

# ISAE 3000A/SOC Type III Auditors' Report

BetterBe BLS-system October 2023 – December 2023

Relevant to Security, Availability, Processing Integrity  
and Confidentiality





## Table of contents

<b>1/ BetterBe B.V.'s Management Statement .....</b>	<b>4</b>
<b>2/ Assurance Report of the Independent Service Auditor .....</b>	<b>6</b>
2.1 Opinion .....	6
2.2 Level of assurance .....	6
2.3 Restrictions on use and distribution .....	7
2.4 Responsibilities of management of service organization.....	8
2.5 Service auditor's responsibilities .....	8
<b>3/ Description of BetterBe B.V. LeaseServices system for the period from 1 October 2023 to 31 December 2023 .....</b>	<b>9</b>
3.1 BetterBe B.V. commitments.....	9
3.1.1 Service commitments.....	9
3.1.2 Description of the services provided .....	9
3.1.3 Services that are out of scope .....	10
3.1.4 Department services.....	10
3.2 System overview .....	10
3.2.1 System Boundaries.....	10
3.2.2 Infrastructure and software.....	10
3.2.3 People.....	11
3.2.4 Procedures.....	11
3.2.4.1 Identity and Access management .....	11
3.2.4.2 Access requests and revocation of access .....	11
3.2.4.3 Change Management.....	11
3.2.4.4 Data backup and disaster recovery .....	11
3.2.4.5 Incident response.....	12
3.2.4.6 System monitoring.....	12
3.2.4.7 Security .....	12
3.2.4.8 Third parties performing incidental activities.....	12
3.2.5 Data .....	12
3.2.6 Sub-service organisations.....	14
3.2.7 Additional checks of the sub-service organization.....	14
3.3 Relevant aspects of internal controls.....	14
3.3.1 Control environment .....	14
3.3.1.1 Integrity and ethical values .....	14



3.3.1.2 Participation of senior management ..... 15

3.3.1.3 Organisational structure and allocation of powers and responsibilities..... 15

3.3.1.4 Commitment to competence ..... 16

3.3.1.5 Responsibility ..... 16

3.3.2 Risk assessment process ..... 17

3.3.2.1 Identification of risks..... 17

3.3.2.2 Risk factors..... 17

3.3.2.3 Risk analysis ..... 18

3.4 Control activities..... 18

3.4.1 Integration with Risk Management ..... 18

3.4.2 Selection and development of Control Activities ..... 18

3.4.3 Trust Services criteria that are in scope on the system in question ..... 19

3.4.4 Information and communication ..... 19

3.4.5 Monitoring and controls ..... 19

3.5 Relevant changes to the system..... 19

3.6 Considerations with regards to verification by the User Organization .....20

3.7 Applicable criteria and controls for trust services designed to achieve BetterBe B.V.'s service commitments and system requirements.....21



## 1/ BetterBe B.V.'s Management Statement

We have prepared the attached description titled "BetterBe B.V.'s BetterBe LeaseServices (BLS) System for the period 1st of October 2023 to 31 December 2023 (the description), based on the criteria in items (a)(i)–(ii) below (the description criteria).

The description is intended to provide users with information about the BLS System, particularly system controls intended to meet the criteria for the security, availability, processing integrity, confidentiality principles set forth in TSP section 100, Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy issued by the Assurance Services Executive Committee of the AICPA (applicable trust services criteria).

We confirm, to the best of our knowledge and belief, that:

The description fairly presents the BLS System throughout the period 1st of October 2023 to 31 December 2023 (the "specified period"), based on the following description criteria:


- 1) The description contains the following information:
  - a. The types of services provided.
  - b. The components of the system used to provide the services, which are the following:
    - i. Infrastructure. The physical and hardware components of a system (facilities, equipment, and networks).
    - ii. Software. The programs and operating software of a system (systems, applications, and utilities).
    - iii. People. The personnel involved in the operation and use of a system (developers, operators, users, and managers).
    - iv. Procedures. The automated and manual procedures involved in the operation of a system.
    - v. Data. The information used and supported by a system (transaction streams, files, databases, and tables).
  - c. The boundaries or aspects of the system covered by the description.
  - d. If information is provided to, or received from, subservice organizations or other parties
    - i. how such information is provided or received; the role of the subservice organization and other parties.
    - ii. the procedures performed to determine that such information and its processing, maintenance, and storage are subject to appropriate controls.
  - e. The applicable trust services criteria and related controls designed to meet those criteria, including, as applicable, the following
    - i. Complementary user entity controls contemplated in the design of the service organization's system.
    - ii. When the inclusive method is used to present a subservice organization, controls at the subservice organization
  - f. If the service organization present the subservice organizations using the carve-out method
    - i. the nature of the services provided by the subservice organization;
    - ii. each of the applicable trust services criteria that are intended to be met by controls at the subservice organization, alone or in combination with controls at the service organization, and the types of controls expected to be implemented at carved-out subservice organizations to meet those criteria.
  - g. Any applicable trust services criteria that are not addressed by a control and the reasons therefore.



ISAE 3000A/SOC Type III Auditors' Report - BETT\_SOCTYPE3\_V1\_2023


- h. In the case of a type 2 report, relevant details of changes to the service organization's system during the period covered by the description.
  - 2) The description does not omit or distort information relevant to the service organization's system while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs.
    - a. the controls stated in the description were suitably designed throughout the period 1st of October 2023 to 31 December 2023 to meet the applicable trust services criteria
    - b. the controls stated in the description operated effectively throughout the period 1st of October 2023 to 31 December 2023 to meet the applicable trust services criteria

Signed for approval

DocuSigned by:  
  
6E73FEF06FBC449 (signature)  
23-1-2024

G.J. Meester (CEO BetterBe B.V.)

Signed for approval

DocuSigned by:  
  
8800543791974A7... (signature)  
23-1-2024

C.A.F.M. Lemaire (CFO BetterBe B.V.)



## 2/ Assurance Report of the Independent Service Auditor

To the Board of Directors of BetterBe B.V.

### 2.1 Opinion

Our opinion has been formed on the basis of the matters outlined in this report. In our opinion, in all material respects, based on the criteria identified in BetterBe's statement and the applicable trust services criteria

- a. The description fairly presents the BetterBe LeaseServices system (BLS) that was designed and implemented throughout the period of October 1, 2023 to December 31, 2023.
- b. The controls stated in the description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated effectively throughout the period of October 1, 2023 to December 31, 2023, and user entities applied the complementary user-entity controls contemplated in the design of BetterBe's controls throughout the period of October 1, 2023 to December 31, 2023.
- c. The controls tested, which together with the complementary user-entity controls referred to in the scope paragraph of this report, if operating effectively, were those necessary to provide reasonable assurance that the applicable trust services criteria were met, operated effectively throughout the period of October 1, 2023 to December 31, 2023.

The specific controls we tested and the nature, timing, and results of our tests are presented in the section of the report titled "Criteria, Controls, Test Procedures, and Results."

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

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

### 2.2 Level of assurance

We have been engaged to obtain reasonable assurance and report on the attached description titled "BetterBe B.V.'s {name or title of system} System for the period of October 1, 2023 to December 31, 2023" (the description) and the suitability of the design and operating effectiveness of controls to meet the criteria for the security, availability, processing integrity, confidentiality principles set forth in TSP section 100, Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity and Confidentiality issued by the American Institute of Certified Public Accountants and the Chartered Professional Accountants of Canada (applicable trust services criteria), throughout the period of October 1, 2023 to December 31, 2023.

The description indicates that certain applicable trust services criteria specified in the description can be achieved only if complementary user-entity controls contemplated in the design of BetterBe B.V.'s ("BetterBe") controls are



suitably designed and operating effectively , along with related controls at the service organization . We have not evaluated the suitability of the design or operating effectiveness of such complementary user-entity controls.

BetterBe uses a service organizations. The description indicates that certain applicable trust services criteria can only be met if controls at the subservice organizations are suitably designed and operating effectively. The description presents betterbe's system; its controls relevant to the applicable trust services criteria; and the types of controls that the service organization expects to be implemented, suitably designed, and operating effectively at the subservice organization to meet certain applicable trust services criteria. For its description BetterBe uses the carve-out method. The description of the system therefore does not include any of the controls implemented at the subservice organizations. Our engagement did not extend to the controls provided by the subservice organizations.

The information attached to the description titled "Other Information Provided by BetterBe That Is Not Covered by the Service Auditor's Report" describes the service organization's BetterBe LeaseServices system. It is presented by the management of BetterBe to provide additional information and is not a part of the service organization's description of its BetterBe's LeaseServices system made available to user entities during the period from October 1, 2023 to December 31, 2023. Information about BetterBe's LeaseServices system has not been subjected to the procedures applied on the "Other Information Provided by BetterBe That Is Not Covered by the Service Auditor's Report" and the suitability of the design and operating effectiveness of controls to meet the related criteria stated in the "Other Information Provided by BetterBe That Is Not Covered by the Service Auditor's Report" and accordingly, we express no opinion on it.

The applicable criteria are identified in BetterBe's statement in combination with the applicable trust services criteria.

BetterBe'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 and inherent limitations, controls at a service organization may not always operate effectively to meet the applicable trust services criteria. Also, the projection to the future of any evaluation of the fairness of the presentation of the description or conclusions about the suitability of the design or operating effectiveness of the controls to meet the applicable trust services criteria is subject to the risks that the system may change or that controls at a service organization may become inadequate or fail.

## 2.3 Restrictions on use and distribution

This report and the description of tests of controls and results thereof are intended solely for the information and use of BetterBe; user entities of BetterBe's LeaseServices during some or all of the period of October 1, 2023 to December 31, 2023; and independent auditors and practitioners providing services to such user entities who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, subservice organizations, or other parties
- Internal control and its limitations
- User entity responsibilities and how they interact with related controls at the service organization
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

This report is not intended to be, and should not be, used by anyone other than these specified parties.



Our assurance report, including the Description of Criteria, Controls, Tests and Results of tests, should only be used for the intended purpose by the intended users. Without our prior written consent, it is not allowed to publish or distribute this document to others, in whole or in part, or to quote from or refer to our assurance-report for the Description of Tests and Results, whether or not with acknowledgement.

## 2.4 Responsibilities of management of service organization

BetterBe has provided the attached statement titled "Management Statement " which is based on the criteria identified in management's statement. BetterBe is responsible for

- (1) preparing the description and statement;
- (2) the completeness, accuracy, and method of presentation of both the description and statement;
- (3) providing the services covered by the description;
- (4) specifying the controls that meet the applicable trust services criteria and stating them in the description; and
- (5) designing, implementing, and documenting the controls to meet the applicable trust services criteria.

## 2.5 Service auditor's responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description based on the description criteria set forth in BetterBe's Management Statement and on the suitability of the design and operating effectiveness of the controls to meet the applicable trust services criteria, based on our procedures to obtain reasonable assurance. We conducted our assurance engagement in accordance with Dutch Law and the International Standard on Assurance Engagements Standard 3000, 'Assurance Engagements other than Audits or Reviews of Historical Financial Information' established by The International Auditing and Assurance Standards Board (IAASB). Those standards require that we plan and perform our engagement to obtain reasonable assurance to express our opinion.

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

Our assurance engagement involved performing procedures to obtain evidence about the fairness of the presentation of the description based on the description criteria and the suitability of the design and operating effectiveness of those controls to meet the applicable trust services criteria. Our procedures depend on the service auditor's judgment and included assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to meet the applicable trust services criteria. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the applicable trust services criteria were met. Our procedures also included evaluating the overall presentation of the description. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

NewDay IT Risk & Assurance Services B.V.

drs A.E. Klaassen RE CIPP/E CIPM  
Managing Partner

DocuSigned by:  
  
F8CC2264E82A4BA...  
23-1-2024





## 3/ Description of BetterBe B.V. LeaseServices system for the period from 1 October 2023 to 31 December 2023

### 3.1 BetterBe B.V. commitments

#### 3.1.1 Service commitments

BetterBe B.V. (BetterBe) transforms the global mobility market. In this market, car ownership shifts to car usership (subscriptions). In addition, the end-user of mobility will take its own mobility related decisions and choices.

BetterBe develops and delivers an IT-platform to accelerate this industry transformation, primarily driven by digital technology. Its Software as a Service (SaaS) platform: the BetterBe LeaseServices (BLS) is a platform specifically engineered to perform the core of tomorrows leasing business. BetterBe works for its corporate international automotive leasing customers.

BetterBe is committed, in order to achieve its objectives, to:

- Undertake to comply with applicable regulations and laws;
- Commit to provide services that are secure according to best practices;
- Commit to guarantee business continuity
- Strive to deliver the service levels as described in the BLS SLA and the related contracts to our utmost best ability.

#### 3.1.2 Description of the services provided

BetterBe manages the BLS with various methods of control, selected to the nature and part of the system.

The BLS enables the customer to:

- Search through vehicles (makes models and types), options, and packages;
- Configure these vehicles using the applicable plausibility ruling;
- Create products and services and create and maintain the underlying price calculations;
- Manage the required data.

As a professional service organization, BetterBe has additional services available, known as "Professional Services."

The provided services are:

- Implementation assistance;
- Consulting Services and knowledge transfer;
- Customer Support.

BetterBe knows that implementing the BLS can be a challenging and complex task. Therefore, BetterBe has product specialists to assist its Customers in implementing and integrating the BLS in their own IT environments in order to execute their roadmaps.

After an initial BLS customer implementation, BetterBe can provide additional business improvement services. These are to ensure that the BLS remains aligned with the Customer's new developments, optimizations or changes.

Finally, questions, incidents, configuration changes or enhancements to the BLS, are handled by BetterBe's Support department.



3.1.3 Services that are out of scope

Customer Data is used to configure the Vehicles, prices, quotations, etc. BetterBe does not provide any data services. As such the data in- and output of the BLS is out of scope for the purposes of this report.

3.1.4 Department services

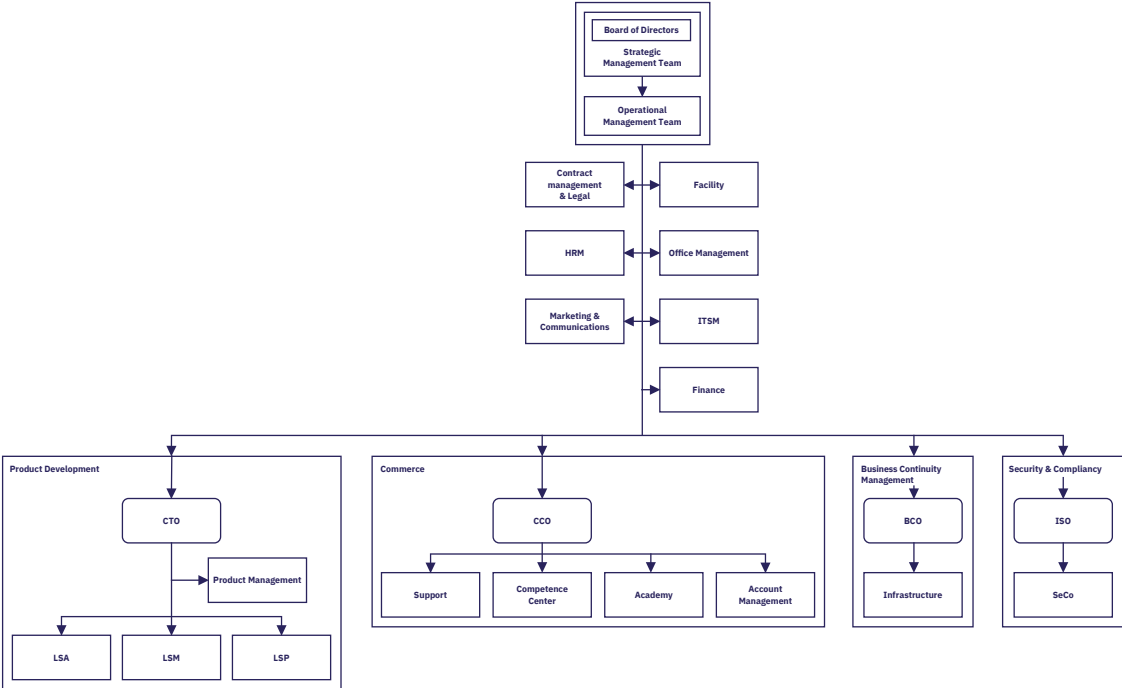


Figure 1: Organizational Chart

3.2 System overview

3.2.1 System Boundaries

As set in TSP Section 100 - 2017, Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality and Privacy, a system is designed, implemented and operated to achieve specific business objectives (e.g. provision of services, production of goods) in accordance with requirements specified by management.

3.2.2 Infrastructure and software

For the delivery of the BLS, BetterBe uses the services provided by CoolTechnologies B.V. (CoolTechnologies) to ensure that a stable infrastructure platform can be used by the Product Development department. As the Service is hosted in the Netherlands, BetterBe ensures that the Service complies with European rules and regulations with regards to Privacy.

The BLS is created and maintained by the Product Development department,. It uses proprietary technologies to ensure a short development cycle and high adaptability to a changes, while keeping consistency in responses, historical accuracy and ability to handle high Service workloads.

To be able to meet BetterBe’s high quality and security standards, BetterBe uses only proven and reliable Sub Service Providers.



For the purpose of this report, two additional software suites are used to provide the services BetterBe relies on to deliver the BLS: the Atlassian software suite and the AFAS suite.

BetterBe uses the Atlassian software suite for software development, testing, documentation, and Customer support. BetterBe uses software from AFAS for the purposes of HRM, CRM and billing.

### 3.2.3 People

The following functional areas/groups are used to support the colocation, and managed services described in this report:

- Product Development
- Commerce
- Business Continuity Management
- IT Service Management

### 3.2.4 Procedures

#### 3.2.4.1 Identity and Access management

Within BetterBe we use a two-tier system for Identity and Access management. The first is who has access, the second is to what does the person require access.

For example, what can be accessed in the BLS Management Application is designed and created by Product Development. Who can access the BLS Management Application is managed by either HRM or Customer Support depending on who requests access. This ensures that multiple steps need to fail before unprivileged access can be obtained.

As principal is applied to both physical and digital access. To verify that access is available to only those required to have it, regular monitoring (both automated and manual) processes are in place.

#### 3.2.4.2 Access requests and revocation of access

As mentioned above, requests are handled by HRM or Customer Support.

HRM ensures that BetterBe personnel have the access required to do fulfill their function. When someone changes function, a request is created to the ITSM department to ensure that the rights are modified to fit their new function.

Access for Customers to the BLS can be managed by the Customer. Should assistance be required, the Customer Support team is available to assist in the management of access to the BLS for that Customer's environments. For the benefit of, and monitoring by, the Customer, an Audit log is available to monitor the work done by BetterBe and the Customer in the Customer environment.

#### 3.2.4.3 Change Management

BetterBe has an extensive Change Management Policy to ensure all Changes meet BetterBe's high standard of quality and security

This Policy is automated where possible to reduce human risks.

This policy sets the standardized workflow of plan, approve, executing and testing of a Change, as well as setting requirements and restrictions for Change requests.

#### 3.2.4.4 Data backup and disaster recovery

Backups concern databases and storage systems. The backup storage is a large (clustered) files server with snapshot technology to create a history.



Backup of databases are created by a special database replica server. It creates file-based backups of database tables and stores these files on the backup fileserver.

The backup of storage systems is arranged by creating a copy on the backup file server and using snapshot technology to maintain a versioned history.

The backup network is an isolated network; it has no gateway to the outside world. It is used to connect the data servers with their backup facilities. These facilities are placed in an additional network layer and DMZ. This separation provides an additional security layer. The backup fileserver is not connected to office networks or other user networks.

BetterBe uses implements its architecture at multiple levels with Disaster Tolerance in mind. Instead of having to fail-over to another set-up, BetterBe uses an architecture in which BetterBe can lose a complete datacentre without consequences.

#### 3.2.4.5 Incident response

BetterBe has a high standard on quality and security, and has a focus on the prevention of Incidents.

Should an incident occur, the Incident Management Policy adopted by BetterBe ensures a consistent, quick and accurate Service recovery.

The Incident Management Policy is used to provide guidelines and define procedures with regards to incidents. In addition, it defines the escalation path from high priority incidents, data leaks, legal and/or regulatory incidents.

BetterBe ensures that all incidents are handled according to their priority, based on (potential) impact and frequency by implementing these policies across all company departments and teams.

#### 3.2.4.6 System monitoring

To ensure the quality of a dynamic internet facing hosting, extensive monitoring and alerting is mandatory within BetterBe. The monitoring covers far more than just 'is the server alive' and 'is the application alive.' In addition to functionality, capacity, validity and availability, BetterBe uses multiple monitoring systems, methods and processes to safeguard the agreed upon SLAs at all times.

Again, monitoring has a focus on preventing incidents and SLA impact.

#### 3.2.4.7 Security

To realize absolute availability, BetterBe must designs all components for absolute availability. From software to infrastructure to networking, including software and infrastructure maintenance. Everything must be designed and implemented according to disaster tolerance, zero downtime maintenance, interrupt-less deploy and sufficient capacity to perform in degraded situations.

#### 3.2.4.8 Third parties performing incidental activities

Third parties must adhere to all applicable BetterBe policies.

### 3.2.5 Data

The BLS Hosting Architecture is the foundation architecture for all High Availability implementations within BetterBe. This includes hosting environments for traditional web-applications and other SaaS environments. All implementations are built on this architecture. Acceptation and development environments follow the same (security) design, be it with lower availability specifications.



BetterBe uses a layered set-up. Each layer is connected on OSI layer 2 (Ethernet) and the networks between these layers are isolated from all other networks. Only the servers that are directly attached to these networks can communicate over them. Routes (OSI layer 3) between these networks and other networks do not exist.

The database located in the deepest layer (DMZ-3). The data backups are stored in an environment that is not available in the user networks. The backup environment is divided into separate zones for the different realms and applications. Only servers with backup requirements have access to their unique zone of the backup environment.

At the proxy layer, access to the BLS API is controlled with IP address-based restrictions per dataset. The BLS management application is controlled by username / password authentication combined with one or more of the following:

- Access to the management module can be restricted to a list of IP addresses that is provided by the customer.
- Client-side certificates can be used to authenticate connections as an additional security measure.

In addition to the above, BetterBe also offers a Single Sign On solution through SAML.

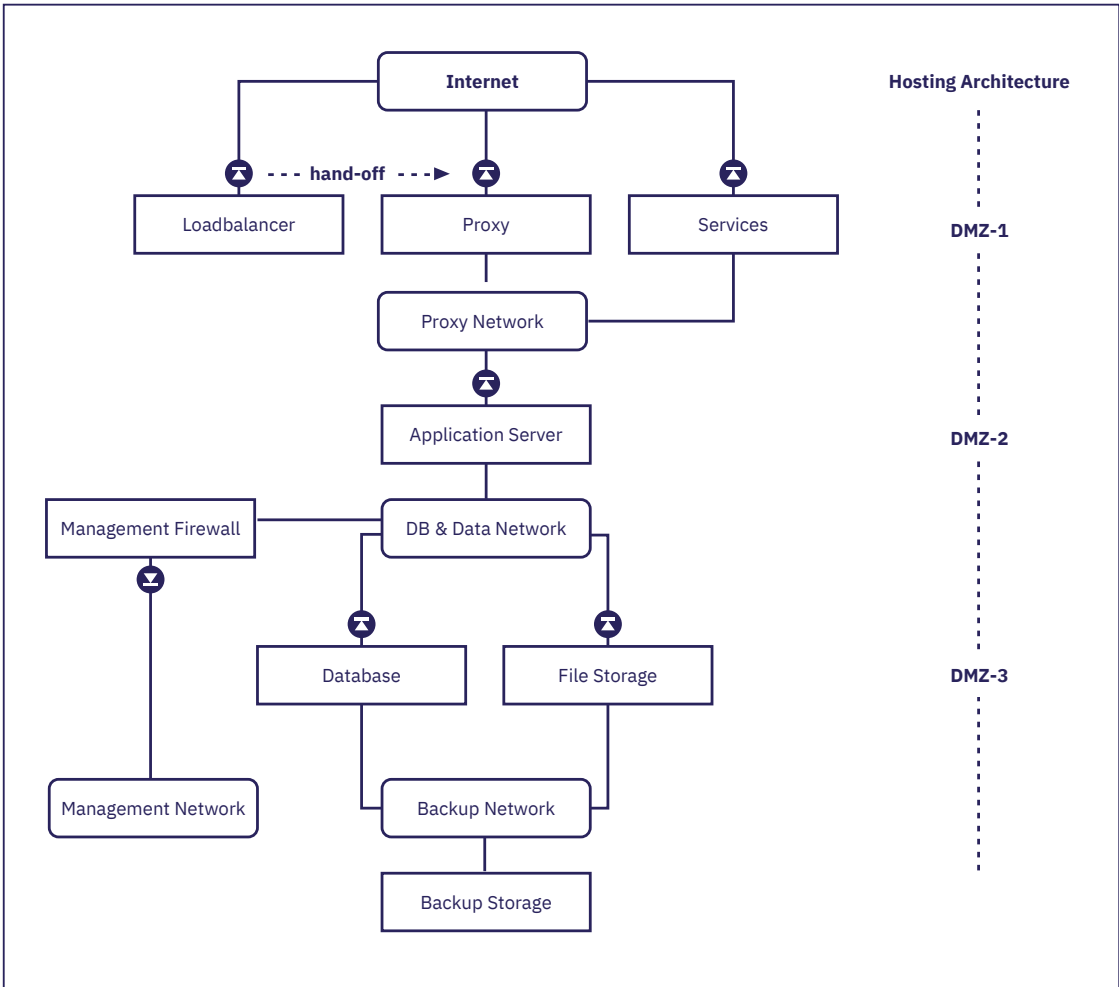


Figure 2: A layered set-up



The cluster technologies that are used in the hosting architecture allow individual servers to fail without consequence. The distribution of the servers over different geographic locations is at a level that a complete datacentre can be lost without disrupting the services and applications. Since all servers and components always participate in the delivery of the services, the concept (or architecture) only has to be tested once. Once it has proven to work, it will always work since there are no 'stand-by servers' that need to be tested from time to time. There is also no data replication needed for fail-over purposes, since there is only data replication for real time service delivery. It is constantly monitored for the correct working and needs no separate testing.

The distances between the datacentres must be large enough to avoid that one event (e.g. a fire) takes down multiple datacentres. The distances must be small enough to keep the latency low. To meet these requirements BetterBe currently uses two commercial datacentres in Hengelo and one commercial datacentre in Enschede.

### 3.2.6 Sub-service organisations

BetterBe applies the carve-out method regarding its sub-service organizations.

BetterBe manages sub-service organizations based on best practices in line with ISO 27002.

BetterBe B.V. uses Cool Technologies BV, a subservice organization, to provide Data center connectivity; AFAS Software B.V., a subservice organization, to provide CRM and Billing Services; Atlassian Pty Ltd, a subservice organization, to provide Customer Support interface, Knowledge Base and workload planning services; Microsoft, a subservice organization, to provide office software and e-mail services.

### 3.2.7 Additional checks of the sub-service organization

For all Software providers, BetterBe demands that they have at least the ISO-27001 certification.

## 3.3 Relevant aspects of internal controls

### 3.3.1 Control environment

The control environment at BetterBe forms the basis for the areas of internal control. It guides the organization and influences the control awareness of employees. Components of the control environment include integrity and ethical values, management's commitment to competence, organizational structure, the allocation of powers and responsibilities, and supervision and direction by senior management.

#### 3.3.1.1 Integrity and ethical values

At BetterBe, we recognize that ethical behavior is the cornerstone of a healthy workplace culture. In order to clarify what Management deems ethical behavior, they have created a Code of Conduct (the Code) for all employees to follow.

The foundation of this Code are the core-values of BetterBe:

"BetterBe You", "Be Better and Dream Big", "Better Together", "Champion Customers" and "Quality first".

BetterBe ensures that all it's employees know the Code through a central mandatory training and in the yearly assessment review it is measured if the employee has deviated from the Code.

BetterBe empowers it's employees to raise concerns with regards to integrity or unethical behavior as outlined in the Code.



### 3.3.1.2 Participation of senior management

BetterBe's management has an active role in the workings of BetterBe. In addition to active leadership, the Management also supports BetterBe's operations more directly.

With this direct role, they gain greater insight in the workings of BetterBe and its employees. Ensuring that incidents, security concerns, development questions and Customer feedback has direct input into the management structure. In turn, Management can disrupt unwanted development before it has negative impact on BetterBe.

### 3.3.1.3 Organisational structure and allocation of powers and responsibilities

BetterBe uses a small and direct management organization. As can be seen in the Company chart, BetterBe has a management team consisting of the Strategic Management Team (SMT) and the Operational Management Team (OMT).

The BetterBe mission, vision, company values, strategy, strategic goals and its strategic control objectives are set by the Strategic Management Team.

The Operational Management Team defines and implements the organizational control framework to achieve those strategic goals in accordance with the strategic control objectives. This control framework must ensure the operational effectiveness of all strategic and operational policies, procedures, guidelines and standards that are in place to meet the strategic goals.

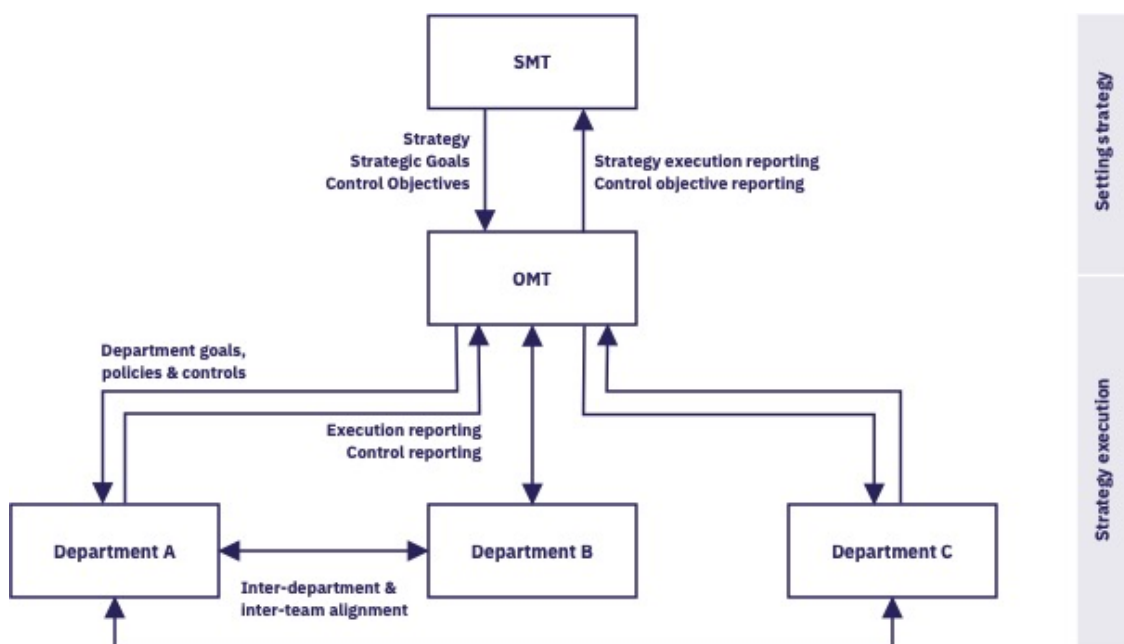


Figure 3: Management structure

#### Setting the strategy

The strategic goals and control objectives are discussed, aligned and evaluated in the bi-weekly OMT-SMT Meeting. In this meeting the relevant strategy execution progress is reported, as well as reporting related to the set control objectives.

**ISAE 3000A/SOC Type III Auditors' Report - BETT\_SOCTYPE3\_V1\_2023****Strategy execution**

The OMT sets the company wide policies consistently and effectively implement the strategic control objectives across all departments.

Company wide quarterly updates are held by the OMT to align all employees on the company goals, policies and controls.

The OMT sets the departments scope, goals, tasks and responsibilities, and is updated on the department execution status.

Departments align their goals, challenges and dependencies using Inter-department & inter-team alignment meetings, to ensure the overall operational success.

The OMT evaluates and discusses the strategy execution status, and changes and improves internal controls where required during the weekly OMT Meeting.

**3.3.1.4 Commitment to competence**

Our five company values serve as a guide for how we conduct our daily business:

**BetterBe You**

We value each person as their authentic self and welcome an honest and respectful dialogue as an avenue to greatness. Together we thrive in a culture of inclusion, equality, and a sense of belonging.

**Be Better and Dream Big**

Don't settle for the status quo. Always pursue the development of the best version of yourself. Investment in the growth and resilience of our people is the foundation for building an iconic company.

**Better Together**

We create success together and learn from failure as one team. We foster a collaboration-first workplace which values individual contributions through transparency, integrity, and accountability.

**Champion Customers**

While we are proud about our achievements, we should remain humble not become complacent. We succeed when our customers succeed: the foundation for sustainable long-lasting partnerships. We empower our customers by solving their most complex business challenges.

**Quality First**

We believe that our passion for quality drives success. It leads to a sustainable foundation to take on the toughest challenges as we empower the transformation of the world of global mobility.

As such, competence is not just a core principle for BetterBe ("Be Better and Dream Big") but it's also part of all other values.

**3.3.1.5 Responsibility**

BetterBe has delegated responsibilities to a departmental level.

For instance, the "Product Development" department develops the BLS and has split this department into three teams, each working on a separate part of the BLS.

These teams report to the head of the department, who reports to the OMT, who reports to the SMT. This ensures that there is a clear line of reporting and an established system of responsibilities.





By placing responsibilities as low in the organization as possible, BetterBe ensures that experts can use their expertise to resolve issues with regards to their work, without requiring extensive meetings. This ensures work can be done efficient and to the highest standards.

### 3.3.2 Risk assessment process

#### 3.3.2.1 Identification of risks

Risks come in all shapes and forms. The following risk types are used within BetterBe:

##### Technical

Availability, performance, creating changes that interrupt the application, IT security and information security, etc.

##### Human

Team cohesion and staffing

##### Process

Deviations of relevant processes

##### External

All risks that come from external sources, like legislation and regulation (e.g.: GDPR, WLTP, health and safety laws), performance of suppliers (e.g.: datacentres, interconnects, and power suppliers).

Risks identification is a key part of all employee's job responsibilities. Each identified risk is assigned a Risk Owner.

The Risk Owner is the department head of the department in which the Risk was identified, unless explicitly recorded otherwise. This Risk ownership can be delegated.

Risk assessment is the compilation of risks associated with various potential threat events. A "threat event" is the occurrence of a risk which may cause a loss of confidentiality, integrity, availability, or privacy of a system and/or information.

#### 3.3.2.2 Risk factors

Although there may be hundreds of potential threat events related to the systems, processes, or resources that the company uses, the threat events can be generally organized into three main categories:

##### Loss of Confidentiality

- Systems or information are compromised by external hackers
- Systems or information are released without approval

##### Loss of Integrity

- Systems or information can no longer be trusted
- Systems or information are not complete or incorrect

##### Loss of Availability

- Systems or information no longer exists (e.g.: hard drive failure, system destroyed)
- Systems or information no longer responds to valid queries from the user or users (system fault)
- Systems or information cannot be retrieved by an authorized user (e.g.: Denial of Service Attack)



A special type of Confidentiality loss is identified separately within BetterBe:

#### **Loss of Privacy**

- Personal information is disclosed without approval

#### **3.3.2.3 Risk analysis**

BetterBe has a Risk Management Policy that describes all steps how to analyze, classify, register, and resolve Risks. This policy is implemented in all Departments.

In addition to policies, BetterBe has automated procedures in place that verify for every bit of code that is created for the BLS, if new Risks have been identified from external sources that can impact the BLS.

For non-BLS related Risks, the CVE list of the NCSC is used to monitor general software and all relevant software CVE's are analyzed and improvements implemented where necessary.

### **3.4 Control activities**

#### **3.4.1 Integration with Risk Management**

In addition to assessing the risks, management has identified and implemented the necessary policies, processes and procedures to address those risks. To address the risks, control activities have been put in place to ensure that the actions are carried out correctly and efficiently. Monitoring activities serve as mechanisms for managing the implementation of security and availability principles.

#### **3.4.2 Selection and development of Control Activities**

When developing Control Activities, BetterBe builds upon industry Standards where applicable, and embeds these best practices into its control framework. As such, the SOC and ISO-27001 controls are integrated within its business processes.

Strategic Goals set by SMT are given to the OMT to execute. The OMT then reports the progress, impediments and successes through quarterly meetings held companywide, and in more detail in bi-weekly Control Objective Reports to SMT in a shared meeting.

The Strategic Goals are translated by department heads to department specific goals, who then report progress, impediments and success back to the OMT.

These Department specific goals are then further spread and specified to the teams inside the departments who regularly report back through companywide "Demo's" and in detail to the head of the Department.

In addition to these Controls, BetterBe has developed the following:

The department heads are responsible for resolving departmental goals and reporting their progress to the OMT.

As the heads of departments are themselves experts in the field they head, the OMT relies on their expertise to set internal control measures that are appropriate for the department, in addition to the controls set through companywide Policies and Processes.

These additional controls are allowed to add to, but not infringe upon, existing controls. As such, the standard is set by the OMT, based upon the goals of the SMT, and made more relevant to the work done by specific teams by the department heads.

If a team decides that it is pertinent to add to this, this can be done in the same manner.



During the weekly OMT session, these controls are measured against the current standards and guidance is given when the controls are deemed irrelevant, are too strict or if they do not align with the Company Policies and Processes.

### 3.4.3 Trust Services criteria that are in scope on the system in question

For the purpose of this report, all Common Criteria are in scope. In addition, some additional criteria have been selected for Availability and Confidentiality to give a greater assurance to the Customer for these two highly relevant fields. The criteria regarding Privacy were excluded because these are not mandatory for the EU (the GDPR is).

### 3.4.4 Information and communication

BetterBe has three main ways to distribute information, namely:

- a Knowledge base
- a Ticketing system
- Direct communication

The knowledge base is used to communicate information that is not used actively but used for specific circumstances as reference documentation.

For Customer questions and Service requests BetterBe uses a ticketing system to manage their workflow and progress. This ensures that all information related to the BLS is networked together, thereby creating a complete overview of all relevant information..

In addition to these systems, BetterBe uses direct communication to communicate with Customers and employees through phone, chat, email and face-to-face where deemed necessary.

### 3.4.5 Monitoring and controls

#### Control Activities

As a Software Development company, BetterBe prefers to automate monitoring where possible, and ensure procedures are in place for manual monitoring when not possible.

For instance, hardware is monitored for thousands of different parameters to ensure that when an up- or downward trend is seen, BetterBe can intervene if required. Doing this manually is impossible, so BetterBe uses high end software and hardware components to keep track of these parameters and give a comprehensive overview.

The BLS itself is monitored in a similar way and tested daily against thousands of tests to ensure that the output delivered by the BLS is kept constant unless explicit change is expected. This ensures the historic capabilities of the BLS and doubles as a Control mechanism to ensure no unexpected changes have occurred.

The Control structure setup by BetterBe, as mentioned under 3.3.3, ensure that all activities are monitored by experts, reported to management when required and followed through to the SMT if escalation is required. Any short comings are directly addressed and corrected before major impact occurs. Using bi-weekly evaluations, the teams ensure that they can change course quickly when necessary, and any course corrections and short comings are communicated to the OMT when they are required and by reporting it in bi-weekly evaluations.

## 3.5 Relevant changes to the system

As this is BetterBe's first SOC report, there are no changes to the previous report.



### 3.6 Considerations with regards to verification by the User Organization

The BLS Service is designed on the assumption that certain checks are performed by the Customer, i.e. user organization. The application of specific controls to the user organization is necessary to achieve the control objectives set out in this report.

This section describes additional checks that need to be performed by the user organizations to complement the checks at BetterBe. User reviewers should verify that the following checks have been implemented at the user organization.

Customers need to ensure that they can, and do, adhere to the Customer obligations as stated in their Master Agreement. These include, but are not limited to:

- Customers need to verify that data processed by the BLS is correct, and inform BetterBe about,
- and assist with resolving, issues with this data.
- The Customer needs to ensure that they adhere to their own security standards.
- Customers need to ensure that no personal end user data is stored in the BLS, as the BLS requires personal data processing for its Service delivery.
- Customers need to ensure that BetterBe has access to all information required to provide its Services to the Customer.
- Customers are responsible for setting up, maintaining and monitoring, physical access to all IT systems that connect, or can connect to, the BLS.
- Customers need to ensure that BetterBe has access to all information required to provide its Services to the Customer.
- After BetterBe notifies the Customer of an update and/or maintenance that impacts Uptime and/or degrades the Performance level during maintenance, the Customer needs to take appropriate action with regards to this maintenance.
- The Customer is responsible for account management within the BLS. Should assistance be required, the Customer shall inform BetterBe in a timely manner using the processes defined in the Service Level Agreement.

The list above of audit considerations for the Customer and the list of control objectives does not constitute a complete package of all controls to be applied by the Customer. Other checks may be required by the user organization. BetterBe's performing transactions for customers cover only part of each customer's overall internal control structure. BetterBe's products and services are not designed as the sole control component in the internal control environment. Additional control procedures are needed at the Customer level. Therefore, each Customer's system of internal controls should be assessed in conjunction with the internal control structure described in this report.



### 3.7 Applicable criteria and controls for trust services designed to achieve BetterBe B.V.'s service commitments and system requirements

#### Common criteria; Security

ID	Categories of Common Criteria	Common Criteria TSP reference	Control Activity number
1	CONTROL ENVIRONMENT	CC1.1	1, 2, 3, 4, 5
2		CC1.2	1, 2, 3, 4
3		CC1.3	1, 2, 3, 4, 5
4		CC1.4	1, 2, 3, 4, 5, 6, 7
5		CC1.5	1, 2, 3, 4, 5
6	COMMUNICATION AND INFORMATION	CC2.1	1
7		CC2.2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11
8		CC2.3	1, 2, 3, 4, 6, 10, 11
9	RISK ASSESSMENT	CC3.1	1, 2, 4, 8, 11, 14, 15, 16
10		CC3.2	1, 2, 3, 4, 5, 6, 7, 8
11		CC3.3	1
12		CC3.4	1, 2, 3, 4, 5
13	MONITORING ACTIVITIES	CC4.1	1, 2, 3, 4, 5, 6, 7, 8
14		CC4.2	1, 2, 3
15	CONTROL ACTIVITIES	CC5.1	1, 2, 3, 4, 5, 6
16		CC5.2	2, 3, 4
17		CC5.3	1, 2, 3, 4, 5, 6
18	Logical and Physical Access Controls	CC6.1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10
19		CC6.2	1, 2, 3
20		CC6.3	1, 2, 3
21		CC6.4	1, 4, 5
22		CC6.5	1, 2
23		CC6.6	1, 2, 3, 4
24		CC6.7	1, 2, 3, 4


**ISAE 3000A/SOC Type III Auditors' Report - BETT\_SOCTYPE3\_V1\_2023**

25		CC6.8	1, 2, 3, 4, 5
26	System Operations	CC7.1	1, 2, 3, 4, 5
27		CC7.2	1, 2, 3, 4
28		CC7.3	1, 3, 5
29		CC7.4	1, 2, 3, 4, 5, 6, 8, 9, 10, 11
30		CC7.5	1, 2, 3, 4, 5, 6
31	Change Management	CC8.1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14
32	Risk Mitigation	CC9.1	1,
33		CC9.2	1, 2, 3, 4, 6, 7, 9, 10, 11, 12

**Additional criteria; Availability**

ID	Additional Criteria Availability TSP reference	Control Activity number
34	A1.1	1, 2, 3
35	A1.2	1, 3, 4, 5, 6, 7, 8, 9, 10
36	A1.3	1, 2

**Additional criteria; Confidentiality**

ID	Additional Criteria for Confidentiality TSP Reference	Control Activity number
37	C1.1	1, 2
38	C1.2	1, 2

© 2023 BetterBe B.V. All rights reserved. No part of this document may be reproduced in any form, by print, photo print, microfilm or any other means without written permission from BetterBe B.V.

**Better**  **Be**

Transforming  
automotive leasing  
worldwide

+31 (0) 53 48 00 680  
[info@betterbe.com](mailto:info@betterbe.com)  
[betterbe.com](https://betterbe.com)

Auke Vleerstraat 140 E  
7547 AN Enschede  
CC no. 08097527