Unified Threat Management from Fortinet inspects every piece of internet traffic and detects malicious code, traffic to/from botnets, compromised websites, spam, proxies, etc. • Enterprise level monitoring and Anti-Virus - N-Able enterprise monitoring and antivirus provides desktop, laptop, and server protection and alerts the IT team in the case of any detection. N-Able also tracks IT assets, and provides remote access and alerting on other issues. • Secure file systems - NTFS security and share permissions lock down unauthorized access to network files. Best practices are implemented to prevent rogue accounts to gain access through security loop holes. • Secure WiFi - Guest and Corporate WiFi is separated. Only approved corporate devices are	• Continued monitoring and monthly meetings between Management and IT consultants to ensure standards are being met.

CALGARY MUNICIPAL LAND CORPORATION – CONTROL ENVIRONMENT ASSESSMENT
June 2024

			connected to the internal WiFi and the password is never given out. • Secure passwords • Security Orders - In response to emerging threats, security orders are implemented and executed at the highest priority. • 3-2-1 Backup Standard for Data - In the case of a successful cybercrime breach, the highest industry standard for data backup has been implemented and is audited regularly. • Education - Staff are educated through IT Bulletins and in person training what to look for and how to respond to unfamiliar requests and system behavior. Requests are escalated immediately with the security team.	