Deloitte
Statsautoriseret
Revisionspartnerselskab
CVR no. 33 96 35 56
Weidekampsgade 6
PO Box 1600
0900 Copenhagen C

Phone: 36102030
Fax: 36102040
www.deloitte.dk

Independent Service Auditor's ISAE 3402 Type 1 Report on General IT Controls at DLX

As of 11.11.2020

Table of Contents

1 Independent Service Auditor's Report

Independent Service Auditor's Assurance Report on the Description of Controls and their Design

To: the management of DLX A/S, DLX A/S' customers and their auditors

Scope

We have been engaged to report on DLX's description of the general IT controls and control environment in section 3 for services used by customers as of November 11, 2020 (the description), and on the design and implementation of controls related to the control objectives stated in the description.

The report covers the control objectives defined by the management of DLX and the controls performed by DLX from the location in Herning.

Some of the control objectives described in DLX's description of its system can only be achieved if the complementary controls at the user organizations are suitably designed and implemented together with the controls at DLX. The opinion does not include the suitability of the design and implementation of these complementary controls.

DLX's Responsibilities

DLX is responsible for preparing the description and accompanying assertion in section 2, Service Organization's Assertion*,* including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; stating the control objectives; and designing, implementing, and effectively operating controls to achieve the stated control objectives.

Service Auditor's Independence and Quality Control

We have complied with the requirements for independence of IESBA's Code of Ethics for Professional Accountants, which is based on the fundamental principles of integrity, objectivity, professional competence and due care, confidentiality, and professional conduct.

Deloitte uses ISQC 1 and therefore maintains a comprehensive system for quality management, including documented policies and procedures for compliance with the Code of Ethics for Professional Accountants, professional standards, and applicable requirements according to the law and other regulations.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on DLX's description and on the design 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 comply with ethical requirements and 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.

An assurance engagement to report on the description and design of controls at a service organization involves performing procedures to obtain evidence about the disclosures in the service organization's description of its system, and the design of controls. The procedures selected depend on the service auditor's judgment, including the assessment that the description is not fairly presented, and that controls are not suitably designed. 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 and described in section 2, Service Organization's Assertion.

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

Limitations of Controls at a Service Organization

DLX'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 system 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.

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 section 2. In our opinion, in all material respects:

(a) The description fairly presents DLX's general IT controls regarding their services as designed and implemented as at November 11, 2020; and
(b) The controls related to the control objectives stated in the description were suitably designed and implemented as of November 11, 2020.

Description of Tests of Controls

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

Intended Users and Purpose

This report and the description of tests of controls in section 4 are intended only for customers who have used DLX's services and their auditors, who have a sufficient understanding to consider the description along with other information, including information about controls operated by the customers themselves, when obtaining an understanding of the customers' information systems relevant to financial reporting.

Copenhagen, November 17, 2020

Deloitte
Statsautoriseret Revisionspartnerselskab

	M.Bagger
Thomas Kühn Partner, State-Authorized Public Accountant	Michael Bagger Director, CISA

2 Service Organization's Assertion

DLX's Assertion

The accompanying description has been prepared for customers who have used DLX's service and their auditors, who have a sufficient understanding to consider the description along with other information, including information about controls operated by the customers themselves, when obtaining an understanding of the customers' information systems relevant to financial reporting. DLX confirms that:

a) The accompanying description in section 3 fairly presents the general controls related to DLX's services used by customers as of November 11, 2020. The criteria used in making this assertion were that the accompanying description:

i. Presents the way in which the system was designed and implemented, including:

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

ii. Does not omit or distort information relevant to the scope of the system being described, while acknowledging that the 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 system that each individual customer may consider important in its own particular environment.

b) The controls related to the control objectives stated in the accompanying description were suitably designed as at November 11, 2020. The criteria used in making this assertion were that:

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

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.

Herning, November 17, 2020
DLX A/S

Mikael Antonsen
CEO

3 Service Organization's Description

Description of General IT Controls in Connection with the Operation, Monitoring, Maintenance, Support, etc. of Hosting Services with DLX

Through operation, monitoring, support, and maintenance, DLX A/S (hereinafter DLX) offers hosting services to DLX's customers. This description concerns the general IT controls offered for operation, monitoring, maintenance, support etc. of hosting services.

The intention with this description is to provide information for the use of DLX's customers and their accountants and to meet the specifications of International Standard on Assurance Engagements 3402, "Assurance Reports on Controls at a Service Organization".

DLX offers its customers to perform controls of the following:

- Server operation
- Monitoring
- Safety backup
- Network
- Support
- Safety and communication.

As for general IT controls, DLX organizes its effort based on a risk assessment and data security policy, with an IT security manual and individual contracts existing between DLX and its customers, as described in the Terms and Conditions for Hosting Services, the General Terms of Sale, and the Service Level Agreement (SLA).

DLX has defined control objectives in support of our services, within the following areas:

- A.5 Information Security Policy
- A.9 Access Security
- A.11 Physical and Environmental Security
- A.12 Operations Security

DLX is responsible for ensuring the implementation and operation of control systems in order to prevent and identify errors, including deliberate errors, for the purpose of complying with the requirements specified in the SLA.

Risk Management
DLX takes a proactive approach and much prefers to address challenges before they turn into problems. For this reason, DLX adheres to a systematic approach using tables to analyze the risk situation for IT systems and hosting services. This ensures that DLX is able to launch procedures and take the measures necessary to minimize the potential risk of errors.

Risk management involves the following:

- Identification of risks that might potentially impact on the IT environments from a technical and a commercial perspective;
- Assessment of the identified risks, significance, probability, and impact on the IT environments;
- Cost-effective implementation of measures to reduce the probability of the occurrence of risks.

Risk assessments are conducted annually and in the event of major organizational and/or technical modifications. Such measures are to ensure that DLX maintains the high standards that are expected, and conducts risk assessment of business partners and reviews SLAs particularly focusing on ensuring that the IT environments support a high level of availability, confidentiality, and integrity of its hosting services.

Based on the risk assessment, DLX has produced and implemented an IT security policy complete with an IT security manual, which is regularly kept up to date and reviewed. The risk assessment and the IT security policy have been approved by DLX's Board of Directors.

A.5 Information Security Policy

Objective: To provide management with direction and support in terms of information security in accordance with business requirements, and relevant laws and regulations.

DLX has set up an IT security policy with the intention to:

- Offer a stable and secure operational environment characterized by high availability;
- Offer a high service level;
- Restrict employee access to data of relevance to the employee's responsibilities;
- Prevent unauthorized access to units (mobile phone, computer, iPad, and other devices) granting access to sensitive data;
- Restore the IT platform and the data as fast as possible and to the widest possible extent in the event of fire, power interruption, and other force majeure-like situations;
- Protect the operational environment against technical and man-made threats. DLX considers all individuals (internal as well as third parties) to be posing a possible security threat.

The areas are identified taking into account the tasks which DLX is responsible for and undertakes on behalf of its customers and which are specified in the SLA, with annexes, and in the IT security policy.

In view of the risk assessment, DLX has decided on:

- Control measures of relevance to the purpose of security control;
- Risks threatening the fulfilment of the control purposes;
- Controls serving as a preventive measure against the risks.

Organizing Data Security

The Board of Directors has the overall responsibility for the company's IT security. The managing director of DLX is responsible for ensuring that the security policy adopted by the Board is implemented and keeping the Board up to date on IT security.

The technical director is DLX's IT security manager, who has the day-to-day responsibility for the company's IT security. The technical director keeps the managing director informed of the IT security level. This person is also responsible for producing an IT security manual, instructing employees and ensuring awareness on their part.

Unless otherwise agreed in writing, the current SLA between the customer and DLX governs the relationship between the parties.

Since January 1, 2018, DLX has been adhering to the Danish Data Protection Act, which has been effective since May 2018.

A.9 Access Security

Objectives: To limit access to information and information processing facilities. To ensure authorized user access and to prevent unauthorized access to systems and services. To make users accountable for safeguarding their authentication information.

DLX ensures correct protection of data based on a formal procedure, which has been put down in writing. Users are only set up, edited, or deleted by written acceptance by the customer's contact.

DLX regularly reviews and reassesses internal users.

DLX requests use of passwords.

All users are set up with their own user profiles, which provides traceability of use in the system.

A.11 Physical and Environmental Security

Objectives: To prevent unauthorized physical access, damage, and interference to the organization's information and information processing facilities. To prevent loss, damage, theft, or compromise of assets and interruption to the organization's operations.

DLX has set up its hosting services at two different, physical locations. One location serves as DLX's primary operational center, whereas the other is a back-up location.

The primary data center offers the following:

- Redundant monitoring and regulation of the indoor environment
- Redundant UPS
- Diesel generator
- Redundant fiber connection
- Minimum gigabyte connection among all physical racks
- Secure access
- Only access for authorized, selected personnel.

A.12 Control of Communication and Operation

Objectives: To ensure correct and secure operation of information processing facilities. To ensure that information and information processing facilities are protected against malware. To protect against loss of data. To record events and generate evidence. To ensure the integrity of operating systems. To prevent exploitation of technical vulnerabilities.

DLX has its own dedicated connections between the primary data center and the back-up location. This ensures unobstructed backup and system migration between the locations, if required.

DLX's hosting platform is built on servers from Dell/HP/Supermicro and storage from Dell.
The platform has virtualization software to control the virtual servers.

DLX has a system in place to manage hosting center operations, customer administration, and documentation.

DLX has guidelines in place for setting up and managing the set routines for operating the hosting services. Thanks to this documentation, the relevant employees are able to re-establish operations in the event of an error or system breakdown.

The routine operation is monitored and followed through logs, error notifications, and alarms.
In terms of backup, DLX differentiates between data servers and non-data servers:

- Data servers are constantly modified as users enter and change data.
- Non-data servers are only modified when an operator actively alters the system set-up or installs/deletes programs on the server.

All servers are regularly backed up in snapshot intervals.
The backup copies are replicated to an external location in Denmark.

DLX periodically checks the backup at file level and server level, as well as the composite customer set-up. A weekly control is performed to verify that the backup includes all servers.

All DLX systems are protected with an anti-virus solution, as relevant, which is regularly updated and monitored.

Complementary Controls at DLX’s Customers
Customers are responsible for the data transmission between DLX and the customer.

The individual customers are responsible for their own administration of access rights to their user systems and virtual networks, including authorization and review of rights. As a consequence, the customers are to control all details of their user administration.

Regular, compulsory change of user profile passwords or the standard of their quality are not requirements for DLX’s customers. Consequently, it is up to the customers to define their own password length and complexity, and intervals for changing them.

The individual customer is responsible for ensuring the correctness of their data. As a result of this, the individual customer must check the quality, integrity, and confidentiality of their data.

The responsibility for controls in relation to emergency preparedness lies with DLX’s customers.

Customers with a local unit back-up solution (also known as remote backup) are responsible for ensuring that backup jobs are conducted correctly and for testing this regularly.

4 DLX’s Control Objectives and Related Controls, and Deloitte’s Tests of Controls and Results of Tests

4.1 Introduction

This report is intended to provide DLX’s customers with information about the controls at DLX that may affect the processing of user organizations’ transactions and to provide DLX’s customers with information about the design and implementation of the controls that were tested.

This report, when combined with an understanding and assessment of the controls at user organizations, is intended to assist user auditors in (1) planning the audit of user organizations’ financial statements and in (2) assessing control risk for assertions in user organizations’ financial statements that may be affected by controls at DLX.

Our testing of DLX’s controls was restricted to the control objectives and related controls listed in the matrices in this section of the report and was not extended to controls that were stated in the system description but not included in the aforementioned matrices, or to controls that may be in effect at user organizations. It is each user auditor’s responsibility to evaluate this information in relation to the controls in place at each user organization. If certain complementary controls are not in place at user organizations, DLX’s controls may not compensate for such weaknesses.

4.2 Test of Controls

The test of controls performed consist of one or more of the following methods:

Method	Description
Inquiry	Interview, i.e., inquiry with selected personnel at DLX
Observation	Observation of the execution of control
Inspection	Review and evaluation of policies, procedures, and documentation concerning the performance of the control. This includes reading and evaluating reports and other documentation to assess whether specific controls are designed and implemented. Furthermore, it is assessed whether controls are monitored and supervised adequately and at appropriate intervals.
Re-performance of control	Repetition of the relevant control to verify that the control operates as intended

4.3 Test of Design and Implementation

Our test of the design and implementation of controls includes such tests as we consider necessary to assess whether those controls performed, and the extent of compliance with them, were sufficient to provide reasonable, but not absolute, assurance that the specific control objectives were achieved as of November 11, 2020.

Control Objectives, Controls, and Test Results

4.4.1 Information Security Policies

Control Activity	DLX’s Control Activity	Audit Procedures Performed	Test Results
Control objective: To provide management with direction and support for information security in accordance with business requirements and relevant laws and regulations.			
4.4.1.1 *Policies for information security*	DLX has prepared an IT policy based on a risk analysis that sums up the probability and consequences regarding the risks identified. The IT security policy and the risk analysis are approved by management.	Deloitte has reviewed the IT security policy and the risk analysis and verified that it contains IT security guidelines and is approved by management.	No deviations noted.
4.4.1.2 *Review of the policies for information security*	DLX’s IT security policy and risk analysis are reviewed on an annual basis by management. The review is performed according to an internal procedure.	Deloitte has inspected documentation for the latest review of the information security policies and verified the results thereof.	No deviations noted.

4.4.2 Access Security

Control Activity	DLX's Control Activity	Audit Procedures Performed	Test Results
Control objective: To limit access to information and information processing facilities.			
4.4.2.1 *Access control policy*	An access control policy is established, documented, and reviewed based on business and information security requirements.	Deloitte has checked by way of inspection whether an access control policy is established, and that the policy is subject to annual review.	No deviations noted.
Control objective: To ensure authorized user access and to prevent unauthorized access to systems and services.			
4.4.2.2 *User Access Provisioning*	Formalized user administration procedures and processes have been implemented to assign and revoke access rights for users to services and systems. User registrations and de-registrations have been formally approved by management and documented.	Deloitte has assessed the procedures used and the controls performed. We were informed that DLX had no new users or leavers in 2020, hence the control cannot be tested.	No deviations noted.
4.4.2.3 *Management of privileged access rights*	The allocation and use of privileged access rights is restricted and controlled. Management has implemented a detective control for users who are granted domain administrative access rights.	Deloitte has assessed the procedures used and the controls performed. Deloitte has reviewed all users with administrative rights on the DLX domain and verified them together with management.	No deviations noted.
4.4.2.4 *Review of user access rights*	Users for internal systems are reviewed on an annual basis by management. The review is performed according to an internal procedure and documented afterwards.	Deloitte has inspected documentation for user access rights reviews performed during the audit period and verified the results thereof.	No deviations noted.
Control objective: To make users accountable for safeguarding their authentication information.			
4.4.2.5 *Use of secret authentication information*	DLX users are required to follow the organization's IT Security Policy and underlying Password Policy governing the use of secret authentication information.	Deloitte has checked by way of inspection that procedures and controls governing the use of secret authentication information are implemented.	No deviations noted.

4.4.3 Physical and Environmental Security

Control Activity	DLX's Control Activity	Audit Procedures Performed	Test Results
Control objective: To prevent unauthorized physical access, damage, and interference to the organization's information and information processing facilities.			
4.4.3.1 *Physical entry controls*	Secure areas are protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	Deloitte has inspected the physical security perimeters. Deloitte has checked by way of inspection whether physical entry controls are implemented for the office, rooms, and facilities.	No deviations noted.
Control objective: To prevent loss, damage, theft, or compromise of assets and interruption to the organization's operations.			
4.4.3.2 *Supporting utilities*	The following supporting utilities are installed: • Alternative power; • Fire detection/suppression; • Environmental monitors; • Cooling system. All environmental security mechanisms are subject to regular maintenance service and testing.	Deloitte has inspected the data center to verify usage of adequate environmental mechanisms and has reviewed the physical considerations. Furthermore, Deloitte has assessed the documentation regarding the latest service on the equipment.	No deviations noted.

4.4.4 Operations Security

Control Activity	DLX's Control Activity	Audit Procedures Performed	Test Results
Control objective: To ensure correct and secure operation of information processing facilities.			
4.4.4.1 *Documented operating procedures*	DLX has written Standard Operating Procedures regarding the controls and procedures performed in connection with the provision of the agreed-upon services.	Deloitte has verified that written Standard Operating Procedures are stored on the intranet and are available to relevant personnel.	No deviations noted.
4.4.4.2 *Capacity management*	DLX has implemented the use of monitoring resources in order to accommodate future capacity requirements to ensure the required system performance.	Deloitte has verified that monitoring systems and alarms are implemented to monitor capacity requirements.	No deviations noted.
Control objective: To ensure that information and information processing facilities are protected against malware.			
4.4.4.3 *Controls against malware*	Detection, prevention, and recovery controls to protect against malware are implemented along with appropriate user awareness.	Deloitte has inspected the controls against malware. Deloitte has inspected the documentation to verify the implementation of controls against malware and confirmed by way of inquiry the existence of appropriate user awareness.	No deviations noted.

Control Activity	DLX's Control Activity	Audit Procedures Performed	Test Results
Control objective: To protect against loss of data.			
4.4.4.4 *Information backup*	DLX has implemented back-up copies of information and software, and system images are taken and tested regularly in accordance with DLX's established back-up policy.	Deloitte has inspected the back-up policy and tested whether the back-up parameters are implemented according to the approved back-up policy.	No deviations noted.
Control objective: To record events and generate evidence.			
4.4.4.5 *Event logging*	Event logs recording user activities, exceptions, faults, and information security events are produced according to the established audit policy.	Deloitte has checked by way of inspection that event logging has been defined and implemented.	No deviations noted.
Control objective: To ensure the integrity of operational systems.			
4.4.4.6 *Installation of software on operational systems*	Procedures are implemented to control the installation of software on operating systems.	Deloitte has inspected procedures for installing and patching software on operating systems.	No deviations noted.
Control objective: To prevent exploitation of technical vulnerabilities.			
4.4.4.7 *Management of technical vulnerabilities*	Information about technical vulnerabilities of information systems being used are obtained in a timely fashion; the organization's exposure to such vulnerabilities is assessed; and appropriate measures are taken to address the associated risk.	Deloitte has checked by way of inspection whether procedures for governing technical vulnerabilities are implemented.	No deviations noted.