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

Phone +45 36 10 20 30
Fax +45 36 10 20 40
www.deloitte.dk

Indicia Danmark A/S

Independent auditor's ISAE 3000 type 1 report on the design and implementation of general IT controls supporting the eTrack1 solution

As of 9 January 2020

Table of Contents

1. Independent Service Auditor's Report

Independent Service Auditor's ISAE 3000 Type 1 Report on the Design and Implementation of General IT Controls Supporting the eTrack1 Solution

To: Indicia Danmark A/S, Indicia Danmark A/S' customers and their auditors

Scope

We have been engaged to report on Indicia Danmark A/S' ("Indicia") selected controls relevant to the eTrack1 service provided to customers as of 9 January 2020.

The report only covers the controls performed by Indicia from the location in Aarhus and does not extend to controls performed by Indicia's sub-service providers:

- IT Security – Hosting and backup of the development environment;
- Itadel – Hosting, operations, backup and network controls related to the production environment.

The control objectives and controls covered by this report are defined by Indicia.

Indicia's Responsibilities

Indicia is responsible for defining the control objectives and specifying the necessary controls in order to achieve the control objectives as stated in section 3.

Indicia's management is responsible for ensuring that the control environment supporting the delivery of eTrack1 is configured according to the client agreements and for ensuring that controls are designed and implemented to meet the stated control objectives, as presented in section 3 of this report.

Independence and Quality Control

We have complied with the requirements of independence of the 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, based on our performed procedures, to form an opinion on the design and implementation of controls related to the control objective stated in section 3.

The criteria we used in forming our opinion on whether the identified controls related to the control objectives in section 3, in all material respects, were suitably designed and implemented as of 9 January 2020, are:

a. The risks that threatened the achievement of the control objectives described in section 3 had been identified by the management;
b. The identified controls, if designed and implemented as intended, would give reasonable assurance that the identified risks do not prevent the achievement of the stated control objective; and
c. The controls had been operating effectively and had been performed by people with appropriate competence as of 9 January 2020.

We conducted our engagement in accordance with International Standard on Assurance Engagements 3000, ”Assurance Engagements Other than Audits or Reviews of Historical Financial Information”, issued by the International Auditing and Assurance Standards Board, to plan our procedures to obtain reasonable assurance about whether, in all material respects, the tested controls are suitably designed and operating effectively.

Our procedures included testing the design, implementation and operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the control objectives stated in section 3 have been achieved. Our procedures included interviews and inspection of documentation to determine whether the controls had been suitably designed and implemented. This auditor’s report is based on our audit performed in the period from October to December 2019.

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 Organisation

Because of their nature, controls at a service organisation 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 organisation may become inadequate or fail.

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 the *“Service Auditor’s Responsibilities”* paragraph. It is our opinion that the implemented general IT controls that support the delivery of the eTrack1 service and the achievement of the control objectives in section 3, in all material respects, were suitably designed and implemented as of 9 January 2020.

Description of Tests of Controls

The specific controls tested are to be found in section 3 of this report.

Intended Users and Purpose

This report and the description of tests of controls in section 3 are intended only for customers who have used Indicia’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.

Copenhagen, 26 February 2020

Deloitte
Statsautoriseret Revisionspartnerselskab
CVR no. 33 96 35 56

M. Bagger

Thomas Kühn
Partner, state-authorised public accountant

Michael Bagger
Director, CISA

2. Service Organisation's Assertion

This assertion relates to general IT controls and processes performed by Indicia Danmark A/S ("Indicia") as part of the provision of the eTrack1 service. This assertion is to acknowledge our responsibility for designing and implementing controls aligned with the general client agreements regarding the delivery of the eTrack1 solution.

Indicia offers a proprietary business solution, eTrack1, a ticketing system which helps the client to handle customer inquiries in an easy and effective manner. Indicia aids their clients through the platform by consulting and streamlining internal processes for higher levels of service and better customer experiences.

Indicia confirms that:

a) Indicia has organised the management of IT Security following the ISO 270001 standards, and all clients are by default operated according to Indicia's common IT processes, controls and security baselines;
b) Relevant control objectives and controls for eTrack1 have been identified and are stated in section 3 of this report;
c) It is the responsibility of Indicia to establish and maintain adequate controls, as stated in section 3. This includes appropriate technical and organisational measures;
d) For some control objectives, the procedures to support them have just been implemented as part of the audit process, and hence these procedures have not yet been performed;
e) The controls stated in section 3 were suitably designed and implemented as of 9 January 2020. The criteria for this statement are:
    1) The risks that threatened the achievement of the control objectives described in section 3 had been identified by the management;
    2) The identified controls, if designed and implemented as intended, would give reasonable assurance that the identified risks do not prevent the achievement of the stated control objectives; and,
    3) The controls had been operating effectively and had been performed by people with appropriate competence as of 9 January 2020.

This report does not include:

a) Controls performed by the clients;
b) Controls performed by sub-service providers;
c) Controls performed on client environments where the client has administrative access rights.

Aarhus, 26 February 2020
Indicia A/S

Brian Mortensen
CEO

3. Indicia's Control Objectives and Related Controls, and Deloitte's Tests of Controls and Results of Tests

Introduction

Our test of Indicia's controls is limited to the control objectives and controls defined by Indicia in the matrix below. Controls performed by the sub-service providers IT Security and Itadel are not within the scope of this report.

Test of Controls

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

Method	Description
Inquiry	Interview, i.e. inquiry with selected personnel at Indicia
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 functions as intended

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 were sufficient to provide reasonable, but not absolute, assurance that the specific control objectives were achieved as of 9 January 2020.

Control objectives, controls and test results

A.5 Information Security Policies

No.	Control objectives	Test performed	Test result
5.1 Management direction for information security			
Objective: To provide management direction and support for information security in accordance with business requirements.			
5.1.1	Policies for information security A set of policies for information security are defined, approved by the management, published and communicated to employees and relevant external parties.	Deloitte has inspected that an information security policy is defined, implemented and approved by the management, communicated to all employees and available for external parties.	No exceptions noted.
5.1.2	Review of the policies for information security The policies for information security are reviewed at planned intervals or when significant changes occur to ensure their continued suitability, adequacy and effectiveness.	Deloitte has inspected that a formalised procedure is in place to ensure that the information security policy is annually reviewed and approved by the management.	No exceptions noted.

A.6 Organisation of Information Security

No.	Control objectives	Test performed	Test result
6.1 Internal organisation			
Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organisation.			
6.1.1	Information security roles and responsibilities All information security responsibilities are defined and allocated.	Deloitte has inspected that the information security responsibilities are defined and allocated in the form of an organisational structure. Furthermore, we have assessed the role set-up based on our understanding of Indicia's organisation.	No exceptions noted.
6.1.2	Segregation of duties Conflicting duties and areas of responsibility are segregated to reduce opportunities for unauthorised or unintentional modification or misuse of the organisation's assets.	Deloitte has inspected that the information security policy describes the user access rights that are assigned to employees based on their work-related needs.	No exceptions noted.
6.2 Mobile devices and teleworking			
Objective: To ensure the security of teleworking and use of mobile devices.			
6.2.1	Mobile device policy A policy and supporting security measures are implemented to manage the risks introduced by using devices.	Deloitte has inspected that the information security policy contains a defined policy for the use of mobile devices.	No exceptions noted.
6.2.2	Teleworking A policy and supporting measures are implemented to protect information accessed, processed or stored at teleworking sites.	Deloitte has inspected that the information security policy contains a defined policy, and supporting measures are in place to support the protection of information accessed, processed or stored at teleworking sites.	No exceptions noted.

A.8 Asset management

No.	Control objectives	Test performed	Test result
8.2 Information classification			
Objective: To ensure that information receives an appropriate level of protection in accordance with its importance to the organisation.			
8.2.1	Classification of information Information is classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.	Deloitte has inspected formalised procedures for the classification of information.	No exceptions noted.

A.9 Access control

No.	Control objectives	Test performed	Test result
A.9.1 Business requirements of access control			
Objective: To limit access to information and information processing facilities.			
9.1.1	Access control policy An access control policy is established, documented and reviewed based on business and information security requirements.	Deloitte has inspected whether the information security policy contains an access control policy and that the underlying policy is subject to an annual review.	No exceptions noted.
9.1.2	Access to networks and network services Users are only granted access to the network and network services they have been specifically authorised to use.	Deloitte has inspected the policy for user access to the network and network services. Deloitte has inspected the documentation for configuration and segregation of networks and whether users have access to the network and/or network services they have been authorised to use.	No exceptions noted.
A.9.2 User access management			
Objective: To ensure authorised user access and to prevent unauthorised access to systems and services.			
9.2.1	User registration and deregistration A formal user registration and deregistration process is implemented to enable assignment of access rights.	Deloitte has inspected that the formalised procedures, processes and controls for user registration and deregistration are in place. Deloitte has tested for one user registration and on user deregistration whether they were documented and approved.	No exceptions noted.
9.2.2	User access provisioning A formal user access provisioning process is implemented to assign or revoke access rights for all user types to all systems and services.	Deloitte has inspected the procedure for user access provisioning and tested for one access provisioning whether this was documented and approved.	No exceptions noted.

No.	Control objectives	Test performed	Test result
9.2.3	Management of privileged access rights The allocation and use of privileged access rights is restricted and controlled. Two-factor authentication of privileged access is an option.	Deloitte has inspected that procedures and controls for managing privileged access rights are implemented. Deloitte has inspected the documentation for privileged access rights and whether the rights have been restricted and controlled.	No exceptions noted.
9.2.5	Review of user access rights Asset owners are reviewing users' access rights at regular intervals.	Deloitte has inspected the procedures for reviewing user access rights and noted that the user access rights have been reviewed.	No exceptions noted.
9.2.6	Removal or adjustment of access rights The access rights of all employees and external users to information and information processing facilities are removed upon termination of their employment, contract or agreement, or adjusted upon change.	Deloitte has inspected that the procedures and controls for user deregistration are in place. We were informed that user terminations had taken place.	No exceptions noted.
A.9.3 User responsibilities			
Objective: To make users accountable for safeguarding their authentication information.			
9.3.1	Use of secret authentication information Users are required to follow the organisation's practice in using secret authentication information.	Deloitte has inspected that the procedures and controls for the use of secret authentication are implemented.	No exceptions noted.
9.4 System and application access control			
Objective: To prevent unauthorised access to systems and applications.			
9.4.1	Information access restriction. Access to information and application system functions shall be restricted in accordance with the access control policy.	Deloitte has inspected that the information security policy contains a defined policy for information access restriction, and that measures to restrict access to information have been implemented.	No exceptions noted.
9.4.2	Secure log-on procedures	Deloitte has inspected the access control policy, which contains log-on procedures and	No exceptions noted.

No.	Control objectives	Test performed	Test result
	Where required by the access control policy, access to systems and applications is controlled by a secure log-on procedure.	configuration of password settings for critical systems, to verify whether a secure log-on procedure has been implemented.	
9.4.5	Access control to program source code Access to program source code is restricted.	Deloitte has inspected the access control policy for protecting source code and tested for a sample of one whether access to source code was approved.	No exceptions noted.

A.10 Cryptography

No.	Control objectives	Test performed	Test result
A.10.1 Cryptographic controls			
Objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.			
10.1.1	Policy on the use of cryptographic controls A policy on the use of cryptographic controls for protection of information is developed and implemented.	Deloitte has inspected the policy on the use of cryptographic controls. Deloitte has inspected that the policy and documentation for certificates and cryptographic controls are implemented.	No exceptions noted.
10.1.2	Key management A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole life cycle.	Deloitte has inspected the documentation for the use of cryptographic keys.	No exceptions noted.

A.11 Physical and environmental security

No.	Control objectives	Test performed	Test result
A.11.1 Secure areas			
Objective: To prevent unauthorised physical access and damage to, and interference of, the organisation’s information and information processing facilities.			
11.1.2	Physical entry controls Secure areas are protected by appropriate entry controls to ensure that only authorised personnel are allowed access.	Deloitte has inspected the physical security perimeters. Deloitte has inspected whether physical entry controls are implemented for the office, rooms and facilities.	No exceptions noted.
A.11.2 Equipment			
Objective: To prevent loss, theft or compromise of, or damage to, assets or interruption of the organisation’s operations.			
11.2.9	Physical entry controls Secure areas are protected by appropriate entry controls to ensure that only authorised personnel are allowed access.	Deloitte has inspected whether the information security policy contains a defined clean-desk and clean-screen policy. Deloitte has inspected the office, rooms and facilities to verify that the clean-desk policy is applied.	No exceptions noted.

A.12 Operations security

No.	Control objectives	Test performed	Test result
A.12.1 Operational procedures and responsibilities			
Objective: To ensure correct and secure operations of information processing facilities.			
12.1.1	Documented operating procedures Operating procedures are documented and made available to all users who need them.	Deloitte has inspected that Indicia has formalised relevant operating procedures in place. Deloitte has inspected whether the documented operating procedures are made available to all users.	No exceptions noted.
12.1.2	Change management Changes to the organisation, business processes, information processing facilities and systems that effect information security are controlled.	Deloitte has inspected the change management procedures. Deloitte has inspected whether relevant operating procedures for change management are implemented, including requirements for testing and approval of changes.	No exceptions noted.
12.1.4	Separation of development, testing and operational environments Development, testing and operational environments are separated to reduce the risks of unauthorised access or changes to the operational environment.	Deloitte has observed that separate operational environments are implemented.	No exceptions noted.

No.	Control objectives	Test performed	Test result
A12.2 Protection from malware			
Objective: To ensure that information and information processing facilities are protected from malware.			
12.2.1	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 exceptions noted.
A12.3 Backup			
Objective: To protect against loss of data.			
12.3.1	Information backup Back-up copies of information, software and system images are taken and tested regularly in accordance with an agreed back-up policy.	Deloitte has inspected the back-up policy and tested a random sample to ensure that backup is performed according to the approved back-up policy.	No exceptions noted.
A12.4 Logging and monitoring			
Objective: To record events and generate evidence.			
12.4.1	Event logging Event logs recording user activities, exceptions, faults and information security events are produced, kept and reviewed according to the policies.	Deloitte has inspected that event logging has been defined and implemented.	We noted that event logs are not reviewed periodically. No further exceptions noted.
12.4.2	Protection of log information Logging facilities and log information are protected against tampering and unauthorised access.	Deloitte has inspected whether logs are protected against tampering and unauthorised access.	We were informed that the logs were in the process of being secured during our audit. No further exceptions noted.
12.4.3	Administrator and operator log System administrator and system operator activities are logged, and the logs are protected and reviewed according to the policies.	Deloitte has inspected whether actions performed by administrators and system operators are logged, and whether logs are protected against tampering and unauthorised access.	We were informed that the logs were in the process of being secured during our audit.

No.	Control objectives	Test performed	Test result
			No further exceptions noted.
12.5 Control of operational software			
Objective: To ensure the integrity of operational systems.			
12.5.1	Installation of software on operational systems Procedures are implemented to control the installation of software on operational systems.	Deloitte has inspected procedures for installing and patching software on operational systems. Deloitte has tested for a sample of released patches whether they were implemented.	No exceptions noted.
12.6 Technical vulnerability management			
Objective: To prevent exploitation of technical vulnerabilities.			
12.6.1	Management of technical vulnerabilities Information about technical vulnerabilities of information systems being used are obtained in a timely fashion; the organisation's exposure to such vulnerabilities is assessed; and appropriate measures are taken to address the associated risk.	Deloitte has inspected whether procedures for governing technical vulnerabilities are implemented.	No exceptions noted.

A.13 Communication security

No.	Control objectives	Test performed	Test result
13.2 Information transfer			
Objective: To ensure protection of information in networks and its supporting information processing facilities.			
13.2.1	Information transfer policies and procedures Formal transfer policies, procedures and controls are in place to protect the transfer of information through the use of all types of communication facilities.	Deloitte has inspected whether the Information Security Policy contains policies, procedures and controls to protect the transfer of information through communication facilities.	No exceptions noted.
13.2.2	Agreements on information transfer Agreements address the secure transfer of business information between the organisation and external parties.	Deloitte has inspected whether the Information Security Policy contains policies for secure transfer of business information. Deloitte has inspected documentation and agreements with external parties to verify that the policies are applied.	No exceptions noted.
13.2.4	Confidentiality or non-disclosure agreements Requirements for confidentiality or non-disclosure agreements reflecting the organisation's needs for protection of information are identified, regularly reviewed and documented.	Deloitte has inspected whether the Information Security Policy contains requirements for confidentiality and non-disclosure agreements. Deloitte has inspected for one external supplier and for one employee that a valid confidentiality agreement is in place.	No exceptions noted.

A.14 System acquisition, development and maintenance

No.	Control objectives	Test performed	Test result
A.14.2 Security in development and support processes			
Objective: To ensure that information security is designed and implemented within the development life cycle of information systems.			
14.2.1	Secure development policy Rules for the development of software and systems are established and applied to organisational developments.	Deloitte has inspected that rules for software development are implemented.	No exceptions noted.
14.2.2	System change control procedures Changes to systems within the development life cycle are controlled by the use of formal change control procedures.	Deloitte has inspected that controls are established and implemented to ensure the use of formal change control procedures. Deloitte has tested one change sample to verify whether the procedure had been followed.	No exceptions noted.
14.2.3	Technical review of applications after operating platform changes Operating platforms are changed and business-critical applications are reviewed and tested to ensure there is no adverse impact on organisational operations or security.	Deloitte has inspected the processes for technical reviews of applications after operating platform changes.	No exceptions noted.
14.2.5	Secure system engineering principles Principles for engineering secure systems are established, documented, maintained and applied to any information system implementation effort.	Deloitte has inspected whether the Information Security Policy contains principles for secure system development.	No exceptions noted.
14.2.6	Secure development environment The organisation has established and appropriately protects secure development environments for systems developments and integration efforts that cover the entire system development life cycle.	Deloitte has inspected whether the Information Security Policy contains procedures for secure development environments. Deloitte has inspected that secure development environments are applied through segregated testing, development and production environments.	No exceptions noted.

No.	Control objectives	Test performed	Test result
14.2.8	System security testing Testing of security functionality is carried out during development.	Deloitte has inspected whether the Information Security Policy contains principles for security testing in relation to development.	We noted that a procedure is in place but not yet in use.
A.14.3 Test data			
Objective: To ensure protection of data used for testing.			
14.3.1	Protection of test data Test data are selected carefully, protected and controlled.	Deloitte has inspected whether the Information Security Policy contains principles for the use and protection of test data.	No exceptions noted.

A.15 Supplier relationships

No.	Control objectives	Test performed	Test result
A.15.1 Information security in supplier relationships			
Objective: To ensure protection of the organisation's assets that are accessible by suppliers.			
15.1.2	Addressing security within supplier agreements All relevant information security requirements are established and agreed with each supplier that may access, process, store, communicate or provide IT infrastructure components for the organisation's information.	Deloitte has inspected documentation for agreements with external suppliers and whether they contain security requirements.	No exceptions noted.
A.15.2 Supplier service delivery management			
Objective: To maintain an agreed level of information security and service delivery in line with supplier agreements.			
15.2.1	Monitoring and review of supplier services The organisation regularly monitors, reviews and audits the delivery of supplier service.	Deloitte has inspected the procedures for monitoring and reviewing supplier services. Deloitte has inspected for one supplier that Indicia has reviewed the third-party auditor's report.	No exceptions noted.