ENGINEERED FOR IT

MCX Holding B.V.
Technical administration of Oracle based applications.

SOC3® report

RELEVANT FOR THE TRUST SERVICES CRITERIA SECURITY AND AVAILABILITY

January 1, 2023 to December 31, 2023

Table of Contents

MCX Administration Services B.V.
Kanaalpad 1
7321 AP Apeldoorn

+31 (0) 55 526 06 70
info@mcx.nl
www.mcx.nl

IBAN NL62 TRIO 039 112 67 84
BIC TRIONL2U

VAT NL8197.37.823.B.06
CoC 08082416

1. MCX's Management Statement

We are responsible for designing, implementing, operating, and maintaining effective controls within the system of MCX throughout the period January 1, 2023 to December 31, 2023, to provide reasonable assurance that MCX's service commitments and system requirements relevant to security and availability were achieved. Our description of the boundaries of the system is presented in chapter 3 and identifies the aspects of the system covered by our assertion.

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 MCX's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (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). MCX'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 chapter 4.

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 organisation may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

MCX uses subservice organisations Solcon, BIT and ITB[2] to perform housing services. The description of the boundaries of the system (chapter 3 of this report) indicates that certain applicable trust services criteria can only be met if controls at the subservice organisation are suitably designed and operating effectively. The description of the boundaries of the system of MCX also indicates the complementary subservice organisation controls assumed in the design of MCX's controls. The description does not disclose the actual controls at the subservice organisation.

The description of the boundaries of the system (chapter 3 of this report) indicates that certain applicable trust services criteria can be achieved only if complementary user-entity controls contemplated in the design of MCX's controls are suitably designed and operating effectively, along with related controls at the service organisation. The description presents MCX's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of MCX's controls.

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

MCX Holding B.V. (MCX Administration Services B.V., MCX Infrastructure Services B.V. & MCX International B.V.)

J.S. van Veen
General Director

Digitaal ondertekend door:
Johan van Veen
29 januari 2024 08:29 +01:00...

Apeldoorn, January 29, 2024

MCX Administration Services B.V.
Kanaalpad 1
7321 AP Apeldoorn

+31 (0) 55 526 06 70
info@mcx.nl
www.mcx.nl

IBAN NL62 TRIO 039 112 67 84
BIC TRIONL2U

VAT NL8197.37.823.B.06
CoC 08082416

2 Independent Service Auditor's Assurance Report

To: Management of MCX Holding BV. (MCX Infrastructure Services B.V., MCX Administration Services B.V. and MCX International B.V.), herafter: MCX.

2.1 Scope

We have examined MCX's accompanying assertion titled "MCX's Management Statement" (assertion) that the controls within the system of MCX were effective throughout the period January 1, 2023 to December 31, 2023, to provide reasonable assurance that MCX's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (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).

2.2 Subservice Organisations

MCX uses subservice organisations Solcon, BIT and ITB[2] to perform housing services. The description of the boundaries of the system (attachment A of this report) indicates that certain applicable trust services criteria can only be met if controls at the subservice organisations are suitably designed and operating effectively. The description of the boundaries of the system of MCX also indicates the complementary subservice organisation controls assumed in the design of MCX's controls. The description does not disclose the actual controls at the subservice organisations. Our examination did not include the services provided by the subservice organisations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organisation controls.

2.3 Complementary User entity controls

The description of the boundaries of the system (attachment A of this report) indicates that certain applicable trust services criteria can be achieved only if complementary user-entity controls contemplated in the design of MCX's controls are suitably designed and operating effectively, along with related controls at the service organisation. The description presents MCX's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of MCX's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

2.4 Service Organisation's Responsibilities

MCX 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 MCX's service commitments and system requirements were achieved. MCX has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, MCX is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

2.5 Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organisation's service commitments and system requirements were achieved based on the applicable trust services criteria.

We conducted our assurance engagement in accordance with Dutch Law and the International Standard on Assurance Engagements Standard 3000, 'Assurance Engagements other than Audits or Reviews of Historical Financial Information' established by The International Auditing and Assurance Standards Board (IAASB). Those standards require that we plan and perform our engagement to obtain reasonable assurance to express our opinion.

We have complied with the independence and other ethical requirements of the Code of Ethics ('Reglement Gedragscode') issued by NOREA, the Dutch IT-Auditors institute, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behavior.

The firm applies the NOREA Standard on Quality Control (Reglement Kwaliteitsbeheersing NOREA – RKBN), and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- obtaining an understanding of the system and the service organisation's service commitments and system requirements;
- assessing the risks that controls were not effective to achieve MCX'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 MCX's service commitments and system requirements based the applicable trust services criteria.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

2.6 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 organisation'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 inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

2.7 Opinion

In our opinion, management's assertion that the controls within the system of MCX were effective throughout the period January 1, 2023 to December 31, 2023, to provide reasonable assurance that MCX's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Amstelveen, January 29, 2024

BDO Audit & Assurance B.V.
On behalf of,

Digitaal ondertekend door:
Wido Dalhuisen
29 januari 2024 09:18 +01:00...

drs. W. Dalhuisen RE CISA
Partner

---

3. ATTACHMENT A – MCX'S DESCRIPTION OF THE BOUNDARIES OF THE SYSTEM

3.1. Background

MCX Administration Services B.V. and MCX International B.V. manage Oracle based applications. By combining knowledge and resources MCX specialises in various forms of technical management of Oracle based applications. Because of the specialist knowledge and organisational flexibility, MCX is able to focus on the needs of their customers, in an efficient and effective way. The most common forms of managed services are: hosting and remote management.

3.1.1. Service scope

The service of MCX is complementary to the service the customer provides internally to it's own customers, meaning the service only has a partial impact on the end-user using the application system. The service of the application system provided is applicable to the fields of:

- security
- availability
- performance
- manageability

MCX has a strong technological approach on managing application systems. This is complemented by a functional management and administration service. This service is either supplied by the customer itself or another supplier contracted by the customer or MCX.
MCX is responsible for maintaining the best and most efficient way of managing applications and databases for its customers. To achieve this, MCX agrees on a communication framework with its customers. Within this framework a set of documents are agreed upon to formalise the service. These documents are:

- contract
- service level agreement (SLA)
- daily agreed procedures (DAP)

3.1.2. Subservice organisations

MCX uses the subservice organisations BIT B.V. in Ede, ITB^2 B.V. in Apeldoorn and Solcon Internetdiensten N.V. in Apeldoorn for housing of the MCX owned hardware. For its description MCX Infrastructure Services B.V. uses the carve-out method. The description of the system therefore excludes the control objectives and related controls of this subservice organisation.

3.2. System overview

An important aspect of the MCX core processes is the efficient and effective implementation of controls within the customer's processes and the entire ICT support process.

3.2.1. Infrastructure

The main ICT components for the services of MCX include a reliable network (including routers, switches, and firewalls) and hardware (servers and data disks) to run a reliable operating system.

MCX Administration Services B.V.
Kanaalpad 1
7321 AP Apeldoorn
+31 (0) 55 526 06 70
info@mcx.nl
www.mcx.nl
IBAN NL62 TRIO 039 112 67 84
BIC TRIONL2U
VAT NL8197.37.823.B.06
CoC 08082416

These activities are owned and delivered by MCX Infrastructure Services B.V. and purchased as a service by MCX Administration Services B.V. MCX International B.V. purchases the service provided by MCX Administration Services B.V. The infrastructure, along with the customer's standard Oracle software, provides the basis for the services of MCX.

MCX uses the sub-service organisations mentioned in 3.1.2. Agreements on physical security, related to these organisations, are made with all entities. MCX employees visit all locations for regular maintenance activities on a periodic basis. The physical security measures are checked and possibly tested during these visits.

3.2.2. Software

To increase efficiency and effectiveness of its services, MCX uses specially developed software. This software provides a high degree of automation with regards to monitoring and reporting functions. As such, incidents are automatically sent to the responsible employees by text message and/or email, ensuring they can respond immediately and adequately.

3.2.3. People

A formal organisation structure exists and is documented in internal policy documents that are freely available to all MCX employees. The organisational structure has two layers: a management and an operational layer. The benefits of such an organisational structure include a quick decision-making process due to delegated responsibilities and a decisive and entrepreneurial culture.
MCX has a strict recruitment policy which assesses potential employees against a pre-established profile, taking into account the job requirements and company culture.

3.2.4. Procedures

MCX has several policies in place ensuring fully documented procedures. A general policy document gives an overview of what MCX is all about. The document details the mission and strategy of MCX.
The security policy document describes the technical and organisational guidelines with respect to security. The contingency plan describes the procedures in case for example a natural disaster strikes. All documents are frequently updated on at least a yearly basis. Update notifications are sent to all MCX employees for information purposes.

3.2.5. Data

The handling of customer data is of the utmost importance. Maintaining the integrity and confidentiality of customer data is one the main responsibilities of MCX. To fulfil this responsibility MCX has laid out several policies. These policies range from the actual data storage to data transfer for new customers and data destruction for parting customers. All data handling is done by multidisciplinary teams. This enables redundant availability of resources possible and opens up the possibility of the four-eyes principle to ensure customer data is properly dealt with.

3.3. Internal control

The internal control of MCX is grouped according to the following aspects:

- control environment
- risk assessment
- control activities

MCX Administration Services B.V.
Kanaalpad 1
7321 AP Apeldoorn
+31 (0) 55 526 06 70
info@mcx.nl
www.mcx.nl
IBAN NL62 TRIO 039 112 67 84
BIC TRIONL2U
VAT NL8197.37.823.B.06
CoC 08082416

- information & communications
- monitoring activities.

3.3.1. Control environment

MCX aims to achieve an outstanding level of technical management for its customers. The flat organisational structure and the focus on specific knowledge of Oracle based applications, allows MCX to meet customer specific needs with the best price/quality ratio. MCX realises this through:

- pro-actively acquiring and sharing knowledge of Oracle based applications and related developments;
- maintaining a fully integrated chain of responsibility by the consultants for the customer;
- being a decisive and entrepreneurial organisation with a flat company structure;
- economies of scale and knowledge advantage;

The key operational objectives of MCX are:

- guaranteeing high uptime of the Oracle applications;
- guaranteeing effective information security.

3.3.2. Risk assessment

The integral management system (IMS), that governs the ISO 9001, 14001, 20000, 22301 and 27001 standards, is used as a tool to perform periodic risk assessments. These risk assessments are used to identify (security) threats. If a risk is identified, then the likelihood of its occurrence is determined along with the impact it can have on MCX or its customers.
The next step in this process is the creation and execution of a mitigation plan. The last step is the verification that the threat is either no longer present or mitigated to an acceptable level.

All risk assessments are addressed in the quarterly management meeting as part of the IMS.

3.3.3. Control activities

The most important external risk is the unauthorised access to the MCX network, granting possible access to the data of MCX or its customers. The most important internal risk is the unauthorised access to customer data by and the loss of data through human error. Within MCX, a set of controls is established, to prevent and repress these external and internal risks. The most important controls that aim for the prevention of these external risks are:

- security of the IT-infrastructure and the network against unauthorised access through user-id/password security, firewalls, and DMZ's;
- access security for the buildings and server rooms;
- access security of specific customer systems and information through user-id/password security and certificates.

3.3.4. Information & communication

Communication about going concern within MCX is conveyed via various communication channels.
The goal is to provide all employees with the correct information at the right time. Correct and effective communication is essential in decision making throughout the entire organisation.

MCX Administration Services B.V.
Kanaalpad 1
7321 AP Apeldoorn
+31 (0) 55 526 06 70
info@mcx.nl
www.mcx.nl
IBAN NL62 TRIO 039 112 67 84
BIC TRIONL2U
VAT NL8197.37.823.B.06
CoC 08082416

3.3.5. Monitoring activities

Several monitoring activities are in place both organisational and technical. These activities are grouped based on the ISO standards:

- ISO 9001: quality assurance management.
- ISO 14001: environmental awareness.
- ISO 20000: service management.
- ISO 22301: business continuity management.
- ISO 27001: information security management.

The IMS, holding these four ISO norms together, monitors the effectiveness of these activities.

3.4. Complementary user entity controls

MCX's technical and remote control of Oracle systems was designed with the assumption that certain complementary user entity controls would be operating effectively at user entities. This paragraph describes the complementary user entity controls that are necessary to achieve the control objectives stated in the description of MCX's system and identifies the control objectives to which the complementary user entity controls relate.

MCX is responsible for maintaining the best and most efficient way of managing applications and databases for its customers. MCX agrees on a framework with its customers. Within that framework, the most important factors are:

- contract
- service level agreement (SLA)
- daily agreed procedures (DAP).

The complementary user entity controls are aspects of the control system for which the user organisation itself is responsible. This involves the following:

- Ensure up-to-date servers and valid Oracle licenses so that authentication configuration can be applied.
- Functional management of the relevant Oracle applications.
- Informing MCX on relevant management decisions, policy changes and changes in circumstances relating to the services provided by MCX.
- Performing and maintaining customisations to the standard Oracle Software.
- Ensuring sufficient physical and logical access security of its own software / hardware which is related to services provided by MCX.
- Managing application user IDs / password controls.
- The customer change process is initiated, authorised, designed, and developed by the customer prior to installation of the change by MCX. After installation, the customer performs testing and authorises installation into production.
- Incidents, problems, changes, service requests and data fixes that require a follow-up from the customer are not actively monitored by MCX for promptly response from the customer.
- Initialisation of restore and recovery testing related to the back-up control activities.

The types of services provided by MCX demand that MCX employees use 'powerful customer accounts' to manage amongst others the customer database. In this context, and regarding the complementary user entity controls, the following aspects that fall under the responsibility of the user organisation are highlighted as:

- monitoring the integrity of the database and access to data including log file analysis that can be made available to MCX by the user organisation.

MCX Administration Services B.V.
Kanaalpad 1
7321 AP Apeldoorn
+31 (0) 55 526 06 70
info@mcx.nl
www.mcx.nl
IBAN NL62 TRIO 039 112 67 84
BIC TRIONL2U
VAT NL8197.37.823.B.06
CoC 08082416

3.5. Complementary subservice organisation controls

The subservice organisations as mentioned in 3.1.2 deliver the housing service to MCX Administration Services B.V. and MCX International B.V. These subservice organisations do not impose controls on MCX for the following, non-exhaustive list of security and availability services they provide:

- Secure access is possible by a combination of a physical device (key, key card etc.) and biometric identification.
- All servers are installed in lock protected racks only accessible by MCX infrastructure team members and data-centre employees.
- Cameras, smoke detectors and an alarm service are present and operational 24x7.
- All hardware modifications (servers, storage, and network) are logged and forwarded to the MCX infrastructure team.
- Datacentres provide the following detailed services that are required for MCX to provide the service to its customers:
    - power supplies for hardware;
    - air-conditioned environment for the cooling of hardware;
    - network connectivity to the Internet and other customer internal networks;
    - rack space to install MCX hardware;
    - site wide power redundancy.
- All datacentres have a ISO27001 certification governing all security related aspects of the datacentre.

Both MCX Administration Services B.V. and MCX International B.V. have implemented several monitoring controls related to these subservice organisations. These monitoring controls make sure that the subservice organisations deliver the service for MCX Administration Services B.V. and MCX International B.V. at the required level. This level is needed to provide the service to the customers of MCX.

All hardware (servers, storage, and network) is owned and operated by MCX Infrastructure Services B.V. On a yearly basis the MCX Security Officers have interviews with the data-centre Security Officers to discuss operating procedures related to security and availability. Next to that, after each visit to the datacentre, a report is created containing any irregularities found during the visit that might impact the security and availability of the service.

With these controls MCX fulfils the objective of the SOC2 criteria Security and Availability.

MCX Administration Services B.V.
Kanaalpad 1
7321 AP Apeldoorn

+31 (0) 55 526 06 70
info@mcx.nl
www.mcx.nl

IBAN NL62 TRIO 039 112 67 84
BIC TRIONL2U

VAT NL8197.37.823.B.06
CoC 08082416

4. ATTACHMENT B – MCX'S PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

4.1. Service commitments

MCX makes service commitments to its customers and has established service requirements as part of the MCX service. A set of documents are agreed upon to formalise this service. These documents are:

- contracts
- service level agreements (SLA)
- daily agreed procedures (DAP)

Service commitments to MCX customers are achieved by designing, implementing and operating effective controls within the system of MCX.

4.2. System requirements

MCX provides various forms of technical management of Oracle-based applications. Because of their specialist knowledge and organisational flexibility, MCX is able to focus on the needs of the customer, in an efficient and effective way. The most common forms of managed services are: hosting and remote management.

Internal controls are developed to ensure MCX complies to legal and regulatory obligations. Furthermore, a quality management system is in place to ensure the appropriate internal functioning of system requirements defined by MCX to meet customer commitments.

Various controls and procedures are implemented to meet MCX requirements and commitments to its customers including:

- Security: MCX has made commitments to its customers related to security of their data by restricting unauthorized access to MCX systems. These commitments are monitored through the functioning of various internal controls implemented for MCX.
- Availability: MCX has made commitments to its customers to ensure availability of MCX services 24 hours a day and 7 days a week.

MCX Administration Services B.V.
Kanaalpad 1
7321 AP Apeldoorn
+31 (0) 55 526 06 70
info@mcx.nl
www.mcx.nl
IBAN NL62 TRIO 039 112 67 84
BIC TRIONL2U
VAT NL8197.37.823.B.06
CoC 08082416