bakertilly

The Enlighten Company

(Free translation from the original issued in Portuguese. In the event of discrepancies, the Portuguese language version prevails.)

Independent Auditors' Assurance Report on controls and related design.
May 19, 2022

Summary

Section I – Independent Auditors' Assurance Report and Assessment of Controls

To
The Enlighten Company
São Paulo – SP

Scope

We have been engaged to report on the description of The Enlighten Company (Company) (pages 11 to 18) on its BEN Portal for processing customers' transactions during the period January 01, 2022 to May 19, 2022 and on the design of controls related to the control objectives stated in the description.

The systems comprising the BEN Portal in this scope are:

- Asken;
- Cleaner;
- Closing;
- Budgeetfy;
- Pagben; and
- URI.

We did not perform any procedures regarding the operating effectiveness of controls included in the description and, accordingly, do not express an opinion thereon.

Service Organization's Responsibilities

The Company is responsible for: (i) preparing the description and accompanying assertion at page (page 8), including the completeness, accuracy and method of presentation of the description and the assertion; (ii) providing the services covered by the description; (iii) stating the control objectives; and (iv) designing, implementing and effectively operating controls to achieve the stated control objectives.

Independent auditors' responsibility

Our responsibility is to express an opinion on the Company'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 NBC TO 3402 – Assurance Reports on Controls at a Service Organization, issued by the Federal Accounting Council. 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 in all material respects.

Independent auditors' responsibility--Continued

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 control objectives stated therein, and the suitability of the criteria specified by the service organization.

As noted above, we did not perform any procedures regarding the operating effectiveness of controls included in the description and, accordingly, do not express an opinion thereon.

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

The Company'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 IV Control Design Test.

In our opinion, in all material respects:

(a) The description fairly presents BEN's Portal system as designed and implemented during the period January 01 to May 19, 2022; and
(b) The controls related to the control objectives stated in the description were suitably designed for the period January 01 to May 19, 2022.

Intended users and purpose

This report is intended only for customers who have used the Company's BEN Portal system, 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 misstatement in their financial statements.

São Paulo, May 19, 2022.

Baker Tilly 4Partners Auditores Independentes S.S.
CRC 2SP-031.269/O-1

Alexandre De Labetta Filho
Accountant CRC 1SP-182.396/O-2

Section II – Service Organization´s Assertion

The Enlighten Company
Independent Auditors' Assurance Report on controls and related design
May 19, 2022

The description was prepared for customers entities using the BEN Portal system and its auditors to have a sufficient understanding to consider it, along with other information about controls operated by customers themselves, when obtaining an understanding of customers' information systems relevant to financial reporting. The Company confirmed that:

(a) The description on pages [11-18] fairly presents the BEN Portal system for processing user entities' transactions in the period January 01, 2022 to May 19, 2022. The criteria used in making this assertion were that the accompanying description:

(i) Presents how 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, including procedures by which transactions are initiated, recorded, processed, corrected as necessary, and transferred to the reports and other information prepared for user entities;
- The related records and supporting information, including specific accounts that are 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 user entities;
- How the service organization's system deals with significant events and conditions, other than transactions;
- The process used to prepare reports and other information for user entities;
- The stated 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 by ourselves alone;
- Other aspects of the service organization's control environment, risk assessment process, information system (including the related business processes) and communication, control activities and monitoring controls that are relevant to the processing and reporting of user 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. 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; 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.

# Section III – Description of the Controls

The Enlighten Company
Independent Auditors' Assurance Report on controls and related design
May 19, 2022

1 Information about the Company

The Company specializes in digital transformation, and is a center of excellence for management operations around the world and considered one of the most respected digital transformation firms.

The company's services include consultancy, services and products to improve organizational efficiency.

2 Organizational structure
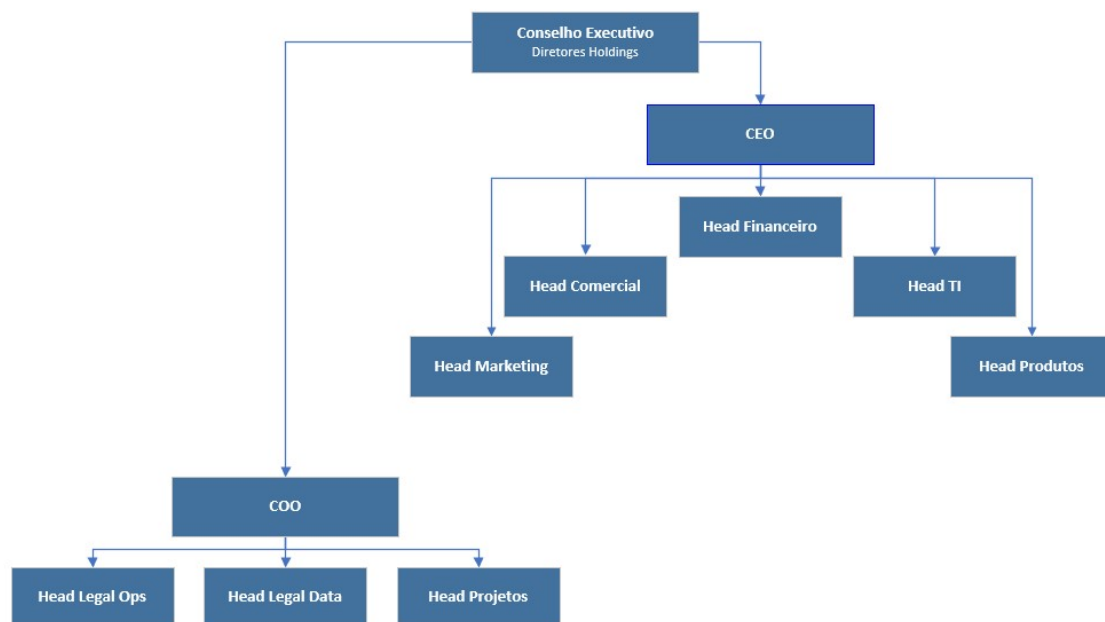
3 Description of products offered

A) **Asken**: Appointment management software using artificial intelligence. Diminishes repetition and controls response quality;

B) **Cleaner**: Software capturing public and private data that handles information in the desired database;

C) **Closing**: Software for closing accounts and circularizing information between the audit, law firms and legal departments. Controlling and monitoring changes in Provisions and Contingencies such as automatic minutes;

D) **Budgeetfy**: Software that enhances financial planning in business departments. Suitable for monitoring resources, approvals, escalation limits and financial planning;

E) **Pagben**: Software that optimizes operation of payments, approvals and financial entries, with predictability, transparency and audits on all parties involved;

F) **URI**: Product intended to control the circularization of procedural data between legal departments and suppliers, that can compare data presented by suppliers, in order to consolidate the information controlled by legal departments.

4 Description of Internal IT Controls

The control objectives were selected according to the Company's services, and control activities are documented through policies and procedures in order to provide a reasonable assurance that the control objectives are achieved.

Logical Access.

Control objective:
A) **Information Security Policy** Guarantee that the Information Security Policy has been duly implemented and the company's users are aware of the document's contents.

LA.A01	The Company has a document called "Information Security Incidents Management Policy", which sets out the guidelines and controls related to information security and management. This document applies to all the organization's employees. During the onboarding process, employees have to sign the "Nondisclosure Agreement", in which employees state they are aware of the policy's contents.

Control objective:
B) **Access restriction** The controls provide a reasonable assurance that only authorized personnel can access IT resources, in order to reduce the risk of unauthorized access to systems and data.

LA.B01	The Company's IT systems are developed in accordance with good IT security practices and have password management parameters in order to mitigate the risk of unauthorized access.
LA.B02	The Company has a document called "Access Management Policy", which describes the control activity for limiting privileged or administrator access to IT resources and systems. Access to the system's configurations is awarded to administrators and is restricted to suitable personnel exercising activities compatible with systems administration. Access is released by controlling accesses awarded.

Control objective:

	C) Awarding, modifying and revoking user access The controls provide a reasonable assurance that the awarding, modification and revoking of user accounts are requested and approved by appropriate personnel, in order to mitigate the risk of unauthorized or improper access to systems and data.
LA.C01	The Company has a document called "Access Management Policy", which describes the control activity for awarding new access to IT resources and systems. The entire process of requesting access to the company's IT systems and resources should be formalized through the ITSM tool and approved by a person with a hierarchal level equal to or higher than supervision of the area which the employee receiving access is allocated or the human resources department. The form completed by the Asken tool should at least contain the following information: Username; User ID; Grounds for awarding access; Access profile or group and Award Date. All users should have an identification key, controlled through a Unique Identification Number (ID) to guarantee traceability, which cannot be repeated. The party requesting access should use the document called "Access Matrix" to consult all profiles available in the systems.
LA.C02	The Company has a document called "Access Management Policy", which describes the control activity for revoking access to IT resources and systems. All requisitions to revoke access for a Company employee should be made or approved by a person in a hierarchical level equal to or higher than coordination, be they in the human resources Department or the employee's department. It is also essential the requisition be made formally, in good time and by completing a form, in accordance with the termination of the employment contract. This form should contain at least the following information: Username; User ID; Grounds for revoking access; date revoked. The Human Resources department shall report employees leaving the company to the Projects and Information Technology Development departments. The employee's termination should be informed at least 24 hours before the end of their employment contract, when applicable, so that access can be revoked on the same day of their departure.

Control objective:

D) Reviewing access Provide a reasonable assurance there is segregation of duties for IT resources systems and users in order to mitigate the risk of unauthorized or improper access to systems and data.

Control objective:	
LA.D01	The Company has a document called "Access Management Policy", which describes the control activity for the periodic reviewing of access rights to IT resources and systems.
	The Information Technology and Development and Projects departments annually review the access rights of all the Company's internal users that are active, checking with each department's managers whether the access rights should be maintained, discontinued or modified.
	The response or validation of managers for each review should be formally registered in order to document the entire process.

Change Management

Control objective:	
A) Authorizing, testing, validating and approving changes Provide a reasonable assurance that modifications to application systems have been duly authorized, tested and approved before being implemented in the production systems.	
CM.A01	The Company has a document called "Changes Management Policy", which describes the control activities for making changes to systems.
	All requisitions to develop / change systems should be made by the business departments or the Company's products department. After requisition from the requesting department, the products area is tasked with analyzing demand and whether development is needed.
	After alignment between the products department and development department, a time frame is established to conclude the new demand, which should be informed to the requester, whose approval should be obtained through the document setting out the production scope.
	After approving the documentation, the scope is included in the next Sprint Planning ceremony, and therefore placed on the development track.
CM.A02	Ratification should occur in a ratification environment separate from production and duly registered/documented in a form setting out evidence of the tests conducted.
	Once ratification has been completed with the products team, it will send it for validation by the requester, who may request adjustments, which will be inserted in the next Sprint Planning ceremonial, or can be sent for production, if the requester agrees with the development made.
CM.A03	Any changes to be made to the production system shall be accompanied by formal documentation approved or prepared by the head of the Company's products team.

Control objective:	
CM.A04	Changes classified as urgent stem from incidents or problems resulting in product or service unavailability, impacting customers. In these cases, there is no need to formalize the production scope document and the product team is responsible for ratification.

Control objective:	
B) Restricting access for migrating changes Ensure that a reasonable number of people have access rights to migrate changes to the production area of the application systems.	
CM.B01	Developers should carry out a Commit and send the code to the version server. This in turn will send a message to the Automatic Deploy system – Build Works, which awaits approval from the owner to execute the Pipeline that makes the Build and the unit tests. If the unit tests are successful, the Deploy is made in the system (online application); if any failure is located in the unit tests, a notification is sent to the Developers, who will repeat the process until it is successful. Access permissions for approval in the Build Works tool should be restricted to authorized personnel.

Incident and Problem Management.

Control objective:	
A) Recording, analyzing and solving incidents and problems Provide reasonable assurance that abnormal events (incidents and problems) are recorded, analyzed and resolved.	
IPM.A01	The Company has a document called "Information Security Incidents Management Policy", which sets out the guidelines and controls related to information security incidents management. The events / incidents can be identified by any company employee and should be recorded in the ITSM tool as "Discovery Record". This record shall be forwarded for analysis by the Information Security team which shall analyze the incident and identify the solution for it.
IPM.A02	Incidents recorded in the ITSM tool should be analyzed by the information security team and classified according to the "Risk Score" defined in the policy.
IPM.A03	The SLA for handling and solving incidents recorded in the ITSM tool is defined in accordance with the Information Security Incidents Management Policy, as managed by the ITSM tool so that the event is duly resolved.

IT Operations.

Control objective:
A) Monitoring servers, systems and infrastructure Provide reasonable assurance that the servers, systems and infrastructure are monitored and controlled in order to detect failures or unavailability.

OP.A01	All the Company's systems and applications associated with the Ben Portal are available through the cloud of the company Digital Ocean, which is responsible for monitoring and sustaining the system.
OP.A02	The systems backup, monitoring and recovery procedures are documented in the "Backup and Recovery Policy", along with information about frequency, content, retention etc. Backups are scheduled according to the information provided in the policy.

Section IV – Control Design Tests

Control Category: Logical Access
A) Information Security Policy
Control Objective: Guarantee that the Information Security Policy has been duly implemented and the company's users are aware of the document's contents.

#	Description of the control stated by the Company	Procedures conducted by Baker Tilly to test the control's design	Result
LA.A01	The Company has a document called "Information Security Incidents Management Policy", which describes the guidelines and controls related to information security and management. This document applies to all the organization's employees. During the onboarding process, employees have to sign the "Nondisclosure Agreement", in which employees state they are aware of the policy's contents.	It consults owners to understand the processes and controls, and inspect policies and procedures, such as the unit test for validating the design.	We did not identify any exceptions.

<table>
<tr><td colspan="4">

Control Category: Logical Access

  B) Access restriction

Control Objective: The controls provide a reasonable assurance that only authorized personnel can access IT resources, in order to reduce the risk of unauthorized access to systems and data.

</td></tr>
</table>

#	Description of the control stated by the Company	Procedures conducted by Baker Tilly to test the control's design	Result
LA.B01	The Company's IT systems are developed in accordance with good IT security practices and have password management parameters in order to mitigate the risk of unauthorized access.	It consults owners to understand the processes and controls, and inspect policies and procedures, such as the unit test for validating the design.	We did not identify any exceptions.
LA.B02	The Company has a document called "Access Management Policy", which describes the control activity for limiting privileged or administrator access to IT resources and systems. Access to the system's configurations is awarded to administrators and is restricted to suitable personnel exercising activities compatible with systems administration. Access is released by controlling accesses awarded.	It consults owners to understand the processes and controls, and inspect policies and procedures, such as the unit test for validating the design.	We did not identify any exceptions.

Control Category: Logical Access
C) Awarding, modifying and revoking user access
Control Objective: The controls provide a reasonable assurance that the awarding, modification and revoking of user accounts are requested and approved by appropriate personnel, in order to mitigate the risk of unauthorized or improper access to systems and data.

#	Description of the control stated the Company	Procedures conducted by Baker Tilly to test the control's design	Result
LA.C01	The Company has a document called "Access Management Policy", which describes the control activity for awarding new access to IT resources and systems. The entire process of requesting access to the company's IT systems and resources should be formalized through the Asken tool and approved by a person with a hierarchal level equal to or higher than supervision of the area which the employee receiving access is allocated or the human resources department. The form completed by the Asken tool should at least contain the following information: Username; User ID; Grounds for awarding access; Access profile or group and Award Date. All users should have an identification key, controlled through a Unique Identification Number (ID) to guarantee traceability, which cannot be repeated. The party requesting access should use the document called "Access Matrix" to consult all profiles available in the systems.	It consults owners to understand the processes and controls, and inspect policies and procedures, such as the unit test for validating the design.	We did not identify any exceptions.

#	Description of the control stated the Company	Procedures conducted by Baker Tilly to test the control's design	Result
LA.C02	The Company has a document called "Access Management Policy", which describes the control activity for revoking access to IT resources and systems. All requisitions to revoke access for a Company employee should be made or approved by a person in a hierarchical level equal to or higher than coordination, be they in the human resources Department or the employee's department. It is also essential the requisition be made formally, in good time and by completing a form, in accordance with the termination of the employment contract. This form should contain at least the following information: Username; User ID; Grounds for revoking access; date revoked. The Human Resources department shall report employees leaving the company to the Projects and Information Technology Development departments. The employee's termination should be informed at least 24 hours before the end of their employment contract, when applicable, so that access can be revoked on the same day of their departure.	It consults owners to understand the processes and controls, and inspect policies and procedures, such as the unit test for validating the design.	We did not identify any exceptions.

Control Category: Logical Access
D) Reviewing access
Control Objective: Provide a reasonable assurance there is segregation of duties for IT resources systems and users in order to mitigate the risk of unauthorized or improper access to systems and data.

#	Description of the control stated by the Company	Procedures conducted by Baker Tilly to test the control's design	Result
LA.D01	The Company has a document called "Access Management Policy", which describes the control activity for the periodic reviewing of access rights to IT resources and systems. The Information Technology and Development and Projects departments annually review the access rights of all the Company's internal users that are active, checking with each department's managers whether the access rights should be maintained, discontinued or modified. The response or validation of managers for each review should be formally registered in order to document the entire process.	It consults owners to understand the processes and controls, and inspect policies and procedures, such as the unit test for validating the design.	We did not identify any exceptions.

Control Category: Change management

A) **Authorizing, testing, validating and approving changes**

Control Objective: Provide a reasonable assurance that modifications to application systems have been duly authorized, tested and approved before being implemented in the production systems.

#	Description of the control stated the Company	Procedures conducted by Baker Tilly to test the control's design	Result
CM.A01	The Company has a document called "Changes Management Policy", which describes the control activities for making changes to systems. All requisitions to develop / change systems should be made by the business departments or the Company's products department. After requisition from the requesting department, the products area is tasked with analyzing demand and whether development is needed. After alignment between the products department and development department, a time frame is established to conclude the new demand, which should be informed to the requester, whose approval should be obtained through the document setting out the production scope. After approving the documentation, the scope is included in the next Sprint Planning ceremony, and therefore placed on the development track.	It consults owners to understand the processes and controls, and inspect policies and procedures, such as the unit test for validating the design.	We did not identify any exceptions.

#	Description of the control stated the Company	Procedures conducted by Baker Tilly to test the control's design	Result
CM.A02	Ratification should occur in a ratification environment separate from production and duly registered/documented in a form setting out evidence of the tests conducted. Once ratification has been completed with the products team, it will send it for validation by the requester, who may request adjustments, which will be inserted in the next Sprint Planning ceremonial, or can be sent for production, if the requester agrees with the development made. After approving the documentation, the scope is included in the next Sprint Planning ceremony, and therefore placed on the development track.	It consults owners to understand the processes and controls, and inspect policies and procedures, such as the unit test for validating the design.	We did not identify any exceptions.
CM.A03	Any changes to be made to the production system shall be accompanied by formal documentation approved or prepared by the head of the Company's products team.	It consults owners to understand the processes and controls, and inspect policies and procedures, such as the unit test for validating the design.	We did not identify any exceptions.
CM.A04	Changes classified as urgent stem from incidents or problems resulting in product or service unavailability, impacting customers. In these cases, there is no need to formalize the production scope document and the product team is responsible for ratification.	It consults owners to understand the processes and controls, and inspect policies and procedures, such as the unit test for validating the design.	We did not identify any exceptions.

Control Category: Change management

B) Restricting access for migrating changes

Control Objective: Ensure that a reasonable number of people have access rights to migrate changes to the production area of the application systems.

#	Description of the control stated by the Company	Procedures conducted by Baker Tilly to test the control's design	Result
CM.B01	Developers should carry out a Commit and send the code to the version server. This in turn will send a message to the Automatic Deploy system – Build Works, which awaits approval from the owner to execute the Pipeline that makes the Build and the unit tests. If the unit tests are successful, the Deploy is made in the system (online application); if any failure is located in the unit tests, a notification is sent to the Developers, who will repeat the process until it is successful. Access permissions for approval in the Build Works tool should be restricted to authorized personnel.	It consults owners to understand the processes and controls, and inspect policies and procedures, such as the unit test for validating the design.	We did not identify any exceptions.

Control Category: Incident and problem management

   A) Recording, analyzing and solving incidents and issues

Control Objective: Ensure that a reasonable number of people have access rights to migrate changes to the production area of the application systems.

#	Description of the control stated by the Company	Procedures conducted by Baker Tilly to test the control's design	Result
IPO.A01	The Company has a document called "Information Security Incidents Management Policy", which sets out the guidelines and controls related to information security incidents management. The events / incidents can be identified by any company employee and should be recorded in the ITSM tool as "Discovery Record". This record shall be forwarded for analysis by the Information Security team which shall analyze the incident and identify the solution for it.	It consults owners to understand the processes and controls, and inspect policies and procedures, such as the unit test for validating the design.	We did not identify any exceptions.
IPO.A02	Incidents recorded in the ITSM tool should be analyzed by the information security team and classified according to the "Risk Score" defined in the policy.	It consults owners to understand the processes and controls, and inspect policies and procedures, such as the unit test for validating the design.	We did not identify any exceptions.
IPO.A03	The SLA for handling and solving incidents recorded in the ITSM tool is defined in accordance with the Information Security Incidents Management Policy, as managed by the ITSM tool so that the event is duly resolved.	It consults owners to understand the processes and controls, and inspect policies and procedures, such as the unit test for validating the design.	We did not identify any exceptions.

Control Category: IT Operations

   A) **Monitoring servers, systems and infrastructure**

Control Objective: Provide reasonable assurance that the servers, systems and infrastructure are monitored and controlled in order to detect failures or unavailability.

#	Description of the control stated by the Company	Procedures conducted by Baker Tilly to test the control's design	Result
OP.A01	All the Company's systems and applications associated with the Ben Portal are available through the cloud of the company Digital Ocean, which is responsible for monitoring and sustaining the system.	It consults owners to understand the processes and controls and inspect the SOC 2 Report of the company Digital Ocean, to validate the controls.	We did not identify any exceptions.
OP.A02	The systems backup, monitoring and recovery procedures are documented in the "Backup and Recovery Policy", along with information about frequency, content, retention etc. Backups are scheduled according to the information provided in the policy.	It consults owners to understand the processes and controls and inspect the SOC 2 Report of the company Digital Ocean, to validate the controls.	We did not identify any exceptions.