EG MainManager

MainManager

Independent Service Auditor Assurance Report under ISAE 3402 – Type 2

On Management Description of a Service Organization's System and the suitability of the design and operating effectiveness of controls for the period 1 January 2022 to 31 December 2022

Table of Contents

Section 1.	**Management's Assertion**	**3**
Section 2.	**Independent Service Auditor's Report**	**5**
Section 3.	**Management's Description of organization and internal control environment**	**9**
Section 4.	**Description Control Objectives, Controls, Tests and Results**	**17**

Section 1.

Örn Software ehf. Iceland's Management Assertion

We have prepared the description of Örn Software's services in relation to software development and operation services of the MainManager solution ("System") for user entities of the system during some or all of the period 1 January 2022 – 31 December 2022, and their user auditors who have a sufficient understanding to consider the description, along with other information, including information about controls operated by user entities of the system themselves, when assessing the risks of material misstatements of user entities' financial statements. We confirm, to the best of our knowledge and belief, that:

a) The accompanying description in Sections 3 and 4 fairly presents the system made available to user entities of the system during some or all of the period. Örn Software ehf. uses subservice organizations for hosting and operational activities. A list of these subservice organizations is provided in Section 3. The description in Sections 3 and 4 includes only the control objectives and related controls for Örn Software ehf. and excludes the control objectives and related controls of the subservice organizations listed in Section 3.

   The criteria we used in making this assertion include the following:

   i. Presents how the services are made available to user entities of the system were designed and implemented to process relevant transactions, including:

      - The types of services provided, including, as appropriate, the classes of transactions processed
      - The procedures, within both automated and manual systems, by which those transactions were initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports prepared for user entities
      - The related accounting records, supporting information and specific accounts that were used to initiate, authorize, record, process and report transactions; this includes the correction of incorrect information and how information was transferred to the reports prepared for user entities
      - How we capture and addressed significant events and conditions, other than transactions
      - The process used to prepare reports or other information for user entities
      - Specified control objectives and controls designed to achieve those objectives
      - Controls that we assumed, in the design of the system, would be implemented by user entities, and which, if necessary to achieve control objectives stated in the accompanying description, are identified in the description along with the specific control objectives that cannot be achieved solely by controls implemented by us
      - Other aspects of our control environment, risk assessment process, information and communication systems (including the related business processes), control activities and monitoring controls that were relevant to processing and reporting user entities' claims

   ii. Does not omit or distort information relevant to the scope of the system being described, while acknowledging that the description was prepared to meet the common needs of a

broad range of user entities and their independent auditors and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment.

b) The description includes relevant details of changes to the services and system during the period covered by the description.

c) The controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively throughout the period to achieve those control objectives and subservice organizations applied the controls contemplated in the design of Örn Software ehf. Iceland's controls. The criteria used in making this assertion were that:

   i. The risks that threatened achievement of the control objectives stated in the description were identified.

   ii. The identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved.

   iii. The controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

Sten-Roger Karlsen
CEO of Örn Software ehf.*
10 May 2023

*Sten-Roger Karlsen was appointed CEO of Örn Software ehf. on 20 September 2022. Guðrún Rós Jónsdóttir was acting CEO of Örn Software ehf. throughout the period of this report and until 20 September 2022

Section 2.

Independent Service Auditor's Report

To: the management of Örn Software ehf.

Scope

We have been engaged to report on Örn Software ehf. Iceland's Management's description in section 3 of its service provided to its customers throughout the period 1 January 2022 to 31 December 2022, and on the design and operation of controls related to the control objectives stated in the description.

Örn Software ehf. Iceland's Responsibilities

Örn Software ehf. Iceland is responsible for: preparing the description in section 3 and accompanying statement in section 1, including the completeness, accuracy, and method of presentation of the description and statement; providing the services covered by the description; stating the control objectives; and designing, implementing and effectively operating controls to achieve the stated control objectives.

Our Independence and Quality Control

We have complied with the independence and other ethical requirements of the International Code of Ethics issued by the International Federation of Accountants (IFAC/IESBA), which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality, and professional behaviour.

The firm applies International Standard on Quality Control 1 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.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on Örn Software ehf. Iceland's description and on the design and operation of controls related to the control objectives stated in that description, based on our procedures. We conducted our engagement in accordance with International Standard on Assurance Engagements 3402, "Assurance Reports on Controls at a Service Organization," issued by the International Auditing and Assurance Standards Board. That standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and the controls are suitably designed and operating effectively.

An assurance engagement to report on the description, design and operating effectiveness of controls at a service organization involves performing procedures to obtain evidence about the disclosures in the service organization's description of its services, and the design and operating effectiveness of controls. The procedures selected depend on the service auditor's judgment, including the assessment of the risks that the description is not fairly presented, and that controls are not suitably designed or operating effectively. Our procedures included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved. An assurance engagement of this type also includes evaluating the overall presentation of the description, the suitability of the objectives stated therein, and the suitability of the criteria specified by the service organization.

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

Basis for Qualified Opinion

Control Objective C.01

CA.C.01.04

Örn Software ehf. states in its description that the use of shared user IDs is generally not allowed. However, as noted in the test results of control activity C.01.04 in section 4, this control was assessed as not operating effectively during the period under review as a shared user ID was noted in the production database environment was in use by the service provider.

Control Objective F.01

CA.F.01.04

Örn Software ehf. states in its description that adequate separation of duties is ensured in the change management process. However, as noted in the test results of control activity F.01.04 in section 4, this control was assessed as not operating effectively during the period under review as, in not all cases segregation of duties is implemented. Furthermore, incidents were categorized and documented incorrectly.

Control Objective G.01

CA.G.01.02

Örn Software ehf. states in its description that tickets are created from helpdesk emails and that personnel who are assigned to a ticket analyse, resolve, and document the resolution of the problem within the ticket. Furthermore, someone aside from the personnel assigned should authorize/test when needed. However, as noted in the test results of control activity G.01.02 in section 4, this control was assessed as not operating effectively during the period under review where incidents were categorized incorrectly, and an incident lacking required documentation.

This resulted in the non-achievement of the following control objectives stated by Örn Software ehf.:

- "Controls provide reasonable assurance that logical access to programs, data, and computer resources is reasonable and restricted to authorized and appropriate users"
- "Controls provide reasonable assurance that source code changes are performed according to change management procedures to ensure secure and stable software application."
- "Controls provide reasonable assurance that application and system processing are authorized and executed in a complete, accurate, and timely manner, and deviations, problems, and errors are identified, tracked, recorded, and resolved in a complete, accurate, and timely manner."

During the period from 1 January 2022 – 31 December 2022.

Limitations of Controls at a Service Organization

Örn Software ehf. Iceland's description is prepared to meet the common needs of a broad range of customers and their auditors and may not, therefore, include every aspect of the services that each individual customer may consider important in its own particular environment. Also, because of their nature, controls at a service organization may not prevent or detect all errors or omissions in processing or reporting transactions. Also, the projection of any evaluation of effectiveness to future periods is subject to the risk that controls at a service organization may become inadequate or fail.

Qualified Opinion

Our opinion has been formed on the basis of the matters outlined in this report. The criteria we used in forming our opinion are those described in Örn Software ehf. Iceland's assertion as included in section 1 of this report. In our opinion, except for the matter described in the Basis for Qualified Opinion paragraph:

a) The description fairly presents the system as designed and implemented throughout the period from 1 January 2022 to 31 December 2022;

b) The controls related to the control objectives stated in the description were suitably designed throughout the period from 1 January 2022 to 31 December 2022; and

c) The controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved operated effectively throughout the period from 1 January 2022 to 31 December 2022.

Description of Tests of Controls

The specific controls tested, and the nature, timing and results of those tests are listed in section 4 of this report.

Intended Users and Purpose

This report and the description of tests of controls in section 4 are intended only for customers who have used Örn Software ehf. Iceland's services, and their auditors, who have a sufficient understanding to consider it, along with other information including information about controls operated by customers themselves, when assessing the risks of material misstatements of customers' financial statements.

10 May 2023

Helga Harðardóttir,
Partner and State Authorized Public Accountant
Risk Consulting, Advisory, KPMG ehf.
Borgartún 27, 105 Reykjavik
Iceland

Section 3

Örn Software's description of organization and internal control environment

Overview of Company and Services

Örn Software ehf. is a software development company developing and providing software for facility management (MainManager and MainManager FM) and associated services.

Örn Software ehf. has three offices, the headquarters in Kópavogur Iceland, a Danish subsidiary in Vallensbæk Strand, Denmark and a Norwegian subsidiary in Oslo, Norway. Örn Software outsources the datacenter operation to subcontractors, Sentia Danmark A/S, Glostrup Denmark for Danish and Norwegian customers and Opin kerfi hf., Reykjavík Iceland for the HQ and Icelandic customers. Örn Software ehf. is a subsidary of Ørn Software AS in Norway. The scope of this report is the operation of Örn Software ehf. relating to the MainManager solution and not design of controls at the Parent company Ørn Software AS. The description of controls relating to Physical Access and Environmental Controls only applies to Örn Software ehf. offices in Kópavogur Iceland and not to the Danish and Norwegian subsidiaries.

This report includes both the software development processes and IT operation processes offered by Örn Software ehf, including for:

- Software development
- Software as a service (SaaS) cloud solution
- Software for self-hosted solution with accompanying hosting operation services.
- Software customization services
- Customer consulting and implementation services

Software development

Örn Software ehf. develops two products, MainManager and MainManager FM. These are, simply put, two versions of the same system where the newer, MainManager FM is derived from the former and is becoming the main product and is backward compatible regarding the functions supported in both systems. The program is used for facility management and is categorized as a Computer Aided Facilities Management (CAFM) or Integrated Workplace Management System (IWMS).

Software customization services

In some cases, customers must have specific needs fulfilled that is not included in the standard solution. Örn Software ehf. offers customization for those customers.

Software as a Service (SaaS)

Örn Software ehf. offers its software as a SaaS cloud solution to customers as a subscription service including updates according to the software release plan. This includes operating hosting facilities support and customer services.

Software for self-hosted solution

The MainManager software solutions are also offered as a self-hosted solution. To accompany this specific remote software operation services can be provided. In most cases, self-hosted solutions include complex customized integrations and monitoring of such integrations can be offered.

Customer consulting and implementation services

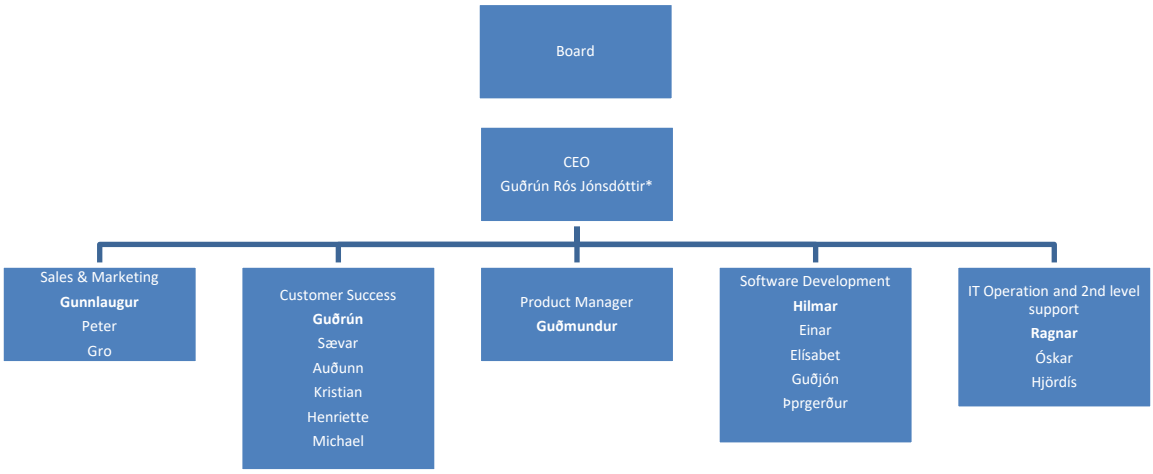
Örn Software ehf. offers the service of experienced facility management specialists and project managers for consulting and implementation of new systems of any size.

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

Control Environment

This report includes exclusively a subset of Örn Software ehf controls and the components of Örn Software ehf. internal verification including controls, that may have a pervasive and permanent effect on the organization as a whole or on processes, applications, interactions and transaction patterns. Certain control components will relate to the organization, where others will be related to specific processes or applications. The total control environment includes the overall organization, governance, policies and procedures defining the general attitude in the organization towards internal controls.

Structure of the organization:



*Guðrún Rós Jónsdóttir was acting CEO of Örn Software ehf. throughout the period of this report and until 20 September 2022

Risk Assessment

Örn Software ehf. has practices in place at corporate and business levels to assist management in identifying and managing risks that could affect the organization's ability to provide a reliable system and services for users. These practices are used to identify and measure the significant risks for the respective organization, initiate the identification and/or implementation of appropriate risk mitigation measures, and assist management in monitoring risk and remediation activities. The risk management practices implemented by Örn Software ehf. consist of internal controls derived from its policies, processes, personnel, and systems. The primary control activities in place to mitigate these risks are regular assessments of challenges facing the business and considering controls that are in place. The management team assesses and treats the residual risks and regularly reviews the risk profile to evaluate whether new risks have arisen and, thus, require additional analysis and handling. The purpose is to identify and classify the risks that may affect the organization's ability to operate according to the obligations the company has. The risk assessment is reviewed and approved by the CEO.

These risk management controls consist of business risk assessment controls. IT specific risk assessment process is being developed and will be implemented within the next year where IT risks will be identified, assessed, classified, prioritized, and corrective actions defined.

Monitoring

Örn Software ehf. conducts periodic reviews of operations to ensure that the set of controls covers all critical services and information security.

Örn Software ehf. uses subcontractors for professional hosting services. Controls at the subcontractor’s location or procedures are not included in this report. Örn Software ehf. monitors the relevant suppliers through receipt and review of external auditor reports and validates that these include requirement and controls for sufficient assurance regarding physical security, access and backup. ISO 27001 certified sub-contractors are deemed valid by the certification.

Information and Communication

Örn Software’s processes information of great importance to its customers. It is therefore crucial for Örn Software that customers always trust that the necessary security is maintained.
As a company, Örn Software is dependent on the security of the IT-based information and production systems.
Örn Software’s level of information security has been established to ensure accessibility, integrity and confidentiality to its systems as well as compliance with relevant regulatory requirements.
Örn Software reviews internal security arrangements at least once a year to ensure that they are adequate and reflect the actual circumstances of Örn Software. Security policies, detailed security rules, and related procedures are available on Örn Software’s intranet for all employees.

Örn Software ehf.’s Description of general operation controls

Security policy

Örn Software ehf. has a security policy which is reviewed at least annually and approved by the CEO. The security policy is made with reference to ITIL and ISO 27001.

All Örn Software ehf.’s employees are responsible for familiarizing themselves with the contents of the security policy.

Physical Access and Environmental Controls

Örn Software’s offices are only accessible for authorized personnel and ensured by electronic access cards and pin codes. Hosting of production servers is handled by qualified hosting providers. The Hosting Provider Guidelines describes the requirements for provider qualifications. Only providers that have appropriate controls are accepted i.e. those providing an ISAE 3402 inspection report or have been ISO 27001 certified.
Controls provide reasonable assurance that physical access to computer equipment, storage media, and program documentation is restricted to authorized individuals.
Controls provide reasonable assurance that environmental controls are established to protect systems housed in the hosting provider(s) data center(s) from environmental hazards.
The scope of this report is bound to Örn Software’s offices and hardware, not the hosting facilities as those are controlled by qualified providers other than ensuring that providers are ISO 27001 certified or provide appropriate controls as reported by ISAE 3402.

Logical Access

Rules for granting, modifying and terminating access and rights are set out in Örn Software ehf’s IT Security Practices.
Procedures and workflows for creating, modifying, and closing access to systems and data is described in Örn Software ehf.’s security practices document.
According to IT security rules, access to Örn Software ehf’s IT systems and data must be group/role based and thereby reflecting the daily functions of the individual employees. By authorizing at the group level Örn Software ehf uses the principle of personal independence, which allows more employees to perform the same functions and work assignments.
Örn Software ehf. only grants authorizations based on specific needs. Authorizations are only granted when there is managerial approval thereof.
The technical administration of system and data authorizations is controlled by the director of IT/software department. The documentation of management approval for each authorization is registered in MainManager's service management tool.

In December 2020 Ørn Software AS in Norway aquired all shares of MainManager ehf, now Örn Software ehf. In March 2021 the Azure tenant of the company was merged into the Ørn Software AS tenant. From that time, techical administration of access to the office network is administered by Ørn Software AS. The system administrators are assigned to the respective logical access tasks by Örn Software ehf. Lead developer. Thus this has no bearing on the design, implementation and compliance of procedures and controls the area for the remainder of the declaration period.
Controls provide reasonable assurance that logical access to critical systems and applications is restricted to authorized personnel.

Data Backup

The Hosting Provider Guidelines documents the operational and backup procedures that must be carried out to ensure adequate operational security.
Application, operating systems, files, and data are backed up on a scheduled basis and rotated to two offsite physical locations by the service providers. Controls related to subservice organizations backup procedures do not fall within the scope of this report.

Production Systems Change Management

Changing of production systems falls under strict change management procedures. To ensure the stability and security for hosted customers, all changes made by Örn Software to the production environment are managed using the IT Operation ticketing system. The only exceptions are routine updates to the MainManager system that are performed according to the update plan for version and maintenance updates. As hosting environments are operated by certified service providers, the change management procedure does not cover normal system updates and maintenance.
Controls provide reasonable assurance that changes to existing systems and implementation of new systems are authorized, tested, approved, implemented, and documented.

Software Development and Change Management

Software source code and version control is managed in a source code management tool (Team Foundation Server). Each software product has three branches: sprint, beta, and release (production code). New development and high-risk changes are carried out in the sprint version. After each sprint (2 weeks) the sprint branch is merged to the beta branch including all new features and changes. When a new version is released, a new release branch is branched from the beta branch. This branch is now the active version branch. Errors and low risk changes are carried out in the release branch.
Controls provide reasonable assurance that new applications and changes to existing applications are authorized, tested, approved, implemented, and documented.

Incident Processing and Problem Management

MainManager helpdesk documents the processing of errors and IT service handling. The helpdesk email and account managers act as 1st level service i.e. first respondent and first point of contact for the customer.
Controls ensure that processing is appropriately authorized and scheduled, and deviations from scheduled processing are identified and resolved within the MainManager helpdesk process.

Controls ensure that problems and errors are recorded, analysed, and resolved according to Service Level Agreement (SLA).

Complementary Controls at User Organizations

To achieve the control objectives specified in this report, controls must be established and handled correctly by the user organizations cf. the terms and conditions in the Supply Agreement with Örn Software. The controls at user organizations are not covered by this report as described below.

Complementary User Entity Controls

The Örn Software ehf. application or system was designed with the assumption that internal controls would be in place by user entities. The application of such internal controls by user entities is necessary to achieve certain control objectives identified in this report. There may be additional control objectives and related controls that would be appropriate for the processing of user entity transactions which are not identified in this report.

Under each section are descriptions of certain controls that user entities should consider in order to fulfil control objectives identified in this report. The complementary user entity controls presented under each section should not be regarded as an exhaustive list of all the controls that should be employed by user entities.

Subservice Organizations

Not subject to examination by KPMG.

Örn Software ehf. uses subservice organizations to perform a range of functions. The following describes the types of subservice organizations used by Örn Software ehf:

Subservice Organization	Function
Sentia Danmark A/S Smedeland 32 2600 Glostrup CVR number: 10008123	Hosting service for Danish and Norwegian customers
Opin kerfi hf. Höfðabakka 9 110 Reykjavík Company ID-number (kennitala): 4201032040	Hosting service for Head Quarters (including development and service) and Icelandic customers

Section 4

Örn Software's Control Objectives and Related Controls and KPMG's Tests of Controls and findings

Following are the control objectives, relevant control activities and test procedures performed as well as the results of the operating effectiveness testing for the period under review.

The carve-out method was used to test controls relating to subservice organizations. This is relevant to control objectives B – Physical access and environmental control and D – Data backup. Subservice organizations (see p.16) perform specific components of these controls that is not reviewed by KPMG as a part of this report. Additionally, the tests of implementation and operating effectiveness of Physical Access and Environmental Controls were only performed in Main Manager. head office in Kópavogur, Iceland and not the Danish or Norwegian subsidiaries.

Furthermore, certain control activities which rely on controls at the user entities were not covered as the scope of this report is limited to those control objectives and control activities performed by Örn Software ehf.. Examples of such controls are included at the end of each control objective chapter; however, this is not an exhaustive list of controls that need to be in place at user entities for the control objectives to be achieved. It is the responsibility of each party to evaluate information on internal controls which are in place at user organizations in order to obtain an overall understanding of internal controls and potential risk.

User organizations' and Örn Software ehf.'s internal controls must be considered together. Örn Software ehf.'s controls do not compensate for potential weaknesses in the service organization's control environment.

During KPMG's review and test of controls consideration was taken of the nature of the controls and items tested, the availability of evidence, and the expected effectiveness of the tests. Various tasks were performed that can broadly be described in the following categories:

- **Inspection:** review of records, reports, files, policies and other documented information that contain an indication of the performance of the control. This included, but was not restricted to, examining management reports, operational logs and other relevant information.
- **Inquiries:** discussions with appropriate management and personnel operating the controls on how controls are performed to gain understanding and additional information about the controls.
- **Observation:** witnessed the performance of activities and operations by observing the application of controls by personnel. Observations were primarily performed where there was no documentary evidence of the operating effectiveness of the controls, either during the period under review, or at all.
- **Sampling:** selected samples from a population to evaluate if activities relating to the control were performed according to Örn Software ehf.'s description.
- **Reperformance:** reperformed the execution of the control procedures that were performed by Örn Software ehf. to determine if the control functions as assumed.

Control Objective A - Information Security Policies

To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

Control ref. #	Controls Specified by Örn Software ehf.	Control Activities Specified by Örn Software ehf	Testing Performed by KPMG and Results of Tests	Results of tests
A.01.01	The IT Security Policy and Information security management procedures are approved by Örn Software's management. Security controls are implemented and in line with policy.	The Security Policy is maintained and reviewed annually by the Security Committee and approved by the CEO. The Security Policy is communicated to all employees prior to employment and when changes occur. All procedures and policies are accessible to all employees and contractors and employees are encouraged and reminded to read through the procedures at least annually.	Inquired with Örn Software's Lead Developer and were informed that the IT Security Policy and Security Controls was reviewed, and the policy is introduced to staff members. Inspected the IT Security Policy and Security Controls and noted they were reviewed in May 2022. The CEO approved the updated version of the IT Security Policy. We reviewed security committee communication to confirm that discussions regarding the policy and its content had taken place and updates been made. Inspected an email that was sent out on June 15th 2022 to employees and noted that the updated IT Security Policy and security control is communicated to all employees. All employees have access to the policies and procedure through SharePoint.	No exceptions noted No exceptions noted. No exceptions noted No exceptions noted.

Complementary User Entity Controls

- User entities are responsible for defining and implementing security policies within their organization.
- User entities are responsible for reviewing on a periodical basis, the fulfilment of those security policies.

Control Objective B – Physical access and environmental control

Controls provide reasonable assurance that physical access to computers and other resources is restricted to authorized and appropriate individuals.

Control ref. #	Controls Specified by Örn Software ehf.	Control Activities Specified by Örn Software ehf	Testing Performed by KPMG	Results of tests
B.01.01	A procedure is in place that ensures that only those who are required to have physical access to Örn Software's headquarters are granted access.	A documented procedure has been developed that outlines the steps required to grant access to the respective office location. Electronic access cards and/or NFC access codes using mobile phones are used for access to office locations. Upon termination or transfer, the employee's physical access privileges are removed.	Inquired with Örn Software's Lead Developer and were informed that 26 people have access to the office and that no employees have left the company within the time period of the report. Inspected documented procedures regarding physical access and noted that electronic access cards are used for access to office locations. Inspected a list of physical access to the office location and noted that 26 access cards are available for Örn Software's offices.	No exceptions noted. No exceptions noted.
B.01.02	Security mechanisms are in place at Örn Software's headquarters.	The respective security service provider calls the Örn Software Iceland's representative in case of physical security alerts at the office in Kópavogur Iceland. The security representative determines if the security service takes action or not.	Inquired with Örn Software's Lead Developer and were informed that the office location in Kópavogur Iceland, has two service providers that provide security arrangements for the building. We were also informed that no physical security incidents took place in the testing period. We noted that the headquarters are equipped with a security system and inspected the contract. Inspected the Jira ticketing system and noted that no incidents took place in the testing period.	No exceptions noted No exceptions noted.

Control ref. #	Controls Specified by Örn Software ehf.	Control Activities Specified by Örn Software ehf	Testing Performed by KPMG	Results of tests
B.01.03	Örn Software outsources all data center related IT services; for its own office system, development, and hosting environments. Örn Software requests documentation from their service providers that provide office and IT hosting services; documentation requested may either include ISO 27001 certification or ISAE 3402 Type II which cover the scope of the data center where MainManager systems are hosted.	All servers are located at service provider (SP) locations. Physical access security is fulfilled by selecting only SP's that are either ISO27001 certified or provide ISAE 3402 Type 2 report covering this area. Örn Software Iceland requests an annual confirmation of the service provider's ISO 27001 certificate, latest audit report and Statement of Applicability or an ISAE 3402/ISAE 3000 (SOC1/SOC2) type II covering a period of 12 months and evaluate if there are any exceptions noted affecting the services used by Örn Software Iceland	Inquired with Örn Software's Lead Developer and were informed that MainManager requests an annual confirmation of the service provider's ISO 27001 certificate, latest audit report and Statement of Applicability or an ISAE 3402/ISAE 3000 (SOC1/SOC2) type II covering a period of 12 months. We noted that an ISO 27001 and ISAE3402 confirmations were in place. Inspected the ISO 27001 and ISAE3402 reports and were informed that the management has evaluated them.	No exceptions noted. No exceptions noted.
B.01.04	MainManager receives notifications and incident reports from service providers in the case of physical access and environmental incidents.	For all incidents that directly affect MainManager or MainManager hosting environments, an incident for the respective category is registered in the MainManager helpdesk system. All incidents are handled according to the respective category.	Inquired with Örn Software's Lead Developer and were informed that one physical access and no environmental incidents took place in the testing period. Reviewed MainManager's helpdesk system and noted that one ticket had been raised. Reviewed the access management ticket and noted that the incident was documented, categorized and follow-up actions were documented.	No exceptions noted. No exceptions noted.

Control Objective C - Logical access

Controls provide reasonable assurance that logical access to programs, data, and computer resources is reasonable and restricted to authorized and appropriate users.

Control ref. #	Controls Specified by Örn Software ehf.	Control Activities Specified by Örn Software ehf	Testing Performed by KPMG	Results of tests
C.01.01	A formal policy for the provision of access rights is implemented, documented, and reviewed along with supporting access control procedures.	An access control policy based on operational and information security requirements is established, documented and reviewed regularly. Users and those providing the service receive a clear message about the operational requirements that must be met for access control. Access rights rules are supported by appropriate procedures and defined responsibilities. A formal process is in place for Access Management that defines scope, process steps, and systems supporting the process and roles and responsibilities.	Inquired with Örn Software's Lead Developer and inspected the Security Policy to determine if a formal policy for the provision of access rights is implemented, documented, and reviewed. The Access Control Policy is a component of the Security Policy. We noted that the Lead Developer who is responsible for the document had reviewed it in May 2022. The policy is available for employees through SharePoint. Inspected access control procedures to verify that access rights rules are supported by appropriate procedures and defined responsibilities.	No exceptions noted. No exceptions noted
C.01.02	Procedures are in place that ensure that only Örn Software employees and contractors have access to restricted systems and data in MainManager operated logical environments; those being the office, development and hosting environments.	A formal process for the provision of access rights for all types of users is implemented. — When a user (employee or contractor) needs access to the MainManager office network (Ørn Software Azure AD), the Lead developer sends an access request to Ørn Software Norway admins. — Users' access shall be based on the roles and responsibilities of each instance.	Inquired with Örn Software's Lead Developer and were informed that there were no new employees in the testing period. The process was reviewed during the meeting. KPMG did not perform any testing for this control as no access requests were made during the test period.	No exceptions noted. No sample to test.

Control ref. #	Controls Specified by Örn Software ehf.	Control Activities Specified by Örn Software ehf	Testing Performed by KPMG	Results of tests
C.01.03	A formal policy is in place for the revocation of access rights along with supporting procedures to ensure that access is revoked in a timely manner.	For all terminated employees and contractors, the Lead developer sends an access revocation request to Ørn Software admins the next working day after termination unless special circumstances require immediate access revocation.	Inquired with Örn Software's Lead Developer and were informed that there were no employee terminations in the testing period. Inspected access revocation processes to verify a formal process is in place for removing access rights in a timely manner. KPMG did not perform any testing for this control as no access revocation were made during the test period.	No exceptions noted. No exceptions noted. No sample to test.
C.01.04	Users have a unique user identifier in order to distinguish one user from another and to establish accountability.	Users are required to have unique user IDs to enable users to be linked to and held responsible for system actions. The use of shared user IDs is generally not allowed. The allocation of system/service account access shall be traceable and approved in work-tickets, The system/service accounts access is limited to the scope of the service.	Inspected a list of all users in Active Directory and noted that users are assigned unique user IDs to ensure traceability of actions. Inquired with Örn Software's Lead Developer and were informed that no shared user ID accounts were established during the testing period. Inspected evidence and noted that no shared user ID accounts were established during the testing period. Inspected an access list to the production and development database environment and noted that one access in the production database environment was shared and used by the service provider.	No exceptions noted. No exceptions noted. No exceptions noted. Exceptions noted.
			Örn Software‘s Management response: The shared access has now been disabled and will not be used anymore. New procedure is now in place to perform the respective service according to the unique user identifier policy.	

Control ref. #	Controls Specified by Örn Software ehf.	Control Activities Specified by Örn Software ehf	Testing Performed by KPMG	Results of tests
C.01.05	Access list is reviewed annually to verify access remains appropriate.	The user access list is reviewed annually. This includes the office environment domain and development environment (i.e. source code domain).	Inquired with Örn Software's Lead Developer and were informed that the office and development environment access list and Production environment access list have been reviewed. Inspected the user access list and noted that reviews are documented.	No exceptions noted.
C.01.06	The MainManager system logs all access and actions performed in the system.	Activity log is available for the MainManager solution as history of all activity in the systems are logged. The logs are kept in the system database. Change logs for individual records is accessible to all users with access to the respective record; however, the log itself is only accessible to administrators in an access-controlled folder/file/repository which is regularly reviewed. Log records are read-only in the system and cannot be deleted or changed. This protects the log against tampering, such as changes, deletion, and unauthorized access on a user level. Logs are generally kept for the lifetime of the system. Logs are bound to the user record, and if the user is pseudo-anonymized, the log cannot be traced to the actual person.	Inquired with Örn Software's Lead Developer and were informed that logs records are read only in the system and are kept in a system database. Inspected a system database selected by the auditor and noted in the system settings that activity logs were available, are read-only and logs are kept for the lifetime of the system.	No exceptions noted. No exceptions noted.

Control ref. #	Controls Specified by Örn Software ehf.	Control Activities Specified by Örn Software ehf	Testing Performed by KPMG	Results of tests
C.01.07	If the standard login (not integrated or single-sign-on) in MainManager is used, the customer can select the strong password policy. Strong password policy is advised (length 8 letters, number, high caps, low caps and symbol)	The system manual which clients receive states that integrated authentication is advised as this simplifies overall user handling. If built in authentication is used, the customer is advised to use a strong password policy (length 8 letters, combination of high caps, low caps, and symbol or number).	Inquired with Örn Software's Lead Developer and were informed that the strong password policy in the MM systems is now a default setting for all customers. Inspected password policy and authentication mechanism which is documented in MainManager's Security Policy as well as the System Manual provided to customers. Customers are advised to use AD Authentication where the System Manual also provides a suggestion for a strong password policy. Password policy in the system manual is in line with the password policy criteria in the MM system: 8 letters, 1 sign or 1 number and 1 capital letter. Inspected whether client had selected strong password policy.	No exceptions noted. No exceptions noted.

Complementary User Entity Controls

- The user entities are responsible for defining their own access control policies, including to the MainManager solution.
- The user entities are responsible for ensuring that privileges assigned to their employees are in line with business needs and that privileged users are limited.
- The user entities are responsible for defining their own password policies in MainManager's system, including whether to use Active Directory Single sign on or the application's standard login.
- The user entities are responsible for reviewing access to their hosted systems.
- The user entities are responsible for ensuring that user identifiers assigned to their users are unique and not shared.
- User entities are responsible for having in place periodic log review process and requesting user activity logs form their MainManager systems.
- User entities are responsible for ensuring that all access, including privileged access, to own database environments hosting the MainManager solution is limited and based on business needs.

Control Objective D – Data backup

Controls provide reasonable assurance that backup and recovery procedures exist to support stable and secure system operation.

Control ref. #	Controls Specified by Örn Software ehf.	Control Activities Specified by Örn Software ehf	Testing Performed by KPMG	Results of Tests
D.01.01	Procedures are in place to ensure that IT service providers carry out satisfactory processes regarding backup and recovering of data and in accordance with hosted customers' SLA.	Örn Software has defined a backup policy. This is the standard backup policy used for all customers unless otherwise specified by the customer.	Inspected the Security Controls procedure for data backup and noted that standard backup policy used for all customers unless otherwise specified by the customer. It was also noted that procedures are documented for performing backups, retention plan and database restore.	No exceptions noted.
D.01.02	Backups are performed on a defined schedule.	Production systems and data are backed up periodically. This is ensured by the service providers. In case of backup error, the service provider notifies Örn Software by email and a ticket raised to follow up on how this is resolved, and the customer is notified if it affects the operation.	Inspected the backup policy and backup reports and noted that backups are conducted periodically. Inquired with Örn Software's Lead Developer and were informed that no backup errors took place in the period. Inspected the service providers reports and noted that no errors came up that did not run successfully when the backup was run again. KPMG did not perform any testing for this control as no backup errors took place during the test period.	No exceptions noted. No exceptions noted. No sample to test

Control ref. #	Controls Specified by Örn Software ehf.	Control Activities Specified by Örn Software ehf	Testing Performed by KPMG	Results of Tests
D.01.03	Restoration tests ensure that backups will perform as expected in a crisis situation.	Annually the service provider conducts backup restoration tests and deliver reports to Örn Software which is responsible for reviewing the reports.	Inspected backup policy to verify that procedures and steps required to perform backups and restores are evident. Inspected backup restoration tests during the test period. Restoration tests were performed in May and June 2022 and confirmation from the service provider is provided. The reports showed that the recovery was performed successfully.	No exceptions noted. No exceptions noted.

Complementary User Entity Controls

- The user entities are responsible for defining their own backup policies, testing and monitoring activities based on their requirements for backup of their own information and systems.
- The user entities are responsible for monitoring and planning backup and recovery for their information systems connected to MainManager's environment.

Control Objective E – System Change Management

Controls provide reasonable assurance that production systems changes are performed according to change management procedures to ensure secure and stable operations.

Control ref. #	Controls Specified by Örn Software ehf.	Control Activities Specified by Örn Software ehf	Testing Performed by KPMG	Results of Tests
E.01.01	The operating procedures for business-critical systems have been documented and have been made available to employees.	The Systems Change Management documented procedure is revised on a regular basis and is available to all employees. The procedure includes evaluating and testing of changes to system software prior to production deployment. Along with the Systems Change Management procedure, Örn Software maintains checklists for standard operations. Standard operations include version and maintenance updates. The checklist describes the procedure for these types of changes. Furthermore, for significant changes, such as new installations, specific guides are maintained detailing the procedure for these types of changes. In case of complex integrated systems, guides/handbooks are maintained for individual customers.	Inquired with Örn Software's Lead Developer and inspected operating procedures for business-critical systems to determine if documentation is in place and has been made available to all employees. We noted that the Systems Change Management documented procedure is in place, has been reviewed and is available to all employees. The policy includes evaluating and testing of changes to system software to assess its potential impact on the system, prior to production deployment. We noted the standard operations check list is in place and Örn Software Iceland employees update the check list in line with what has been done in the process. Release schedule is in place and specific guides are maintained for significant changes and individual customers in case of complex integrated systems.	No exceptions noted. No exceptions noted. No exceptions noted.

Control ref. #	Controls Specified by Örn Software ehf.	Control Activities Specified by Örn Software ehf	Testing Performed by KPMG	Results of Tests
E.01.02	Segregation of duties is implemented and documented in operational procedures.	The change management procedure describes how the segregation of duties is implemented in change management. The document defines 6 different roles: change initiator, change manager, CAB, change builder, change tester, and change implementer. It is documented in each ticket in the helpdesk system who conducts each role for each change. Furthermore, the change management document states that certain roles should not be conducted by the same person. For example, the Change Tester should not be the Change Builder.	Inspected the Change management policy and noted that it describes the requirements for segregation of duties in change management. Inspected a selection of system change tickets and noted that the segregation of duties is implemented.	No exceptions noted.
E.01.03	Controls have been established, that provide reasonable assurance, that Örn Software has established a formal change management process, which ensures testing and approval of relevant changes.	All changes are documented in the helpdesk system. In line with the Systems change management process, documentation in the helpdesk system must include information on authorization, testing, approval, implementation management. Depending on the change category, documentation may vary, including assessment requirement.	Inspected the helpdesk system and noted that tickets include information on authorization, testing, approval and implementation management.	No exceptions noted

Control ref. #	Controls Specified by Örn Software ehf.	Control Activities Specified by Örn Software ehf	Testing Performed by KPMG	Results of Tests
E.01.04	Change Advisory Board (CAB) approves significant, major and emergency changes.	CAB approves significant and major changes that affect production environments. CAB approves emergency changes that affect production environments.	Inquired with Örn Software's Lead Developer and were informed that the CAB team approves larger changes that affect the production environments. Observed three change tickets for emergency changes to the production environment and noted that the CAB team approved the changes, and the approval was documented.	No exceptions noted. No exceptions noted.

Complementary User Entity Controls:

— User entities are responsible for reviewing and assessing the impact to their operations of any changes proposed by MainManager and reporting any problems experienced on their production environments after a change has been implemented.

Control Objective F – Source Code Change Management

Controls provide reasonable assurance that source code changes are performed according to change management procedures to ensure secure and stable software application.

Control ref. #	Controls Specified by Örn Software ehf.	Control Activities Specified by Örn Software ehf	Testing Performed by KPMG	Results of Tests
F.01.01	The source code change management procedures for Örn Software products have been documented and have been made available to staff.	Örn Software uses formal change management procedures for application development. Major application enhancements are managed using SCRUM process and user stories. Minor application changes and error fixes are managed using helpdesk tickets (Release items).	Inquired with Örn Software's Lead Developer and were informed that the formal change management procedures for application development has been reviewed. Inspected the formal change management procedures for application development and noted that the procedure is in place and had been reviewed according to schedule. We noted that major application enhancements are managed using SCRUM processes and user stories and this is documented under User stories in the helpdesk system. We noted as well that minor application changes and error fixes are managed using helpdesk tickets.	No exceptions noted. No exceptions noted. No exceptions noted.
F.01.02	Source code is managed in a source code management tool. Branches are used to ensure quality in active versions. Release schedule is issued annually.	Version control is managed in Team Foundation Server utilizing Development Beta and version branches to ensure the quality of released versions. Release plan is issued for each year containing periodic version updates and maintenance updates.	Inquired with Örn Software's Lead Developer and were informed that the version control is managed in Team Foundation Server utilizing Development Beta and version branches to ensure the quality of released versions. Reviewed release plan for the year containing periodic version updates and maintenance updates. Inspected the version branches and noted the newest release is the same as on the release schedule. Obtained a list of all users with access to the program source code and noted that 22 users have access.	No exceptions noted. No exceptions noted. No exceptions noted.

Control ref. #	Controls Specified by Örn Software ehf.	Control Activities Specified by Örn Software ehf	Testing Performed by KPMG	Results of Tests
F.01.03	Controls have been established, that provide reasonable assurance, that Örn Software has established a formal change management process, which ensures testing and approval of relevant changes.	All changes are tested before deployed to production system.	Inquired with Örn Software's Lead Developer and inspected a sample of user story tickets for the testing period and noted that the change was tested before deployment to the production system.	No exceptions noted.
F.01.04	Segregation of duties is implemented in software development procedures.	Adequate separation of duties is ensured in the change management process.	Inquired with Örn Software's Lead Developer and inspected a sample of software changes in the ticketing system for the testing period and noted that segregation of duties is not implemented in all cases. Also noted that the list had incidents that are categorized and documented incorrectly.	Exceptions noted.
			Örn Software's Management response: The source of the exceptions have been addressed by 1. Informing employees of the importance of correct segregations of duties and correct categorization. 2. Improving the 2nd level service helpdesk processing to verify categorization.	
F.01.05	To ensure stability in the active version, procedure ensures that only error fixes and low risk changes are performed in the active version source code branch.	Before a version release, new code branch is created with the development code for that release. This branch becomes the active version branch once the version is released. Only minor changes and error fixes are allowed in this branch. This branch is used for maintenance updates.	Inquired with Örn Software's Lead Developer and inspected code branches. Observed the Lead Developer demonstrating a code branch in the testing environment, Sprint FM, and noted it is used for maintenance updates, error fixes and minor changes. Also noted for a new version release the branch becomes the active version branch.	No exceptions noted. No exceptions noted.

Control Objective G - Processing and Problem Management

Controls provide reasonable assurance that application and system processing are authorized and executed in a complete, accurate, and timely manner, and deviations, problems, and errors are identified, tracked, recorded, and resolved in a complete, accurate, and timely manner.

Control ref. #	Controls Specified by Örn Software ehf.	Control Activities Specified by Örn Software ehf	Testing Performed by KPMG	Results of Tests
G.01.01	A formal documented process is in place for Incident Management.	A formal documented process is in place for Incident Management that defines scope, process steps, and systems supporting the process as well as roles and responsibilities.	Inquired with Örn Software's Lead Developer and were informed that a Incident Management Policy is in place. Inspected functionality of the process compared to process documentation and noted that the process had an assigned process owner and had been reviewed according to schedule.	No exceptions noted.
G.01.02	A helpdesk process ensures that all production system processing, customer service, errors and security incidents are logged and tracked and resolved in an accurate and timely manner.		Inquired with Örn Software's Lead Developer and inspected the incidents in the ticketing system for the testing period and noted that the list had incidents that were categorized incorrectly and an incident that was unapproved.	Exceptions noted.

Control ref. #	Controls Specified by Örn Software ehf.	Control Activities Specified by Örn Software ehf	Testing Performed by KPMG	Results of Tests
		The production environment is monitored by service providers for infrastructure incidents and failures. Operations personnel are notified by E-mail and if the incident affects customers or action is needed then an IT Service incident ticket is opened in MainManager's helpdesk system. Tickets from customers are typically created via an email to the helpdesk mailbox or created by the customer's account manager. First responders to tickets created from helpdesk email are the respective customer account managers. Account managers categorizes the ticket and assigns to 2nd level service if appropriate. Personnel assigned to a ticket analyze, resolve, and document the resolution of the problem within the ticket. Tickets are prioritized from 1 - 5 where anything higher than 2 is prioritized on the Service department's Kanban Board. Someone aside from the personnel assigned should authorize/test when needed (e.g. in software error incidents). In case of errors, the resolution should always be carried out in according to the customers SLA.	**Örn Software's Management response:** The source of the exceptions have been addressed by 1. Informing employees of the importance of correct categorization, and approval of all incidents that have been resolved. 2. Improving the 2nd level service helpdesk processing to verify categorization and registration.	

Control ref. #	Controls Specified by Örn Software ehf.	Control Activities Specified by Örn Software ehf	Testing Performed by KPMG	Results of Tests
G.01.03	Security incidents are reported to management and the affected customer(s) as soon as possible, and they are managed in a consistent and efficient way.	When incidents are categorized as security incidents then they are notified immediately to management. A security incident ticket is created and prioritized for immediate resolution. The security committee is responsible for the prompt resolution of security incidents.	Inquired with Örn Software's Lead Developer and were informed that no security incidents had taken place in the period. Inspected the incident tickets in the ticketing system and noted that no security incidents were documented during the test period.	No exceptions noted. No sample to test.

Complementary User Entity Controls

— Where vulnerabilities or security incidents are discovered in configurations maintained by user entities, user entities are responsible for taking necessary actions to remediate the risk by patching or modifying configuration.