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) and Platform as a Service (PaaS) Solutions for the period January 1, 2025 to December 31, 2025

Table of Contents

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) and Platform as a Service (PaaS) Solutions ("system") were effective throughout the period January 1, 2025 to December 31, 2025, 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) and Platform as a Service (PaaS) Solutions 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) and Platform as a Service (PaaS) Solutions 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"), Oracle Corporation ("Oracle"), OnX Enterprise Solutions Ltd. ("OnX"), and Microsoft Corporation ("Microsoft") (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) and Platform as a Service (PaaS) Solutions 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) and Platform as a Service (PaaS) Solutions 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, 2025 to December 31, 2025.

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.

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; and
- 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 and PaaS Solutions were effective throughout the period January 1, 2025, to December 31, 2025, 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
February 13, 2026

Section 2 – Statement by Management of CMiC

We are responsible for designing, implementing, operating, and maintaining effective controls within Computer Methods International Corp. ("CMiC", the "Company" or the "Service Organization") related to the Software as a Service (SaaS) and Platform as a Service (PaaS) Solutions throughout the period January 1, 2025, to December 31, 2025, 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, 2025, to December 31, 2025, 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"), Oracle Corporation ("Oracle"), OnX Enterprise Solutions Ltd. ("OnX"), and Microsoft Corporation ("Microsoft") (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) and Platform as a Service (PaaS) Solutions 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) and Platform as a Service (PaaS) Solutions based on the applicable trust services criteria. The accompanying Description of the Boundaries of CMiC's Software as a Service (SaaS) and Platform as a Service (PaaS) Solutions 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) and Platform as a Service (PaaS) Solutions 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) and Platform as a Service (PaaS) Solutions based on the applicable trust services criteria. The accompanying Description of the Boundaries of CMiC's Software as a Service (SaaS) and Platform as a Service (PaaS) Solutions 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, 2025, to December 31, 2025, to provide reasonable assurance that CMiC's service commitments and system requirements were achieved based on the applicable trust services criteria.

Computer Methods International Corp.
February 13, 2026

Section 3 – Description of the Boundaries of CMiC's Software as a Service (SaaS) and Platform as a Service (PaaS) Solutions

3.1 Company Background

Founded in 1974, CMiC is headquartered in Toronto, Canada and delivers a 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 and Service Commitments

CMiC has a complete and flexible software solutions for construction firms and project owners. The solutions are not just accounting or project management software; it's construction management software, purpose-built and refined for over five decades to fulfill customer's unique needs. After deploying CMiC's intelligent construction platform, customers can operate their 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, customers can choose from a robust enterprise-wide platform to a more narrowly focused solution to run their financials or empower their field staff.

CMiC software is licensed as an enterprise-wide software solution offered with the following options:

- Clients can choose to self-host CMiC's software in their own environment.
- Client can subscribe to CMiC's Platform as a Service (PaaS) Solution hosted by CMiC in the Oracle Cloud Infrastructure (OCI) environment.
- Client can subscribe to CMiC's Software as a Service (SaaS) Solution as hosted in Amazon Web Services (AWS) environment.

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

This report is intended to provide information sufficient to understand the relevant aspects of CMiC's control environment for the delivery of services to user entities for the period January 1, 2025, through to December 31, 2025, specifically as it relates to the security, availability, and confidentiality criteria.

The scope of this report does not include:

- Clients who are self-hosting CMiC's application suite in their own environment.

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

1. CMiC Software – NEXUS

CMiC NEXUS allows customers to manage financials, project controls, human capital and assets (equipment and inventory). It unifies *Corporate Financials (General Ledger, Accounts Payables, Accounts Receivables, Payroll & Asset Management) and Project Controls (Project Costing & Forecasting, Subcontract Management, Change Management & Project Billing) alongside a robust Project Management system* in one secure solution and data repository. These core capabilities provide real-time insights leveraging operational transactions to maximize control over project completion and profitability. CMiC's risk management capabilities are embedded throughout the NEXUS platform 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 include:

- Construction Accounting
- Project Controls
- Equipment & Inventory
- Opportunity Management
- Construction Payroll & Human Capital Management (HCM)

Construction Accounting

CMiC's Construction Accounting, designed for general and specialty contractors, includes Accounts Payable, Accounts Receivable, Billing and Consolidated General Ledger applications. NEXUS provides robust financial reporting solutions to help finance teams optimize revenue, expenses, and financial management practices.

Beyond helping manage financial transactions, Construction Accounting flows data into both the general ledger and job costing simultaneously, eliminating the need for a duplicate or manual transaction.

Project Controls

CMiC's Project Controls solution allows users to effectively monitor project budgets, including time, expenses, suppliers, and costs. On top of that, it equips users to identify issues early in the process and course correct in a timely manner. By providing access to every version of a team's project documents, the customer will be able to stay on top of all project changes and deliver results with seamless execution.

Equipment & Inventory

CMiC's Equipment & Inventory offers complete process integration, from purchase orders for acquisition of capital assets and ordering consumable items for day-to-day operations, to enabling complete financial transparency, from purchasing to AP and GL management.

CMiC Equipment & Inventory helps manage all physical assets the firm needs to run field operations effectively, including material inventory and equipment.

This module enables users to control material costs, accelerate the procurement process, optimize inventory management, generate accurate job costing and client billing, and boosts operational performance.

Opportunity Management

Managing construction company's sales funnel is a critical element to maintaining growth targets. Utilizing the right construction CRM software allows leaders to accurately forecast revenue, track sales, profitability, and ensure that customer relationships are optimized.

CMiC Opportunity Management (OM) is a modern CRM tool that focuses on forecasting construction projects and managing processes. It helps gauge the health of a client's sales pipeline in real-time. This robust CRM tool enables construction leaders to make accurate revenue, profitability, and growth projections, and to manage leads effectively.

To effectively manage the sales funnel and meet growth targets, construction firms use CMiC's OM to help drive automation, manage sales-focused tasks, nurture leads, drive collaboration and manage business relationships — including those with general contractors, subcontractors, and integration partners.

Payroll & HCM

CMiC's Payroll and HCM software solution brings together technology, workflows, and people to enable a fully connected workplace with a truly engaged workforce, supporting everything from small business payroll to complex construction payroll issues. At its core, CMiC is purpose-built to satisfy the unique Payroll and HCM processing needs of the construction industry.

This application is designed to simplify and streamline processes with construction firm's human capital management team. It helps the customer track jobsite workers, with visibility into their credentials, payroll data and the projects they are working on.

2. CMiC Software – Project Management

With CMiC's Project Management offerings, project managers and site supervisors' control relevant aspects of project planning, execution and tracking from their laptops, tablets and smartphones. Key modules include:

- Project Controls
- CONSTRUCT Document Management
- CONSTRUCT Prequalification & Procurement
- Quality & Safety

CONSTRUCT Document Management

CONSTRUCT Document Management is designed to streamline and centralize the handling of construction project drawings, enhancing collaboration and minimizing errors across the project lifecycle. This module allows teams to upload, organize, review, and distribute drawings directly within the CMiC platform, ensuring that all stakeholders have access to the latest versions and revisions in real time. Key features include version control, markup tools, and advanced search capabilities, which help project teams quickly locate and review specific drawing details.

Additionally, Document Management integrates with other CMiC modules, such as Project Control and Drawing Management, creating a seamless workflow where drawings can be connected with RFIs, submittals, and other key project documentation. This centralization reduces duplication of efforts, helps prevent costly rework, and keeps all team members aligned with the most current project information.

CONSTRUCT Prequalification & Procurement

CONSTRUCT Prequalification & Procurement streamlines the bidding and procurement processes, enabling construction companies to manage these critical project phases with increased accuracy, efficiency, and control. The module supports end-to-end workflows for issuing requests, tracking bids, evaluating proposals, and awarding contracts, all from a unified platform. It simplifies bid management by automating invitation distribution, providing vendors with a clear portal to submit bids, and offering tools to compare proposals against pre-set criteria.

On the procurement side, the module manages purchasing workflows from requisition through to purchase order and receipt. It allows project teams to track orders, manage supplier relationships, and ensure that materials and services are procured within budget and schedule constraints. Integration with CMiC's Project Controls and Financial modules gives teams real-time insights into project costs and procurement timelines, helping them make data-informed decisions to prevent budget overruns and delays. Overall, the Bid & Procurement module minimizes manual tasks, reduces errors, and fosters a transparent and competitive bid process while ensuring timely and cost-effective procurement.

CONSTRUCT Prequalification & Procurement application is designed to help organizations manage subcontractors from start to finish by integrating all subcontracting activity into a client's organization. It provides transparency for both general contractors and subcontractors with an automated pre-qualification process.

Quality & Safety

CMiC's Quality & Safety solution helps teams streamline key jobsite processes such as quality assurance and safety audits. It allows for real-time monitoring of tasks through built-in checklists, daily journals, and issue tracking. This ensures timely identification and resolution of any safety or quality issues. By optimizing operational workflows and maintaining comprehensive documentation, CMiC supports project delivery on time and within budget, reducing risks and improving overall performance.

3. CMiC Workflow

CMiC Workflow is designed to enhance a construction firm's operational effectiveness by developing workflows to support business objectives. Users can create sophisticated, customizable and flexible workflows that improve the timeliness of transaction processing as well as stakeholder response times.

By automating processes, such as sending messages and communications to all project stakeholders, CMiC Workflow enables users to receive, analyze and respond to notifications through messaging systems.

4. CMiC Analytics

CMiC Analytics allows users to create a tailored workspace – essentially a canvas that can be used to launch Object Cards, including Dashboards, Queries and Card Views. Users can customize canvases by dragging and dropping Object Cards into logical groupings called Buckets. Users can also leverage analytics to measure key KPIs, such as sales pipeline, sub-contractor performance and aging reports.

By embedding directly into the core CMiC interface, the widgets and components function within existing screens, displaying reports and dashboards in an environment already familiar to users. This capability enhances the immediacy and relevancy of fact-based insights within existing applications, providing teams with the relevant information required to make better decisions.

5. CMiC CONSTRUCT

CONSTRUCT is part of the Single Database Platform™, which reduces data conflicts between operations and financials and improves communication and collaboration for all project stakeholders.

Purpose-built for the construction industry, this suite of solutions is designed to deliver on industry-specific functionality and workflows. On top of that, its mobile functionality helps streamline data collection, optimize workflow management, and provide robust analytical reporting for a client's field teams.

From a foundation perspective, CONSTRUCT is built with a next generation technology platform "layered in" with Business Intelligence to help teams make data-driven decisions in real-time.

CMiC CONSTRUCT user interface is designed to adapt across all devices and adapts to each user's input method — be it a mouse, keyboard, or touchscreen device. Visually, it has a consistent user interface across all devices, making for a seamless user experience.

The CONSTRUCT suite of applications include:

- CONSTRUCT Project Management (PM)
- CONSTRUCT Crew Time (CT)
- CONSTRUCT Approvals
- CONSTRUCT Employee Self-Service (ESS)
- CONSTRUCT Opportunity Management (OM)

CONSTRUCT Project Management

Empower teams with the tools designed to complete complex projects with tightly managed costs and timeframes.

CONSTRUCT Crew Time

This comprehensive solution enables managers to accurately track labor hours, equipment usage and work order durations across various projects and tasks. On top of that, it equips leaders to field managers to track crew productivity.

CONSTRUCT Approvals

This app streamlines the approval process for construction projects, automating routine tasks while ensuring key decisions, like invoice approvals and change requests, are efficiently managed. The app keeps stakeholders informed, minimizing delays and maintaining project workflow momentum.

CONSTRUCT Employee Self-Service

Employees can view personal details, access information, review, and email pay slips, and gain quick insights into their benefits. In addition, this application streamlines leave management processes by allowing employees to submit requests, and provides supervisors with easy-to-use features to accelerate leave approvals.

CONSTRUCT Opportunity Management

Opportunity Management offers a rich CRM experience for construction professionals on smartphones and tablets. It grants users in the field access to valuable information in real-time - no matter where they are - to stay connected with customers

& prospects and make important decisions during the sales process. Executives in Sales, Business Development & Marketing can easily access Opportunities, Organizations, Contacts, and Action items while on the go.

3.3 Components of the SaaS and PaaS Solutions Used to Provide the Services

3.3.1 Infrastructure and Software

Despite residing on different cloud provider environments, CMiC's application suite infrastructure for both the SaaS and PaaS Solutions are similar, consisting of servers, storage, and networking, with cloud-based security including but not limited to Distributed Denial of Service (DDoS) protection, Web Application Firewall (WAF) and host-based threat protection.

For PaaS customers, VPN access and minor infrastructure customization can be accommodated upon the customer's request.

Cloud Infrastructure Service:

1. 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 such as:
    a. Table space creation and storage settings adjustment.
    b. Allocating space for temporary segments.
    c. Rollback segment management.
4. Backup and restore of customer data and customer environment
5. Capacity management for in-scope devices.

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 for the SaaS and the PaaS Solutions

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

1. For the CMiC SaaS Solution, SSO (Single Sign On) capabilities are available through federation with Microsoft Entra, simplifying the login process and providing clients' IT teams full control over authentication security features, such as MFA and conditional access policies.
2. For the CMiC PaaS Solution, Single Sign-On (SSO) capabilities are supported and implemented at the customer's discretion. This capability can be implemented directly by the customer or delivered via CMiC's consulting services.

3. 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).

4. Data at rest is encrypted within both AWS and OCI environments.

5. 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.

6. Periodic code reviews on the application are performed during development and prior to releasing into production.

7. 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 for cyber security by executing the appropriate oversight function. For example, CMiC has an InfoSec and Privacy Governance Committee that meets quarterly 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 technology 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.

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 and OCI, CMiC leverages the controls implemented by AWS and OCI 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 system resource usage, performance and capacity, business continuity testing, and backup and recovery processes in order to manage the 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. Chief Information Security Officer (CISO)
5. Legal Counsel
6. Representatives from the Advisory Board

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

1. Director of Cloud Operations Support
2. IT Analysts

The following roles are involved in the maintenance and support of the CMiC application suite:

1. Director of Engineering, Tools
2. Director of Engineering, Project Controls
3. Director of QA & Documentation
4. Database Administrators (additional contracted service for PaaS customers)
5. Hosting & Infrastructure Support Team

To enforce segregation of duties, the Development Team (except for the CTO, the Director of Engineering, Tools, and the Director of Engineering, Project Controls), and all other staff do not normally have access to make changes in CMiC's Production Environment. Any temporary access to the production environment must be approved by the CTO or the Director of Engineering, Tools, and access will be revoked by IT when access is no longer required.

3.5.3 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 NEXUS Platform. CMiC's Information, Privacy and Governance Committee (IPGC) meets quarterly, 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. The CMiC IT Team performs regular patches to address known vulnerabilities.

For the SaaS Solution, CMiC provides a secure multitenant SaaS environment.

For the PaaS Solution, CMiC provides a secure single tenancy in its PaaS environment. CMiC team manages the security of the servers and infrastructure PaaS environment while providing recommendations to customers regarding regular patches to address known vulnerabilities. The approval and implementation of application patches are the responsibility of the customers.

Some of CMiC's PaaS customers request to have administrative rights to the servers (operating system and/or database) to install customized applications that interface with CMiC's application suite. As this would make responsibility ambiguous, in these cases, CMiC mandates that a waiver be signed by the customer absolving CMiC of all responsibility for the environment. That is, the customer is asked to accept all responsibility for the environment.

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, OCI, Microsoft 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 changes 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 Manage, Detect and Response (MDR) 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 or PaaS Solutions 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.

For both SaaS and PaaS Solutions, 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

For SaaS, 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.

For PaaS, encrypted backups of systems and data are performed nightly and transferred to an offsite location. CMiC also offers an optional service to forward database Redo logs every 15 minutes to cloud object storage, giving the PaaS customer the ability to recover their data with a 15-minute recovery point objective.

System Account Management

CMiC uses a password management system behind a 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 Confidentiality 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 its SaaS Solution and OCI for its PaaS Solution services. CMiC also uses Microsoft Azure to provide limited corporate infrastructure services, such as ID and authentication for its own staff with OnX's Data Centre Services to providing a backup. The use of the OnX was decommissioned at the end of May 2025.

The AWS, OCI, Microsoft 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 semi-annually with CMiC's Executive Management to discuss strategy, growth and organizational objectives.

Security Oversight Committee – A senior representative of ECAB meets with CMiC Management team quarterly to review risks and offers insights on any required remediation.

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/PaaS customer contacts for any:

1. Scheduled maintenance to the CMiC SaaS and PaaS Solutions
2. Unplanned or emergency maintenance to the CMiC SaaS and PaaS Solutions
3. Security notifications affecting the CMiC application suite
4. New CMiC application suite software releases or hotfixes

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

3.4.4 Significant Changes

As of May 31, 2025, the OnX facility and the server room at CMiC's office building, which used to house the domain controller are no longer in use as the authentication services have migrated to Microsoft's Entra ID service. As such the OnX facility and server room are no longer in scope as of June 1, 2025.

3.5 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.

3.5.1 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 has 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.

Oracle Corporation

Controls expected to be implemented by Oracle
Access to network devices, servers supporting the services and multi-tenanted hosts required multi-factor authentication and traversing three separate levels of access control. The user must authenticate to OCNA using multi-factor authentication, the appropriate bastion server, and the individual devices. Logical access controls restrict access to customer block storage volumes. Upon termination, OCNA access is revoked.
Upon termination, OCNA access is revoked. Logical access controls restrict access to customer block storage volumes.
Oracle Operations Command Centers are staffed 24x7. Security Incidents are assigned a severity, follow the incident handling process, and are tracked through resolution.

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. Environmental systems in the data centers are monitored continuously with alerts sent to administrators when previously defined thresholds are exceeded.

Microsoft Corporation

Controls expected to be implemented by Microsoft
Azure enables customers to articulate who has access to Azure Entra ID enabled services and resources (if resource-level permissions are applicable to the service) that they own. Azure prevents customers from accessing Azure associated resources that are not assigned to them via access permissions. Content is only returned to individuals authorized to access the specified Azure service or resource (if resource-level permissions are applicable to the service).
Physical access to data centres 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 centres is reviewed on a quarterly basis by appropriate personnel. 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. Microsoft-owned data centres are protected by fire detection and suppression systems. Microsoft-owned data centres 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 Microsoft-owned data centres.

Controls expected to be implemented by Microsoft
Microsoft-owned data centres 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. Microsoft performs periodic reviews of colocation service providers to validate adherence with AWS security and operational standards. All Microsoft production media is securely decommissioned and physically destroyed prior to leaving Azure Secure Zones.
Microsoft provides publicly available mechanisms for customers to contact Microsoft to report security events and publishes information including a system description and security and compliance information addressing Microsoft commitments and responsibilities.

3.5.2 Complementary User Entity Controls

CMiC's SaaS & PaaS Solutions were 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 the SaaS and PaaS Solutions 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.

For SaaS Solution User Entities, the following additional Complimentary User Entity Controls apply:

#	Complementary User Entity Control for SaaS Solution
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.

#	Complementary User Entity Control for SaaS Solution
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.

For PaaS Solution User Entities, the following additional Complimentary User Entity Controls apply:

#	Complementary User Entity Control for PaaS Solution
1	User Entity is responsible for all common criteria related to organization and management.
2	User Entity is responsible for all common criteria related to communications.
3	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 User Entity's access control policy.
5	Prior to issuing system credentials and granting system access, the User Entity registers and authorizes new internal and external users whose access is administered by the User Entity. For those users whose access is administered by the User Entity, user system credentials are removed when user access is no longer authorized.
6	The 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 User Entity implements logical access security measures to protect against threats from sources outside its system boundaries.
8	The 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.
9	End User Entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.
10	End User Entity identifies vulnerabilities and remediates through the development and execution of remediation activities.
11	End User Entity with elevated privilege accounts to the App Servers retains the responsibility of managing changes implemented by its users with such elevated privilege.
12	End User Entities requiring read-only access to their database, the User Entity implements policies and procedures to ensure the confidentiality of information made available through means other than the CMiC application (i.e., programmatic (API) or direct database (e.g., ODBC) access).

Section 4 – Principal Service Commitments and System Requirements

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

For the PaaS Solution, CMiC provides the infrastructure (network, virtual servers, and operating systems) in the OCI environment with a dedicated CMiC application suite and database for each customer. While out of scope for this report, CMiC customers also have the option to contract CMiC's DBA services to provide additional database support.

CMiC's SaaS and PaaS Solutions are 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 & PaaS environments:

1. Software as a Service (SaaS)

   - 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.

   - Availability – CMiC strives to provide a highly available SaaS Solution 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 overall disaster resiliency. Redo logs are kept for 24 hours.

   - Support and maintenance – Support for the SaaS Solution 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.

2. Platform as a Service (PaaS)

   - Monitoring service – CMiC provides 7x24 monitoring of the PaaS infrastructure (network, virtual servers, and operating systems). CMiC staff are alerted to any major outages initiate remediation activities as soon as possible.

   - Availability – For customers subscribing to the PaaS environment, which resides in OCI, terraform scripts are used to allow CMiC to restore the operating environment quickly. Daily backups are performed to safeguard against data loss and annual restoration tests are performed.

- Support and maintenance – Support for CMiC's PaaS physical infrastructure is provided by OCI and maintenance is carried out without interruption. Patch and software upgrades to the CMiC application suite are managed by the client.