Computer Methods International Corp.

System and Organization Controls 3 (SOC 3) report relevant to Security, Availability and Confidentiality for the CMiC Software as a Service (SaaS) Solution for the period January 1, 2023 to December 31, 2023

Table of Contents

Deloitte.

Section 1 – Independent Service Auditor's Report

To: Management of Computer Methods International Corp. ("CMiC", the "Company" or the "Service Organization")

Scope

We have been engaged to report on CMiC's accompanying management statement titled "Statement by Management of CMiC" ("statement") that the controls within CMIC's Software as a Service (SaaS) Solution ("system") were effective throughout the period January 1, 2023 to December 31, 2023, to provide reasonable assurance that CMiC's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability and confidentiality ("applicable trust services criteria") set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, "*Trust Services Criteria"*).

The accompanying statement and the Description of the Boundaries of CMiC's Software as a Service (SaaS) Solution indicate that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at CMiC, to achieve CMiC's service commitments and system requirements based on the applicable trust services criteria. The Description of the Boundaries of the CMiC's Software as a Service (SaaS) Solution presents the complementary user entity controls assumed in the design of CMiC's controls. Our engagement did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

CMiC uses Amazon Web Services, Inc. ("Amazon" or "AWS") and OnX Enterprise Solutions Ltd. ("OnX") (collectively "subservice organizations" or "cloud service providers") for cloud infrastructure services. The accompanying management statement and the Description of the Boundaries of CMiC's Software as a Service (SaaS) Solution indicate that certain service commitments and system requirements based on the applicable trust services criteria can be met only if certain types of controls that management expects to be implemented at the subservice organizations are suitably designed, implemented and operating effectively. The Description of the Boundaries of the CMiC's Software as a Service (SaaS) Solution presents the types of complementary subservice organizations controls assumed in the design of the CMiC's controls. Our engagement did not include the services provided by the subservice organizations, and we have not evaluated whether the controls management expects to be implemented at the subservice organizations have been implemented or whether such controls were suitability designed and operating effectively throughout the period January 1, 2023 to December 31, 2023.

Service Organization's Responsibilities

CMiC is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that CMiC's service commitments and system requirements were achieved. CMiC has also provided the accompanying statement about the effectiveness of controls within the system. When preparing its statement, CMiC is responsible for selecting, and identifying in its statement, the applicable trust services criteria and for having a reasonable basis for its statement by performing an assessment of the effectiveness of the controls within the system.

Deloitte.

Our Independence and Quality Management
We have complied with the relevant rules of professional conduct / code of ethics applicable to the practice of public accounting and related to assurance engagements, issued by various professional accounting bodies, which are founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

The firm applies Canadian Standard on Quality Management 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements*, which requires the firm to design, implement and operate a system of quality management, including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Service Auditors' Responsibilities
Our responsibility, under this engagement, is to express an opinion, based on the evidence we obtained , on whether management's statement that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.

Our engagement was conducted in accordance with Canadian Standard on Assurance Engagements 3000, *Attestation Engagements Other than Audits or Reviews of Historical Financial Information*, set out in the CPA Canada Handbook – Assurance. This standard requires that we plan and perform our engagement to obtain reasonable assurance about whether management's statement is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our reasonable assurance engagement included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve CMiC's service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve CMiC's, service commitments and system requirements based on the applicable trust services criteria
- Performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations
There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become ineffective because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's statement that the controls within CMiC's SaaS Solution were effective throughout the period January 1, 2023, to December 31, 2023, if complementary subservice and user entity controls contemplated in the design of CMiC's controls operated effectively, to provide reasonable assurance that CMiC's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Deloitte LLP
Chartered Professional Accountants
Toronto, Ontario, Canada
March 19, 2024

Section 2 – Statement by Management of CMiC

We are responsible for designing, implementing, operating, and maintaining effective controls within Computer Methods International Corporation ("CMiC", the "Company" or the "Service Organization") related to the Software as a Service (SaaS) Solution throughout the period January 1, 2023, to December 31, 2023, to provide reasonable assurance that CMiC's service commitments and system requirements relevant to security, availability, and confidentiality were achieved. Our description of the boundaries of the system is presented in Section 3 and identifies the aspects of the system covered by our statement.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period January 1, 2023, to December 31, 2023, to provide reasonable assurance that CMiC's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*. CMiC's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Sections 3 and 4.

CMiC uses Amazon Web Services. Inc. ("Amazon" or "AWS") and OnX Enterprise Solutions Ltd. ("OnX") (collectively "subservice organizations" or "cloud service providers") for cloud infrastructure services. This statement and the Description of the Boundaries of CMiC's Software as a Service (SaaS) Solution indicate that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls for CMiC, to achieve its service commitments and system requirements related to the delivery of its services as it relates to CMiC's Software as a Service (SaaS) system based on the applicable trust services criteria. The accompanying Description of the Boundaries of CMiC's Software as a Service (SaaS) Solution presents the types of complementary subservice organization controls assumed in the design of CMiC's controls. The actual controls at the subservice organization are not disclosed.

This statement and the Description of the Boundaries of CMiC's Software as a Service (SaaS) Solution indicate that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at CMiC to achieve its service commitments and system requirements related to the delivery of its services as it relates to CMiC's Software as a Service (SaaS) Solution based on the applicable trust services criteria. The accompanying Description of the Boundaries of CMiC's Software as a Service (SaaS) Solution presents the complementary user entity controls assumed in the design of CMiC's controls.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We confirm that the controls within the system were effective throughout the period January 1, 2023, to December 31, 2023, to provide reasonable assurance that CMiC's service commitments and system requirements were achieved based on the applicable trust services criteria.

Computer Methods International Corporation
March 19, 2024

Section 3 – Description of the Boundaries of CMiC's Software as a Service (SaaS) Solution

3.1 Company Background

Founded in 1974, CMiC is headquartered in Toronto, Ontario, Canada and delivers the most comprehensive and advanced ERP and field operations solutions, purpose-built for construction and capital projects companies. CMiC's customers span the spectrum of construction firms, from general and specialty contractors to heavy/highway and project owners. CMiC's powerful software transforms how firms optimize productivity, minimize risk and drive growth by planning and managing financials, projects, resources, and content assets – all from a single database platform.

3.2 Overview of Products

CMiC has the most complete and flexible software platform for construction firms and project owners. The platform isn't just accounting or project management software; it's construction management software, purpose-built and refined for over three decades to fulfill our customer's unique needs. After deploying CMiC's intelligent construction platform, our customers can operate their entire business with a full array of unified capabilities – sitting on top of a single database platform – that will serve as their foundation for business execution. Given the flexibility of the CMiC solution, our customers can choose from a robust enterprise-wide platform to a more narrowly focused solution to run their financials or empower their field staff.

SSO (Single Sign On) capabilities are available through federation with Microsoft Entra, simplifying the login process and providing IT teams full control over authentication security features, such as multi-factor authentication (MFA) and conditional access policies.

CMiC SaaS Platform can be licensed as a single enterprise-wide software platform, or it can also be deployed as one of two standalone suites of applications ("Application Suite"):

1. CMiC Software – Construction Financials Suite

CMiC ERP and Financials allows customers to manage financials, project controls, human capital and assets (equipment and inventory) effortlessly. It unifies Budgeting, Corporate & Project Forecasting, General Ledger, Accounts Receivable and Accounts Payable in one secure platform and data repository. These core capabilities leverage real-time insights from operational transactions to maximize control over project completion and profitability. CMiC's risk management capabilities are embedded throughout the platform – within ERP & Financials – and beyond, in several components of the system, such as vendor pre-qualification, workers compensation codes and rates tied to jobs, and cash flow management.

Key modules:

CMiC Accounting or Financials

The accounting processes and financial controls specific to construction companies demand attention, as they represent unique challenges when handled through non-specialized tools, such as generic spreadsheets or corporate financial packages. Legacy systems limit individual productivity and increase opportunities for potentially damaging human error to occur.

CMiC Accounting & Financial Controls core functions include:

- General Ledger (GL)
- Corporate Budgeting
- Accounts Receivable (AR)
- Corporate & Project Forecasting
- Accounts Payable (AP)

Financial teams at construction companies can monitor their cash flow more closely, optimize spending, maximize the ability to win new business and ensure on-time, accurate payments which can boost vendor relationships.

CMiC Project Controls

A project manager who has access to accurate and up-to-date reports can manage more effectively than one who must learn from sporadic updates. Furthermore, a team with automation features to assist with everything from bid management to the project schedule can be more productive than one relying too heavily on manual operations.

CMiC Project Controls gives project managers full visibility into their projects. Construction firms continuously monitor project budgets, including time, expenses, suppliers and costs such as, subcontracts and change orders. With seamless access to every version of every document, users stay on top of project changes – and their full impact. Project teams manage subcontractors from start to finish by integrating subcontractor activity into their workflows. Project Controls facilitates the management of data, information and communications related to the bid process, from estimates to buyout, eliminating unnecessary steps and allowing users to drill down into details and make better procurement decisions.

CMiC Asset Management

Construction companies rely heavily on physical assets to run their field operations. As such, their ability to manage their assets efficiently, accurately and on a real-time basis is vital. Furthermore, automating the material requisition and ordering process will help control material costs and optimize equipment spend. Rigorous asset management processes – enabled by the right tools – can make a material difference in the profitability of projects and the overall health of the business.

CMiC Asset Management empowers construction firms to manage fixed assets and equipment more effectively by providing real-time access to information on inventory, maintenance and repair status. With CMiC Asset Management, construction teams take control of material costs, accelerate the procurement process, optimize inventory management and boost operational performance.

CMiC Resource Planning

CMiC Enterprise Planning delivers an enterprise view, a project view, and a sub-activity view of everything that must happen now, and where it's going tomorrow, making this capability essential for forecasting. With CMiC's graphical interface, construction teams easily administer – from an enterprise perspective – both equipment and human soft and hard allocation planning. *CMiC Resource Planning* helps match individual resources to a project's requirements by finding team members according to their skills and availability and pulls the information for each project together into a simple, user-friendly interface. With *Opportunity Management*, construction firms automate their sales force by streamlining bid process tracking and optimizing contact management by storing contacts – whether project related or otherwise – on a single database. *Financial Forecasting* is a high-performance financial budgeting, planning and reporting application that provides flexible, 'what-if' financial modeling capabilities to help construction firms meet their budgeting and ongoing forecasting needs.

CMiC Human Capital Management & Payroll

The construction industry has a multitude of unique labor management requirements – such as strict worker safety compliance and certifications, as well as numerous challenges – such as rapidly fluctuating labor costs driven by intermittent periods of labor shortages. Always knowing where resources are situated, what projects they are working on and what certifications and training programs they have completed is essential for running a profitable construction operation. In

addition, employees – especially those in the field – can greatly benefit from self-service tools to organize and access personal data – including their personal profiles, payroll details, vacation and time off requests, performance reviews and other HR-related information.

CMiC Human Capital Management (HCM) is designed to manage the entire employee lifecycle and meet the unique labor force requirements of the construction industry. *CMiC HCM* is ready out-of-the-box with regulatory reports to make safety compliance and certifications easy. The broad spectrum of capabilities to support operational and administrative staff include talent acquisition, human resource management, payroll, mobile timesheets and employee self-service.

CMiC Enterprise Content Management

The content that builds up during the lifecycle of a construction project, let alone during running a business over several years, can overwhelm any company.

CMiC Enterprise Content Management (ECM) allows users to move content – with simple drag and drop actions – from emails and storage devices into the CMiC platform for easy access and future retrieval. Construction firms enhance organizational effectiveness with *CMiC Workflow*, proactively manage information assets with *Document Control* and easily search through content using *Enterprise Search*. The *Analytics* tool is an embedded dashboard built directly into the CMiC platform to visualize key metrics.

In addition to offering native ECM capabilities, CMiC has built-in integrations with Kofax, DocuSign, BlueBeam, AutoDesk, Oracle/Textura and a plethora of other third-party applications.

2. Construct PM (Project Management), formerly known as CMiC Field

CMiC FIELD has been rebranded as Construct PM and retains and expands all its functionality and capabilities

With Construct PM, project managers and site supervisors control every aspect of project planning, execution and tracking from their laptops, tablets and smartphones. Key modules:

Construct PM

Construct PM is a comprehensive suite of project management and collaboration capabilities. Construct PM enables construction firms to manage project-related communications and subcontractor activity – and gain instant access to information captured from every job site. Construction firms can manage RFIs, drawings & specifications, submittals, meeting minutes, documents & progress photos, daily journals and checklists, punch lists. Users receive proactive alerts and make better-informed decisions backed by accurate and timely data. *Collaboration Management* helps firms to proactively manage and guide communications with vendors during the bid process. With *Site Management*, users enter critical information from the job site in real-time, ensuring that project executives always have access to up-to-date project status information as well as insights about where the project is heading. *Document Management* gives users complete control of the design execution process by facilitating the exchange of plans, documents and communications throughout the design and approval process.

Construct PM – for iOS and Android

Construction companies' teams are always split between multiple locations, with some construction professionals on the job site and others in the office. When both groups of employees have access to the same information in real-time, contractor firms can save time and money, with every department and individual on the same page, guiding the job to completion.

With anytime, anywhere real-time access, an intuitive interface, and the power of CMiC's ERP and Construct PM solutions, CMiC's mobile apps streamline data collection, workflow management and analytical reporting for a construction firm's entire field team. Compatible with iOS and Android devices, CMiC's mobile apps allow users to review, create and edit actionable project data both on and offline.

The scope of this report addresses the security, confidentiality and availability criteria related to CMiC's SaaS Platform.

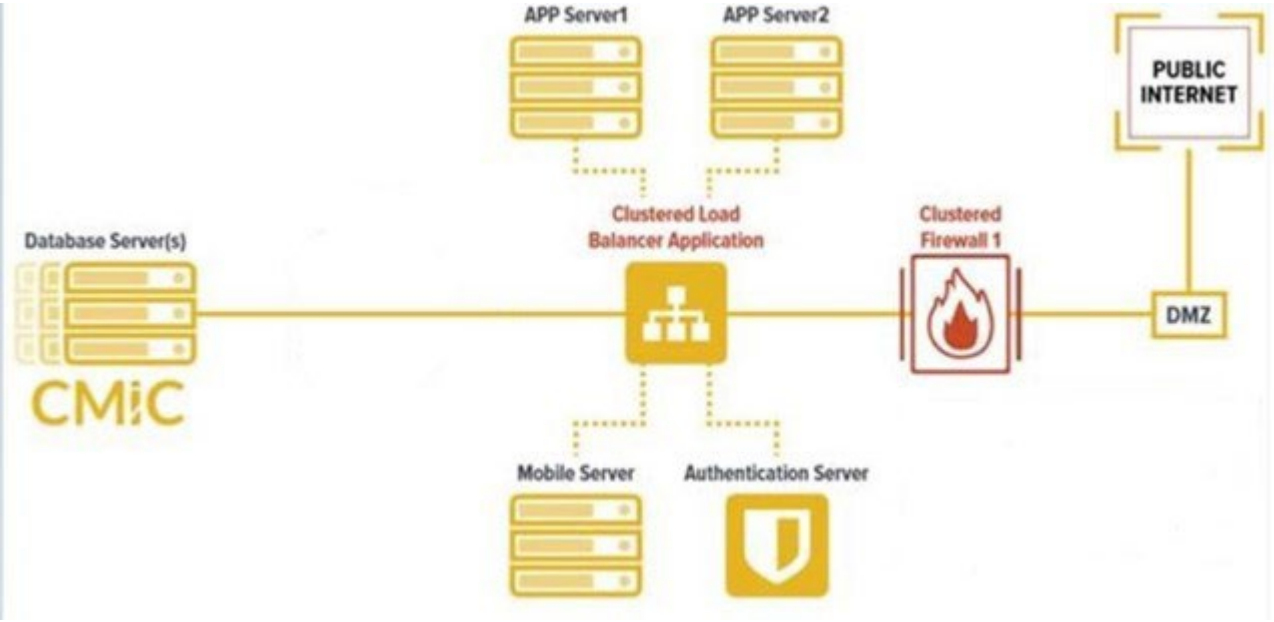
This report is intended to provide information sufficient to understand the relevant aspects of CMiC's control environment for delivery of services to user entities for the period January 1, 2023 trough to December 31, 2023 specifically as it relates to the security, availability and confidentiality criteria.

The scope of this report does not include:

- Processes and controls of other operations performed by CMiC;
- External processes and controls that are performed by user entities of the system; and
- Controls at various organizations that CMiC has made arrangements with to facilitate the delivery of services to its user entities, such as AWS and OnX.

3.3 Components of the SaaS Solution Used to Provide the Services

3.3.1 Infrastructure, Software and Data



The SaaS infrastructure consists of servers, storage, and networking, with cloud-based security including but not limited to Distributed Denial of Service (DDoS) protection and Web Application Firewall (WAF).

1. Cloud Infrastructure Service: Network infrastructure, virtual servers, and operating systems
2. Cloud-based web application firewall for secure access to CMiC Application Suite
3. Server storage and maintenance

Application Support Service:

1. Install patches and updates to the CMiC Application Suite
2. Database start-up and shut down and response to database errors
3. Database management such as: database roll backs, restoration and log management
4. Database parameter management
5. Database optimization

Description of Security Services

CMiC uses a multi-layered security model and provides the following:

1. Data protection – data in transit is encrypted using multiple methods including but not limited to Hypertext Transfer Protocol Secure (HTTPS), Secure Shell (SSH) and Transport Layer Security (TLS).
2. Data at rest is encrypted within the AWS environment.
3. The infrastructure employs various network-level threat protection mechanisms including a web application firewall, distributed denial of services protection, and ingress and egress traffic filtering.
4. Periodic code reviews on the application are performed during development and prior to releasing into production.
5. Using third party penetration testing and other techniques, the production applications and infrastructure are regularly reviewed for vulnerabilities.

CMiC protects its corporate infrastructure by implementing the following controls:

1. Senior Management of CMiC demonstrated their support to cyber security by executing the appropriate oversight function. For example, CMiC has an InfoSec and Privacy Governance Committee that meets bi-monthly to provide management governance and oversight for matters related information, including cyber security, and privacy.
2. Perimeter boundary enforcement through:
    a. Use of a next-generation firewall with policies that control ingress and egress traffic.
    b. Use of Virtual Private Network (VPN) for staff access to support the remote work environment.
3. Implementation of a secure password policy and secure password management tool for appropriate authentication of users.
4. Implementation of user administration processes for granting, modifying and revoking access.
5. A formal risk management framework is used to monitor and manage risks identified.
6. A formal change management process has been implemented to manage changes to infrastructure.
7. A formal incident management process has been implemented to manage security and IT system incidents.
8. SSO (Single Sign On) capabilities are available through federation with Microsoft Entra, simplifying the login process and providing IT teams full control over authentication security features, such as multi-factor authentication (MFA) and conditional access policies.

Description of Confidentiality Service

In addition to the controls implemented to meet the security criteria, CMiC further enforces secure recycling or disposal of physical assets that may contain confidential customer information.

For confidential information stored in AWS, CMiC leverages the controls implemented by AWS for the secure disposal of its physical assets.

Description of Availability Service

To ensure overall system availability targets are met, CMiC has implemented additional controls for monitoring performance and capacity in order to manage availability of critical system components.

3.3.2 People

The following members of the Senior Management are involved in providing oversight and governance to the Cyber Security Program:

1. President and Chief Executive Officer (CEO)
2. Chief Operating Officer (COO)
3. Chief Technology Officer (CTO)
4. Legal Counsel
5. Representatives from the Advisory Board
6. Chief Information Security Officer (CISO)
7. Manager, Information Security

The following roles are involved in the support of the Corporate and SaaS infrastructure:

1. Director of IT and Cloud Infrastructure
2. IT Analysts

The following roles are involved in the maintenance and support of the CMiC Application Suite:

1. Vice President, Application Development / Director of Cloud Operations Support
2. Director of QA & Documentation
3. Database Administrators
4. Hosting & Infrastructure Support Team

To enforce segregation of duties, the Development Team (except the CTO and the Vice President, Application Development) does not normally have access to make change in CMiC's Production Environment. Any temporary access to the production environment must be approved by the CTO or the Vice President, Application Development, and access will be revoked by IT when access is no longer required.

3.3.3 Processes and Procedures

The automated and manual procedures involved in system operations are described in formal documents including but not limited to:

1. Risk Management Framework
2. Change Management Manual
3. Secure Development Manual
4. Systems Security Manual
5. Security Incident Management Manual

3.4 Relevant Aspects of the Control Environment, Risk Assessment Process, Information and Communication, and Monitoring

3.4.1 Control Environment

Management Philosophy

CMiC's control environment reflects the philosophy of senior management concerning the importance of security, availability and confidentiality of the CMiC Application Suite. CMiC's Information, Privacy and Governance Committee (IPGC) meets bi-monthly, under the direction of the Advisory Board and the Officers of CMiC, overseeing the security activities of CMiC. The committee members, comprised from each of the lines of business and include two members on CMiC's Advisory Board, are charged with establishing overall security policies and procedures for CMiC. The importance of security is emphasized within CMiC, through the establishment and communication of policies and procedures, and is supported by investment in resources and people to carry out those policies. In designing its controls, CMiC has taken into consideration the relevance of controls to meet the relevant trust criteria.

Security Management

Policies, practices, and controls have been implemented to secure customer data. CMiC provides a secure multitenant SaaS environment. CMiC IT Team performs regular patches to address known vulnerabilities.

Security Policies and Procedures

The following security policies and related processes are in place for CMiC:

1. Information Security Governance Manual
2. Risk Management & Assessment Methodology (Manual)
3. Information Security Policy
4. Acceptable Use Policy
5. Mobile Device and BYOD Policy
6. Human Resource Security Policy
7. Asset Management Policy
8. Access Control Policy
9. Encryption Policy
10. Physical and Environmental Security Policy
11. Systems Security Policy
12. Network Security Policy
13. Secure Development Policy
14. Vendor and Third-Party Management Policy
15. Information Security Incident Management Policy

Personnel Security

Hiring practices are based on objective criteria and take education, experience and responsibility into consideration. Background checks are conducted as appropriate, and information security awareness training is provided to CMiC staff, with additional secure coding practices training provided to development staff.

Management performs external background checks on final candidates. Employees are required to acknowledge and sign a confidentiality agreement with CMiC. CMiC maintains a Business Ethics Policy that provides clear guidelines for expected conduct for employees as representatives of CMiC.

Physical Security and Environmental Controls

CMiC leverages AWS and OnX for infrastructure services. As such, physical security and environmental controls are addressed by the data centre and cloud service providers.

CMiC is responsible for monitoring the subservice organization relationships and commitments. On an annual basis, CMiC reviews the third-party reports provided by critical service providers, for investigation and resolution of identified deficiencies in physical and environmental controls, where applicable. CMiC also receives and reviews incidents reports and service updates from providers to monitor changes to physical and environmental controls and any incidents that occurred, which may require investigation and resolution.

Change Management

CMiC has a rigorous change management process, and the Change Advisory Board (CAB) meets on a weekly basis to review and approve change requests. Changes are reviewed prior to implementation and monitored post implementation.

Where possible, changes are first carried out in a test environment prior to the being applied to the production environment.

Prior to a change being scheduled, a proper change plan, test plan, back-out plan, and post-implementation review plan is documented and reviewed. Supporting change documentation and approvals are attached within a ticket.

The CAB, in accordance with change management policies, will perform periodic reviews to determine whether procedures were properly documented and followed.

Unplanned or emergency changes may occur if a change is deemed to be critical or is required for resolution of an incident, where the severity of the issue and potential risk require action prior to the next scheduled maintenance window. The change requester would open an emergency change request ticket, log the technical details of the change and request verbal approval from management prior to making the changes. The emergency change will be reviewed in the next CAB meeting and approval granted retroactively.

As an additional control, CMiC uses a cloud-based Security and Incident Event Management (SIEM) tool to monitor the health of the application, the operating systems, and the infrastructure. The SIEM tool produces a list of in scope changes to the SaaS environment on a regular basis.

System Monitoring and Cyber Security Incident Response

CMiC uses a SIEM tool to monitor the security health of the application, the operating systems, and the infrastructure. The SIEM tool utilizes connectors and agents to collect and correlate logs from the critical system components such as, AWS CloudTrail and Microsoft Azure, to provide a high level view of events and incidents across the organization. CMiC leverages the SIEM tool to identify changes to critical systems, threat detection and incident response.

The SIEM is monitored by a 3rd party MDR (Manager, Detect and Response) provider on a 24/7 basis, to detect and respond to incidents and alerts. Any anomalies are addressed by the MDR provider and instances with high severity are escalated to CMiC for review and action.

Access Management

Logical access to information systems security, and administrator privileges to the CMiC SaaS Platform cloud internal infrastructure resources (i.e., host machines, Oracle databases, monitoring servers, etc.) are limited to CMiC employees whose role require such access rights.

Internal infrastructure resources require passwords that comply with strict CMiC password policies. Unique user IDs and strong passwords are in place for administration and client virtual machines. This policy is applicable to CMiC employees. Additions and changes of access rights to cloud servers and databases for CMiC team members are approved and documented. A review process is regularly followed to confirm that Cloud Administrator access privileges remain authorized and appropriate.

Established procedures are in place to protect information systems and technology infrastructure from intrusions and computer infections. Network traffic is encrypted via Transport Layer Security, Secure Shell, or Secure File Transfer Protocol (SFTP) to protect sensitive information during transmission against unauthorized access or modification. Data is also encrypted at rest. Security events are monitored and aggregated by the SIEM tool and incidents are reported to the IT and InfoSec Teams. Any identified security violations are reported to Senior Management.

Data Backup and Recovery

Encrypted backups of systems and data are performed nightly and transferred to an offsite location. CMiC forwards Database Redo logs every 15 minutes to cloud object storage, giving us the ability to recover the data with a 15-minute recovery point objective.

System Account Management

CMiC uses a password management system behind an multi-factor authentication (MFA) protected VPN that grants the appropriate access to the appropriate individuals. Individual MFA protected VPN accounts with unique usernames providing privileged access to specific isolated networks are enforced. Both the password management system and the VPN access are required for specific mission critical networks. Both VPN and the password management system keep a record of logs for a period of one year.

Application Development and Maintenance

CMiC's Systems Development Life Cycle methodology (SDLC) includes the security, availability and processing integrity requirements of the organization. It is regularly reviewed, updated and approved by management.

CMiC's software development process uses an Agile methodology wherein the Quality Assurance (QA) practices include approval and revision/change control during SDLC stages. Application releases follow a formal documentation, design, configuration, and QA stages, with a final review and approval performed prior to release to Production.

Application software changes undergo peer reviews prior to submission to the Quality Assurance Department for QA. CMiC has a dedicated Quality Assurance Department that uses a combination of automated test scripts, software regressions and manual validations, across supported platform combinations. They are the final "gatekeeper" prior to releasing the changes to the production environment within CMiC's SaaS environment.

Regular vulnerability testing by an independent third party is used to provide validation of the security controls as well as identify any outstanding risks that may require remediation.

Vendor Management

Vendors are vetted for appropriate services and service levels. Vendor performance and service levels are monitored on a regular basis.

3.4.2 Risk Assessment Process and Monitoring

A risk management framework has been implemented. As such relevant risks are identified, recorded in a risk register, and reviewed by management on a regular basis.

CMiC has practices in place to assist executive management in identifying and managing risks that could affect CMiC's ability to provide reliable application access and performance for customers. Risk assessments are performed regularly (monthly or as required), with involvement from the Director of IT and Cloud Infrastructure, the Manager of Information Security, and the CTO.

Open incidents with a severity of critical / very high are reviewed on a regular basis to assess underlying cause, identify risks, assist in implementing risk mitigation measures, and ensure incidents are investigated to resolution and remediation activities followed up on.

Regular penetration tests are performed to identify new risks and vulnerabilities.

Use of Subservice Providers

CMiC uses AWS for cloud infrastructure services. CMiC also uses OnX's Data Centre Services to provide limited corporate infrastructure services for its own staff.

The AWS and OnX SOC reports are reviewed to ensure their scope covers the services consumed by CMiC, the report period is aligned with CMiC's requirements, end user control requirements listed are consistent with the terms and conditions of CMiC's contracts, and exceptions (if any) identified by their auditors are not of material impact to CMiC's overall security posture.

The controls described in Section 4 include only the applicable trust services criteria and related controls of CMiC and exclude the applicable trust services criteria and related controls of the subservice providers. The scope of this report did not extend to controls of the subservice providers.

3.4.3 Information and Communication Systems

ECAB – Executive Customer Advisory Board. ECAB is a group of senior executives from CMiC's largest Enterprise customers that meets quarterly with CMiC's Executive Management to discuss strategy, growth and organizational objectives.

CMUG – Computer Methods User Group. CMUG is a non-profit group of CMiC users, representing hundreds of companies in North America. Independent of CMiC, CMUG is run by a team of users who have deployed CMiC software. CMiC uses the CMUG forum to listen and respond to customer concerns.

Additionally, CMiC provides e-mail communication and notification to CMiC SaaS customer contacts for any:

1. Scheduled maintenance to the CMiC SaaS Platform
2. Unplanned or emergency maintenance to the CMiC SaaS Platform
3. New CMiC Application Suite software releases or hotfixes
4. Security notifications affecting the CMiC Application Suite

For any issues that occur within the CMiC SaaS Platform, CMiC customers can enter and view tickets in the ticketing system.

3.5 Changes to the System During the Period

For added security on customer user access management, Single Sign On capability has been added through federation with Microsoft Entra. This simplifies user login process and provides customer's IT team full control over authentication security features, such as, strong password enforcement, Multi-Factor-Authentication (MFA) and conditional access policies. Apart from the enhancement in security control there have been no significant changes to the CMiC SaaS Platform and its controls during the period January 1, 2023 to December 31, 2023.

3.6 Complementary Control Considerations

The following section outlines complementary user entity and subservice control considerations that would be relevant as they relate to the design of controls at CMiC. These control considerations were not subject to evaluation by the Service Auditor.

3.6.1 Complementary Subservice Organization Controls (CSOCs)

The following trust services criteria are intended to be met by controls at the cloud service providers, either alone, or in combination with controls at CMiC.

Amazon Web Services, Inc.

Controls expected to be implemented by AWS
AWS enables customers to articulate who has access to AWS services and resources (if resource-level permissions are applicable to the service) that they own. AWS prevents customers from accessing AWS resources that are not assigned to them via access permissions. Content is only returned to individuals authorized to access the specified AWS service or resource (if resource-level permissions are applicable to the service).
VPC (Virtual Private Cloud)-Specific – Network communications within a VPC are isolated from network communications within other VPCs.
Physical access to data centers is approved by an authorized individual. Physical access is revoked within 24 hours of the employee or vendor record being deactivated. Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.

Controls expected to be implemented by AWS
Physical access points to server locations are recorded by closed circuit television camera (CCTV). Images are retained for 90 days, unless limited by legal or contractual obligations.
Physical access points to server locations are managed by electronic access control devices.
Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.
Amazon-owned data centers are protected by fire detection and suppression systems.
Amazon-owned data centers are air conditioned to maintain appropriate atmospheric conditions. Personnel and systems monitor and control air temperature and humidity at appropriate levels.
Uninterruptible Power Supply (UPS) units provide backup power in the event of an electrical failure in Amazon-owned data centers.
Amazon-owned data centers have generators to provide backup power in case of electrical failure.
Contracts are in place with third-party colocation service providers which include provisions to provide fire suppression systems, air conditioning to maintain appropriate atmospheric conditions, Uninterruptible Power Supply (UPS) units, and redundant power supplies.
AWS performs periodic reviews of colocation service providers to validate adherence with AWS security and operational standards.
All AWS production media is securely decommissioned and physically destroyed prior to leaving AWS Secure Zones.
AWS provides publicly available mechanisms for customers to contact AWS to report security events and publishes information including a system description and security and compliance information addressing AWS commitments and responsibilities.

OnX Enterprise Solutions Ltd.

Controls expected to be implemented by OnX
A smoke detection system is installed in the data centers to detect and alert data center personnel to the presence of a fire at its early stages. The Toronto data center features VESDA system (Very Early Smoke Detection).
The facilities are equipped with fire suppression systems, including: • Wet pipe sprinklers in office areas • Dry pipe sprinklers in data centers.
Inspections of fire detection and suppression systems are performed annually to ensure proper operation of equipment.
The data centers are equipped with dedicated HVAC systems used to control temperature and humidity.
The data centers were equipped with backup HVAC systems should a failure occur to primary units.
Certain portions of the data centers have been configured with hot and cold aisles to maximize cooler airflow to the front of systems.
Preventative maintenance inspections are performed periodically on HVAC systems.
Uninterruptible Power Supply (UPS) systems are in place to provide alternate power in the event of a momentary interruption in commercial power.
Tests and inspections are performed and documented on the UPS systems on a periodic basis to ensure proper operation.
Generators are in place to provide power to data center systems in the event of an extended power outage.
The generators are regularly maintained, inspected, and tested to ensure proper operation.
The data centers were equipped with water detection devices to prevent water damage in the event of a flood or water leak.

Controls expected to be implemented by OnX
Environmental systems in the data centers are monitored continuously with alerts sent to administrators when previously defined thresholds are exceeded.

3.6.2 Complementary User Entity Controls

CMiC's SaaS Platform was designed with assumption that certain controls would be implemented by user entities. These controls should be in operation at user entities to complement CMiC's controls. The user entity controls presented below should not be regarded as a comprehensive list of all controls that should be employed by user entities.

CMiC provides a secure software application environment in the cloud where customer data is logically separated. However, the users of this SaaS Platform are responsible for access control and user management of their environment. Although CMiC deploys security best practices for the protection of customer data, it is the users' responsibility to confirm the correctness of its data and validate the results of CMiC's processing algorithm.

#	Complementary User Entity Control
1	End User Entity is responsible for all common criteria related to organization and management.
2	End User Entity is responsible for all common criteria related to communications.
3	End User Entity is responsible for advising CMiC of any suspected, or confirmed, security, availability and confidentiality incidents encompassing logical; and physical security breaches, failures and identified vulnerabilities.
4	Logical access to information assets (application systems, hardware, software, data, mobile devices and others) are restricted in accordance with End User Entity's access control policy.
5	Prior to issuing system credentials and granting system access, the End User Entity registers and authorizes new internal and external users whose access is administered by the End User Entity. For those users whose access is administered by the End User Entity, user system credentials are removed when user access is no longer authorized.
6	The End User Entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, considering the concepts of least privilege and segregation of duties, to meet the entity's objectives.
7	The End User Entity implements logical access security measures to protect against threats from sources outside its system boundaries.
8	The End User Entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.

Section 4 – Principal Service Commitments and System Requirements

CMiC's SaaS Platform is a multitenant solution operated using the AWS environment whereby CMiC customers share one Application Suite and database. CMiC's support of its SaaS Platform service includes support of a virtual network infrastructure, virtual servers, operating systems, the CMiC Application Suite and database.

CMiC's SaaS Platform is monitored 24/7 for infrastructure failures, application errors and performance. Redundancy and diversity principles are built into the components to ensure the highest level of availability and uptime. CMiC provides the following in support of its SaaS environment:

1. Monitoring service – CMiC provides 7x24 monitoring of the SaaS infrastructure (network, virtual servers, and operating systems) and the CMiC Application Suite. CMiC staff are alerted to any major outages initiate remediation activities as soon as possible.
2. Availability – CMiC strives to provide a highly available service to customers using AWS's Regional Availability Zone to guard against catastrophic failures. Database Redo Logs are taken frequently to ensure the integrity of the database, protecting it from instance failures. The Redo logs store changes made to the database as they occur. Every instance of an Oracle Database has an associated Redo log to protect the database in case of an instance failure. Real time "DataGuard" is set up to replicate the Redo logs to another cloud provider to enhance our overall disaster resiliency. Redo logs are kept for 24 hours.
3. Support and maintenance – Support for the SaaS Platform physical infrastructure is provided by AWS where maintenance is carried out without interruption. Patches and software upgrades to the CMiC Application Suite are managed by CMiC.