

# **Independent Service Auditor's Assurance Report on the Description of Controls, their Design and Operating Effectiveness**

## **ISAE 3402 SOC 1 Type 2**

prepared in accordance with

International Standard on Assurance Engagements (ISAE)

in the period of

**January 1, 2025 to December 31, 2025**

for

**SEEBURGER INFORMATIK EOOD**

G.M. Dimitrov Blvd. 16A

1797 Sofia, Bulgaria

**BFMT AUDIT GMBH**  
WIRTSCHAFTSPRÜFUNGSGESELLSCHAFT  
FLURSTRASSE 9  
94234 VIECHTACH  
DEUTSCHLAND

TELEPHONE: +49 (0)9942 - 94951 - 0  
TELEFAX: +49 (0)9942 - 94951 - 11  
E-MAIL: info@bfmt.net

ORDER NUMBER: CP/78/2025

## Table of Contents

<b>Abbreviations</b> .....	<b>5</b>
<b>Definitions</b> .....	<b>7</b>
<b>Section I – Independent Auditor’s Report</b> .....	<b>9</b>
1. <b>To the Management of SEEBURGER INFORMATIK EOOD</b> .....	<b>9</b>
2. <b>Scope</b> .....	<b>9</b>
3. <b>SEEBURGER INFORMATIK EOOD Service Organization’s Responsibilities</b> .....	<b>10</b>
4. <b>Independence and Quality Management BFMT</b> .....	<b>10</b>
5. <b>Service Auditor’s Responsibilities</b> .....	<b>10</b>
6. <b>Limitations of Controls at a Service Organization</b> .....	<b>11</b>
7. <b>Performance of Audit Procedures</b> .....	<b>11</b>
7.1 <b>Testing Procedure</b> .....	<b>11</b>
7.2 <b>Sample sizes</b> .....	<b>12</b>
7.3 <b>Testing Results</b> .....	<b>15</b>
7.4 <b>Reporting Structure</b> .....	<b>15</b>
8. <b>Opinion</b> .....	<b>16</b>
9. <b>Intended Users and Purpose</b> .....	<b>16</b>
<b>Service Organization’s Statement</b> .....	<b>17</b>
<b>Section II – Description of Controls provided by SEEBURGER INFORMATIK EOOD</b> .....	<b>19</b>
1. <b>The SEEBURGER INFORMATIK EOOD Internal Control System</b> .....	<b>19</b>
2. <b>Control Environment</b> .....	<b>19</b>
2.1 <b>Information Security Committee</b> .....	<b>20</b>
2.2 <b>Sustainability and corporate responsibility at SEEBURGER INFORMATIK EOOD</b> .....	<b>20</b>
2.3 <b>Principles</b> .....	<b>21</b>
2.4 <b>Scope of the ISAE 3402 report</b> .....	<b>23</b>
2.5 <b>Information technology platform</b> .....	<b>25</b>
3. <b>Information and communication measures</b> .....	<b>30</b>
4. <b>Monitoring Activities</b> .....	<b>30</b>
5. <b>Risk Management</b> .....	<b>30</b>
5.1 <b>Risk management process</b> .....	<b>31</b>
5.2 <b>Controls in the ISAE 3402 audit</b> .....	<b>39</b>
6. <b>User &amp; Access Management</b> .....	<b>40</b>
6.1 <b>Concept and implementation</b> .....	<b>40</b>
6.2 <b>Controls in the ISAE 3402 audit</b> .....	<b>41</b>
7. <b>Physical Security</b> .....	<b>45</b>

7.1	High availability .....	46
7.2	Controls in the ISAE 3402 audit.....	47
8.	Go-Live Management.....	48
8.1	Process description .....	48
8.2	Controls of the ISAE 3402 audit .....	50
9.	Monitoring Management .....	51
9.1	Process description .....	51
9.2	Controls in the ISAE 3402 audit.....	52
10.	Incident Management.....	56
10.1	Process description .....	56
10.2	Controls in the ISAE 3402 audit.....	59
11.	System-Based Change Management .....	60
11.1	Process description .....	62
11.2	Controls in the ISAE 3402 audit.....	63
12.	Backup and Recovery Management.....	65
12.1	Controls in the ISAE 3402 audit.....	65
13.	Business Continuity Management .....	66
13.1	Purpose.....	66
13.2	Process Flow .....	66
13.3	Disaster/recovery capacity .....	74
13.4	Controls in the ISAE 3402 audit.....	75
14.	Control Considerations for SEEBURGER INFORMATIK EOOD Customers.....	79
14.1	Purpose, General IT Controls & Data and Information Management .....	79
14.2	General IT controls.....	79
14.3	Data and information management.....	79
14.4	Backup and Recovery Management.....	80
14.5	Incident Management.....	80
14.6	System-Based Change Management .....	80
15.	Complementary Subservice Organization Controls .....	80
16.	Changes to the System Since the Last Report .....	81
17.	System incidents.....	82
18.	Complementary User Entity Controls (CUEC's) .....	82
Section III – Information provided by BFMT .....		83
1.	Risk Management .....	85
2.	User & Access Management.....	89
3.	Physical Security .....	99

<b>4.</b>	<b>Go-Live Management.....</b>	<b>103</b>
<b>5.</b>	<b>Monitoring Management .....</b>	<b>107</b>
<b>6.</b>	<b>Incident Management.....</b>	<b>114</b>
<b>7.</b>	<b>System-Based Change Management .....</b>	<b>117</b>
<b>8.</b>	<b>Backup &amp; Recovery .....</b>	<b>122</b>
<b>9.</b>	<b>Business Continuity Management .....</b>	<b>127</b>

## Abbreviations

AD	Active Directory
B2B	business-to-business
BCP	Business continuity planning
BFMT	BFMT Audit GmbH Wirtschaftsprüfungsgesellschaft, Flurstraße 9, D-94234 Viechtach
BIA	Business Impact Analysis
CAB	change advisory board
CIP	Continuous Improvement Process
COBIT	Control Objectives for Information and Related Technology
CR	Change Request
CSP	Cloud Service Portal
GC	Global Compact
GoBD	Principles for the proper keeping and storage of books, records and documents in electronic form and for data access
GTS	Global Trade Services
ICS	Internal Control System
IDW	Institute of Public Auditors
IDW PS 951 n.F. (03.2021)	Institut der deutschen Wirtschaftsprüfer Prüfungsstandard 951 n.F. (03.2021)
iPaaS	Integration Platform as a Service
ISAE 3402	International Standard on Assurance Engagements 3402
ISMS	Information Security Management System
MDM	master data system
PR	procurement request
PRA	Protection Requirement Analysis
QA	Quality Assurance
QR	query representative
RPN	Risk Priority Number

RTO	recovery time objectives
SLA	service level agreement
SPOC	Single Point of Contact
SSAE 18	Statement on Standards for Attestation Engagements 18
VM	virtual machine

## Definitions

For purposes of this ISAE 3402 SOC 1 Type 2 report, the following terms have the meanings attributed below:

- (a) **Carve-out method** – Method of dealing with the services provided by a subservice organization, whereby the service organization’s description of its system includes the nature of the services provided by a subservice organization, but that subservice organization’s relevant control objectives and related controls are excluded from the service organization’s description of its system and from the scope of the service auditor’s engagement. The service organization’s description of its system and the scope of the service auditor’s engagement include controls at the service organization to monitor the effectiveness of controls at the subservice organization, which may include the service organization’s review of an assurance report on controls at the subservice organization.
- (b) **Complementary user entity controls** – Controls that the service organization assumes, in the design of its service, will be implemented by user entities, and which, if necessary to achieve control objectives stated in the service organization’s description of its system, are identified in that description.
- (c) **Control objective** – The aim or purpose of a particular aspect of controls. Control objectives relate to risks that controls seek to mitigate.
- (d) **Controls at the service organization** – Controls over the achievement of a control objective that is covered by the service auditor’s assurance report.
- (e) **Controls at a subservice organization** – Controls at a subservice organization to provide reasonable assurance about the achievement of a control objective.
- (f) **Criteria** – Benchmarks used to evaluate or measure the underlying subject matter. The “applicable criteria” are the criteria used for the particular engagement.
- (g) **Inclusive method** – Method of dealing with the services provided by a subservice organization, whereby the service organization’s description of its system includes the nature of the services provided by a subservice organization, and that subservice organization’s relevant control objectives and related controls are included in the service organization’s description of its system and in the scope of the service auditor’s engagement.
- (h) **Internal audit function** – A function of an entity that performs assurance and consulting activities designed to evaluate and improve the effectiveness of the entity’s governance, risk management and internal control process.
- (i) **Internal auditors** – Those individuals who perform the activities of the internal audit function. Internal auditors may belong to an internal audit department or equivalent function.
- (j) **Report on the description, design, and operating effectiveness of controls at a service organization** (referred to in this ISAE 3402 SOC 1 as a “Type 2 Report”) – A report that comprises:
  - (i) The service organization’s description of its system;

- (ii) A written statement by the service organization that, in all material respects, and based on suitable criteria:
- The description fairly presents the service organization's system as designed and implemented throughout the specified period;
  - The controls related to the control objectives stated in the service organization's description of its system were suitably designed throughout the specified period; and
  - The controls related to the control objectives stated in the service organization's description of its system operated effectively throughout the specified period; and
- (iii) A service auditor's assurance report that:
- Conveys reasonable assurance conclusion about the matters in (ii) above; and
  - Includes a description of the tests of controls and the results thereof.
- (k) **Service auditor** – A professional accountant in public practice who, at the request of the service organization, provides an assurance report on controls at a service organization.
- (l) **Service organization** – A third-party organization (or segment of a third-party organization) that provides services to user entities that are likely to be relevant to user entities' internal control as it relates to financial reporting.
- (m) **Service organization's statement** – The written statement about the matters referred to in (j)(ii).
- (n) **Service organization's system (or the system)** – The policies and procedures designed and implemented by the service organization to provide user entities with the services covered by the service auditor's assurance report. The service organization's description of its system includes identification of: the services covered; the period to which the description relates; control objectives; and related controls.
- (o) **Service organization's statement** – The written statement about the matters
- (p) **Subservice organization** – A service organization used by another service organization to perform some of the services provided to user entities that are likely to be relevant to user entities' internal control as it relates to financial reporting.
- (q) **Test of controls** – A procedure designed to evaluate the operating effectiveness of controls in achieving the control objectives stated in the service organization's description of its system.
- (r) **User auditor** – An auditor who audits and reports on the financial statements of a user entity.<sup>1</sup>
- (s) **User entity** – An entity that uses a service organization.

---

<sup>1</sup> In the case of a subservice organization, the service auditor of a service organization that uses the services of the subservice organization is also a user auditor.

## Section I – Independent Auditor’s Report

### 1. To the Management of SEEBURGER INFORMATIK EOOD

The International Standard on Assurance Engagements 3402 deals with assurance engagements undertaken by a professional accountant in public practice to provide a report for use by user entities and their auditors on the controls at a service organization that provides a service to user entities, that is likely to be relevant to user entities’ internal control as it relates to financial reporting.

It supplements ISA 402 (Audit Considerations in relation to an Entity that uses a Service Organization) to the effect that reports prepared in accordance with this ISAE may provide appropriate evidence in accordance with ISA 402. ISA 402 addresses the user auditor’s responsibility to obtain sufficient and appropriate audit evidence when a user entity uses the services of one or more service organizations.

### 2. Scope

We have been engaged to report on **SEEBURGER INFORMATIK EOOD** (below mentioned “**SEEBURGER INFORMATIK EOOD**” or **Client**) Service Organization’s description of its EDI/B2B/GTS and iPaaS system for processing customers’ transactions in the period of **January 1, 2025 to December 31, 2025** and on the design and operation of controls related to the control objectives stated in the description.

The description indicates that certain complementary user entity controls must be suitably designed and implemented at user entities for related controls at the service organization to be considered suitably designed to achieve the related control objectives. We have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

**SEEBURGER INFORMATIK EOOD** uses subservice organizations for physical and environmental security processes as described in the service organization’s description of its system. For its description **SEEBURGER INFORMATIK EOOD** uses the carve-out method. The description also indicates that certain control objectives specified by **SEEBURGER INFORMATIK EOOD** can be achieved only if complementary subservice organization controls assumed in the design of Sample Service Organization’s controls are suitably designed and operating effectively, along with the related controls at Sample Service Organization. We have not evaluated the design or operating effectiveness of such complementary subservice organization controls.

### 3. SEEBURGER INFORMATIK EOOD Service Organization's Responsibilities

SEEBURGER INFORMATIK EOOD Service Organization is responsible for: preparing the description and accompanying statement, including the completeness, accuracy, and method of presentation of the description and statement; providing the services covered by the description; stating the control objectives; and designing, implementing and effectively operating controls to achieve the stated control objectives.

### 4. Independence and Quality Management BFMT

We have complied with the independence and other ethical requirements of the International Ethics Standards Board for Accountants' *International Code of Ethics for Professional Accountants (including International Independence Standards)* (IESBA Code), which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behavior.

The firm applies International Standard on Quality Management 1<sup>2</sup>, which requires the firm to design, implement and operate a system of quality management including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

### 5. Service Auditor's Responsibilities

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

An assurance engagement to report on the description, design and operating effectiveness of controls at a service organization involves performing procedures to obtain evidence about the disclosures in the service organization's description of its system, and the design and operating effectiveness of controls. The procedures selected depend on the service auditor's judgment,

---

<sup>2</sup> ISQM 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements*

including the assessment of the risks that the description is not fairly presented, and that controls are not suitably designed or operating effectively. Our procedures included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved. An assurance engagement of this type also includes evaluating the overall presentation of the description, the suitability of the objectives stated therein, and the suitability of the criteria specified by the service organization and described in section II.

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

## 6. Limitations of Controls at a Service Organization

**SEEBURGER INFORMATIK EOOD** Service Organization'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. Also, the projection of any evaluation of effectiveness to future periods is subject to the risk that controls at a service organization may become inadequate or fail.

## 7. Performance of Audit Procedures

### 7.1 Testing Procedure

We performed tests of specific controls, as described in this report, to obtain evidence about their design to achieve the corresponding control objectives. The results of these tests are presented in section III.

Testing procedures performed of controls are described below.

Testing Procedure	Description
<b>Inquiry</b>	Interviewed appropriate personnel about timing, performance, and review of relevant controls
<b>Walkthrough</b>	Explanation and demonstration of provided process description of documentation (including control activities) by responsible staff
<b>Inspection</b>	Review documents and reports that contain performance indication of the control. This includes among other things: <ul style="list-style-type: none"> <li>• Reading and reviewing of management reports if certain actions were performed</li> <li>• Inspection of documentation for evidence of performance</li> </ul>

	<ul style="list-style-type: none"> <li>• Inspection of operation manuals, flow charts, system documentation</li> </ul>
<b>CAI</b>	Computer-Aided Inspection; Assertions are based on SQL / Reporting Tools / Wikis (Confluence). The following inspections are more effective because this testing technique allows for a risk-based sampling.
<b>Observation</b>	View the application of specific controls
<b>Re-performance</b>	Re-performance of selected transactions described in the provided process description or documentation.

In the case of a **“Test of Design”** the auditor examined of its controls presents fairly, in all material respects, the relevant aspects of the service organization’s controls that had been placed in operation as of a specific date, and whether the controls were suitably designed to achieve specified control objectives.

By the **“Test of Operating Effectiveness”** the auditor examined the same items noted above in **“Test of Design”**, and whether the controls that were tested were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives were achieved during the period specified.

**Assessing the completeness and accuracy of the information provided**

When using information produced by client, which includes, but is not limited to, management’s report used in the performance of controls and reports generated to facilitate testing of control populations (e.g. controls which require system-generated populations for sample based testing), we evaluated whether the information was sufficiently reliable for our purpose, including, as necessary, obtaining evidence about the completeness and accuracy of the information and evaluating whether the information was sufficiently precise and detailed for our purposes.

**7.2 Sample sizes**

**7.2.1 Automatic control**

Automatic control is applied when the workflow is automated or enforced by a system. If we have tested the general IT controls in terms of their design and implementation, the sample size is 1 during the audit.

If the general IT controls have not been tested or the design and implementation are not suitable, the sample size depends on the following parameters:

- Frequency of control implementation,
- Frequency of change,
- Assessment of inherent risk, especially inherent fraud risk

### 7.2.2 Manual control

For manual controls and the expectation of finding no control deviations, we determine the minimum sample size depending on the *risk of failure and frequency*:

Frequency of checks	Minimum sample size	
	Risk of failure: low	Risk of failure: high
Annual	1	1
quarterly (and at the end of the period)	1+1	1+1
Monthly	2	3
Weekly	5	8
Daily	15	25
Several times a day	25	40

If the frequency of manual checks falls between the check frequencies listed above, we determine the minimum sample size as follows:

Frequency of checks	Minimum sample size	
	Risk of failure: low	Risk of failure: high
Monthly $x=12$	2	3
$12 < x \leq 20$	3	5
$20 < x \leq 36$	4	7
Weekly ( $36 < x \leq 52$ )	5	8
$52 < x \leq 100$	8	13
$100 < x \leq 200$	12	19
Daily ( $200 < x \leq 365$ )	15	25
$365 < x \leq 450$	19	30
$450 < x \leq 550$	22	35
$x > 550$	25	40

If we expect control deviations, we determine the sample size according to the following table:

Number of control deviations	Minimum sample size	
	Risk of failure: low	Risk of failure: high
1	50	80
2	60	95
3	71	111
4	85	133
5	98	154

### 7.2.3 Selection method

To ensure that every element of the population has a chance of being selected, we use a random selection method (such as MUS, random-like selection).

#### Control on several homogeneous locations

Homogeneous locations are characterized by uniform process activities, systems, process level controls, entity level controls or higher Level Controls.





When planning the nature, scope, and timing of our audit procedures, we can take into account the effective design, implementation, and execution of monitoring controls (such as monthly reporting on incidents).

#### Qualitative assessment of control deviations

Before we assess the overall result of a sample to determine whether the control was carried out effectively, we assess the qualitative causes of the control deviation (such as employee turnover, seasonal fluctuations, human error).

### 7.3 Testing Results

The definition is of the test result obtained in connection with determining the design and operating effectiveness of controls are described below:

Testing Result	Description
	No deviations noted during the audit.
	IT systems/processes were modified during the audit, resulting in redesigned controls and testing procedures. Testing of these controls has been prioritized over stable processes.
	Deviations were found during the audit, but corrective action was implemented/planned before the end of the audit.
	Deviations noted at the end of the audit.

### 7.4 Reporting Structure

The functional test documented in section III is carried out according to a standardized scheme. This is described below in italics.

<b>Control Objective</b>	
<i>Definition of the thematic focus that is set during the audit of the respective control point.</i>	
<b>Management Practice</b>	
<i>Definition of the controls</i>	
<b>Test to be performed by BFMT</b>	
<i>General description of the audit procedure in accordance with the BFMT standard. Corresponds to the general, non-company-specific target status for achieving the control objective.</i>	
<b>Management Practice by client</b>	
<i>Description of the specific audit procedure used by the client to achieve the audit objective. This corresponds to the target state of the audit defined by the client and provides information on how the client implements its controls in practice.</i>	
<b>Result</b>	
<i>Current status and evaluation</i>	

## 8. Opinion

Our opinion has been formed on the basis of the matters outlined in this report.

In our opinion, in all material respects:

- The description fairly presents the internal control system as designed and implemented in the period of **January 1, 2025 to December 31, 2025**; and
- The controls related to the control objectives stated in the description were suitably designed in the period of **January 1, 2025 to December 31, 2025**.
- The controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively in the period of **January 1, 2025 to December 31, 2025**.

## 9. Intended Users and Purpose

This report and the description of tests of controls are intended only for customers who have used **SEEBURGER INFORMATIK EOOD's** EDI/B2B/GTS and iPaaS 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 misstatements of customer's financial statements.

We are issuing this report based on the contract concluded with **SEEBURGER INFORMATIK EOOD**, applying also to third parties on the underlying General Engagement Terms for German Public Auditors and Public Audit Firms from January 1, 2024 including a limitation of the liability agreement.

**Viechtach, January 12, 2026**

BFMT Audit GmbH  
Wirtschaftsprüfungsgesellschaft





WP Dr. Martin Trost  
Partner



Tobias Kraus  
Head of Compliance & IT Assurance

## Service Organization's Statement

The accompanying description has been prepared for customers who have used the internal control system and their auditors who have a sufficient understanding to consider the description, along with other information including information about controls operated by customers themselves, when assessing the risks of material misstatements of customer's financial statements.

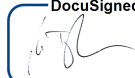
**SEEBURGER INFORMATIK EOOD** confirms that:

- (a) The accompanying description fairly presents the EDI/B2B/GTS and iPaaS system for processing customers' transactions in the period of **January 1, 2025 to December 31, 2025**. The criteria used in making this statement were that the accompanying description:
- (i) Presents how the system was designed including:
- The types of services provided, including, as appropriate, classes of transactions processed.
  - The procedures, within both information technology and manual systems, by which those transactions were initiated, recorded, processed, corrected as necessary, and transferred to the reports prepared for customers.
  - The related accounting records, supporting information and specific accounts that were used to initiate, record, process, and report transactions; this includes the correction of incorrect information and how information was transferred to the reports prepared for customers.
  - How the system deals with significant events and conditions, other than transactions.
  - The process used to prepare reports for customers.
  - Relevant 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 our control environment, risk assessment process, information system (including the related business processes) and communication, control activities and monitoring controls that were relevant to processing and reporting customers' transactions.
- (ii) Includes relevant details of changes to the service organization's system the period of **January 1, 2025 to December 31, 2025**.
- (iii) 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.

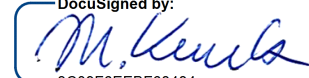
- (b) The controls related to the control objectives stated in the accompanying description were suitably designed in the period of **January 1, 2025 to December 31, 2025**. The criteria used in making this statement were that:
- (i) The risks that threatened achievement of the control objectives stated in the description were identified;
  - (ii) The identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved; and
  - (iii) The controls were consistently applied as designed, including that manual controls were applied by individuals who have the appropriate competence and authority, in the period of **January 1, 2025 to December 31, 2025**.

**Bretten, January 12, 2026**

**Bretten, January 12, 2026**

DocuSigned by:  
  
DCDCCE409E554AD

Matthias Feßenbecker  
Director, Executive Board  
SEEBURGER INFORMATIK EOOD

DocuSigned by:  
  
3C09F6EEBF68484...

Dr. Martin Kuntz  
Director, Executive Board  
SEEBURGER INFORMATIK EOOD

## Section II – Description of Controls provided by SEEBURGER INFORMATIK EOOD

### 1. The SEEBURGER INFORMATIK EOOD Internal Control System

As one of the leading providers of B2B integration solutions, **SEEBURGER INFORMATIK EOOD** considers the safe exchange of information between companies as a fundamental part of company operations that is used in numerous **SEEBURGER INFORMATIK EOOD** products and services. At **SEEBURGER INFORMATIK EOOD**, the transparency of business processes along the entire value chain is an essential tool for building trust with our customers. The trust that our customers have placed in our products, solutions and services for more than 35 years is reason enough for us to expand, operate and continuously develop the internal control system described in this document as well as have it regularly audited by an independent third party. It essentially consists of the following components:

- Control environment
- Information and communication measures
- Monitoring activities
- Risk assessments
- Control activities

### 2. Control Environment

For over 35 years, the safe exchange of information between companies has been a strategic corporate objective used for numerous products, cloud services and standard services provided by **SEEBURGER INFORMATIK EOOD**. We and our customers both attach great importance to information security, including confidentiality, integrity and availability of the exchanged information.

This includes both the provision of services and applications required for the business activity as well as programs developed during the business activity, cloud services offered to customers, other services provided and the necessary infrastructure.

They also include all administrative relief processes at **SEEBURGER INFORMATIK EOOD** and its subsidiaries.

In order to react appropriately to constantly increasing security requirements as well as rapidly changing and ever more complex threat situations, **SEEBURGER INFORMATIK EOOD** has developed an internal control system (ICS) according to COSO as a central management process. In this way it is ensured that the system is integrated in business processes within the scope of the inspection and responsibilities are determined.

The purpose of the ICS is to protect all information received, generated, distributed, archived and destroyed over the course of business activities in compliance with legal regulations, national and international standards, internal company standards as well as contractual obligations.

The **SEEBURGER INFORMATIK EOOD** Executive Board encourages and promotes the necessary structures and processes. It appoints representatives, defines information security provisions, and demands the integration and monitoring of regulations and procedures in all national and international business units, which are formulated in guidelines, documentation and work instructions.

**SEEBURGER INFORMATIK EOOD** implements measures promoting training and awareness that ensure the relevant persons are familiar with requirements and aware how important they are within the company.

## 2.1 Information Security Committee

An information security committee has been installed on a management level within the **SEEBURGER INFORMATIK EOOD** organization together with an information security management team as part of the information security organization. The method chosen by **SEEBURGER INFORMATIK EOOD** to implement this requirement, as well as the structure and frequency of regular meetings, are documented. The issues and results of these meetings are documented and integrated in the annual report on **SEEBURGER INFORMATIK EOOD** information security.

## 2.2 Sustainability and corporate responsibility at SEEBURGER INFORMATIK EOOD

In June 2010, **SEEBURGER INFORMATIK EOOD** joined the international Global Compact (GC) network of the United Nations, thereby committing itself to recognizing and promoting ten principles in the areas of human rights, labor standards, anticorruption and environmental standards as a code of conduct within the company.

As a member of Global Compact, we are committed to reporting our progress on the path towards realizing the ten principles (“Communications on Progress”) because the vision of operating with economic success, environmental responsibility and social fairness has become a strategic task for **SEEBURGER INFORMATIK EOOD**.

As a company and business software provider operating on a global scale, **SEEBURGER INFORMATIK EOOD** develops products and pioneering software solutions that shape the business process with greater control, transparency and sustainability, while paving the way for innovations worldwide and generating added value for **SEEBURGER INFORMATIK EOOD**, our customers and their business partners from different sectors all over the world.

We offer a solution suite that not only integrates and improves our own business processes, but also in particular those of our customers. **SEEBURGER INFORMATIK EOOD** helps companies design their supplier and supply chain management systems more efficiently, connect business partners

and integrate business processes on a global scale beyond corporate boundaries. As a result, we create ideal conditions for sustainable ecological development and successful growth.

**SEEBURGER INFORMATIK EOOD** is committed to different international F&E projects and plays an active role in various research projects funded by the Federal Ministry for Economics, such as Software Cluster, Trusted Cloud / PeerEnergyCloud, “The Intelligent Container” and THESEUS.

The management emphatically stands by the objectives of Global Compact.

An integral part of the **SEEBURGER INFORMATIK EOOD** Code of Conduct, the principles of the Global Compact were explained to our workforce at all levels of our organization through a large number of informal and formal information channels such as business principles, website, intranet, sales meetings, regular meetings with the heads of specialist departments, etc.

At **SEEBURGER INFORMATIK EOOD**, information security is considered a collective corporate task.

## 2.3 Principles

The principles of information security form the cornerstones of the **SEEBURGER INFORMATIK EOOD** Information Security Management System (ISMS) and therefore the central requirements of this system. These requirements are subject to continuous monitoring and reassessment as part of a continuous improvement process. Measures are derived that take into account constantly changing boundary conditions and further develop the objective of providing information security as well as protecting the confidentiality, integrity and availability of information. The principles listed in the following are universal and based on statutory boundary conditions, standards and norms valid in the relevant country. If they conflict with applicable national laws, these national laws must be applied.

### **Integral security**

Information security is an integral part of the **SEEBURGER INFORMATIK EOOD** business strategy. The objective is to embed information security within the company so that it becomes an indispensable component of the overall company policy at **SEEBURGER INFORMATIK EOOD**.

### **Compliance with legal requirements**

Information security must always comply with existing legal requirements if it is to become a central corporate objective. Compliance is firmly embedded in the **SEEBURGER INFORMATIK EOOD** quality guidelines together with the responsibilities of globally operating specialist departments.

### **Protection of data and resources**

Suitable technical and organizational measures must be introduced to protect data and resources in order to meet the information security objectives of confidentiality, integrity and availability. If weaknesses are identified or these objectives are compromised, this must be reported immediately.

### **Protection of personal data**

Personal data must be protected from misuse by unauthorized individuals. All **SEEBURGER INFORMATIK EOOD** employees are sworn to data and telecommunications secrecy as defined in

relevant applicable national laws. The data protection officer at **SEEBURGER INFORMATIK EOOD** is a central contact for all questions relating to data protection.

### **Guaranteeing traceability**

It must always be possible to trace any activities relating to safety. Corresponding documentation or other suitable measures must be implemented with the aim of defining responsible persons and as a form of proof.

### **Compliance with norms, standards and regulations**

National, international and other relevant norms, standards and regulations that define **the state of the art** must be observed when implementing information security requirements.

The **state of the art** is determined by:

- Internal corporate standards,
- Industry standards/Best Practice: (e.g. CMM/CMMI (SEI), COBIT/COSO, ITIL, Scrum, Microsoft SDLC, ISAE 3402, PRINCE2, NIST, FIPS),
- International norms (e.g. ISO 20000, ISO 15504 (SPICE), ISO 27001) and
- Laws: (e.g. SOX, AktG, GoBD, German Commercial Code).

Compliance with national and international norms and Best Practices for the relevant field of activity and the alignment of processes and methods with the “state of the art” standards is a central aspect in the area of responsibility of the specialist department.

### **Protection from attacks and disasters**

Information security is designed to protect the security objectives of availability, confidentiality and integrity of information against any kind of threat. This is partly achieved through the utilization of structural and technical facilities as well as organizational measures and guidelines.

A risk assessment system must be established to identify vulnerabilities and evaluate the criticality of the threat.

### **Guaranteeing contractual relations**

Agreements between **SEEBURGER INFORMATIK EOOD** and employees, customers, suppliers and partners must be protected by contract. This is the only way to create the necessary degree of transparency of the services and measures agreed between all the parties involved.

### **Guaranteeing operation**

The structure and organization of the processes from the **SEEBURGER INFORMATIK EOOD** value chain must be documented using suitable means. This includes core, auxiliary and management processes. A suitable asset management system must be introduced and operated continuously for documentation purposes. Measures for maintaining and restoring operation after a disaster situation must also be defined and included in work instructions and other regulations for employees.

**Guaranteeing suitability and economic efficiency**

All measures for maintaining information security must be subject to a feasibility study. This study must compare all relevant costs with the benefits or the risk of failure.

**2.4 Scope of the ISAE 3402 report**

As one of the most dynamic divisions of **SEEBURGER INFORMATIK EOOD** with a strong international orientation, Cloud Services was selected as the scope of the ISAE 3402 Type 2 audit. Protection of customer data transferred to **SEEBURGER INFORMATIK EOOD** has top priority. In order to guarantee this, **SEEBURGER INFORMATIK EOOD** has introduced an effective Internal Control System that includes the “Basic”, “Advanced” and “Premium” Service Level Agreements that focuses on the EDI/B2B/GTS processes of customers operated in a Full Integration Services model or provided as iPaaS. ISAE 3402 audits cover both operational and administrative processes. Customer processes are implemented on **SEEBURGER INFORMATIK EOOD** Business Integration Server 6 and access to productive systems is regulated and monitored via the Cloud Service Portal. The virtualized IT infrastructure with high availability is hosted in four data centers and are operated by the provider TelemaxX, AWS and Equinix. The scope of the ISAE 3402 audit is shown in detail in the following illustration.

SEEBURGER Service: EDI/B2B, GTS and iPaaS	
Application	Business Integration Server 6, Managed Service Portal
Operating System	Linux Red Hat, Microsoft Windows
Data Base	Oracle
Physical Location	TelemaxX Telekommunikation GmbH (IPC 1, IPC 3, IPC 4 and IPC 5), AWS, Equinix (ATDC1 and ATDC4)
SLA's	Basic, Advanced, Premium
Processes in the Scope	
Risk Management	Risk detection and mitigation process
User & Access Management	Protection against unauthorized access
Physical Security	Perimeter security of the locations in the scope of the attestation
Go Live Management	Quality assurance process for the change of responsibility between initial project and operations
Monitoring Management	Completeness and correctness of EDI availability of the IT Infrastructure
Incident Management	Guarantee of the services within the contractual agreed SLA's
Change Management (system based)	Avoiding unauthorized or incorrect changes, traceability
Backup & Recovery	Restore and Disaster Recovery for productive systems
Business Continuity Management	Measures to restore operations after a crisis

Illustration 1: Scope of ISAE 3402 audit

**2.4.1 The SEEBURGER INFORMATIK EOOD Services in Scope**

**SEEBURGER INFORMATIK EOOD** provides a comprehensive suite of cloud-based integration solutions designed to facilitate seamless business-to-business (B2B) communication, EDI processing, and global trade management. The services offered include:

Cloud Integration Services for **B2B/EDI**:



- Securely manages and exchanges electronic business documents between trading partners.
- Ensures compliance with industry standards and regulations.
- Provides robust data mapping, transformation, and validation capabilities.
- Offers integration with **SEEBURGER INFORMATIK EOOD** Supplier Portal Service for web-based supplier connections.

**Integration Services for SAP Global Trade Services (GTS):**

- Integrates with SAP GTS to streamline global trade processes.
- Supports customs compliance, export control, and trade finance activities.
- Provides real-time visibility into global trade operations.

**SEEBURGER INFORMATIK EOOD iPaaS:**

- Offers a fully managed Integration Platform as a Service (iPaaS) solution.
- Enables the integration of applications, data, and processes across various systems and environments.
- Provides a centralized platform for managing and monitoring integration workflows.
- Offers scalability, flexibility, and reduced infrastructure management overhead.

For all services **SEEBURGER INFORMATIK EOOD** provides:

- Service delivery, operation, and maintenance of the cloud-based integration solutions.
- Provisioning of access to the **SEEBURGER INFORMATIK EOOD** cloud platform.
- Technical support and assistance for users.
- Regular updates and maintenance of the integration services and iPaaS.

**SEEBURGER INFORMATIK EOOD** Cloud Services are built upon the robust foundation of the **SEEBURGER INFORMATIK EOOD** Business Integration Suite. This comprehensive platform provides a unified, scalable, and flexible environment for managing and integrating business processes. By leveraging the capabilities of the Business Integration Suite, **SEEBURGER INFORMATIK EOOD** Cloud Services inherits:

- a single platform for managing all integration needs,
- scalability and flexibility,
- a wide range of features and capabilities for data integration, transformation, and process automation,
- built-in security measures and compliance with industry standards to protect sensitive data,
- seamless integration with existing on-premises systems and applications.

**2.4.2 Control Objectives for the Processes in Scope**

Below is a list of the control objectives for the processes in scope:

Process	Control Objective
Risk Management	Controls provide reasonable assurance that risks are identified, mitigated and reviewed by management.

<b>User &amp; Access Management</b>	Controls provide reasonable assurance that only authorized individuals have access to productive systems used for the EDI/B2B/GTS/iPaaS services and the Active Directory systems.
<b>Physical Security</b>	Controls provide reasonable assurance that access to data center is approved, infrastructure is protected against environmental factors and assets entering the data center are tracked.
<b>Go-Live Management</b>	Controls provide reasonable assurance that go-lives are authorized, documented and processed in a suitable manner.
<b>Monitoring Management</b>	Controls provide reasonable assurance that all relevant systems and processes are constantly monitored and follow-up activities are initiated.
<b>Incident Management</b>	Controls provide reasonable assurance that operational procedures are monitored, service level agreement (SLA)-deviations are identified and incidents are handled quickly to recover service availability.
<b>System-Based Change Management</b>	Controls provide reasonable assurance that system-based changes (including emergency changes) to applications are authorized, tested, approved and documented.
<b>Backup &amp; Recovery</b>	Controls provide reasonable assurance that back-up is accurate, available, complete, monitored and readability of media is ensured through regular tests.
<b>Business Continuity Management</b>	Controls provide reasonable assurance that Business Continuity measures are established and applied.

## 2.5 Information technology platform

**SEEBURGER INFORMATIK EOOD** software solutions are not only operated independently by customers, **SEEBURGER INFORMATIK EOOD** also offers EDI/B2B/GTS data exchange as a service. Several data centers in Germany and North America receive our customers' data via secure communication channels (VPN, MPLS), where it is handled according to customer requirements and then sent to various trading partners.

### 2.5.1 The architecture

The EDI IT infrastructure operated and provided by **SEEBURGER INFORMATIK EOOD** is displayed in a simplified diagram together with the services offered as follows:

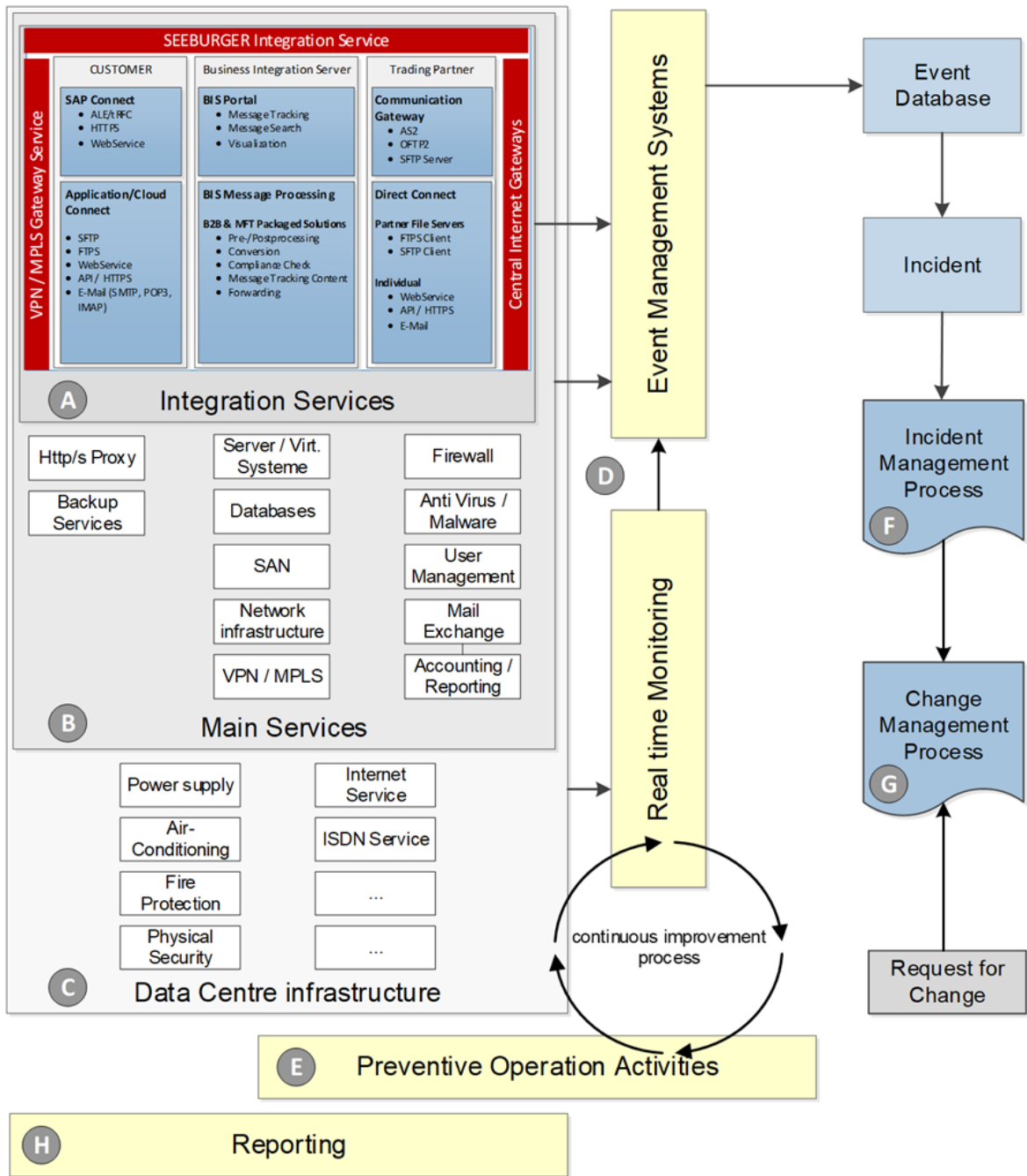


Illustration 2: Architecture and processes of Managed Services and IT infrastructure

The processes and sub processes that were implemented to operate **SEEBURGER INFORMATIK FOOD** services as well as the data centers are ISO/IEC 27001 certified. This combination guarantees a consistently high security level of the IT infrastructure and during operation as well as a continuous comprehensive improvement process.

### 2.5.2 IT infrastructure landscape

The main objective of information security in this sector is to protect the flow of data between customers and trading partners against any activities capable of compromising the availability, integrity and confidentiality of information. In order to consistently maintain the maximum possible

security level, **SEEBURGER INFORMATIK EOOD** has implemented several security concepts on an organizational, hardware and software level. The basic principle of data exchange is shown in the following illustration.

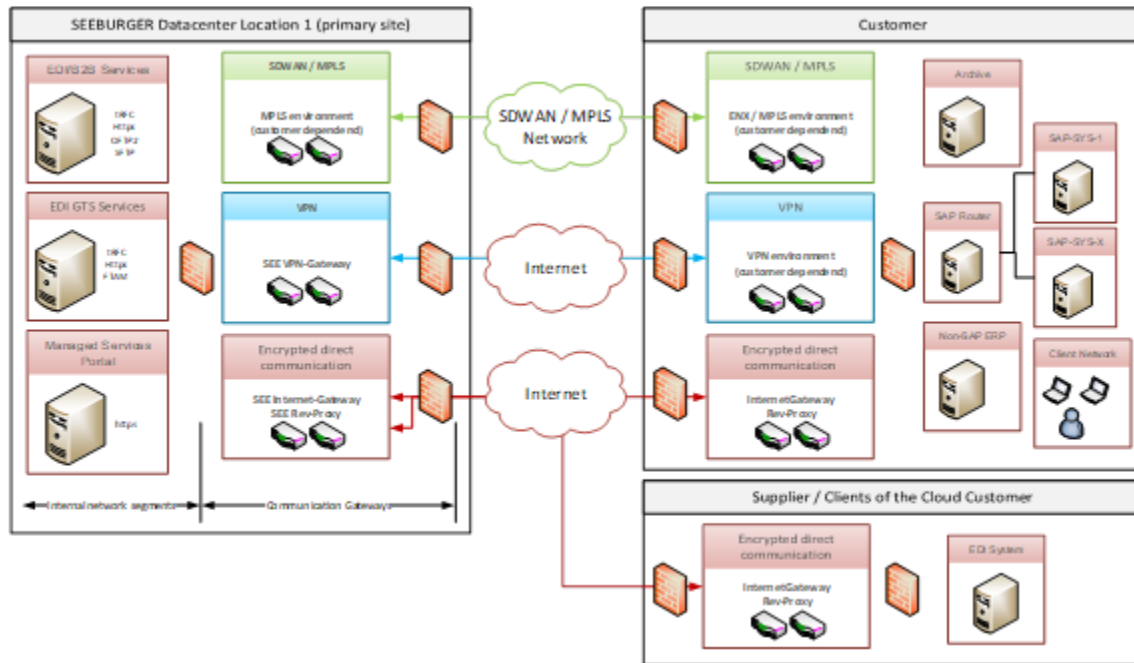


Illustration 3: System Landscape

Like every technical component or physical infrastructure of a data center, each interface in the IT infrastructure can become a point of attack to various applications of our customers. For this reason, the availability, confidentiality and integrity of **SEEBURGER INFORMATIK EOOD** services on offer must be protected on different levels.

### 2.5.3 Connection security

Connection security poses a challenge to every service provider because vulnerabilities in this area are particularly critical for the availability, confidentiality and integrity of the services on offer. That is why **SEEBURGER INFORMATIK EOOD** has introduced the following regulations:

- Incoming connections from the external networks are terminated on specific communication endpoints within separated network segments.
- Only defined communication protocols between the communication gateways and the internal **SEEBURGER INFORMATIK EOOD** applications (like EDI/B2B System) are allowed.
- The number of opened ports must be kept to a minimum.
- Only secure connections (VPN, MPLS or encrypted communication protocols) are allowed.
- Systems within the internal network segments are separated from each other.

Furthermore, the “Corporate” (**SEEBURGER INFORMATIK EOOD** internal) and “Cloud Services” Cloud areas must be separated completely from one another and checked for vulnerabilities by external security experts at regular intervals.

Based on many years of experience, **SEEBURGER INFORMATIK EOOD** has defined parameters for customers and partners, which must be observed when establishing connections with a customer or partner in order to avoid errors in a complex firewall configuration.

#### 2.5.4 IT monitoring

Extremely simple problems can cause networks to crash during normal operation. Such problems can be resolved relatively easily, provided the IT administration still has access to the network. Out-of-band management offers network administrators an alternative way to access network devices remotely if the primary network is no longer available. **SEEBURGER INFORMATIK EOOD** has already implemented this out-of-band management system. If the redundant direct connections fail, the IT infrastructure team can use the out-of-band connection. Should a disaster ever occur, **SEEBURGER INFORMATIK EOOD** would be able to manage internal systems and Cloud services securely.

#### 2.5.5 Data centers at locations in Germany and North America

To support local communications endpoints and data processing services in North America for customers and their trading partners, **SEEBURGER INFORMATIK EOOD** operates its services in data center locations in the United States of America.

#### 2.5.6 Overview of data centers used by SEEBURGER INFORMATIK EOOD

**SEEBURGER INFORMATIK EOOD** provides the services by using the following data centers:

Data center	Location
TelemaxX IPC 1	Karlsruhe
TelemaxX IPC 3	Karlsruhe
TelemaxX IPC 4	Karlsruhe
TelemaxX IPC 5	Karlsruhe
AWS	EU
Equinix AT1	Atlanta
Equinix AT4	Atlanta
(Equinix AT5)	Atlanta

The following controls are designed and implemented by **SEEBURGER INFORMATIK EOOD** for the physical and environmental security measures in the data centers TelemaxX and Equinix:

Control Ref.	Control Description
PS_01	Access rights to the data centers used by <b>SEEBURGER INFORMATIK EOOD</b> are allocated and checked in a formal multi-stage process.
PS_05	All inputs and outputs are implemented by <b>SEEBURGER INFORMATIK EOOD</b> employees and managed in a central database. The Global Head of Governance, Risk and Compliance checks the correctness on an annual basis.
PS_07	Control owner reviews attestation report(s) of the data center providers to ascertain that physical access and environmental controls are implemented and complied with. Follow-up activities are carried out in case of relevant deviations.

Equinix issues SOC 1 and SOC 2 reports for its data center sites including controls not covered by this report. TelemaxX issues an ISAE 3402 Type 2 report for its data center sites including controls not covered by this report.

### 2.5.7 Risk management on a virtualization layer

**SEEBURGER INFORMATIK EOOD** uses the advantages of virtualization for its own internal systems as well as for the Cloud Services Cloud infrastructure. Technical and organizational measures that address the following risks were implemented to counteract the risks of virtualization:

- The uncontrolled proliferation of virtual machines (VM),
- Loss of sensitive data through snapshots,
- Security risk from deactivated virtual machines,
- Security risk from preconfigured VMs,
- Security risk from virtual networks,
- Uncontrolled use of physical resources,
- Hypervisor security and
- Unauthorized access to the hypervisor.

Effectiveness and compliance are checked in regular audits.

### 3. Information and communication measures

Information and communication measures are fundamental components of **SEEBURGER INFORMATIK EOOD's** ICS, ensuring the effective and timely flow of relevant information within the organization. These measures encompass the collection, processing, and dissemination of information vital for decision-making and process monitoring.

Clear communication channels are established to ensure that all employees are informed about policies, procedures, and changes. Regular training, internal reports, and meetings facilitate the exchange of information.

Moreover, **SEEBURGER INFORMATIK EOOD** prioritizes the accuracy, comprehensibility, and accessibility of information to prevent misunderstandings and maintain compliance. These measures not only enhance transparency within the organization but also minimize the risk of errors and fraud, ultimately contributing to improved governance and oversight.

### 4. Monitoring Activities

Monitoring activities are an integral part of **SEEBURGER INFORMATIK EOOD's** internal control system. These measures ensure that business activities comply with policies and procedures, and they identify and correct discrepancies or inefficiencies. Essentially, they include regular monitoring and evaluation of various processes and activities, compliance with regulations, and key performance indicators. They help identify potential risks and promptly implement corrective actions. This fosters an environment of accountability and continuous improvement.

In addition to the general monitoring framework, **SEEBURGER INFORMATIK EOOD** performs regular internal and external audits to evaluate the effectiveness of its internal controls, risk management processes, and compliance with relevant laws, regulations, and industry standards.

### 5. Risk Management

External and internal threats present a risk to business operations at **SEEBURGER INFORMATIK EOOD** if existing vulnerabilities in the infrastructure, organizational structure, process organization, products, Cloud services and standard services are exploited. **SEEBURGER INFORMATIK EOOD** uses the ISMS tool IRIS from ibi systems based on ISO/IEC 27005 to systematically identify, assess, handle and reassess these threats.

The purpose of a standardized company-wide risk management system is to identify and assess existing or potential risks and derive economically justifiable measures for sustainable treatment. As a critical component of overall company-wide risk management, Information Security Risk Management focuses specifically on identifying, assessing, and mitigating risks that could compromise the confidentiality, integrity, or availability of sensitive information. This includes risks related to data breaches, cyberattacks, unauthorized access, and other security threats. The division managers or **SEEBURGER INFORMATIK EOOD** management team, which has overall responsibility,

is always responsible for identifying, assessing and deriving measures. The information security organization performs internal audits to help with the identification process and provides the methodical framework for assessing, handling and following up on these risks.

The risk management system is the engine room of the Continuous Improvement Process (CIP), which **SEEBURGER INFORMATIK EOOD** obliges its employees, customers and partners to participate in. The methodology of the **SEEBURGER INFORMATIK EOOD** risk management system is presented as part of the security concept.

## 5.1 Risk management process

The risk management process is a core component of the **SEEBURGER INFORMATIK EOOD** risk management system. It is implemented throughout the group due to its universally valid nature. This process consists of seven process steps, which are shown in the following illustration. It is also used for risks that have been recently identified or already exist. Existing risks must be reassessed at regular intervals to ensure the sustainability of the adopted measures.

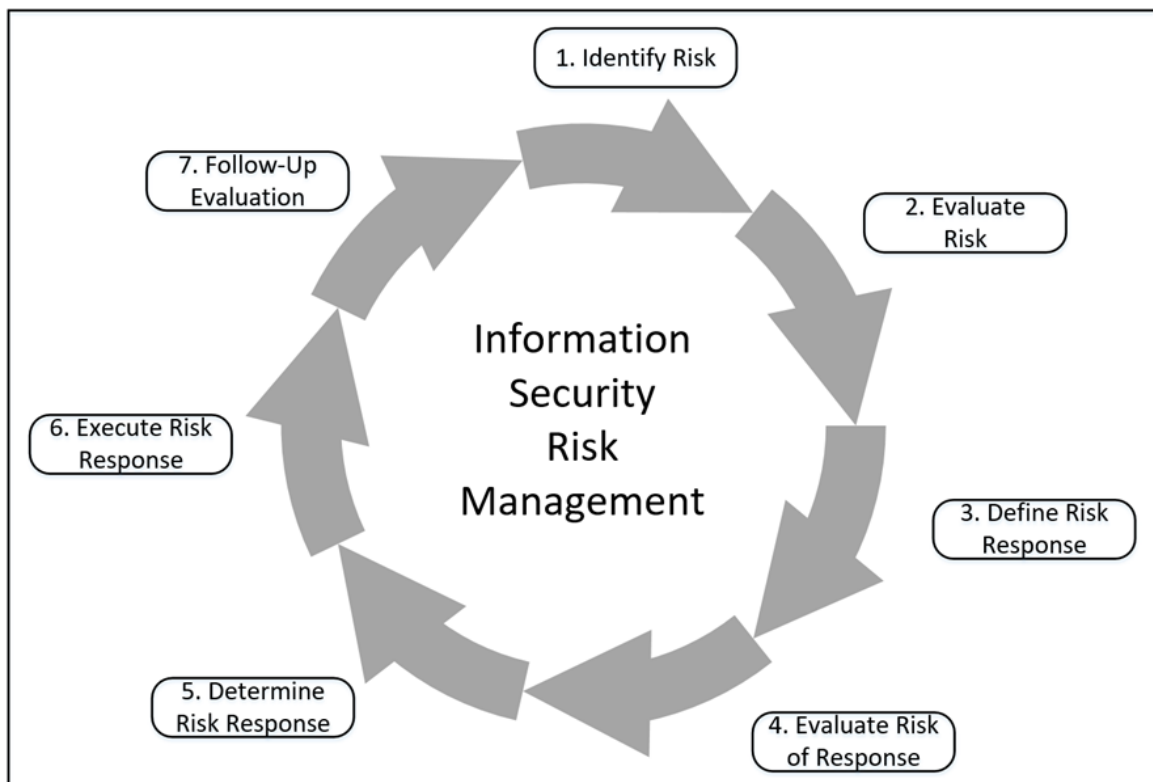


Illustration 4: Risk management process

**The sub-process steps are described in more detail in the following sections.**

### 5.1.1 Identifying risks

The identification of existing risks is the first step of the risk treatment process, because risks are an economic threat for each company. To identify risks on a structured base, it is required that

information security requirements are defined as a baseline. Against this baseline internal audits have to be performed and Information security guidelines have to be adapted.

For a systematic risk identification approach, **SEEBURGER INFORMATIK EOOD** fused the Information assets with any potential internal and external threads which are defined in the ISO 27005 and created new generic risks. These risks will help with effective identification and assessment of threads for the (operational) business and to minimize the potential damage impact.

The objective of continuous analysis and identification of risks falls within the responsibility of the Director or the Executive of **SEEBURGER INFORMATIK EOOD**. The information security supports here. Gathering all of the information and reporting to the executive board is carried out centrally by the Information Security Team.

### 5.1.2 (Re)-Evaluation of Risks

Identified risks are described in terms of the likelihood of damage and the expected Impact of damage. In order to make an objective assessment possible, uniformly applicable threat classes are equated with the protection requirements scales, so that the assessment of probabilities can be objectified using a simple rating scale or optionally an OWASP related methodology. These are presented in the context of this process. The likelihood of the risk and the threat classes are compared in a risk assessment matrix. The different acceptable ranges are indicated in green, yellow and red. On one hand, this evaluation is used to determine the probability that the risk occurs and on the other hand to determine and document the effects on the information safety goals such as availability, integrity and privacy as well as other negative impact on the organization.

The assessment of risks is carried out by the experts of the respective department. Information Security Department provides a supportive role. Reviews are distinguished in the context of this evaluation as initial and subsequent reviews. The initial evaluation takes place after the risk was created.

Risks with a Risk Priority Number (RPN) higher or equal than 4 are re-evaluated semiannually.

Because of the rhythm of the re-evaluation it is required, that new risks with  $RPN \geq 4$  undergo re-evaluation only in case their initial cycle is completed.

The evaluation and re-evaluation process are shown in the following illustration.

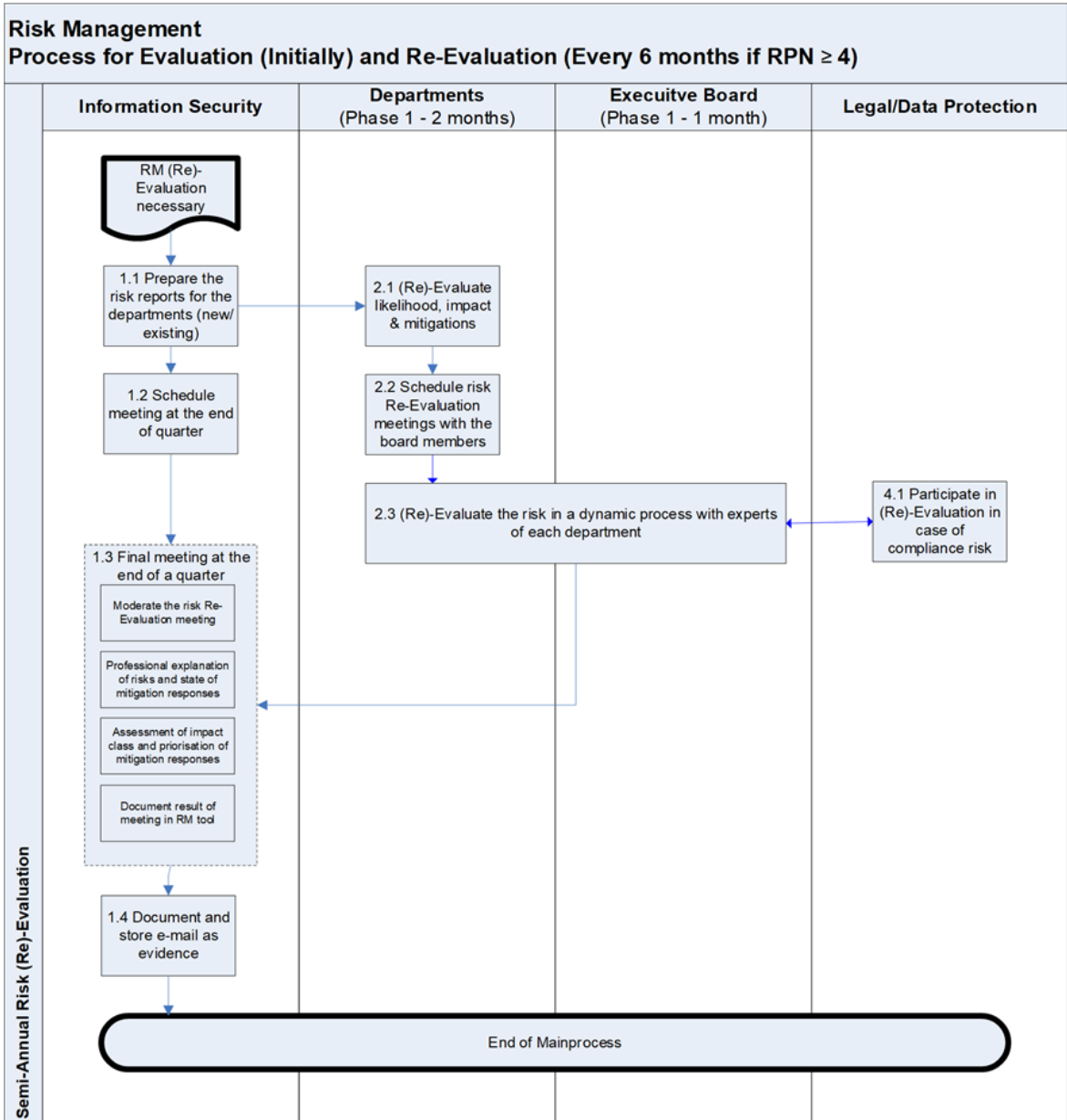


Illustration 5: The Risk Evaluation process

**Step 1.1: Prepare the Risk Reports for the Departments**

On a quarterly base, the Information Security department creates risk reports. These risk reports contain new identified risks in the former quarter and risks, which must be reevaluated. The experts of the specific department have a three-month period to evaluate the risks. This will give them time to discuss the current or initial evaluation of the risk and to prioritize or track the state of the mitigation responses. Regular meetings with the responsible board member are part of the iterative (re)-evaluation process of risks.

**Step 1.2: Schedule a Risk (Re)- Evaluation with the Board Member**

In parallel to step 1, the Information Security Team schedules meetings with the concerned Board Member in the third month of the quarter. This meeting will replace the semi-annual risk treatment report meeting with the board member.

**Step 2.1: (Re)-Evaluation of probability of occurrence of the risk**

In the first phase of the (re)-evaluation of risks, the experts of the departments evaluate the probability of occurrence of the risk. The impact class will be evaluated initially. Because of the three-month period for the risk evaluation the experts can use this time to organize expert meetings to define risk mitigation responses and the track of the progress. The evaluation depends not only on a single meeting with one expert and the Information Security department. In the three-month evaluation phase different opinions might be considered.

**Step 4.1: Participate in the (Re)-Evaluation in case of Compliance Risks**

In case of legal, compliance or data protection risks, the legal department, compliance officer and the Data Protection Officer must be involved into the evaluation process as needed.

**Step 2.2/2.3: Schedule iterative (Re)-Evaluation Meeting with the Board Member**

Phase two starts with iterative risk assessment and evaluation meetings with participation of the responsible Board Members. The departments are organizing these meeting independently.

The department specialist and management are responsible to present the risks and the current state of the mitigation responses to the board member.

**Step 1.3: (Optional) Final Meeting at the end of the quarter**

Based on the professional explanation of the department specialists and management, the Board Member decides about the correct impact class and the likelihood he expects. The final risk (re)-evaluation will be discussed in the meeting with Information Security.

The results of the assessment and evaluation meeting will be documented in the Information Security Risk Management. The documentation is the base for the next quarterly (re)-evaluation.

**Step 1.4: Send E-Mail to Information Security**

As part of the risk mitigation process the responsible Board Member sends an e-mail to Information Security with the content that he agrees with the evaluation, the mitigation responses and that he will accept the remaining risk.

This Board Member decision will be documented as verification. As a basis for the risk assessment, protection requirement scales were defined for the categories:

- Violation of laws,
- Negative impact on task fulfillment,
- Negative external effect and
- Financial damage

and assigned to a corresponding damage class. The actual assessment is conducted using the risk assessment matrix. The protection requirement class (damage class) and probability of a risk occurring are correlated in the risk assessment matrix. The risk indicator is calculated by adding the indicators of the protection requirement class (damage classes) and indicators of the probability of the risk occurring. This is shown as an example in the following illustration:

Risk classes and risk values					
Likelihood of damage	Certain	II (5)	III (6)	III (7)	III (8)
	Almost Certain	II (4)	II (5)	III (6)	III (7)
	Moderate	II (3)	II (4)	II (5)	III (6)
	Small	I (2)	II (3)	II (4)	II (5)
		Low	Significant	High	Very High
<b>Damage impact</b>					

Illustration 6: Risk classes and risk values

### 5.1.3 Evaluate a risk with the simple Methodology of IRIS

These scales are assigned to a corresponding damage class. The actual assessment is conducted using the risk assessment matrix. The protection requirement class (damage class) and probability of a risk occurring are correlated in the risk assessment matrix. The risk indicator is calculated by adding the indicators of the protection requirement class (damage classes) and indicators of the probability of the risk occurring.

Likelihood of damage			
Class	Qualitative scale	Quantitative scale	Description
1	Small	0 % to < 10 %	Damage (threat exploits vulnerability) is expected to occur <b>every 3-5 years</b>
2	Moderate	10 % to < 50 %	Damage (threat exploits vulnerability) is expected to occur <b>every 1-3 years</b>
3	Almost Certain	50 % to < 75 %	Damage (threat exploits vulnerability) is expected to occur <b>every year</b>
4	Certain	Greater than 75 %	Damage (threat exploits vulnerability) is expected to occur <b>more often than once every year</b>

Illustration 7: Likelihood of Damage

In the ISMS tool further categories to determine the Likelihood of the Damage are available:

- By vulnerability (Technical vulnerabilities; Technical failure; Human malpractice; Infrastructural deficiencies; Vulnerabilities in communication; Coupling of services) in the steps small, moderate, almost certain and certain
- By categories (Threat Agent Motivation; Threat Agent Opportunity; Exploitability; Discoverability; Awareness of the vulnerability) in the small, moderate, almost certain and certain

Damage impact / Financial			
Class	Qualitative scale	Quantitative scale	Description
1	Low	0 to < 300,000	Damage with <b>limited financial impact</b> on daily operations
2	Significant	300,000 to < 1,000,000	Damage with <b>bearable financial impact</b> that requires countermeasures
3	High	1,000,000 to < 6,000,000	Damage with <b>painfully financial impact</b> that requires immediate countermeasures
4	Very High	Greater than 6,000,000	Damage with <b>life-threatening financial impact</b> on the organization that requires immediate countermeasures

Illustration 8: Damage Impact

In the ISMS tool further categories to determine the Impact of the Damage are available:

- By protection requirements (confidentiality, integrity, availability) in the levels low, significant, high and very high
- By categories (Financial; Legal, Contract, Compliance; Business Disruption, Operational; Data privacy violation; Reputation) in the levels low, significant, high, very high



Illustration 9: Sample Screen of Risk after Re-Evaluation

#### 5.1.4 Define Risk Response

The identification of measures follows the assessment of a risk. A distinction is made between the following types of activities:

1. Measures to avoid the risk,
2. Measures to minimize the impact of the risk,
3. Measures to transfer the risk to third parties and
4. No measures. In this case the risk is accepted.

The measures are to be identified by the experts of the responsible department. This is also described in the evaluation process. The Information Security Team provides both a supporting role as well as oversight.

(New measure) ✕

**Data**

**General**

iris ID: -      Caption (\*):

Keywords:       External ID (\*):

Topics: - 🔍      Responsibility: - 👤 👥

Measure Owner: - 👤      Lifecycle (\*):

**Properties**

Measure categories: - 🔍

Priority:       Deadline:

**Cost of implementation**

One-time costs	Annual costs	One-time personnel costs	Annual personnel costs
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

**Fundamentals**

Chapters: - 🔍      Compendia: - 🔍

**Affected elements**

Illustration 10: Define a Risk Response

### 5.1.5 Evaluate risk of the response

Since measures are also subject to risks, these risks are assessed in the next process step. This assessment is optional, depending on the measure.

### 5.1.6 Determine risk response

The definition of the measures follows the risk assessment of the measures. The measure is to be approved by the risk owner and the planned implementation periods, as well as the responsibilities, are to be documented. The experts of the department are responsible for the definition of the measures. The Information Security Team provides a supporting role.

When specifying concrete measures that do not affect the risk-taking it is important to ensure the sustainability of the measure.

### 5.1.7 Implementing the risk response

The implementation of measures follows the definition of measures. The implementation of measures is the responsibility of the department. The Information Security Team provides both a supporting role as well as oversight. The implementation status of a risk response is shown in the following figure.

Implementation status		
Number	Value	Description
1	Open	The measure is not yet in progress.
2	In progress	The measure is in progress.
3	Completed	The measure is complete.
4	Discontinued	The measure is discontinued.

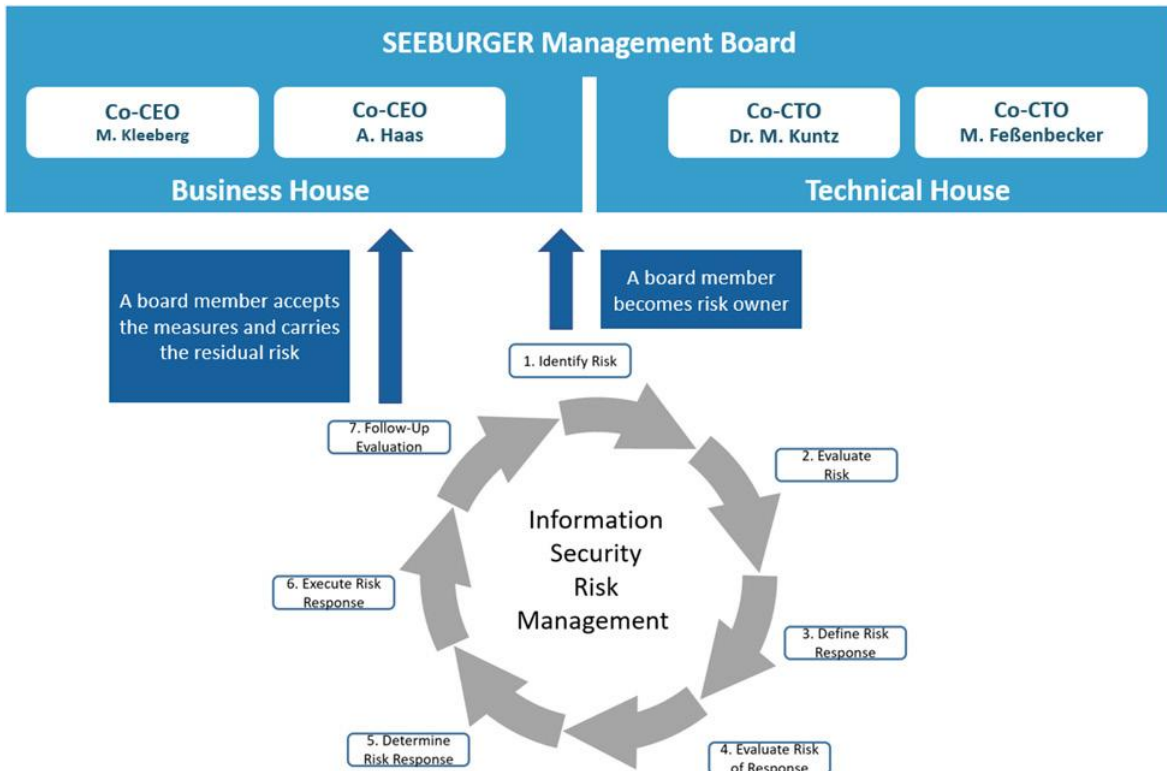
Illustration 11: Implementation status of a Risk Response

### 5.1.8 Follow-Up Evaluation

Regardless of the nature of the action, a new risk assessment is performed following each measure. With the help of this risk assessment, the impact of the measure in terms of the potential loss and / or probability of risk are documented. In order to document the sustainability of the measures, or appropriate control of them, the identified risks are periodically re-evaluated. These evaluations shall be documented as subsequent reviews.

### 5.1.9 The risk owner

Each identified risk is assigned to at least one member of the **SEEBURGER INFORMATIK EOOD** Management Board “risk-owner”. These risk-owners are also involved in risk treatment. As part of the regular risk re-evaluation phase, they have an influence on the risk assessment and the currently defined risk treatment measures. This is shown in the figure below.



## 5.2 Controls in the ISAE 3402 audit

### 5.2.1 RM\_01 - "Risk management" guideline

#### Definition

Risks are identified in a formal process. This process is documented in an information security management document and implemented based on a risk management program.

#### Implementation

The information security management document entitled "Risk Management" describes the formal process used to identify and assess risks. It also describes how risks are managed by deriving and tracking measures. The information security guideline is regularly adapted to changing boundary conditions and audited by an external third-party organization as part of the annual ISO/IEC 27001 certification.

### 5.2.2 RM\_02 - Systematic risk management

#### Definition

Risks are managed as part of the risk management process. Here, risks pass through the following stations:

- Identification
- Assessment
- Derivation of measures for minimizing the risk
- Reassessment of the risk

#### Implementation

1. Risks are identified using the top-down or bottom-up methodology.
2. To identify risks on a structured base, it is required that information security requirements are defined as a baseline. Against this baseline internal audits must be performed. **SEEBURGER INFORMATIK EOOD** starts to implement the security requirements of the BSI Basic Protection Compendium as baseline.
3. Evaluation by the relevant experts and measures for minimizing, avoiding or delegating risks of the **SEEBURGER INFORMATIK EOOD** management team are proposed in collaboration with the risk manager and experts.
4. Based on the decision made by the management team, the measures are implemented, or the risk is adopted by the management team.
5. In a semi-annual assessment, the risks are regularly (re)assessed.

### 5.2.3 RM\_03 - Regular risk reassessments

#### Definition

The risk manager regularly inquires experts with risks assigned to them for reassessment. During reassessments, progress is checked while the adopted measures are implemented.

## Implementation

On a semi-annual base, the Information Security department creates risk reports. These risk reports contain new identified risks in the last half year and risks, which must be re-evaluated. The experts of the specific department have a three-month period to evaluate the risks. This will give them time to discuss the current or initial evaluation of the risk and to prioritize or track the state of the mitigation responses. Regular meetings with the responsible board member are part of the iterative (re)-evaluation process of risks.

After the semi-annual risk evaluation phase of a board area, the next evaluation phase starts three months later (e.g. Q1 → Q3). In a worst-case scenario, new risks identified in Q1 are presented to the board member six months later. For this period the ownership of new risks is unclear. Because of the rhythm of the (re)-evaluation it is required, that at the end of the evaluation phase (e.g. Q1) a risk report with new risks identified during the last half year sent to the experts and the board member.

## 6. User & Access Management

### 6.1 Concept and implementation

The User Access Management system is designed to prevent unauthorized users from accessing an IT service or application system. Essentially, the User Access Management system fulfills the specifications defined in the Information Security Management system.

If any changes are made relating to the user, roles and access rights, the User Access Management system accesses the **SEEBURGER INFORMATIK EOOD** Cloud Services systems and applications.

There are three levels that must be accessed to perform the Managed Services:

- Application,
- Operating system,
- Database.

The following regulations apply here:

- Only authorized users are permitted to access certain resources,
- Access is limited to the permissions and time period required for the respective application,
- Allocated access rights and actual accesses are documented.

Access is monitored via a central application. Access data is stored in encrypted format. Systems are accessed via a defined rights and role concept. Access permissions are requested via a central change management process.

## 6.2 Controls in the ISAE 3402 audit

### 6.2.1 UAM\_01 - Cloud Services permission concept

#### Definition

A permission concept for accessing EDI/B2B/GTS systems in the Cloud Services department is available and updated at regular intervals.

#### Implementation

The permission concept for accessing EDI/B2B/GTS systems is documented and communicated within the **SEEBURGER INFORMATIK EOOD** organization.

The document is managed centrally in a document management system. A history of changes to the document is kept. New main versions of the document are checked and released in a formal approval process carried out by the head of Managed Services. The relevant valid version is stored centrally in the **SEEBURGER INFORMATIK EOOD** intranet and can be accessed by all employees.

### 6.2.2 UAM\_02 - Implementing the password guideline

#### Definition

A global password guideline is provided, communicated, technically implemented and enforced by the Active Directory.

#### Implementation

IT is responsible for the password directory for the SUB domain.

The following password policy is enforced for all **SEEBURGER INFORMATIK EOOD** domains automatically.

	Regulation	Definition
Account types	<b>Standard Account</b>	Min. PW length: 12 characters, complex password in addition either a conditional access policy or MFA are recommended.
	<b>Standard Account “Plus”</b>	Min. PW length: 12 characters, complex In addition either a conditional access policy in MS Entra or MFA are required for the specific application.
	<b>Admin Account</b>	Min. PW length: 16 characters, complex MFA.: required
	<b>Higher Admin Account (such as domain admin accounts etc.)</b>	Min. PW length: 24 characters, complex MFA.: required
	<b>Service Accounts</b>	Min. PW length: 24 characters, complex MFA.: if feasible

General rules applying for all account types	<b>Password Complexity</b>	At least 3 of the following: Upper, lowercase letters, numbers and symbols
	<b>Password Maximum Length</b>	not configured
	<b>Password Expires</b>	event based
	<b>Lockout Threshold</b>	6 failed attempts
	<b>Password History Kept</b>	10 iterations
	<b>Blocking and resetting time of the account</b>	1 h
	<b>Passwords must not contain parts of the first, last, or logon name</b>	configured

### 6.2.3 UAM\_03 - Assigning permissions in the Active Directory

**Definition**

Access to general resources/information is requested in a formal process (incident). The relevant data owner is responsible for granting approval.

**Implementation**

Requests are submitted via e-mail. When the mail is sent, an incident is created automatically at the **SEEBURGER INFORMATIK EOOD** Service Desk. If it is a CR, the relevant IT employee generates a Change Request (CR) from the incident, which is then assessed. At **SEEBURGER INFORMATIK EOOD**, an Access Management Change is categorized as a Complex Change, which means that an approval by the data owner of the resource/information is always needed. This is ensured by the “four eyes” principle. With the approval of the data owner in the automated process of the identity and access management application the access is granted.

### 6.2.4 UAM\_04 - Access control for customer systems

**Definition**

A process for requesting and granting access to customer systems within Cloud Service is defined, documented and technically regulated.

The technical implementation of the assignment of rights ensures that access can only be requested via the defined and documented path and that the assignment of rights is always carried out via an approval process and is logged in a traceable manner.

**Implementation**

The request process for accessing customer systems is documented and communicated within the **SEEBURGER INFORMATIK EOOD** organization.

The document is managed centrally in a document management system. A history of changes to the document is kept. New main versions of the document are checked and released in a formal approval process carried out by the head of Cloud Services. The relevant valid version is stored centrally in the **SEEBURGER INFORMATIK EOOD** intranet and can be accessed by all employees.

As part of the initial training plan, new employees in the Cloud Services department receive training regarding the process documentation.

### 6.2.5 UAM\_05 - Removing user access privileges

#### Definition

User accounts on the Active Directory (AD) (access to **SEEBURGER INFORMATIK EOOD** networks) that are no longer required are blocked promptly (within three days) by IT Admin. Users are deactivated automatically when the “Valid To” date expires.

#### Implementation

- Change of employees
  - Change of division
  - Change of subsidiary
- Change of employees
  - Employee check-out list from HR (DE)
  - HR Sofia: Generates incident by mail sent to [edv-helpdesk@seeburger.de](mailto:edv-helpdesk@seeburger.de)
  - Intranet

#### Check of effectiveness

Audit every three months through information security:

- Actual incident available prior to retirement.
- Was incident processed on time?
- Was account processed in AD in line with incident specifications?
- Was the “Valid To” date set?

### 6.2.6 UAM\_06 - Expiry of user permissions for the EDI application

#### Definition

Internal **SEEBURGER INFORMATIK EOOD** user permissions for productive EDI CS applications are limited to a maximum of 90 days. If the permissions are not renewed, the central Access Management Tool automatically blocks access.

#### Implementation

The central Access Management Tool limits the internal access permissions for customer systems to a maximum of 90 days. Longer access times cannot be selected and are therefore not technically possible.

After the authorization period elapses, the central Access Management Tool blocks access to the customer system automatically.

## 6.2.7 UAM\_08 - Checking users and rights for productive customer systems

### Definition

Regular checks are performed to ensure that no unauthorized users have been created on the application level of BIS6 customer systems.

### Implementation

Authorized users are selected and added to a white list. Regular checks are performed to determine whether the users on the application level correlate with those in the white list. New users and changes are added/modified via a Change Request in the white list.

## 6.2.8 UAM\_09 - Separating Access to Cloud Services from Corporate Access Management

### Definition

All Cloud Service relevant activities require an AD authentication and an additional authorization in the central access application. This ensures that only authorized employees can gain access to customer-relevant data.

### Implementation

- Only authorized users managed by the **SEEBURGER INFORMATIK EOOD** Active Directory can access the central access application.
- Employees who require access to productive customer systems in the Cloud Services area due to their job description requires an additional authorization in the central access application.
- The Cloud Services Domain Account is requested by way of the central Change Management process and must be approved by the Cloud Services division.

## 6.2.9 UAM\_11 - Assigning administrative rights for productive customer systems on an application level

### Definition

On productive customer systems, **SEEBURGER INFORMATIK EOOD** employees are only allocated application rights that were defined during the Access Management process for the assigned employee role.

### Implementation

Employee roles are defined in the Access Management process and assigned to the employee during the change process. Existing Access Management roles on productive customer systems are checked on a regular basis. The application rights assigned for each role are compared with the rights defined during the Access Management process. Checks are performed once a month by way of an automatically generated report documented during the Incident Management process.

## 6.2.10 UAM\_12 - Network security between the corporate and the cloud services networks

### Definition

Cloud Systems are separated from other networks. Access to Cloud Systems is only possible over the IT Admin Access tool or over a specific tunnel service provided and managed by the central Cloud Services Access Management Tool.

### Implementation

**SEEBURGER INFORMATIK EOOD** has defined and implemented network zones and subzones. Networks are implemented within each subzone and separated according to network type. Each network type is assigned a defined protection class (low, medium, high, very high). Strict communication rules apply between zones, subzones, networks and each subnet or device within the network. Communication from any network to the cloud service networks is denied by default. Only very few and specific communication channels are implemented to allow administrative and operational access to systems and applications within the cloud.

For administrative access to Cloud Systems a specific IT Admin access tool is required. This tool is located in a separate network accessible over a jump station where only defined IT admins can login.

For standard users access to Cloud Systems is only possible via a tunnel which is provided by the central Cloud Services Access Management Tool.

## 7. Physical Security

**SEEBURGER INFORMATIK EOOD** subdivides the protection requirement zones of physical security into a total of 6 zones. The protection requirements and therefore the restrictions resulting from physical security measures increase in line with the zone numbers. As part of a protection requirements analysis, the protection requirements of the information are determined as per ISO/IEC 27001 and corresponding protective measures are derived.

Information outlined in ISO/IEC 27001 includes:

- the employees,
- the organizational structure at **SEEBURGER INFORMATIK EOOD**,
- contracts with customers, partners and service providers,
- the process organization,
- products, products and services,
- the IT infrastructure,
- the virtualization platform,
- the **SEEBURGER INFORMATIK EOOD** building and
- the data centers used by **SEEBURGER INFORMATIK EOOD**.

Not all buildings used by **SEEBURGER INFORMATIK EOOD** have all zones. Normal office buildings usually have zones zero to three whereas data centers used by **SEEBURGER INFORMATIK EOOD** have zones zero to five.

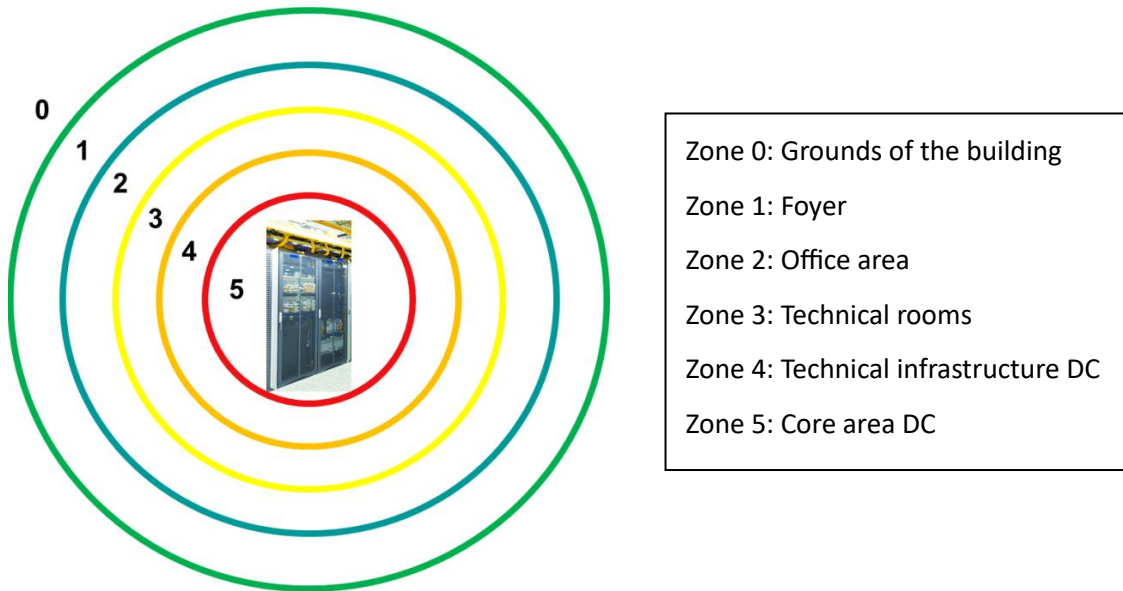


Illustration 12: Protection requirement zones

The EDI/B2B/GTS services within the scope of the ISAE 3402 audit is provided in zone five of the data centers used by **SEEBURGER INFORMATIK EOOD**. Since the physical security i.e. control of employees’ access to systems, is essential in enabling the data centers to reach their availability targets, the controls in ISAE 3402 focus both on access control processes and the availability measures of data centers used by **SEEBURGER INFORMATIK EOOD**.

### 7.1 High availability

The redundancy of all relevant systems ensures the high availability of the services offered. The diagram in the following figure illustrates this.

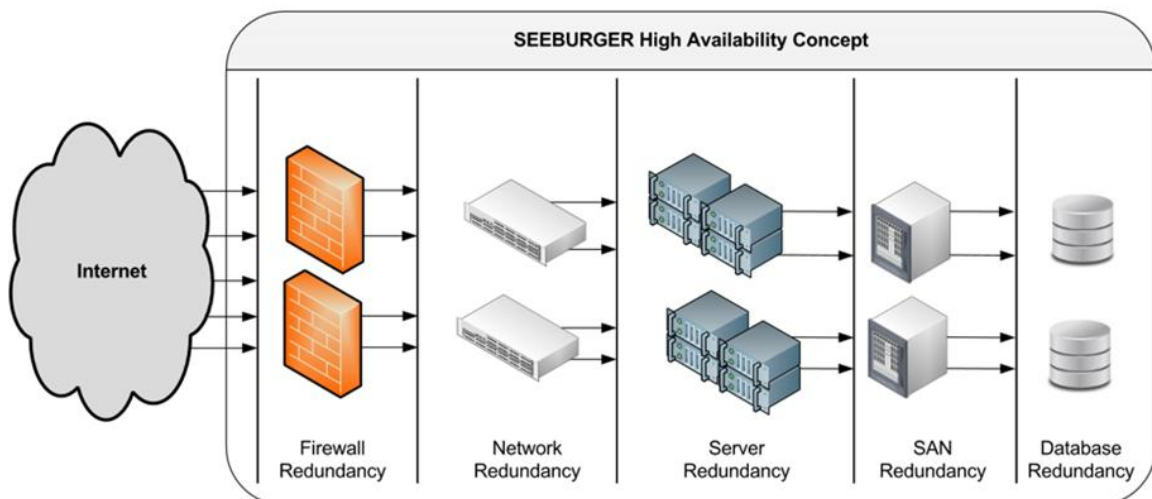


Illustration 13: High availability (schematic)

## 7.2 Controls in the ISAE 3402 audit

### 7.2.1 PS\_01 - Access control to data centers

#### Definition

Access rights to the data centers used by **SEEBURGER INFORMATIK EOOD** are allocated and checked in a formal multi-stage process.

#### Implementation

Access to the data center must be requested from a **SEEBURGER INFORMATIK EOOD** query representative (QR), who forwards the query to the DC administration team. The DC administration prepares the access authorizations and issues the personalized PIN / card to the QR. The QR passes the access authorizations to the person who submitted the request. If the working relationship ends or there is a switch to another department, the QR collects the DC access authorizations from the employee. The list from the QR and person with access authorization is checked annually by DC Administration.

### 7.2.2 PS\_05 - Managing equipment

#### Definition

All inputs and outputs are implemented by **SEEBURGER INFORMATIK EOOD** employees and managed in a central database. The Global Head of Governance, Risk and Compliance checks the correctness on an annual basis.

#### Implementation

All equipment orders are placed with assistance from tools. When the order is created using a procurement request (PR), a unique PR number is generated. If a standard item already stored in the system is ordered, approval is granted according to the “four eyes” principle. If the item is not standard, however, technical approval is required before the final approval.

The unique PR number makes it possible to uniquely assign the business letters associated with the purchase of the equipment. When the equipment is delivered, the inventory is created immediately after the goods are received by assigning and including a unique **SEEBURGER INFORMATIK EOOD** number in an asset database.

### 7.2.3 PS\_07 - Data center security

#### Definition

Control owner reviews attestation report(s) of the data center providers to ascertain that physical access and environmental controls are implemented and complied with. Follow-up activities are carried out in case of relevant deviations.

#### Implementation

**SEEBURGER INFORMATIK EOOD** has ordered the following services:

- Fixed connections,
- Internet connection,
- Server housing (air conditioning, power supply, emergency power management and fire protection (FAS, extinguishing system and early fire detection) and
- The focus of the security assessment based on the review of the ISAE reports is evidence that the data center infrastructure used by **SEEBURGER INFORMATIK EOOD** in AT1, AT4 and AT5 as well for the TelemaxX data centers is maintained correctly.

## 8. Go-Live Management

### 8.1 Process description

The Go-live process describes the transfer of an initial project to Service Operation. After successfully passing on at least one productive process, the Cloud Service Operation assumes responsibility for the system and any other related productive process is handed over to Cloud Service Operation.

In case an initial project contains several milestones and several processes go productive at different times, these are part of the handover process.

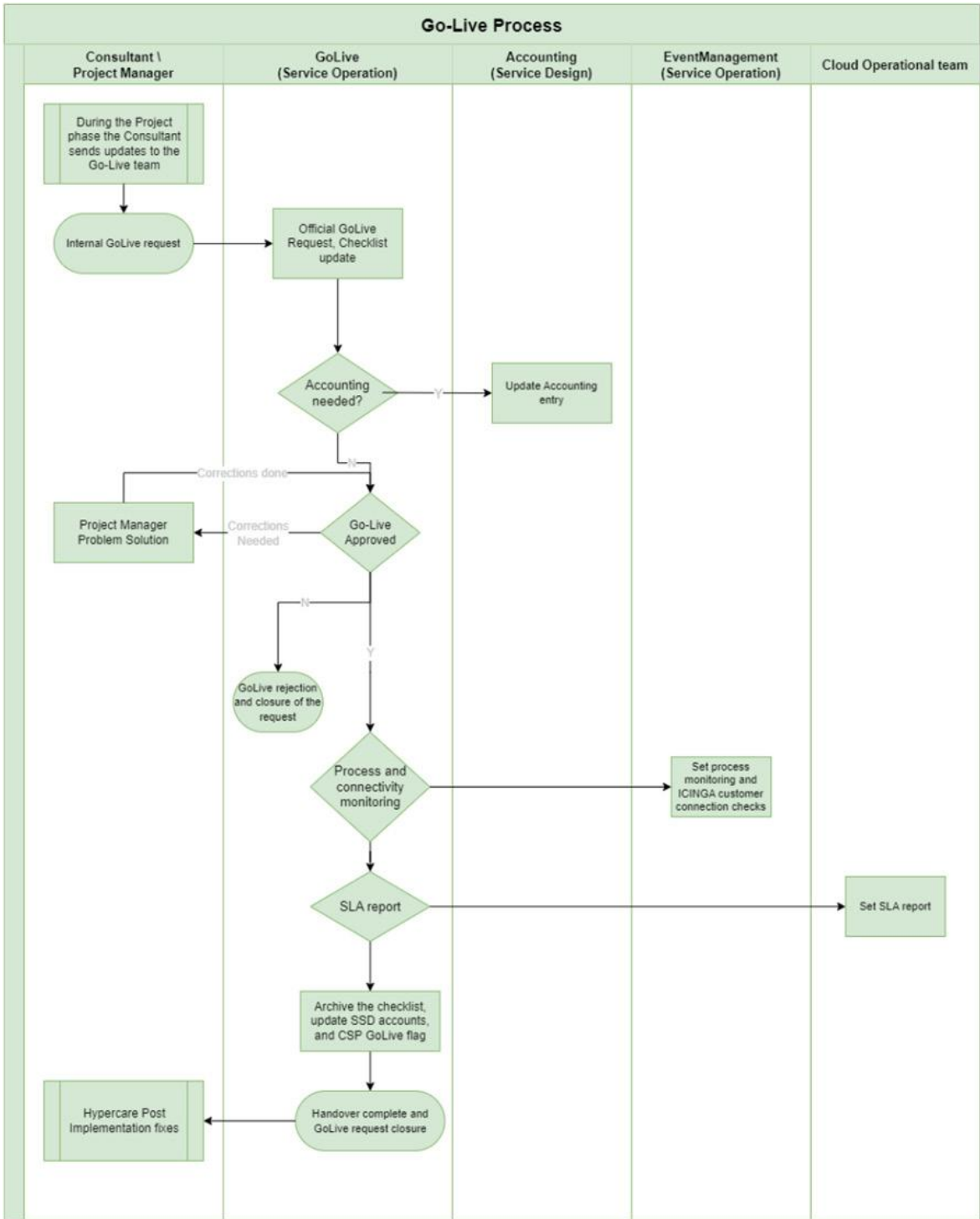


Illustration 14: Go-Live Process

**Role description:**

**Consultant / Project Manager:**

The consultant / project manager is responsible for the configuration, the documentation and the initiation of the go-live process. He also bears the responsibility until the completion of the go-live process.

The consultant / project manager has to send a given “go-live” mail to service.am, application services and GoLive.MS, which contains all relevant information (e.g. process, partner, communication, contacts) in order to start the live delivery process.

**Operation Team:**

The operation team is responsible for ensuring that all necessary cloud services standards are maintained and ensured. This includes the correct monitoring and the transfer to the billing.

**Service Operation:**

The Service Operation Team is responsible for activating invoicing, storing the contractually agreed SLA in the **SEEBURGER INFORMATIK EOOD** Service Desk, and creating new customer users (as required).

Only the **SEEBURGER INFORMATIK EOOD** internal Go-live process is valid for a successful handover to Cloud Services. The notification of the customer about the successful go-live is part of the initial project.

## 8.2 Controls of the ISAE 3402 audit

### 8.2.1 GO\_01 - All initial go-lives are documented in a go live request

**Definition**

BIS6 initial go-lives are documented and authorized in a go live request.

**Implementation**

To generate a go live request the project manager / consultant sends an e-mail to GoLive.MS@seeburger.de, which automatically generates a unique incident ID or can directly create a go live request within the **SEEBURGER INFORMATIK EOOD** Cloud Service Portal (CSP). This go live request is assigned to the Service Operations team for processing. The development of the processing is documented in the go live request until successful completion.

**Control of the effectiveness of the control**

A monthly report is generated showing all go live requests of the past month. The report generated is checked by the Service Operations team, and any defects in request processing are analyzed, corrected and, if necessary, measures taken for future avoidance.

### 8.2.2 GO\_02 - Go-Lives are processed within five days

**Definition**

The Service Operations team will start processing a BIS6 initial go live request within five working days.

**Implementation**

An initial go-live request is assigned to the queue of the responsible operating team. The operation team checks this queue and starts the processing within five working days from the opening of the go live request.

### **Control of the effectiveness of the control**

To control the effectiveness, a monthly report is produced containing the following information and the report is also verified by the operations team:

- Date and time of the go live request opening
- Start of processing (with date and time)
- Name of the Request Opener
- Subject of the request (Initial Go-Live)
- Name of the request Owner
- Completion of the request (with date and time)

#### **8.2.3 GO\_03 - The Go-live handover check list is to be completed and stored centrally**

##### **Definition**

For each BIS6 initial - go-live, a hand over is created that contains all relevant and necessary information for the go-live. These documents are stored centrally in a clearly assignable customer folder.

##### **Implementation**

For each BIS6 initial go-live, the Service Operations team creates a separate handover, which is saved in the customer folder when the handling is complete.

##### **Control of the effectiveness of the control**

The hand over lists are stored centrally in the customer folder of the respective customer. The operations team is responsible for the completeness and correctness of the information stored in the handover. The check lists are checked monthly for completeness and correctness by the operations team.

## **9. Monitoring Management**

### **9.1 Process description**

As soon as a new service is productive and has been successfully transferred to the Cloud Services operating team by the **SEEBURGER INFORMATIK EOOD** project manager, real-time monitoring and event management is activated for this service. The main objectives of real-time monitoring and event management are:

- identification of problems and errors during productive processing of EDI Cloud Services,
- pre-classification of the error and
- generation of the incident in the **SEEBURGER INFORMATIK EOOD** Incident Management system to start the Incident Management process.

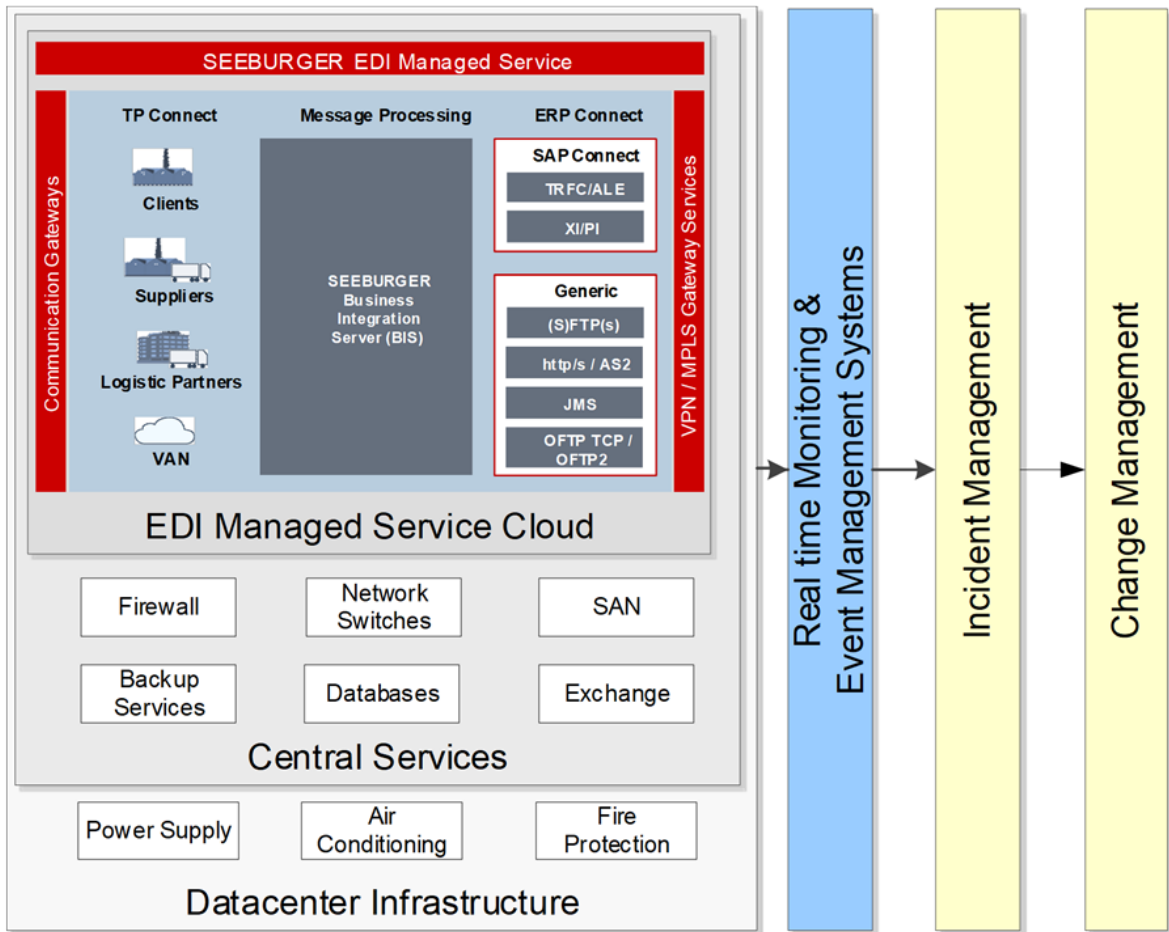


Illustration 15: Implementation of new services (schematic)

The checks described in the following are defined based on the importance of secure productive operations.

## 9.2 Controls in the ISAE 3402 audit

### 9.2.1 EM\_01 - Initial set-up of the system monitoring system

#### Definition

Within the EDI Cloud Services, **SEEBURGER INFORMATIK EOOD** uses a monitoring system to monitor important components fully automatically such as networks, servers and storage as well as applications and queues. The monitoring system ensures that error events are detected immediately. On every newly installed EDI system, a series of standard tests is set up, activated and tested in the system monitoring system during system deployment or by the go live at the latest.

#### Implementation

The system monitoring system is set up in a multistage process. A productive system undergoes several development stages here. The IT infrastructure team implements the basic installation of the **SEEBURGER INFORMATIK EOOD** business integration server on a virtual host. On completion of the basic installation, this system is transferred to the Cloud Services division. During the second phase, the current state of the installation is checked and accepted, and the standard system

monitoring system is set up. The tests are conducted independently of the customerspecific installation and standardized to suit all productive systems. Examples of standard monitoring tests include e.g. availability of storage space, RAM, CPU and application-specific parameters.

When the standard monitoring system is completed, it is transferred to **SEEBURGER INFORMATIK EOOD** Consulting. During the initial project, customer-specific installations are set up and tested in collaboration with the customer. On successful completion of the installation and test phase, Consulting hands the system back to the Cloud Services division as part of the go live process, which represents a dedicated handover of responsibility. The installation implemented by Consulting is accepted and then the customer-specific part of the system monitoring system is set up. This can involve setting up special tests to check the connection to the customer's ERP system, for example. The go live signals the end of the set-up phase.

### 9.2.2 EM\_02 - Initial set-up of process monitoring

#### Definition

A process monitoring system monitors the processing errors of individual EDI processes and errors are reported to Incident Management. The process monitoring system must be set up and activated before the go live is announced (formal handover to the MS operating team) (part of "go live handover" checklist).

#### Implementation

While the system monitoring system monitors the availability of the application, the connections and the resources required for faultless EDI operation, the process monitoring system monitors the completeness and correctness of messages handled within the implemented processes. Here, a "process" is defined as follows:

EDI messages are processed within a defined process sequence. The EDI system executes these processes as well as the process steps defined within the process (components).

If an error occurs within a component during process handling (e.g. due to an error in the received message), the process switches to error status and is assigned a corresponding process status.

Examples of process errors include:

- Unexpected termination of a process,
- Errors within a processing step or
- Excessive runtime of a process.

The purpose of the process monitoring system is to identify faulty processes at regular intervals as well as transfer this information to an Event Management System (component of the process monitoring system). The Event Management System consolidates and qualifies errors according to defined criteria and generates incidents in the Incident Management System in line with defined rules.

During the go live process, Consulting hands over the completed EDI system to the Managed Services operating team. The MS operating team checks the configuration of the process monitoring

system to determine whether process monitoring has been activated for the transferred EDI system and the corresponding client(s).

The initial set-up of the process monitoring system is the final step before the operating team rolls out the Managed Services system.

**9.2.3 EM\_03 - Monitoring of the monitoring system**

**Definition**

Productive EDI systems are monitored by various monitoring systems (system monitoring and process monitoring systems) on a 24/7 basis. It must be ensured that all relevant monitoring checks are also performed. The operating team must respond to incomplete or abandoned checks with defined actions.

**Implementation of process monitoring**

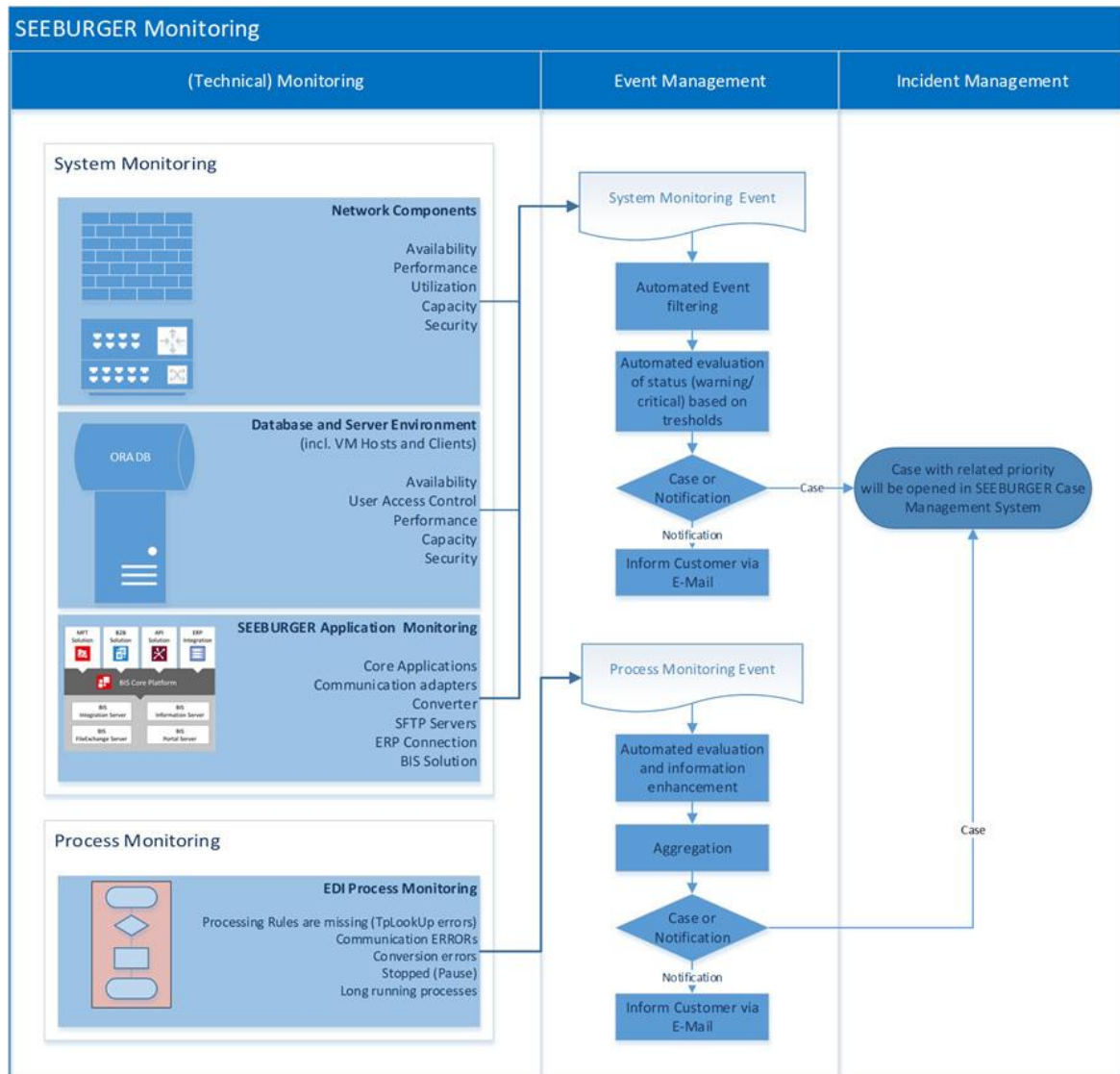


Illustration 16: Monitoring process monitoring checks

The process monitoring system is monitored from the system monitoring system. The fact that there are two different applications on different platforms ensures that mutual interference is excluded in the event of a fault.

A minimum of one scheduler is configured for each host on the process monitoring system. The process checks (scheduler) are performed during the intervals stored in the scheduler configuration. In the system monitoring system (Icinga), an analog check that performs the following tests is scheduled for each host and configured scheduler:

Check whether the last two process monitoring schedules were completed. The Icinga check monitors whether any checks were performed within the last 30 minutes and whether they were successful or failed:

1. If one of the two checks fails, a warning is issued
2. If both checks fail, an error message is issued and a case is created in the **SEEBURGER INFORMATIK EOOD** Case Management System and processed by the operating team.
3. A case is also created if no checks were performed within the defined 30-minute time frame.

#### **Implementation of system monitoring**

The redundant design at different locations ensures the high availability (HA) of the system monitoring system. The operating team monitors the system monitoring system (Icinga) manually. If the system monitoring system no longer functions, the operating team can identify this from the system monitoring frontend and a case is then generated and processed.

#### **9.2.4 EM\_04 - Error identification using the system monitoring system**

##### **Definition**

Monitoring checks are set up in such a way that errors are detected by defined threshold values / status and incidents are generated in the system monitoring system. The operator is notified of these events. Moreover, defined error events generate cases that are processed in the incident management process.

##### **Implementation**

The threshold values that change the status of the monitoring checks are defined centrally and are equally valid for all productive systems within the scope of the ISAE 3402 audit.

#### **9.2.5 EM\_05 - Error identification using the process monitoring system**

##### **Definition**

If errors occur when messages are processed in productive EDI systems, these are identified by the process monitoring system and transferred as a case or added to an existing case to the case management system together with a unique reference relating to the error. Each case will be handled as part of the incident process.

## Implementation

EDI Process errors are detected by the monitoring system and forwarded to the case management system. Within the case management system:

- A rule engine evaluates each error by mathematical expressions.
- Additional information is added to the process error record to provide further details for resolution and information to the customer or its trading partner.
- Multiple rules are triggered in succession based on a weighting.
- Each rule can add more detail to the case record or trigger a specific action.
- The criticality of a case is determined and defines the priority of the further processing of a case.
- Same EDI process errors are added to an existing case rather than opening many cases for the same issue. Speeding up handling and resolution of issues significantly.
- If a case requires to involve customers or trading partners into further root cause evaluation a regular incident is opened at the Servicedesk.

The handling of cases follows the incident management process. Thus, the same Incident Management SLA criteria applies. The advantages of the case handling in the new Case Management system are:

- Much faster evaluation of a process error,
- More specific enrichment of further details to analyze and solve a case,
- Faster information to customers and trading partners if issues are detected which needs to be solved on their site,
- Provides new options to further automate error and incident handling.

## 10. Incident Management

### 10.1 Process description

The purpose of the Incident Management process is managing the incident lifecycle holistically from the moment of creation to solution identification on the assumption that compliance with the contractually agreed SLA is guaranteed as well as immediately restoring service following a disruption. The following graphic illustrates all building blocks, secondary roles and their responsibilities in a RACI flow diagram.

The tool-based processing sequence is documented fully and transparently in the **SEEBURGER INFORMATIK EOOD** ticket system, whereby the **SEEBURGER INFORMATIK EOOD** Service Desk serves as a Single Point of Contact (SPOC) that can be reached via the internet portal, e-mail or telephone (see below).

No other communication channels are authorized for Incident Management.

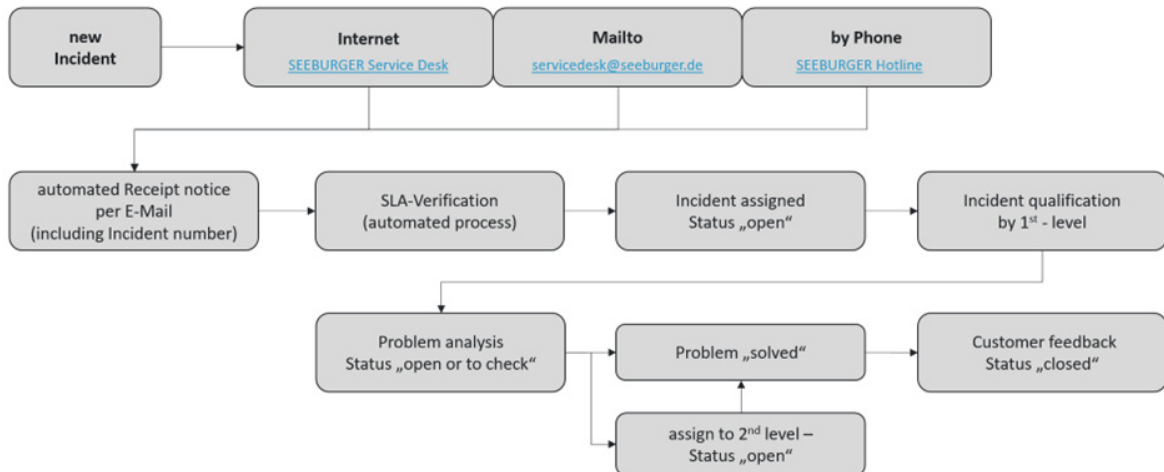


Illustration 17: Incident Management Process

### Responsibilities and tasks within the Incident Management process:

1. 1st level employees:
  - Responsible for resolving incidents and process events
  - Escalation to 2nd level employees
2. 2nd level employees:
  - Responsible for resolving complex incidents in collaboration with 1st level employee
  - Supporting Problem Management and the team coordinator
3. Team coordinator:
  - Assuring the quality of incident processing
  - Ensuring SLA compliance
  - Responsible for escalation to the 3rd level along agreed communication channels
4. Incident Manager (leader of Cloud Service Operating Team)
  - Responsible for the Incident Management process
  - Responsible for the efficiency and effectiveness of processes
  - Continuous improvement of the Incident Management process
  - Ensuring and complying with all defined KPI

**SEEBURGER INFORMATIK EOOD distinguishes between three SLA categories that are contractually governed with the customer:**

Priority	Agreed SLA Type		
	BASIC	ADVANCED	PREMIUM
<b>Prio 1</b>	24 hours a day, including Sundays and public holidays	24 hours a day, including Sundays and public holidays	24 hours a day, including Sundays and public holidays
<b>Prio 2</b>	24 hours a day, including Sundays and public holidays	24 hours a day, including Sundays and public holidays	24 hours a day, including Sundays and public holidays
<b>Prio 3</b>	Monday - Friday from 9 am to 5 pm (excluding public holidays at <b>SEEBURGER INFORMATIK EOOD's</b> location)	Monday - Friday from 7 am to 8 pm (excluding public holidays at <b>SEEBURGER INFORMATIK EOOD's</b> location)	24 hours a day, including Sundays and public holidays
<b>Prio 4</b>	Monday - Friday from 9 am to 5 pm (excluding public holidays at <b>SEEBURGER INFORMATIK EOOD's</b> location)	Monday - Friday from 7 am to 8 pm (excluding public holidays at <b>SEEBURGER INFORMATIK EOOD's</b> location)	24 hours a day, including Sundays and public holidays
SLA Response Time			
<b>Prio 1</b>	max. 4 Clock Hours	max. 2 Clock Hours	max. 1 Clock Hours
<b>Prio 2</b>	max. 8 Clock Hours	max. 4 Clock Hours	max. 2 Clock Hours
<b>Prio 3</b>	max. 2 Business Days	max. 8 Business Hours	max. 8 Clock Hours
<b>Prio 4</b>	max. 4 Business Days	max. 2 Business Days	max. 1 Calendar Day

**Incident priorities are defined as follows:**

Priority	Classification by SEEBURGER INFORMATIK EOOD	Description
<b>Prio 1</b>	“Emergency”	Serious interruptions of the Cloud Service productive operation at the Risk Transfer Point to the CUSTOMER and/or to the Trading Partners. This is caused either by a complete failure of the Cloud Service or by essential core functions. The malfunction must be

		<p>dealt with immediately in order to avoid serious damage to the CUSTOMER.</p> <p>Example: Complete Cloud service is not available (e.g. failure of Cloud core system or database).</p>
Prio 2	“Critical”	<p>Critical interruptions of Cloud Service productive operation at the Risk Transfer Point to CUSTOMER and/or Trading Partners. This is either caused by malfunctions of the Cloud Service or unavailable subfunctions. The malfunction requires fast processing, as a longer-lasting malfunction can cause serious interruptions in all processes of the production system.</p> <p>Examples: Significant performance problems of one or more IT components.</p> <p>One or more of the components listed in Appendix A, point 2 is/are not available.</p>
Prio 3	“Non-Critical”	<p>Uncritical disruptions to Cloud Service productive operations. This is either caused by a malfunction or unavailable feature in the Cloud Service.</p> <p>Example: If a file is not deliverable because a partner / system is not reachable, the service will execute the number of configured delivery attempts within a defined time unit. If a file is finally not deliverable, an error is raised and the <b>SEEBURGER INFORMATIK EOOD</b> support starts solving the error.</p>
Prio 4	“Minor”	<p>All other incidents, including but not limited to those where there are no or only minor interruptions to the Cloud Service productive operation at the Risk Transfer Point to CUSTOMER and/or Trading Partners. This is either caused by a malfunction or unavailable function in the Cloud Service, which is not needed daily or regularly.</p>

**10.2 Controls in the ISAE 3402 audit**

**10.2.1 IM\_01 - Service Level Agreements and priorities in Incident Management**

**Definition**

Contractually agreed Service Level Agreements for each specific customer are stored in the **SEEBURGER INFORMATIK EOOD** Service Desk.

## Implementation

The SLAs and service times contractually agreed with the customer form the basis for processing incidents. These form part of the service and performance description for each specific customer and are stored in the **SEEBURGER INFORMATIK EOOD** Service Desk.

When a contract is concluded with the customer, the signed documents are digitalized and stored in the **SEEBURGER INFORMATIK EOOD** master data system (MDM). The Service Level Agreement modules relevant for incident processing are transferred to the **SEEBURGER INFORMATIK EOOD** Service Desk. The MDM system is also a data source here. An automated comparison is performed on a daily basis to ensure data consistency between both systems. If any discrepancies are identified, a ticket is generated and a manual follow-up inspection is initiated.

### 10.2.2 IM\_02 - Escalation of the Initial Response Time (IRT)

#### Definition

For priority level 1 (emergency) and 2 (critical) incidents, an escalation process is initiated after 80 % of the response time elapses.

#### Implementation

Response times for incidents form part of “Premium” quality Service Level Agreements contractually agreed with the customer. The escalation process handles the prioritization of levels 1 (emergency) and 2 (critical) because related faults can have a severe impact on the customer’s EDI business processes. The processing of such faults has to start within the defined response times, which is why an escalation process is initiated once 80 % of the respective response time has elapsed.

When a ticket is opened, it is assigned an entry time stamp, the SLA of the customer and prioritization information. The response times agreed contractually with the customer are stored in the ticket system.

When a priority 1 or 2 incident reaches 80 % of the agreed response time and an advisor has not yet started to process the incident, the ticket system sends an escalation mail to a defined target group automatically. Members of the group then initiate the actions required to ensure the ticket is processed in compliance with SLA.

## 11. System-Based Change Management

Every modification made to a productive system poses the risk that modified objectives will compromise information security. This may result in consequential losses for the customer. The following sections describe the measures implemented, continuously reviewed and improved by **SEEBURGER INFORMATIK EOOD** to minimize risks of this kind.

Whether in-house development or products from reputable manufacturers, applications have vulnerabilities and contain errors that could be exploited by attackers, even if quality standards are high. Like many other manufacturers, **SEEBURGER INFORMATIK EOOD** reacts promptly to such

threats by launching new hotfixes. These eliminate the vulnerability efficiently or rectify the error identified. **SEEBURGER INFORMATIK EOOD** accumulates the individual hotfixes for a patch within a release. The principle “Never Touch A Running System” has fatal consequences in terms of the security level of applications because without regular security updates, vulnerabilities can accumulate. Consequently, the application ages over time and becomes a steadily growing operating risk. **SEEBURGER INFORMATIK EOOD** continuously updates systems and applications in order to minimize the associated risks.

Patch and software update management is a central component of the **SEEBURGER INFORMATIK EOOD** information security concept. In the patch and update management system for **SEEBURGER INFORMATIK EOOD** applications, **SEEBURGER INFORMATIK EOOD** distinguishes between the following types:

- Bugfix/Hotfix installation
- Service pack installation
- Solution update / adaptation

**SEEBURGER INFORMATIK EOOD** Development provides all the necessary installation packages. Prior to delivery, these packages are tested and approved in a Quality Assurance process integrated in the development.

Implementation is based on the System-Based Change Process.

11.1 Process description

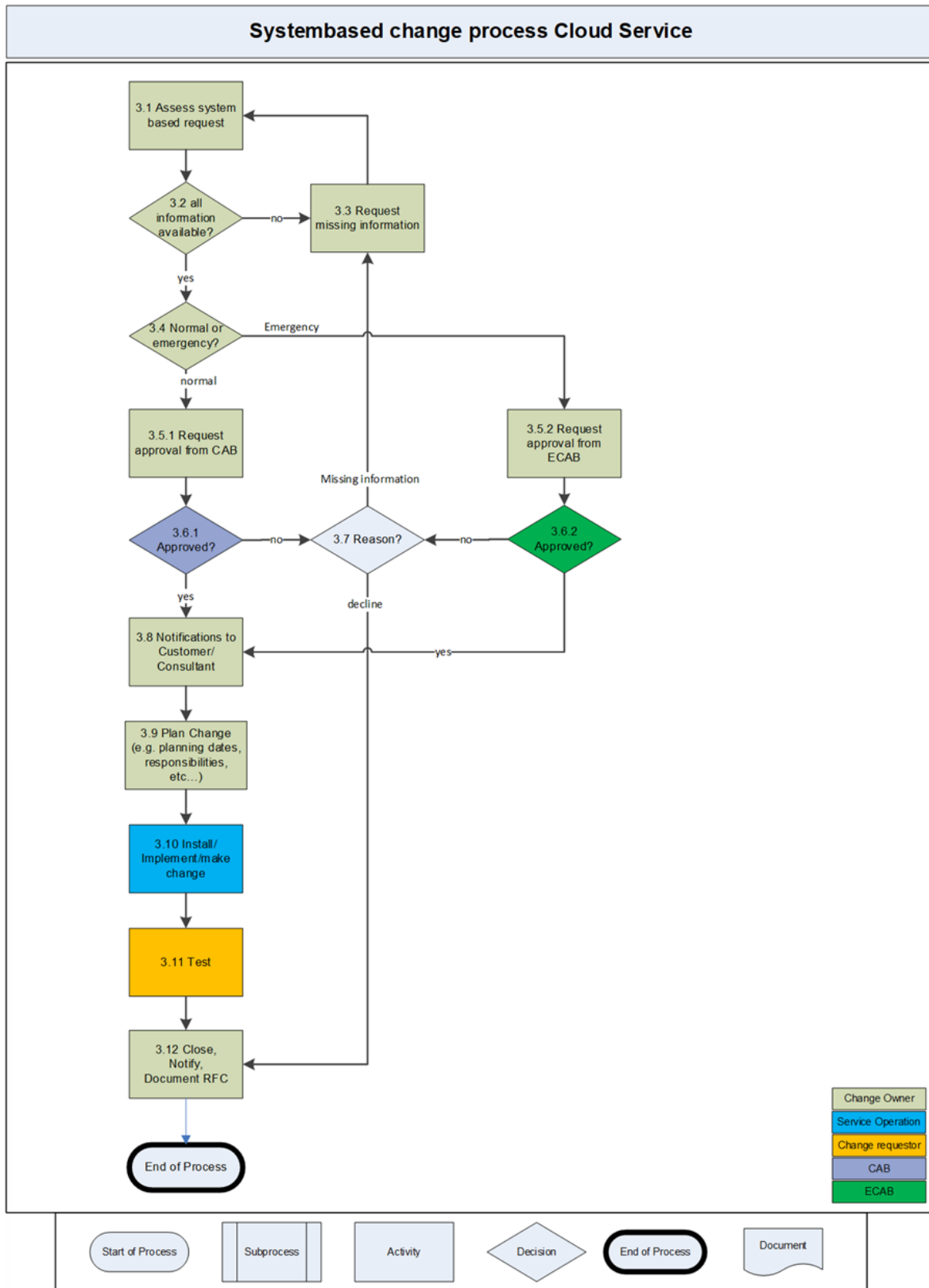


Illustration 18: Change Management Process

The System-Based Change Process illustrated here describes the procedure for planning and implementing patches and updates of **SEEBURGER INFORMATIK EOOD** applications in Managed Services.

Strict adherence to the process guarantees the controlled evaluation, planning and implementation of changes to the **SEEBURGER INFORMATIK EOOD** application. Defined measures should be introduced to exclude or minimize any risks identified during planning. Furthermore, defined test criteria should make it possible to measure and examine the success of a change. The “four eyes principle” of a defined approval process allows the identification of planning errors and provides additional security.

Documenting the individual parameters of a Change Request makes it possible to conduct retrospective assessments relating to the implementation and success of a change and allows the implementation of derived improvements for future changes.

## 11.2 Controls in the ISAE 3402 audit

### 11.2.1 CM\_01 - Documented Change Management process

#### Definition

Changes are managed in a formal process.

#### Implementation

The procedure for handling system-based changes is described in central documentation. The document is managed centrally in a document management system. A history of changes to the document is kept. New main versions of the document are checked and released in a formal approval process carried out by the head of Cloud Services. The relevant valid version is stored centrally in the **SEEBURGER INFORMATIK EOOD** intranet and can be accessed by all employees.

### 11.2.2 CM\_02 - Testing and quality assurance of changes

#### Definition

As part of System-Based Change Management, only software updates and service packs approved by Quality Assurance (QA) are imported. A QA approval for Emergency Changes can also be issued at a later time.

#### Implementation

The QA department at **SEEBURGER INFORMATIK EOOD** stores software elements (releases, service packs, hotfixes) approved by QA in a central location (HadDock).

For system-based Changes, only software elements from HadDock are imported.

Exception: Development may also provide a hotfix directly in particularly critical cases (Emergency Changes). This must either be approved by QA at a later time, or an official hotfix / service pack must be implemented in an additional system-based change.

### 11.2.3 CM\_03 - Documentation of implemented changes

#### Definition

Each change is checked to determine whether all mandatory information has been provided.

#### Implementation

In the CSP mandatory fields are defined that require the input of necessary information. Without the correct indication of the information, the change request cannot be forwarded for approval. It is the responsibility of the CAB to check the Change Request for completeness and reject approval, if necessary.

### 11.2.4 CM\_04 - Change Advisory Approval

#### Definition

CAB approval is obtained for normal changes.

#### Implementation

In the **SEEBURGER INFORMATIK EOOD** CSP the complete change process is implemented. The approval of changes is firmly implemented in the CSP and must always take place before a change can be implemented.

The approval can only be given by members of the change advisory board (CAB). Those CAB members are defined and documented in the related work instruction.

### 11.2.5 CM\_05 - Approval and documentation in emergency cases

#### Definition

ECAB approval is required for emergency changes, but this can be obtained at a later time.

#### Implementation

In the CSP, the approval step is stored permanently in the Change process. In emergency situations, the Change Owner of an Emergency Change can implement the change without written approval and instead obtain verbal confirmation from an ECAB member. The Change Owner documents the verbal approval from the ECAB member in the change (separate service unit in the change).

A CAB member can provide written approval the next working day in the CSP.

### 11.2.6 CM\_06 - Final approval and documentation of changes

#### Definition

Function tests must be conducted once the change is implemented. The test results are documented in the change.

#### Implementation

A PIR (Post Implementation Review) section in the Change Request specifies the tests required following a change (mandatory fields). The Change Owner must conduct these tests after a change is implemented and then enter the test results in the Change Form.

## 12. Backup and Recovery Management

The availability of the EDI Cloud Services is the most important contractually agreed performance parameter of the EDI/B2B/GTS processes. In order to guarantee availability, **SEEBURGER INFORMATIK EOOD** has developed a comprehensive data security and restoration concept.

This concept ensures that productive systems are backed up at regular intervals and can be restored again as quickly as possible in the event of loss.

### 12.1 Controls in the ISAE 3402 audit

#### 12.1.1 BR\_01 - Formal process

##### Definition

The backup and restoration of data is regulated in a formal process. The finer details are outlined in management manuals and the service catalog.

##### Implementation

The data backup and restoration process are described in a formal process and published in management manuals within the IT organization.

#### 12.1.2 BR\_02 - Specifying the backup data

##### Definition

All EDI systems are implemented according to a backup set-up guideline, which defines the directories and database schemata that need to be backed up. The implementation is documented in a ticket.

##### Implementation

The following data is backed up during the standard data backup:

- EDI system configuration data,
- Database and EDI runtime data and
- Communication master data of trading partners.

#### 12.1.3 BR\_03 - Verification of successful data backup

##### Definition

The successful implementation of the backup is verified by:

- Regular reviews of the log files written during the backup.
- Monitoring and notification from the manufacturer in the case of irregularities.

##### Implementation

Data backup logs are examined and any faults that occur are analyzed and managed.

#### 12.1.4 BR\_04 - Actuality and regulations

##### Definition

The interval and storage periods of the backups are defined and described in the service catalog.

## Implementation

All EDI productive data from the EDI Cloud Service is backed up incrementally once a day and fully once a week (referred to as “standard data backup” in the following). The relevant data backups are stored for ten days. The configuration data of the EDI system (**SEEBURGER INFORMATIK EOOD** Business Integration Server) in the data center, the EDI database and the runtimes of the EDI system are backed up.

### 12.1.5 BR\_05 - Restoration tests

#### Definition

Restoration tests are conducted and documented at regular intervals.

#### Implementation

Regular restoration tests are conducted to guarantee the usability of the data backup systems.

## 13. Business Continuity Management

### 13.1 Purpose

Business continuity planning (BCP) is the process involved in creating a system of prevention and recovery from potential threats to a company. The plan ensures that personnel and assets are protected and are able to function quickly in the event of a disaster. The BCP is generally conceived in advance and involves input from key stakeholders and personnel.

BCP involves defining any and all risks that can affect the company’s operations, making it an important part of the organization’s risk management strategy. Risks may include natural disasters, fire, flood, or weather-related events- and cyber-attacks. Once the risks are identified, the plan should also include:

- Determining how those risks will affect operations.
- Implementing safeguards and procedures to mitigate the risks.
- Testing procedures to ensure they work.
- Reviewing the process to make sure that it is up to date.

### 13.2 Process Flow

Business Continuity Management is an iterative process, which enables companies to react in a coordinated way on unexpected situations, e.g. Force majeure or cyber-attacks. At **SEEBURGER INFORMATIK EOOD**, the Business Continuity Management process is divided in five phases, as shown in the following illustration.

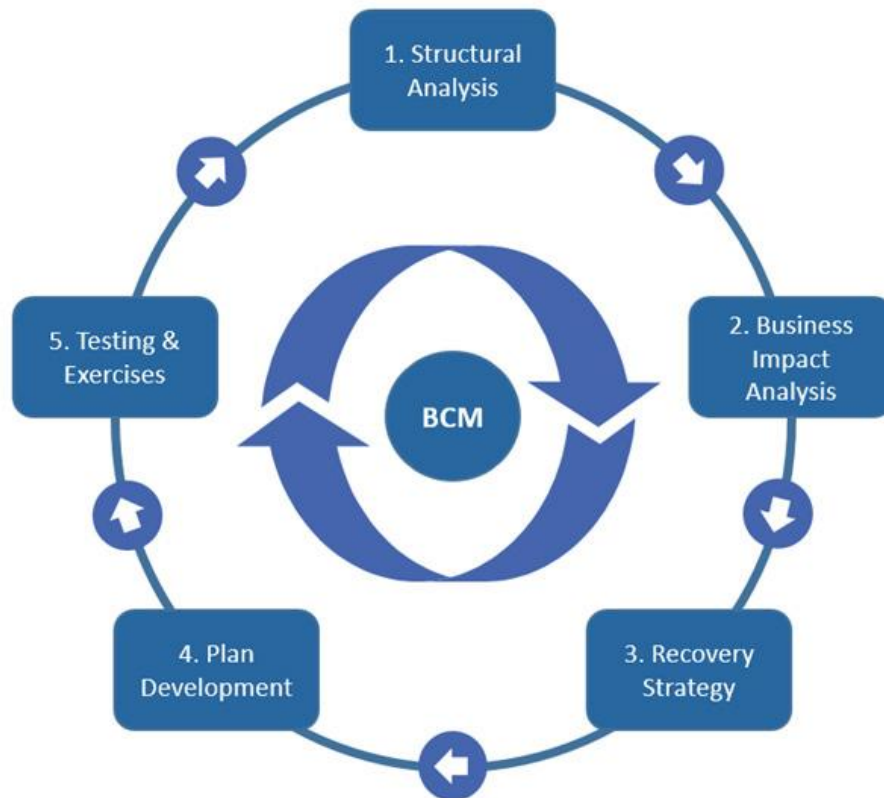


Illustration 19: Business Continuity Management Process

### 13.2.1 Structural Analysis

The knowledge about the scope of the certification is the most important part of the entire risk management process. The structural analysis is the methodology to set up the base for all other information security analysis (e.g. Business Impact Analysis (BIA) or Protection Requirement Analysis (PRA)).

The cost center activities are split into processes and services. Processes are activities the cost center organization needs for their own, services are provided to other cost centers. Processes and services are divided into sub processes and sub services. As part of the Information Asset Management, sub processes and sub services assembled with other services or information asset groups.

### 13.2.2 Business Impact Analysis

The BIA determines the criticality of business process in relation to the information security objective "Availability". The process owner assesses his processes in the categories "Maximum tolerable outage" of and the "Consequences of the process outage". The values he determines in the different categories are multiplied by each other. The result is the process criticality.

The category “Maximum tolerable outage” describes the acceptable downtime of the process for the process owner. The category values are:

1. < three Days
2. three Days and
3. > three Days

The outage value varies between one and three.

### 13.2.3 The Protection Requirement Analysis

As part of the protection requirements analysis, the criticality of the information processed in the process is evaluated in the categories of confidentiality, integrity and availability.

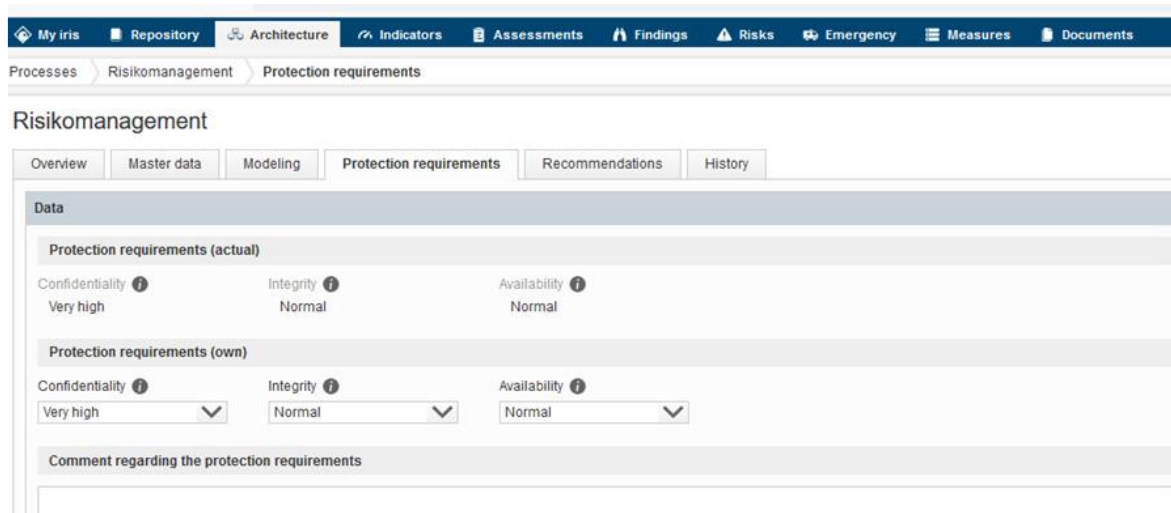


Illustration 20: Risikomanagement

For this analysis the following values are available:

#### Confidentiality

Number	Value	Description
1	Low	Public information <b>without any restrictions</b> , e.g. published by the organization in a newspaper or on the internet.
2	Normal	Information <b>for internal use</b> only. Disclosure to the public may have minor consequences.
3	High	<b>Confidential information</b> that can threaten the achievement of product or project related goals when accessed by unauthorized third parties or fraudulent employees. Disclosure to the public will most likely have quantifiable consequences.
4	Very high	<b>Strictly confidential Information</b> that can permanently threaten company goals when accessed by unauthorized third parties or fraudulent employees. Disclosure to the public will have massive financial or reputational consequences for the organization.

## Integrity

Number	Value	Description
1	Low	A breach of integrity has <b>no noticeable</b> financial or reputational impact on the organization.
2	Normal	A breach of integrity has a <b>small</b> financial or reputational impact on the organization and may trigger minor consequences.
3	High	A breach of integrity has a <b>noticeable</b> financial or reputational impact on the organization and will most likely trigger conceivable consequences.
4	Very high	A breach of integrity has a <b>major</b> financial or reputational impact on the organization and will definitely trigger massive consequences.

## Availability

Number	Value	Description
1	Low	Required availability is <b>low</b> . Significant financial or reputational impact when asset is unavailable for several weeks.
2	Normal	<b>Interruption for up to one week</b> can be covered. Significant financial or reputational impact when asset is unavailable for more than seven days.
3	High	<b>Interruption for up to one day</b> can be covered. Significant financial or reputational impact when asset is unavailable for more than 24 hours.
4	Very high	<b>Immediate significant financial</b> or reputational impact when asset is unavailable.

The required degree of protection is inherited from the information to the application, the processing system, the room, the building, the existing connections and the business process.

The currently implemented technical and organizational methods are suitable up to the PRA factor “high”. For processes processing information of the PRA level “very high”, additional security methods (e.g. redundancy, encryption etc.) are required.

### 13.2.4 Recovery Strategy

Recovery strategies are alternate means to restore business operations to a minimum acceptable level following a business disruption and are prioritized by the recovery time objectives (RTO) developed during the business impact analysis.

Recovery strategies require resources including people, facilities, equipment, materials and information technology. An analysis of the resources required to execute recovery strategies should be conducted to identify gaps.

**SEEBURGER INFORMATIK EOOD** divides the recovery strategy into two parts. These are:

- Recovery strategy of the IT infrastructure and
- Recovery strategy of the **SEEBURGER INFORMATIK EOOD** departments.

### **Recovery Strategy of the IT Infrastructure**

To mitigate risks of Force Majeure and cyber-attacks, **SEEBURGER INFORMATIK EOOD** has implemented security concepts on the IT Infrastructure level. The recovery strategy of the IT Infrastructure department based on the following concepts:

1. All high-risk IT assets are located in ISO/IEC 27001 certified data centers.
2. All productive systems are virtualized, and high availability concepts are implemented.
3. The IT infrastructure is designed redundant.
4. All **SEEBURGER INFORMATIK EOOD** employees are enabled to work from home (e.g. VPN access and usage of a collaboration platform e.g. Microsoft Teams for meetings).
5. Disaster/Recovery plans for an outage of the data centers.
6. Information chain internally and externally and
7. Communication guidelines.

The IT Infrastructure performs regular tests according to these concepts. The result of these tests are KPIs of the **SEEBURGER INFORMATIK EOOD** Information Security Management System.

### **Recovery Strategy of the SEEBURGER INFORMATIK EOOD departments**

For each department, there is an emergency organization plan in place. These plans are documented in the **SEEBURGER INFORMATIK EOOD** Crisis Plan and updated regularly. They cover the different scenarios of Force majeure or cyber-attacks.

#### **13.2.5 Plan Development**

##### **Structure of the SEEBURGER INFORMATIK EOOD Emergency Plan**

In 2009, work started on the development of the first comprehensive database-assisted emergency plan. Since this point in time, this plan has been updated regularly and adapted to the changing boundary conditions.

**SEEBURGER INFORMATIK EOOD** Emergency Plans have been further developed and now includes the following key aspects:

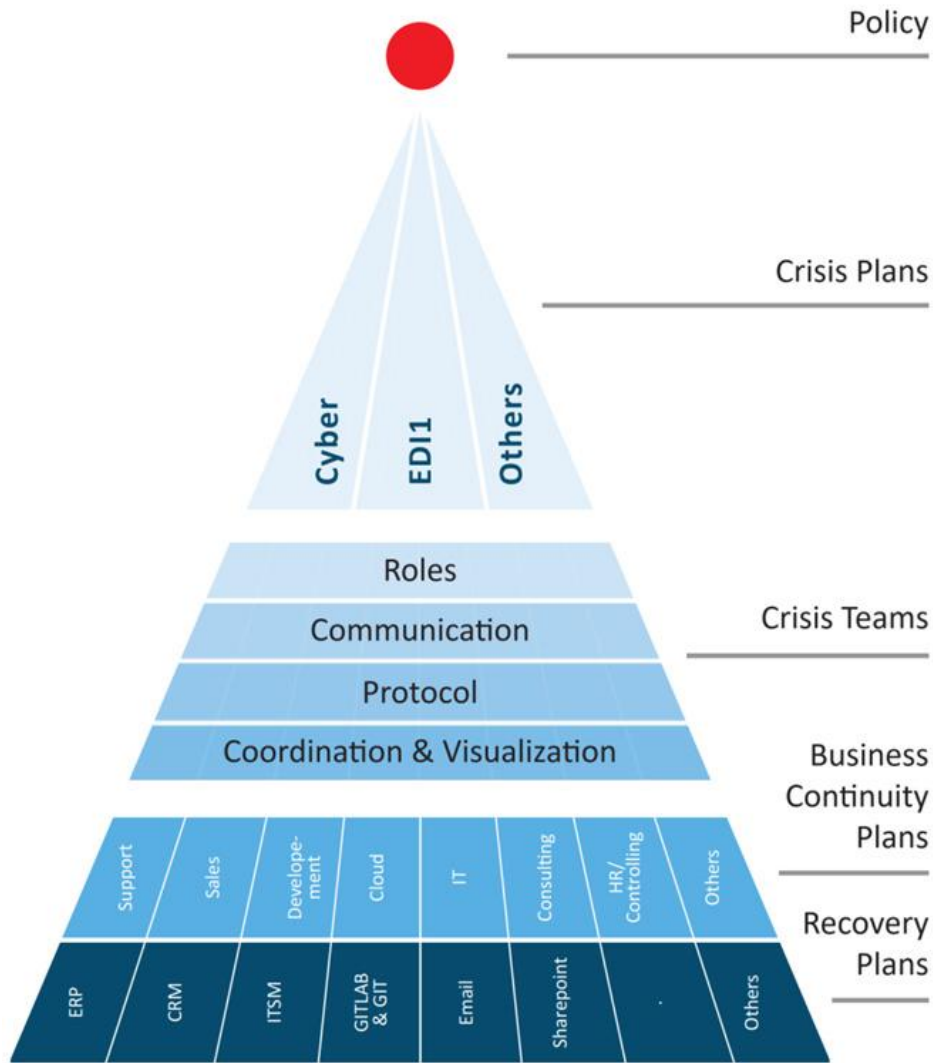


Illustration 21: Structure of the SEEBURGER INFORMATIK EOOD BCM

**Crisis definition**

We have extended previous scenarios such as the loss of data center and office locations due to various causes such as fire or natural events, the absence of personnel due to e.g. a pandemic, the failure of information infrastructure, etc. to include current threats from cyber attacks such as encryption by ransomware, compromise of networks and systems, theft of data and large-scale disruptions of communications.

**Crisis treatment initiation**

Within the Crisis Plan criteria and processes have been defined to evaluate if a crisis treatment has to be initiated. This also contains the definition of immediate containment actions as well as the involvement of external specialists with service contracts that cover direct support 24/7/365.

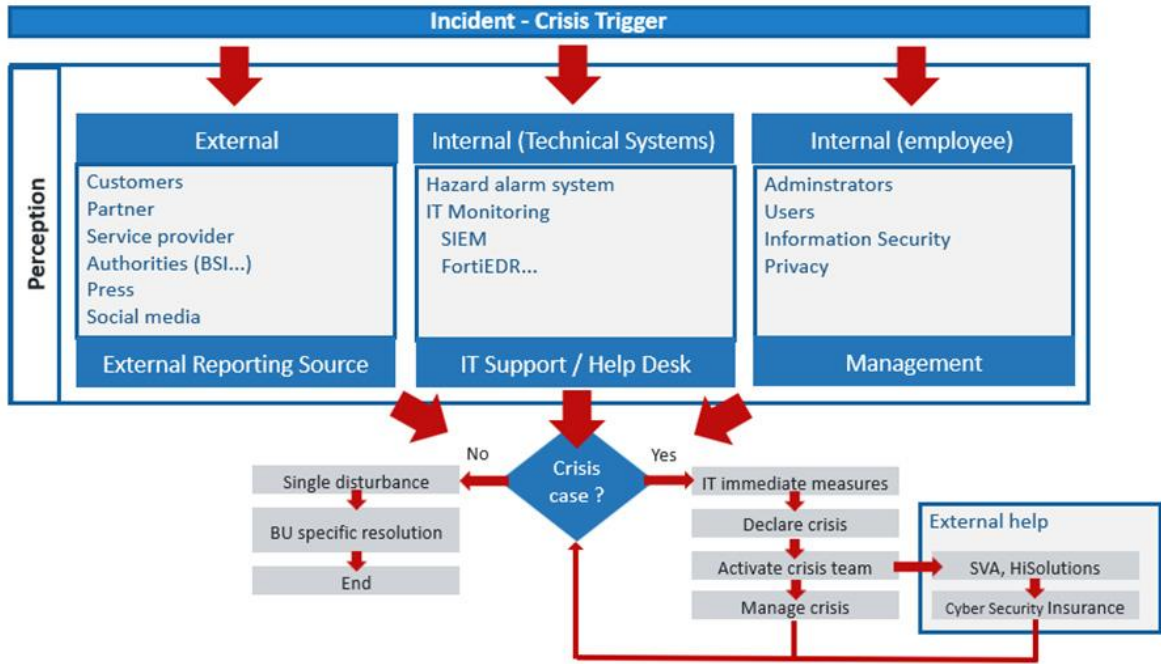


Illustration 22: Basic Process how a Crisis treatment is initiated

**Structure of the Crisis Team**

The crisis management organization is structured as follows: The composition of the crisis team adapts flexibly to the respective crisis situation and its impact on physical assets. Contingency plans also include detailed descriptions of roles and responsibilities. In addition to a defined information chain and an organizational chart of the crisis team, all relevant information is available in physical form and is handed out to team members. All components of the emergency plans are updated regularly.

**Content**

1. OBJECTIVE, SCOPE, RESPONSIBILITIES, DEPENDENCIES ..... 1

2. MEASURES: IMPLEMENTATION OF THE SECURITY STRATEGY ..... 1

2.1 LOCATION ..... 1

2.2 EXPECTED CYBER CRISIS SCENARIOS AT SEEBURGER ..... 2

2.3 STRUCTURE OF THE CRISIS TEAM ..... 2

2.4 START OF CRISIS TEAM OPERATION ..... 3

2.4.1 ALERTING PROCESS FROM SUSPICION TO ESTABLISHMENT OF CRISIS TEAM ..... 3

2.4.2 IMMEDIATE MEASURES BY THE IT DEPARTMENT ..... 4

2.4.3 ASSESSMENT TEAM FOR ACTIVATION OF CRISIS MANAGEMENT TEAM ..... 5

2.4.4 CRITERIA FOR A CYBER CRISIS ..... 5

2.4.5 EXTERNAL HELP ..... 6

2.5 CRISIS TEAM - ROLES ..... 8

2.5.1 MEMBERS OF THE CYBER CRISIS TEAM ..... 8

2.5.2 ROLES ..... 8

2.5.3 SUPPORTING ROLES ..... 10

2.6 CRISIS TEAM - START FROM HOUR 0 ..... 11

2.6.1 LOCATIONS AND MEANS OF COMMUNICATION ..... 11

2.6.2 TOOLS ..... 12

2.6.3 EVENT MANAGEMENT ..... 12

2.7 CRISIS TEAM - EMERGENCY OPERATION DAY 0 TO 7 ..... 15

2.7.1 ACTIVATE BUSINESS CONTINUATY PLANS (BCP) ..... 15

2.7.2 INVOLVEMENT OF THE SUPERVISORY BOARD (AR)\* ..... 17

2.7.3 INSURANCE INVOLVEMENT ..... 18

2.7.4 NOTIFICATION TO BSI ..... 18

2.7.5 DATA PROTECTION INTEGRATION ..... 18

2.7.6 COMMUNICATION ..... 19

2.8 CRISIS TEAM - RESTART DAY 0 TO 180 ..... 19

2.8.1 CRITICAL SEEBURGER INFRASTRUCTURE ..... 19

2.8.2 CRITICAL SEEBURGER LOCATIONS ..... 20

2.8.3 IT PHASE PLAN ..... 21

2.8.4 CRITICAL DATA BACKUPS ..... 21

2.9 APPENDIX A: CHECKLIST CRISIS TEAM MANAGEMENT CYCLE ..... 23

3. EFFECTIVENESS ..... 29

4. DOCUMENTATION ..... 29

5. APPLICABLE LEGAL AND REGULATORY REQUIREMENTS ..... 29

Illustration 23: Cyber Crisis Management Plan - Table of Content

**13.2.6 Testing & Exercises**

The effectiveness of these crisis plans is ensured by test runs of the different scenarios at regular intervals. These tests include exercises of the crisis team by simulating a critical situation. Test runs of the crisis team are afterwards analyzed and evaluated if reactions or processes can be optimized. These crisis team exercises do not involve the majority of employees. Mobile work from the home

office for all employees has been used intensively during the Covid pandemic situation and this has worked out very well.

Evacuation exercises are also performed so employees know how to behave in emergency situations. Reaction times are evaluated and reviewed afterwards.

Another test scenario are IT system failures as well as disaster recovery tests. With these, the proper function of redundancy as well as fallback scenarios for certain departments are exercised and evaluated for business impact. This includes test runs of whole datacenter failures and switching productive systems between these.

With these test scenarios we are covering the different levels from top management to employee level. Test results are used for improvement as well as analyzing the efficiency of current crisis plans.

### 13.3 Disaster/recovery capacity

The provision of resources required for a service at more than one location (data center) ensures that the service can be provided at the second location if one of the data centers fails.

The diagram in the following illustration demonstrates this.

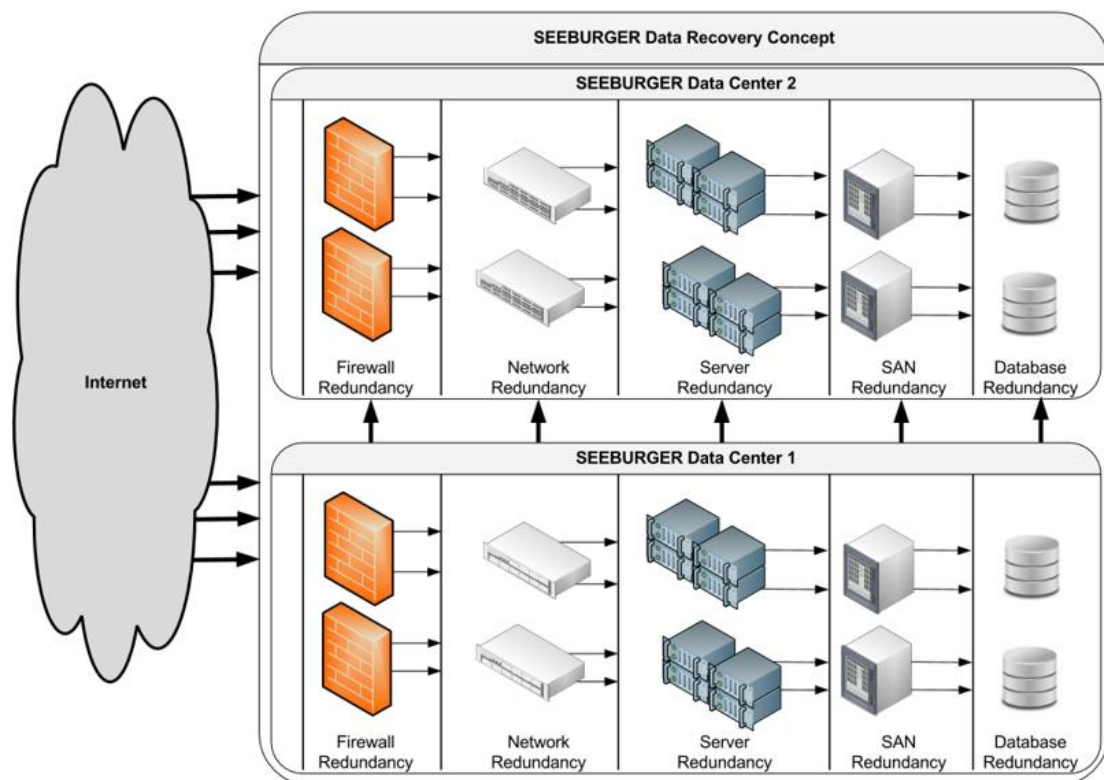


Illustration 24: DR capability (schematic)

In addition recovery of defined services and systems within a public cloud environment (AWS, Azure) is designed, documented and verified during exercises.

## 13.4 Controls in the ISAE 3402 audit

### 13.4.1 BC\_01 - SEEBURGER INFORMATIK EOOD emergency plan

#### Definition

The organization is prepared for defined crisis scenarios and there are set procedures for assembling the emergency operation organization. These procedures are reviewed on a regular basis.

#### Implementation

**SEEBURGER INFORMATIK EOOD** maintains a crisis plan that covers major crisis scenarios such as building damage, loss of personnel and damage to IT infrastructure due to e.g. fire, natural disasters, pandemics or cyber-attacks.

The crisis plan defines the crisis team, internal and external communication as well as initial measures and the organization in the emergency run and restart phase. In addition, each critical area maintains and tests concrete emergency run and recovery plans of its business processes.

### 13.4.2 BC\_02 - Handling unforeseen events like force majeure or critical Cyber Security attack

#### Definition

In the event of an unforeseen event like force majeure or critical cyber security attack with a potential to affect many systems and/or staff and/or customers, BCM ensures that the **SEEBURGER INFORMATIK EOOD** organization and **SEEBURGER INFORMATIK EOOD** business processes continue to operate, e.g. functions are assumed by other locations.

#### Implementation

Based on defined criteria either a specific disaster situation or a major crisis situation will be detected and the crisis plan activated. The crisis team immediately is activated and will work according the defined procedures.

In case of a technical disaster situation the disaster recovery procedures will be initiated and infrastructure and systems activated on the disaster recovery location.

In case of a major crisis situation the departments activate their emergency procedures and work according to the defined emergency plans. Recovery teams are activated and start the recovery of the infrastructure according the recovery plans. The recovery plans contain the recovery of critical business processes, supporting processes and assets from day 0 of a crisis situation.

### 13.4.3 BC\_03 - Safety of equipment

#### Definition

The relevant company values for the scope of the ISAE 3402 audit are included in an asset management system. Information about:

- Identification,
- Software,

- Employees,
- Spatial assignment and
- saved or processed information

is related to one another in this asset management system.

### **Implementation**

The relevant company values for the scope of the ISAE 3402 audit are stored in an inventory system managed by the IT infrastructure. They are uniquely identified by a sequential number. “Employee” and “hardware” information is included in this inventory system. The “employee” and “unique **SEEBURGER INFORMATIK EOOD** number” information included in an asset management system maintained by Information Security Management forms the basis for a protection requirements analysis. In this system, the assets are supplemented with “spatial assignment” and “saved” information.

#### **13.4.4 BC\_04 - Protection requirements analysis**

### **Definition**

The criticality and restoration sequence of the systems are determined during the protection requirements analysis.

### **Implementation**

The protection requirements for information stem from the possible consequences of a security incident. This is illustrated by the classification of information as per IS guideline “Classifying information”. The task of determining the protection requirements is the responsibility of specialist and/or technical information managers.

All information must be assessed in relation to the information security objectives of:

- Availability,
- Confidentiality and
- Integrity

in the five defined protection requirement classes (damage classes):

- low,
- medium,
- high and
- very high

in the categories

- Violation of laws,
- Negative impact on task fulfilment,
- Negative external effect and
- Financial damage.

The protection requirements of information values are aggregated along the hierarchy and define the protection requirements for the next stage. This inheritance hierarchy is shown in the following illustration.

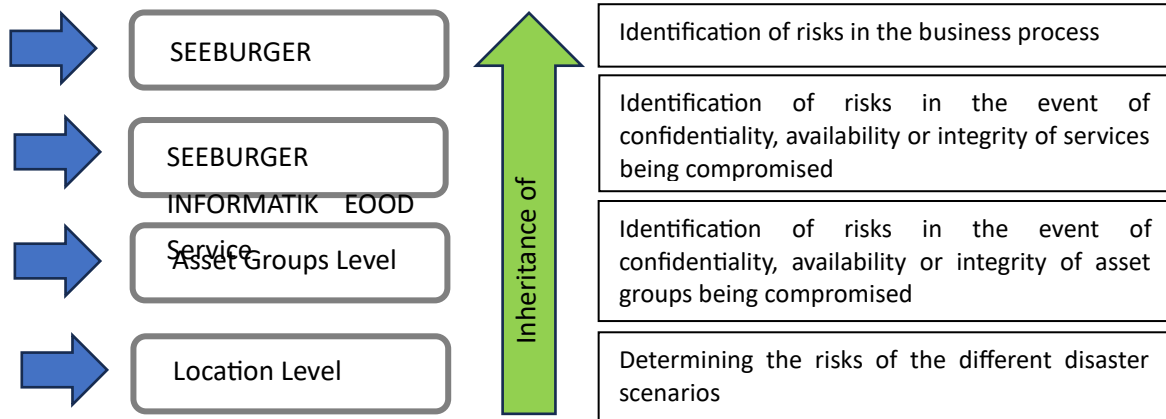


Illustration 25: Inheritance of protection requirement

The connection between “Asset” and “Information” is established in the **SEEBURGER INFORMATIK EOOD** asset management system.

13.4.5 BC\_05 - Evidence of the effectiveness of measures

**Definition**

The replication of the data is configured in accordance with the contractually agreed DR option.

**Implementation**

**SEEBURGER INFORMATIK EOOD** offers a range of optional disaster recovery services for restoring the availability of EDI Managed Services within a reasonable time frame in the event of a disaster situation. A “disaster situation” arises if the entire data center in which **SEEBURGER INFORMATIK EOOD** provides and operates the EDI IT infrastructure for CUSTOMERS fails (e.g. as a result of an explosion or flooding). **SEEBURGER INFORMATIK EOOD** offers this disaster recovery service in different performance classes.

Description	Disaster Recovery Options (“DR Options”)		
	DR BASIC	DR ADVANCED	DR PREMIUM
<b>Procedure</b>	Only backup services in a second <b>SEEBURGER INFORMATIK EOOD</b> data center	Backup services and replication of the system in a second <b>SEEBURGER INFORMATIK EOOD</b> data center	Backup services and replication of the system in a second <b>SEEBURGER INFORMATIK EOOD</b> data center
<b>Standard data backup</b>	Data backup 1x per day incrementally, 1x per week in full		

<b>Backup of configuration data of System</b>	Same as standard data backup	Replication every 20 minutes	Replication every 10 minutes
<b>Backup of database and runtime data</b>	Same as standard data backup	Replication every 24 hours	Replication every 12 hours
<b>Backup of master communication data for trading partners</b>	Same as standard data backup	Replication every 24 hours	Replication every 12 hours
<b>System recovery</b>	Within 48 hours	Within 24 hours	Within 8 hours
<b>Recovery of data from backup</b>	Within 96 hours	Within 24 hours	Within 8 hours

The following data is backed up during the standard data backup (see also BR\_0x controls):

- Configuration data of system
- Database and runtime data
- Master communication data of trading partners.

Within the context of this service certificate, “replication” means that the EDI system used by the CUSTOMER is mirrored in a second **SEEBURGER INFORMATIK EOOD** data center. The system and configuration data required for the restoration of the entire EDI Cloud Services as well as the database and EDI runtime data in the relevant cycle presented in the above table are replicated in the second **SEEBURGER INFORMATIK EOOD** data center.

The following services are included in the different forms.

**“DR BASIC” option**

In the “DR BASIC” DR Option, the recovery of the Cloud Services after a Disaster Event has occurred shall be carried out in accordance with the following procedure:

- Recovery and configuration of the system at the **SEEBURGER INFORMATIK EOOD** data center;
- Importing the last data backup; and
- Resumption of operation of the agreed Cloud Service.

**“DR ADVANCED” and “DR PREMIUM” options**

With the DR-Options “DR ADVANCED” and “DR PREMIUM” the recovery of the Cloud Services after a Disaster Event has occurred shall be carried out in accordance with the following procedure:

- Re-configuration of the external IP-Addresses to the second **SEEBURGER INFORMATIK EOOD** data center
- Re-configuration of the customer connection to the second **SEEBURGER INFORMATIK EOOD** data center

- Resumption of operation of the agreed Cloud Service.

### Implementation of the replication

**SEEBURGER INFORMATIK EOOD** uses Oracle Data Guard to replicate data to a redundant system in another data center location. Replication of data is typically done immediately. EDI systems are configured in a way that the data base connection is switched within less than ten minutes in case of a disaster.

Restoration of systems is done according to the Recovery settings as described in the BR\_05 controls.

## 14. Control Considerations for SEEBURGER INFORMATIK EOOD Customers

### 14.1 Purpose, General IT Controls & Data and Information Management

**SEEBURGER INFORMATIK EOOD's** service was designed with the assumption that certain procedures and controls would exist at or implemented by clients. In certain circumstances, specific controls related to the services provided might be necessary to achieve certain control objectives included in this report. Those additional procedures and controls should be in operation by the client to complement the **SEEBURGER INFORMATIK EOOD's** service and corresponding controls. The user organizations auditor should consider whether the following controls have been placed in operation by the client.

The below listed complementary user entity controls do not represent a comprehensive set of all controls that should be employed by clients. Other controls may be required to achieve the clients' security or business requirements with regards the services provided by SEEBURGER INFORMATIK EOOD.

### 14.2 General IT controls

It is the customer's responsibility to implement sound and consistent internal controls regarding General IT system access and system usage appropriateness for all internal user entity components associated with the service organization.

### 14.3 Data and information management

It is the customer's responsibility to read and be familiar with all terms and conditions of the **SEEBURGER INFORMATIK EOOD's** service agreement and operating policies regarding services provided by **SEEBURGER INFORMATIK EOOD**.

Customers are responsible for communicating and maintaining accurate organizational contact information to **SEEBURGER INFORMATIK EOOD**. With respect to the Change-, Incident- and Back-up & Restore Management it is the customer's responsibility that:

1. an authorization list is provided to **SEEBURGER INFORMATIK EOOD** at production start of the applicable services/systems;
2. the authorization list contains authorized employees only;
3. changes to authorization list due to leaving or moving of customers’ employees are communicated to **SEEBURGER INFORMATIK EOOD** in a timely manner.
4. a regular review of the authorization list is performed by the client and changes are communicated to **SEEBURGER INFORMATIK EOOD**.

#### 14.4 Backup and Recovery Management

It is the customer’s responsibility to initiate the restore process and to validate performed restores.

#### 14.5 Incident Management

It is the customer’s responsibility to report occurred incidents and to validate the provided resolution/workaround.

#### 14.6 System-Based Change Management

It is the customer’s responsibility to handle changes in compliance with the change management policy of **SEEBURGER INFORMATIK EOOD**. This includes the validation of implemented changes.

### 15. Complementary Subservice Organization Controls

**SEEBURGER INFORMATIK EOOD** uses subservice organizations to perform physical and environmental procedures that support the delivery of services. The control objective for Physical Security can be met only if the subservice organization’s controls, assumed in the design of **SEEBURGER INFORMATIK EOOD**’s controls, are suitably designed, and operating effectively along with related controls at **SEEBURGER INFORMATIK EOOD**. The following is a description of services provided by subservice organizations. The controls relating to the infrastructure services provided by the subservice organizations below have been carved out of the scope of this report. They refer to co-location data centers.

Subservice Organization	Services Provided
<b>Equinix</b>	Co-location Data Center: Service provider with physical access but no logical access.
<b>TelemaxX</b>	Co-location Data Center: Service provider with physical access but no logical access.

In the design of their internal procedures and controls, **SEEBURGER INFORMATIK EOOD** has assumed the following procedures and controls by subservice organizations:

Area	Controls Expected to be Implemented at Subservice Organizations
<p><b>Physical and Environmental Security</b></p>	<p>The co-location data center providers are responsible for implementing physical security and environmental safeguards for premises, buildings, and data centers. The co-location data center providers need to ensure proper operation of their physical environments and data centers, including:</p> <ul style="list-style-type: none"> <li>• Vendor and employee access</li> <li>• Intrusion detection</li> <li>• Fire detection and suppression systems</li> <li>• Power management capabilities</li> </ul> <p>The following controls are expected to be implemented by the subservice organizations:</p> <ul style="list-style-type: none"> <li>• Access to the facility hosting production systems is restricted to personnel or visitors authorized by the tenant.</li> <li>• Access to the facility hosting production systems is not granted to personnel or visitors unless authorized by the tenant previously.</li> <li>• Access to the facility hosting production systems is removed/disabled upon tenant notification.</li> <li>• Access to the facility is controlled via keycard system or other preventative access control systems.</li> <li>• Access to entrances and sensitive areas are monitored and/or recorded by security cameras.</li> <li>• Access to the facility is periodically reviewed.</li> <li>• A documented procedure that defines and communicates the process for employees and customers to report suspected security violations and other security issues has been documented and communicated.</li> <li>• Security incidents are reported to <b>SEEBURGER INFORMATIK EOOD</b>, as needed, to assist with resolution.</li> <li>• Security incidents are communicated to <b>SEEBURGER INFORMATIK EOOD</b>. Documentation of the communication, impact and resolution of the incident is retained in an enterprise ticketing system.</li> <li>• A root cause analysis is prepared and reviewed for critical security incidents that require remediation.</li> </ul>

**16. Changes to the System Since the Last Report**

No changes have been made to the system since the last report.

## 17. System incidents

No system incidents occurred since the last report.

## 18. Complementary User Entity Controls (CUEC's)

Certain control objectives outlined in this report assume that **SEEBURGER INFORMATIK EOOD** cloud customers implement appropriate controls within their own environments. This includes taking responsibility for complementary measures that ensure the secure and compliant use of the **SEEBURGER INFORMATIK EOOD** cloud service.

Such measures involve defining and managing responsibilities, coordinating interfaces, and establishing effective processes for reporting security incidents to **SEEBURGER INFORMATIK EOOD**. Customers must also classify their information, determine the required level of protection, and ensure that data is appropriately safeguarded during processing, storage, and transmission, including the use of segregation and encryption where necessary.

Customers are responsible for monitoring and managing the resources within their control and confirming that **SEEBURGER INFORMATIK EOOD's** backup, redundancy, capacity, and availability arrangements meet their operational and regulatory requirements. They also regularly review the audit logs provided by **SEEBURGER INFORMATIK EOOD**, carry out vulnerability assessments, and implement hardening measures for the systems under their control.

In addition, customers must ensure that security incidents and weaknesses are detected, reported, and handled appropriately, and that insights gained are incorporated into their ISMS. Business continuity requirements identified through their Business Impact Analysis must be reflected in their continuity planning, regularly tested, and aligned with **SEEBURGER INFORMATIK EOOD's** BCM measures.

Finally, customers are responsible for meeting contractual, legal, and technical requirements, such as configuring authentication and logging mechanisms, managing roles and permissions, assessing subservice providers, responding to governmental inquiries, and selecting compliant data processing locations.

By implementing these controls, customers help ensure that the **SEEBURGER INFORMATIK EOOD** cloud service meets their security, availability, and compliance requirements within the shared responsibility model.

## Section III – Information provided by BFMT

The internal control environment of the **SEEBURGER INFORMATIK EOOD** represents the collective impact of various elements aimed at establishing, improving, or mitigating the effectiveness of specific controls. Management is responsible for the design, description of controls, and related control objectives. BFMT conducted audit work as part of the ISAE 3402 SOC 1 Type 2 audit, which was deemed necessary to assess the extent to which key control activities are being performed. This provides reliable, though not absolute, assurance that the established control objectives have been achieved during the audit in the period of **January 1, 2025 to December 31, 2025**.

This ISAE 3402 Report on Internal Controls Implemented is intended to provide interested third parties with sufficient information to gain an understanding of those aspects of internal controls that may be relevant to a user Organization's internal control environment.

Accordingly, this audit report on **Client's** system of internal control is intended to provide interested parties with sufficient information to enable them to understand those aspects of the controls that are significant to a **SEEBURGER INFORMATIK EOOD** report reader. The result of the ISAE 3402 audit was provided by the independent auditor BFMT.

It is BFMT's responsibility to assess the extent to which the controls were appropriately designed in achieving the relevant control objectives of **SEEBURGER INFORMATIK EOOD** as a service provider during the audit in the period of **January 1, 2025 to December 31, 2025**.

Our audit of the **Client's** internal control environment was performed using appropriate tests during the period of **January 1, 2025 to December 31, 2025**, taking into account the control objectives predefined by the organization. The audit procedures considered the following factors:

- The design of the control objectives;
- The characteristics of audited control activities;
- The effectiveness of controls;
- The audit evidence available.

We reviewed the extent to which the **Client's** controls are appropriately designed during the audit period and the relevant control objectives have been achieved. The audit included the following procedures to the extent we considered necessary:

- Interviewing relevant management and technical personnel to evaluate the design of internal controls;
- Reviewing the organizational structure of the service provider **SEEBURGER INFORMATIK EOOD**;
- Including the segregation of functional responsibilities; and observing personnel in the performance of their activities;
- Inspection of documents and records and observation of activities and procedures implemented by the **SEEBURGER INFORMATIK EOOD** service provider; and
- Tests of organization's controls based on predefined tests.

During the audit period, **January 1, 2025 to December 31, 2025** we examined more than 50 process documents and technical concepts as well as more than 150 related samples.

The results of the **Client's** audit procedures performed in accordance with ISAE 3402 SOC 1 Type 2 provide the basis for our audit opinion on **Client's** internal controls in the period of **January 1, 2025 to December 31, 2025** based on the requirements of Auditing Standard ISAE 3402. All controls within the scope of the audit under ISAE 3402 were appropriately designed, implemented in the period of **January 1, 2025 to December 31, 2025**. As a result of the audit of **SEEBURGER INFORMATIK EOOD**, we were able to determine a high level of internal control and key business processes based on the process documents and audit evidence provided to us.

## 1. Risk Management

Control Objective
<p><b>RM - Risk Management</b></p> <p>Controls provide reasonable assurance that risks are identified, mitigated and reviewed by management.</p>
Management Practice
<p><b>RM_01 - “Risk management” guideline</b></p> <p>Risks are identified in a formal process. This process is documented in an information security management document and implemented based on a risk management program.</p> <p><b>RM_02 - Systematic risk management</b></p> <p>Risks are managed as part of the risk management process. Here, risks pass through the following stations:</p> <ul style="list-style-type: none"> <li>• Identification</li> <li>• Assessment</li> <li>• Derivation of measures for minimizing the risk</li> <li>• Reassessment of the risk</li> </ul> <p><b>RM_03 - Regular risk reassessments</b></p> <p>The risk manager regularly inquires experts with risks assigned to them for reassessment. During reassessments, progress is checked while the adopted measures are implemented.</p>
Test to be performed by BFMT
<p><b>Test of Design</b></p> <p>The risk management audit includes an assessment of the processes for identifying, managing, and reassessing risks. This includes inspection and observation procedures. The risk management policy is inspected to determine whether a risk management approach has been defined and documented. Furthermore, the</p>

risk management process description and the audit plan are inspected to verify defined and documented relevant process steps. The procedures for identifying, assessing, and mitigating risks are also defined by inspecting the risk management process description. In addition, the risk management process description is inspected to determine whether a procedure has been defined for reassessing identified risks and for regular review.

**Test of Operating Effectiveness**

With regard to the implementation and operation of the risk management system, the risk management tool is monitored to determine whether a dedicated tool has been implemented. The catalog of all risks is inspected to determine the definition and documentation of relevant risks. For a selection of identified risks, the risk description and the corresponding protocols are inspected to determine whether risks have been assessed, tracked, and, if necessary, reassessed. Finally, for a selection of risks, the risks and the corresponding protocols are inspected to determine whether the risks have been reassessed by a dedicated expert and the follow-up measures have been reassessed. These checks serve to ensure the adequacy, design, and effectiveness of the risk management process.

**Management Practice by SEEBURGER INFORMATIK EOOD**

**RM\_01 - “Risk management” guideline**

The information security management document entitled “Risk Management” describes the formal process used to identify and assess risks. It also describes how risks are managed by deriving and tracking measures. The information security guideline is regularly adapted to changing boundary conditions and audited by an external third-party organization as part of the annual ISO/IEC 27001 certification.

**Result**



The documented risk management process and accompanying documentation describing in detail how risks are identified, assessed, and categorized were reviewed. The inspection included examples of risk assessments from the audit period and a list of identified risks with information on potential impacts and the status of risk mitigation measures taken. The interview also confirmed the clear definition of roles and responsibilities and the regular application of the process. Overall, it was found that risks are systematically identified, assessed, tracked, and documented in the risk catalog, and that the results are consistently incorporated into the subsequent process steps.

Risk management was revised during the audit year, and the matrix was changed from 5x5 to 4x4 because the 5x5 matrix was no longer useful for the company. The risks were too detailed and there were too many small risks. This allows for a better focus on the larger risks.

**By inspecting the documentation prepared by SEEBURGER INFORMATIK EOOD and through our IT-supported audit procedures, we were able to satisfy ourselves that this process is implemented and operated effectively and complies with the requirements of ISAE 3402 SOC 1 Type 2.**

**Management Practice by SEEBURGER INFORMATIK EOOD**

**RM\_02 - Systematic risk management**

1. Risks are identified using the top-down or bottom-up methodology.
2. To identify risks on a structured base, it is required that information security requirements are defined as a baseline. Against this baseline internal audits must be performed. SEEBURGER INFORMATIK EOOD starts to implement the security requirements of the BSI Basic Protection Compendium as baseline.
3. Evaluation by the relevant experts and measures for minimizing, avoiding or delegating risks of the SEEBURGER INFORMATIK EOOD management team are proposed in collaboration with the risk manager and experts.
4. Based on the decision made by the management team, the measures are implemented, or the risk is adopted by the management team.
5. In a semi-annual assessment, the risks are regularly (re)assessed.

**Result**



A risk register was reviewed, which contains a detailed list of the identified risks, including their assessment according to probability of occurrence and impact, as well as the persons responsible for each risk. In addition, documentation on the measures taken to minimize individual risks was available. During the interviews, it was possible to understand how risks are monitored, adjusted, and, if necessary, addressed with new measures. The evidence also shows that risks are regularly reassessed, including the adjustment of risk levels and risk mitigation strategies. Overall, it was found that risks are not only formally recorded, but also actively managed, tracked, and adapted to changing conditions.

**By inspecting the documentation prepared by SEEBURGER INFORMATIK EOOD and through our IT-supported audit procedures, we were able to satisfy ourselves that this process is implemented and operated effectively and complies with the requirements of ISAE 3402 SOC 1 Type 2.**

**Management Practice by SEEBURGER INFORMATIK EOOD**

**RM\_03 - Regular risk reassessments**

On a semi-annual base, the Information Security department creates risk reports. These risk reports contain new identified risks in the last half year and risks, which must be re-evaluated. The experts of the specific department have a three-month period to evaluate the risks. This will give them time to discuss the current or initial evaluation of the risk and to prioritize or track the state of the mitigation responses. Regular meetings with the responsible board member are part of the iterative (re)-evaluation process of risks.

After the semi-annual risk evaluation phase of a board area, the next evaluation phase starts three months later (e.g. Q1 → Q3). In a worst-case scenario, new risks identified in Q1 are presented to the board member six months later. For this period the ownership of new risks is unclear. Because of the rhythm of the (re)-evaluation it is required, that at the end of the evaluation phase (e.g. Q1) a risk report with new risks identified during the last half year sent to the experts and the board member.

<b>Result</b>	
---------------	---

Evidence of regular requests by the risk manager to the responsible experts was reviewed, which are documented in a schedule for reassessments. The reports contain an overview of the reassessments performed, the experts consulted, and the results of the assessments, including any changes to the risk assessments. In addition, evidence was available that the results were tracked, progress reviewed, and appropriate risk mitigation measures implemented. The interviews confirmed that there is close coordination between risk management and experts and that the reassessment process is applied systematically. Overall, it was found that the regular reassessment of risks is ensured and documented by documented processes and evidence.

**By inspecting the documentation prepared by SEEBURGER INFORMATIK EOOD and through our IT-supported audit procedures, we were able to satisfy ourselves that this process is implemented and operated effectively and complies with the requirements of ISAE 3402 SOC 1 Type 2.**

## 2. User & Access Management

Control Objective
<p><b>UAM - User &amp; Access Management</b></p> <p>Controls provide reasonable assurance that only authorized individuals have access to productive systems used for the EDI/B2B/GTS/iPaaS services and the Active Directory systems.</p>
Management Practice
<p><b>UAM_01 - Cloud Services permission concept</b></p> <p>A permission concept for accessing EDI/B2B/GTS systems in the Cloud Services department is available and updated at regular intervals.</p> <p><b>UAM_02 - Implementing the password guideline</b></p> <p>A global password guideline is provided, communicated, technically implemented and enforced by the Active Directory.</p> <p><b>UAM_03 - Assigning permissions in the Active Directory</b></p> <p>Access to general resources/information is requested in a formal process (incident). The relevant data owner is responsible for granting approval.</p> <p><b>UAM_04 - Access control for customer systems</b></p> <p>A process for requesting and granting access to customer systems within Cloud Service is defined, documented and technically regulated.</p> <p>The technical implementation of the assignment of rights ensures that access can only be requested via the defined and documented path and that the assignment of rights is always carried out via an approval process and is logged in a traceable manner.</p> <p><b>UAM_05 - Removing user access privileges</b></p> <p>User accounts on the AD (access to SEEBURGER INFORMATIK EOOD networks) that are no longer required are blocked promptly (within three days) by IT Admin. Users are deactivated automatically when the “Valid To” date expires.</p> <p><b>UAM_06 - Expiry of user permissions for the EDI application</b></p>

Internal SEEBURGER INFORMATIK EOOD user permissions for productive EDI CS applications are limited to a maximum of 90 days. If the permissions are not renewed, the central Access Management Tool automatically blocks access.

#### **UAM\_08 - Checking users and rights for productive customer systems**

Regular checks are performed to ensure that no unauthorized users have been created on the application level of BIS6 customer systems.

#### **UAM\_09 - Separating Access to Cloud Services from Corporate Access Management**

All Cloud Service relevant activities require an AD authentication and an additional authorization in the central access application. This ensures that only authorized employees can gain access to customer-relevant data.

#### **UAM\_11 - Assigning administrative rights for productive customer systems on an application level**

On productive customer systems, SEEBURGER INFORMATIK EOOD employees are only allocated application rights that were defined during the Access Management process for the assigned employee role.

#### **UAM\_12 - Network security between the corporate and the cloud services networks**

Cloud Systems are separated from other networks. Access to Cloud Systems is only possible over the IT Admin Access tool or over a specific tunnel service provided and managed by the central Cloud Services Access Management Tool.

### **Test to be performed by BFMT**

#### **Test of Design**

The process descriptions for user access management and document histories are inspected to determine the definition and documentation of a role-based authorization concept. The password policy and Active Directory configurations are checked to verify password security requirements. In addition, process descriptions for accessing resources and customer systems as well as the configurations of the cloud service portal are reviewed to ensure procedures for requesting, approving, logging, automatically locking, and deactivating accounts as well as for limiting permissions to 90 days. In addition, process descriptions and documentation that provide for the separation of cloud services and enterprise access management, as well as network security measures, are reviewed.

#### **Test of Operating Effectiveness**

Active Directory configurations are inspected to verify that the password policy is actually enforced. Incident tickets, access requests, and system logs are randomly checked to verify that requests are submitted, approved, and logged correctly. System settings and logs of the Cloud Services Portal are checked to determine the

effectiveness of automatic account locking and compliance with the 90-day rule. System logs and reports are examined to rule out unauthorized access and verify the implementation of the separation of cloud services and enterprise access management as well as network security measures.

**Management Practice by SEEBURGER INFORMATIK EOOD**

**UAM\_01 - Cloud Services permission concept**

The permission concept for accessing EDI/B2B/GTS systems is documented and communicated within the SEEBURGER INFORMATIK EOOD organization. The document is managed centrally in a document management system. A history of changes to the document is kept. New main versions of the document are checked and released in a formal approval process carried out by the head of Managed Services. The relevant valid version is stored centrally in the SEEBURGER INFORMATIK EOOD intranet and can be accessed by all employees.

**Result**



A documented authorization concept was reviewed, which contains detailed information on roles, responsibilities, and assigned access rights. In addition, a history of updates and revisions was available, demonstrating that the concept is regularly reviewed and adapted to current requirements. The evidence confirms that a clearly defined access control framework is in place, which is regularly maintained and provides a traceable basis for user and access management in the relevant systems.


**By inspecting the documentation prepared by SEEBURGER INFORMATIK EOOD and through our IT-supported audit procedures, we were able to satisfy ourselves that this process is implemented and operated effectively and complies with the requirements of ISAE 3402 SOC 1 Type 2.**

**Management Practice by SEEBURGER INFORMATIK EOOD**

**UAM\_02 - Implementing the password guideline**

IT is responsible for the password directory for the SUB domain.  
The following password policy is enforced for all SEEBURGER INFORMATIK EOOD domains automatically.


	Regulation	Definition
Account	<b>Standard Account</b>	Min. PW length: 12 characters, complex password in addition either a conditional access policy or MFA are recommended.

<b>General rules applying for all account types</b>	<b>Standard Account “Plus”</b>	Min. PW length: 12 characters, complex In addition either a conditional access policy in MS Entra or MFA are required for the specific application.
	<b>Admin Account</b>	Min. PW length: 16 characters, complex MFA.: required
	<b>Higher Admin Account (such as domain admin accounts etc.)</b>	Min. PW length: 24 characters, complex MFA.: required
	<b>Service Accounts</b>	Min. PW length: 24 characters, complex MFA.: if feasible
	<b>Password Complexity</b>	At least 3 of the following: Upper, lowercase letters, numbers and symbols
	<b>Password Maximum Length</b>	not configured
	<b>Password Expires</b>	event based
	<b>Lockout Threshold</b>	6 failed attempts
	<b>Password History Kept</b>	10 iterations
	<b>Blocking and resetting time of the account</b>	1 h
	<b>Passwords must not contain parts of the first, last, or logon name</b>	configured
<b>Result</b>		
<p>A documented password policy was reviewed that specifies requirements for password complexity, length, and rotation intervals. In addition, evidence of communication with users was available, including logs of email distribution and training materials explaining the policy. The technical implementation was reviewed based on the Active Directory configurations that ensure enforcement of the defined requirements. Overall, the audit confirmed that the global password policy is not only formally defined, but also effectively communicated, technically implemented, and enforced. In addition, the audit included random checks of user accounts, review of role and authorization concepts, and evaluation of the handling of password resets and locked accounts.</p>		







SEEBURGER



**By inspecting the documentation prepared by SEEBURGER INFORMATIK EOOD and through our IT-supported audit procedures, we were able to satisfy ourselves that this process is implemented and operated effectively and complies with the requirements of ISAE 3402 SOC 1 Type 2.**

<b>Management Practice by SEEBURGER INFORMATIK EOOD</b>	
<p><b>UAM_03 - Assigning permissions in the Active Directory</b></p> <p>Requests are submitted via e-mail. When the mail is sent, an incident is created automatically at the SEEBURGER INFORMATIK EOOD Service Desk. If it is a CR, the relevant IT employee generates a Change Request (CR) from the incident, which is then assessed. At SEEBURGER INFORMATIK EOOD, an Access Management Change is categorized as a Complex Change, which means that an approval by the data owner of the resource/information is always needed. This is ensured by the “four eyes” principle. With the approval of the data owner in the automated process of the identity and access management application the access is granted.</p>	
<b>Result</b>	
<p>A report from the incident management system was reviewed, which contains logs of access requests, including the resources requested, the data owners involved, and the approval status. In addition, documentation and workflows describing the formal request and approval process were available. The evidence shows that access is requested exclusively through the defined process and granted after approval by the responsible data owner. The review confirmed that the formal process is followed and that access requests are fully documented.</p> <p><b>By inspecting the documentation prepared by SEEBURGER INFORMATIK EOOD and through our IT-supported audit procedures, we were able to satisfy ourselves that this process is implemented and operated effectively and complies with the requirements of ISAE 3402 SOC 1 Type 2.</b></p>	
<b>Management Practice by SEEBURGER INFORMATIK EOOD</b>	
<p><b>UAM_04 - Access control for customer systems</b></p> <p>The request process for accessing customer systems is documented and communicated within the SEEBURGER INFORMATIK EOOD organization.</p> <p>The document is managed centrally in a document management system. A history of changes to the document is kept. New main versions of the document are checked and released in a formal approval process carried out by the head of Cloud Services. The relevant valid version is stored centrally in the SEEBURGER INFORMATIK EOOD intranet and can be accessed by all employees.</p> <p>As part of the initial training plan, new employees in the Cloud Services department receive training regarding the process documentation.</p>	

Result	✓
<p>A detailed process description was reviewed, documenting the formal steps for requesting and granting access to customer systems. In addition, technical configurations of the access management system were available, demonstrating the enforcement of access controls. Access logs showed that requests, approvals, and the actual granting of authorizations are fully documented. The audit confirmed that the defined process is implemented, the technical controls are effective, and compliance with access policies can be demonstrated in a traceable manner.</p> <p><b>By inspecting the documentation prepared by SEEBURGER INFORMATIK EOOD and through our IT-supported audit procedures, we were able to satisfy ourselves that this process is implemented and operated effectively and complies with the requirements of ISAE 3402 SOC 1 Type 2.</b></p>	
<p><b>Management Practice by SEEBURGER INFORMATIK EOOD</b></p>	
<p><b>UAM_05 - Removing user access privileges</b></p> <ul style="list-style-type: none"> <li>• Change of employees                             <ul style="list-style-type: none"> <li>○ Change of division</li> <li>○ Change of subsidiary</li> </ul> </li> <li>• Change of employees                             <ul style="list-style-type: none"> <li>○ Employee check-out list from HR (DE)</li> <li>○ HR Sofia: Generates incident by mail sent to edv-helpdesk@seeburger.de</li> <li>○ Intranet</li> </ul> </li> </ul> <p><b>Check of effectiveness</b></p> <p>Audit every three months through information security:</p> <ul style="list-style-type: none"> <li>• Actual incident available prior to retirement.</li> <li>• Was incident processed on time?</li> <li>• Was account processed in AD in line with incident specifications?</li> <li>• Was the “Valid To” date set?</li> </ul>	

<b>Result</b>	
<p>Logs from Active Directory were checked for locked or disabled user accounts containing the relevant lockout and deactivation data. The evidence shows that accounts in the cases examined were locked or disabled in a timely manner. The audit thus confirmed that an effective process for promptly locking inactive accounts is in place and is reliably implemented by IT administrators.</p> <p><b>By inspecting the documentation prepared by SEEBURGER INFORMATIK EOOD and through our IT-supported audit procedures, we were able to satisfy ourselves that this process is implemented and operated effectively and complies with the requirements of ISAE 3402 SOC 1 Type 2.</b></p>	
<b>Management Practice by SEEBURGER INFORMATIK EOOD</b>	
<p><b>UAM_06 - Expiry of user permissions for the EDI application</b></p> <p>The central Access Management Tool limits the internal access permissions for customer systems to a maximum of 90 days. Longer access times cannot be selected and are therefore not technically possible.</p> <p>After the authorization period elapses, the central Access Management Tool blocks access to the customer system automatically.</p>	
<b>Result</b>	
<p>A list of user permissions was reviewed, which included expiration dates and renewal status. In addition, evidence was provided that permissions that were not renewed within the specified 90-day period were automatically blocked. The audit confirmed that internal user permissions are effectively limited to 90 days and that the defined controls for automatic suspension are reliably implemented.</p> <p><b>By inspecting the documentation prepared by SEEBURGER INFORMATIK EOOD and through our IT-supported audit procedures, we were able to satisfy ourselves that this process is implemented and operated effectively and complies with the requirements of ISAE 3402 SOC 1 Type 2.</b></p>	
<b>Management Practice by SEEBURGER INFORMATIK EOOD</b>	
<p><b>UAM_08 - Checking users and rights for productive customer systems</b></p> <p>Authorized users are selected and added to a white list. Regular checks are performed to determine whether the users on the application level correlate with those in the white list. New users and changes are added/modified via a Change Request in the white list.</p>	

<b>Result</b>	
<p>The audit reviewed records of regular checks that document in detail the process for identifying and removing unauthorized users. In addition, evidence was provided that no unauthorized users were found in the system during the audit period. The audit confirmed that an effective monitoring process is in place and is reliably implemented to prevent unauthorized access to BIS6 customer systems.</p> <p><b>By inspecting the documentation prepared by SEEBURGER INFORMATIK EOOD and through our IT-supported audit procedures, we were able to satisfy ourselves that this process is implemented and operated effectively and complies with the requirements of ISAE 3402 SOC 1 Type 2.</b></p>	
<b>Management Practice by SEEBURGER INFORMATIK EOOD</b>	
<p><b>UAM_09 - Separating Access to Cloud Services from Corporate Access Management</b></p> <ul style="list-style-type: none"> <li>• Only authorized users managed by the SEEBURGER INFORMATIK EOOD Active Directory can access the central access application.</li> <li>• Employees who require access to productive customer systems in the Cloud Services area due to their job description requires an additional authorization in the central access application.</li> <li>• The Cloud Services Domain Account is requested by way of the central Change Management process and must be approved by the Cloud Services division.</li> </ul>	
<b>Result</b>	
<p>Configuration overviews of the central access application were reviewed, as well as logs documenting AD authentication and additional authorization for cloud service activities. The evidence confirms that all relevant activities pass through the defined authentication and authorization process. The audit found that the controls are effectively implemented and that compliance with the security requirements is reliably ensured.</p> <p><b>By inspecting the documentation prepared by SEEBURGER INFORMATIK EOOD and through our IT-supported audit procedures, we were able to satisfy ourselves that this process is implemented and operated effectively and complies with the requirements of ISAE 3402 SOC 1 Type 2.</b></p>	
<b>Management Practice by SEEBURGER INFORMATIK EOOD</b>	
<p><b>UAM_11 - Assigning administrative rights for productive customer systems on an application level</b></p> <p>Employee roles are defined in the Access Management process and assigned to the employee during the change process. Existing Access Management roles on productive customer systems are checked on a regular basis. The application rights assigned for each role are compared with the rights defined during the Access Management process. Checks are performed once a month by way of an automatically generated report documented during the Incident Management process.</p>	

<b>Result</b>	
<p>A report was reviewed that compares the application rights actually assigned with the rights defined for the employee role. In addition, documentation was available that identified any deviations and how they were corrected. The evidence confirms that application rights are assigned consistently with the defined roles and that deviations are corrected promptly. The audit found that access rights to productive customer systems are controlled and assigned on a role-based basis.</p> <p><b>By inspecting the documentation prepared by SEEBURGER INFORMATIK EOOD and through our IT-supported audit procedures, we were able to satisfy ourselves that this process is implemented and operated effectively and complies with the requirements of ISAE 3402 SOC 1 Type 2.</b></p>	
<b>Management Practice by SEEBURGER INFORMATIK EOOD</b>	
<p><b>UAM_12 - Network security between the corporate and the cloud services networks</b></p> <p>SEEBURGER INFORMATIK EOOD has defined and implemented network zones and subzones. Networks are implemented within each subzone and separated according to network type. Each network type is assigned a defined protection class (low, medium, high, very high). Strict communication rules apply between zones, subzones, networks and each subnet or device within the network. Communication from any network to the cloud service networks is denied by default. Only very few and specific communication channels are implemented to allow administrative and operational access to systems and applications within the cloud. For administrative access to Cloud Systems a specific IT Admin access tool is required. This tool is located in a separate network accessible over a jump station where only defined IT admins can login.</p> <p>For standard users access to Cloud Systems is only possible via a tunnel which is provided by the central Cloud Services Access Management Tool.</p>	
<b>Result</b>	
<p>A network diagram showing the separation of the cloud systems from other networks was reviewed. In addition, details were provided on the controls implemented, such as firewall rules and access restrictions, which ensure separation from a technical perspective. The evidence confirms that the cloud systems are effectively isolated and that the defined network controls are reliably implemented, preventing unauthorized access from other networks.</p> <p><b>By inspecting the documentation prepared by SEEBURGER INFORMATIK EOOD and through our IT-supported audit procedures, we were able to satisfy ourselves that this process is implemented and operated effectively and complies with the requirements of ISAE 3402 SOC 1 Type 2.</b></p>	

### 3. Physical Security

Control Objective
<p><b>PS - Physical Security</b></p> <p>Controls provide reasonable assurance that access to data center is approved, infrastructure is protected against environmental factors and assets entering the data center are tracked.</p>
Management Practice
<p><b>PS_01 - Access control to data centers</b></p> <p>Access rights to the data centers used by SEEBURGER INFORMATIK EOOD are allocated and checked in a formal multi-stage process.</p> <p><b>PS_05 - Managing equipment</b></p> <p>All inputs and outputs are implemented by SEEBURGER INFORMATIK EOOD employees and managed in a central database. The Global Head of Governance, Risk and Compliance checks the correctness on an annual basis.</p> <p><b>PS_07 - Data center security</b></p> <p>Control owner reviews attestation report(s) of the data center providers to ascertain that physical access and environmental controls are implemented and complied with. Follow-up activities are carried out in case of relevant deviations.</p>
Test to be performed by BFMT
<p><b>Test of Design</b></p> <p>The controls in the area of physical security are reviewed to determine whether they are adequately designed to achieve the control objectives. To this end, the description of the physical security process is reviewed to determine whether a multi-level process for granting access to data centers and a concept for managing data center assets have been defined and documented. In addition, the supplier evaluation form is reviewed to determine whether procedures and requirements for third-party activities have been defined and documented.</p>

**Test of Operating Effectiveness**

An assessment is made as to whether the physical security controls designed have functioned effectively over the audit period. To this end, the change history of the lists of employees granted access to data centers is reviewed to determine whether changes to authorized personnel have been made and documented. In addition, the access history to the data centers is reviewed to determine whether multi-level physical access controls have been implemented and enforced. The data center facilities are observed to determine whether a multi-level process is implemented. With regard to equipment management, the asset lists of the data centers are inspected to determine whether inventory records have been documented in a central database. The verification documentation is also inspected to determine whether entries and exits have been checked annually. The asset monitoring system is observed to determine whether procedures for monitoring assets at a high and individual asset level have been implemented. Finally, supplier evaluation documentation for data center security is inspected to determine whether audit reports have been reviewed in accordance with defined requirements.

**Management Practice by SEEBURGER INFORMATIK EOOD**

**PS\_01 - Access control to data centers**


Access to the data center must be requested from a SEEBURGER INFORMATIK EOOD QR, who forwards the query to the DC administration team. The DC administration prepares the access authorizations and issues the personalized PIN / card to the QR. The QR passes the access authorizations to the person who submitted the request. If the working relationship ends or there is a switch to another department, the QR the collects the DC access authorizations from the employee. The list from the QR and person with access authorization is checked annually by DC Administration.

**Result**



The documented process for granting and reviewing access rights was reviewed, including details on the multi-level procedure. In addition, logs of actual access grants and reviews were available. The interviews confirmed the application of the multi-level process and its effectiveness in practice. The audit found that access rights to the data centers are formally regulated, assigned in a traceable manner, and regularly monitored to ensure compliance with security guidelines.

**By inspecting the documentation prepared by SEEBURGER INFORMATIK EOOD and through our IT-supported audit procedures, we were able to satisfy ourselves that this process is implemented and operated effectively and complies with the requirements of ISAE 3402 SOC 1 Type 2.**

<b>Management Practice by SEEBURGER INFORMATIK EOOD</b>	
<p><b>PS_05 - Managing equipment</b></p> <p>All equipment orders are placed with assistance from tools. When the order is created using a PR, a unique PR number is generated. If a standard item already stored in the system is ordered, approval is granted according to the “four eyes” principle. If the item is not standard, however, technical approval is required before the final approval.</p> <p>The unique PR number makes it possible to uniquely assign the business letters associated with the purchase of the equipment. When the equipment is delivered, the inventory is created immediately after the goods are received by assigning and including a unique SEEBURGER INFORMATIK EOOD number in an asset database.</p>	
<b>Result</b>	
<p>Records of entries and exits managed in the central database were reviewed. In addition, evidence of the annual accuracy checks performed by the Global Head of Governance, Risk and Compliance was available. The interviews confirmed that entries and exits are systematically reviewed and that annual accuracy checks are performed. The audit found that the management of inputs and outputs is carried out properly and that the data is documented in a consistent and traceable manner.</p> <p><b>By inspecting the documentation prepared by SEEBURGER INFORMATIK EOOD and through our IT-supported audit procedures, we were able to satisfy ourselves that this process is implemented and operated effectively and complies with the requirements of ISAE 3402 SOC 1 Type 2.</b></p>	
<b>Management Practice by SEEBURGER INFORMATIK EOOD</b>	
<p><b>PS_07 - Data center security</b></p> <p>SEEBURGER INFORMATIK EOOD has ordered the following services:</p> <ul style="list-style-type: none"> <li>• Fixed connections,</li> <li>• Internet connection,</li> <li>• Server housing (air conditioning, power supply, emergency power management and fire protection (FAS, extinguishing system and early fire detection) and</li> <li>• The focus of the security assessment based on the review of the ISAE reports is evidence that the data center infrastructure used by SEEBURGER INFORMATIK EOOD in AT1, AT4 and AT5 as well for the TelemaxX data centers is maintained correctly.</li> </ul>	

Result	✓
<p>Copies of the audited certification reports from the data center providers were reviewed. In addition, documentation of all follow-up measures taken as a result of deviations was available. The audit confirmed that the data center providers are regularly monitored, the required standards are met, and necessary corrective measures are systematically implemented.</p> <p><b>By inspecting the documentation prepared by SEEBURGER INFORMATIK EOOD and through our IT-supported audit procedures, we were able to satisfy ourselves that this process is implemented and operated effectively and complies with the requirements of ISAE 3402 SOC 1 Type 2.</b></p>	

## 4. Go-Live Management

Control Objective
<p><b>GO - Go-Live Management</b></p> <p>Controls provide reasonable assurance that go-lives are authorized, documented and processed in a suitable manner.</p>
Management Practice
<p><b>GO_01 - All initial go-lives are documented in a go live request</b></p> <p>BIS6 initial go-lives are documented and authorized in a go live request.</p> <p><b>GO_02 - Go-Lives are processed within five days</b></p> <p>The Service Operations team will start processing a BIS6 initial go live request within five working days.</p> <p><b>GO_03 - The Go-live handover check list is to be completed and stored centrally</b></p> <p>For each BIS6 initial - go-live, a hand over is created that contains all relevant and necessary information for the go-live. These documents are stored centrally in a clearly assignable customer folder.</p>
Test to be performed by BFMT
<p><b>Test of Design</b></p> <p>The controls in go-live management are reviewed to ensure that go-lives are approved, documented, and carried out properly. The description of the go-live process is examined to determine whether a standardized procedure has been defined and documented for determining the scope, handling, and documentation of go-lives, response times and follow-up options, and the content and storage of handover documentation. In addition, the checklist is used to verify whether a standardized procedure for reviewing the necessary information and data prior to transfer has been developed and implemented.</p> <p><b>Test of Operating Effectiveness</b></p> <p>An assessment is made as to whether the controls designed in go-live management have functioned effectively over the audit period. To this end, the corresponding go-live ticket is inspected for a selection of go-lives to determine whether the go-lives were authorized and documented prior to processing. In addition, the list</p>

of all go-lives is inspected to determine whether processing was triggered within five working days of ticket creation. Finally, for a selection of go-lives, the go-live ticket and the handover checklist are inspected to determine whether the handover was processed and checked correctly.

**Management Practice by SEEBURGER INFORMATIK EOOD**

**GO\_01 - All initial go-lives are documented in a go live request**

To generate a go live request the project manager / consultant sends an e-mail to GoLive.MS@seeburger.de, which automatically generates a unique incident ID or can directly create a go live request within the SEEBURGER INFORMATIK EOOD CSP. This go live request is assigned to the Service Operations team for processing. The development of the processing is documented in the go live request until successful completion.

**Control of the effectiveness of the control**

A monthly report is generated showing all go live requests of the past month. The report generated is checked by the Service Operations team, and any defects in request processing are analyzed, corrected and, if necessary, measures taken for future avoidance.

**Result**



A report documenting all go-live requests was reviewed. In addition, documentation detailing the approval process was available. The evidence confirms that go-live requirements are formally recorded and properly approved. The review found that the process is applied consistently and that compliance with the defined go-live procedures is ensured.

**By inspecting the documentation prepared by SEEBURGER INFORMATIK EOOD and through our IT-supported audit procedures, we were able to satisfy ourselves that this process is implemented and operated effectively and complies with the requirements of ISAE 3402 SOC 1 Type 2.**

**Management Practice by SEEBURGER INFORMATIK EOOD**

**GO\_02 - Go-Lives are processed within five days**

An initial go-live request is assigned to the queue of the responsible operating team. The operation team checks this queue and starts the processing within five working days from the opening of the go live request.

**Control of the effectiveness of the control**

To control the effectiveness, a monthly report is produced containing the following information and the report is also verified by the operations team:

- Date and time of the go live request opening

- Start of processing (with date and time)
- Name of the Request Opener
- Subject of the request (Initial Go-Live)
- Name of the request Owner
- Completion of the request (with date and time)

<b>Result</b>	
---------------	---

Protocols of go-live requests documenting processing times were reviewed. In addition, key figures indicating the average time until processing begins were available. The evidence confirms that the Service Operations Team adheres to the specified time frame and starts processing initial go-live requests in a timely manner. The audit found that the process is applied consistently and that compliance with the defined deadlines is verifiable.

**By inspecting the documentation prepared by SEEBURGER INFORMATIK EOOD and through our IT-supported audit procedures, we were able to satisfy ourselves that this process is implemented and operated effectively and complies with the requirements of ISAE 3402 SOC 1 Type 2.**


**Management Practice by SEEBURGER INFORMATIK EOOD**

**GO\_03 - The Go-live handover check list is to be completed and stored centrally**

For each BIS6 initial go-live, the Service Operations team creates a separate handover, which is saved in the customer folder when the handling is complete.

**Control of the effectiveness of the control**

The hand over lists are stored centrally in the customer folder of the respective customer. The operations team is responsible for the completeness and correctness of the information stored in the handover. The check lists are checked monthly for completeness and correctness by the operations team.

<b>Result</b>	
---------------	---

The logs of the transfer documents created and stored were reviewed. In addition, confirmation was provided that the documents contain all relevant and necessary information for the go-live. The evidence confirms that the transfers have been completed and archived and that all necessary information for the successful implementation of the initial go-lives has been provided. The audit revealed that the process is applied consistently and that the documentation is traceable.



SEEBURGER

**By inspecting the documentation prepared by SEEBURGER INFORMATIK EOOD and through our IT-supported audit procedures, we were able to satisfy ourselves that this process is implemented and operated effectively and complies with the requirements of ISAE 3402 SOC 1 Type 2.**

## 5. Monitoring Management

Control Objective
<p><b>EM - Monitoring Management</b></p> <p>Controls provide reasonable assurance that all relevant systems and processes are constantly monitored and follow-up activities are initiated.</p>
Management Practice
<p><b>EM_01 - Initial set-up of the system monitoring system</b></p> <p>Within the EDI Cloud Services, SEEBURGER INFORMATIK EOOD uses a monitoring system to monitor important components fully automatically such as networks, servers and storage as well as applications and queues. The monitoring system ensures that error events are detected immediately. On every newly installed EDI system, a series of standard tests is set up, activated and tested in the system monitoring system during system deployment or by the go live at the latest.</p> <p><b>EM_02 - Initial set-up of process monitoring</b></p> <p>A process monitoring system monitors the processing errors of individual EDI processes and errors are reported to Incident Management. The process monitoring system must be set up and activated before the go live is announced (formal handover to the MS operating team) (part of “go live handover” checklist).</p> <p><b>EM_03 - Monitoring of the monitoring system</b></p> <p>Productive EDI systems are monitored by various monitoring systems (system monitoring and process monitoring systems) on a 24/7 basis. It must be ensured that all relevant monitoring checks are also performed. The operating team must respond to incomplete or abandoned checks with defined actions.</p> <p><b>EM_04 - Error identification using the system monitoring system</b></p> <p>Monitoring checks are set up in such a way that errors are detected by defined threshold values / status and incidents are generated in the system monitoring system. The operator is notified of these events. Moreover, defined error events generate cases that are processed in the incident management process.</p> <p><b>EM_05 - Error identification using the process monitoring system</b></p> <p>If errors occur when messages are processed in productive EDI systems, these are identified by the process monitoring system and transferred as a case or added to an existing case to the case management system together with a unique reference relating to the error. Each case will be handled as part of the incident process.</p>

### Test to be performed by BFMT

#### Test of Design

The monitoring management controls are reviewed to determine whether they are appropriately designed to achieve the control objectives. To this end, the description of the event management process is reviewed to determine whether procedures for detecting events on customer systems and for checking the monitoring of newly installed EDI systems have been defined and documented by the go-live date at the latest. In addition, the list of mandatory monitoring of established standard tests is reviewed to determine whether a procedure for implementing and testing a series of standard tests has been defined and implemented. The description of the event management process is also inspected to determine whether procedures for setting up and activating process monitoring prior to go-live and for processing errors in individual EDI processes have been defined and documented. In addition, it is checked whether a monitoring concept including mandatory tests for customer systems has been developed and documented. Finally, the description of the event management process is inspected to determine whether controls and procedures for monitoring the operation of EDI systems have been defined and documented. The description of the event management process with regard to the operation of EDI processes is also inspected to determine whether the monitoring system and monitoring procedures have been defined and implemented.

#### Test of Operating Effectiveness

An assessment is made as to whether the controls designed in monitoring management have functioned effectively over the audit period. To this end, the Icinga system configurations of a selection of newly installed EDI systems are inspected to determine whether the standard tests for go-live setup have been performed and monitoring is activated. In addition, the system configurations and handover lists for a selection of newly installed EDI systems are inspected to determine whether monitoring was set up, activated, and tested prior to go-live. An online demonstration of the Icinga monitoring tool is also observed to determine whether procedures for implementing monitoring schedules and events have been defined and implemented for each host. In addition, the list of all registered customer systems from Icinga and all relevant customer systems are inspected to determine whether monitoring of all relevant customer systems has been implemented. The list of mandatory monitoring of established standard tests is reviewed to determine whether controls and tests for detecting error events have been defined and implemented. For a selection of error events, incident tickets are checked to determine whether errors have been identified and tracked. Finally, for a selection of errors, the monitoring system and the corresponding incident tickets are inspected to determine whether the errors have been confirmed and tracked.

**Management Practice by SEEBURGER INFORMATIK EOOD**

**EM\_01 - Initial set-up of the system monitoring system**

The system monitoring system is set up in a multistage process. A productive system undergoes several development stages here. The IT infrastructure team implements the basic installation of the SEEBURGER INFORMATIK EOOD business integration server on a virtual host. On completion of the basic installation, this system is transferred to the Cloud Services division. During the second phase, the current state of the installation is checked and accepted, and the standard system monitoring system is set up. The tests are conducted independently of the customerspecific installation and standardized to suit all productive systems. Examples of standard monitoring tests include e.g. availability of storage space, RAM, CPU and application-specific parameters.

When the standard monitoring system is completed, it is transferred to SEEBURGER INFORMATIK EOOD Consulting. During the initial project, customer-specific installations are set up and tested in collaboration with the customer. On successful completion of the installation and test phase, Consulting hands the system back to the Cloud Services division as part of the go live process, which represents a dedicated handover of responsibility. The installation implemented by Consulting is accepted and then the customer-specific part of the system monitoring system is set up. This can involve setting up special tests to check the connection to the customer’s ERP system, for example.

The go live signals the end of the set-up phase.

**Result**



A report from the monitoring system was reviewed, documenting the monitored components, the tests performed, and the status of each component. The evidence confirms that critical components are continuously monitored and that the results of the tests are traceable. The review found that automated monitoring is effectively implemented and that the status of components is regularly checked.

**By inspecting the documentation prepared by SEEBURGER INFORMATIK EOOD and through our IT-supported audit procedures, we were able to satisfy ourselves that this process is implemented and operated effectively and complies with the requirements of ISAE 3402 SOC 1 Type 2.**

**Management Practice by SEEBURGER INFORMATIK EOOD**

**EM\_02 - Initial set-up of process monitoring**

While the system monitoring system monitors the availability of the application, the connections and the resources required for faultless EDI operation, the process monitoring system monitors the completeness and correctness of messages handled within the implemented processes. Here, a “process” is defined as follows:

EDI messages are processed within a defined process sequence. The EDI system executes these processes as well as the process steps defined within the process (components).

If an error occurs within a component during process handling (e.g. due to an error in the received message), the process switches to error status and is assigned a corresponding process status.


Examples of process errors include:

- Unexpected termination of a process,
- Errors within a processing step or
- Excessive runtime of a process.

The purpose of the process monitoring system is to identify faulty processes at regular intervals as well as transfer this information to an Event Management System (component of the process monitoring system). The Event Management System consolidates and qualifies errors according to defined criteria and generates incidents in the Incident Management System in line with defined rules.


During the go live process, Consulting hands over the completed EDI system to the Managed Services operating team. The MS operating team checks the configuration of the process monitoring system to determine whether process monitoring has been activated for the transferred EDI system and the corresponding client(s).

The initial set-up of the process monitoring system is the final step before the operating team rolls out the Managed Services system.

<b>Result</b>	
---------------	--

A report from the process monitoring system was reviewed, which contains a log of processing errors and details on how these errors were reported to incident management. The evidence confirms that detected errors are reliably recorded and forwarded to incident management. The audit found that process monitoring is effectively implemented and ensures that errors are reported and processed in a timely manner.

**By inspecting the documentation prepared by SEEBURGER INFORMATIK EOOD and through our IT-supported audit procedures, we were able to satisfy ourselves that this process is implemented and operated effectively and complies with the requirements of ISAE 3402 SOC 1 Type 2.**

<b>Management Practice by SEEBURGER INFORMATIK EOOD</b>	
<p><b>EM_03 - Monitoring of the monitoring system</b></p> <p><b>Implementation of process monitoring</b></p> <p>The process monitoring system is monitored from the system monitoring system. The fact that there are two different applications on different platforms ensures that mutual interference is excluded in the event of a fault.</p> <p>A minimum of one scheduler is configured for each host on the process monitoring system. The process checks (scheduler) are performed during the intervals stored in the scheduler configuration.</p> <p>In the system monitoring system (Icinga), an analog check that performs the following tests is scheduled for each host and configured scheduler:</p> <p>Check whether the last two process monitoring schedules were completed. The Icinga check monitors whether any checks were performed within the last 30 minutes and whether they were successful or failed:</p> <ol style="list-style-type: none"> <li>1. If one of the two checks fails, a warning is issued</li> <li>2. If both checks fail, an error message is issued and a case is created in the SEEBURGER INFORMATIK EOOD Case Management System and processed by the operating team.</li> <li>3. A case is also created if no checks were performed within the defined 30-minute time frame.</li> </ol> <p><b>Implementation of system monitoring</b></p> <p>The redundant design at different locations ensures the high availability (HA) of the system monitoring system. The operating team monitors the system monitoring system (Icinga) manually. If the system monitoring system no longer functions, the operating team can identify this from the system monitoring frontend and a case is then generated and processed.</p>	
<b>Result</b>	
<p>A report documenting the schedule of surveillance audits and responses to incomplete or discontinued audits was reviewed. The evidence confirms that the productive EDI systems are monitored around the clock and that appropriate measures are taken in the event of interruptions or errors. The audit found that continuous monitoring is effectively implemented and ensures a timely response to problems.</p>	

**By inspecting the documentation prepared by SEEBURGER INFORMATIK EOOD and through our IT-supported audit procedures, we were able to satisfy ourselves that this process is implemented and operated effectively and complies with the requirements of ISAE 3402 SOC 1 Type 2.**

**Management Practice by SEEBURGER INFORMATIK EOOD**

**EM\_04 - Error identification using the system monitoring system**

The threshold values that change the status of the monitoring checks are defined centrally and are equally valid for all productive systems within the scope of the ISAE 3402 audit.

**Result**



A report was reviewed that documents the defined thresholds and status configurations and contains a log of the incidents generated. The evidence confirms that the monitoring checks are set up correctly, errors are reliably detected, and corresponding incidents are generated automatically. The audit found that the monitoring setup is effective and ensures timely detection and reporting of system problems.

**By inspecting the documentation prepared by SEEBURGER INFORMATIK EOOD and through our IT-supported audit procedures, we were able to satisfy ourselves that this process is implemented and operated effectively and complies with the requirements of ISAE 3402 SOC 1 Type 2.**

**Management Practice by SEEBURGER INFORMATIK EOOD**


**EM\_05 - Error identification using the process monitoring system**

EDI Process errors are detected by the monitoring system and forwarded to the case management system. Within the case management system:

- A rule engine evaluates each error by mathematical expressions.
- Additional information is added to the process error record to provide further details for resolution and information to the customer or its trading partner.
- Multiple rules are triggered in succession based on a weighting.
- Each rule can add more detail to the case record or trigger a specific action.
- The criticality of a case is determined and defines the priority of the further processing of a case.
- Same EDI process errors are added to an existing case rather than opening many cases for the same issue. Speeding up handling and resolution of issues significantly.
- If a case requires to involve customers or trading partners into further root cause evaluation a regular incident is opened at the Servicedesk.

The handling of cases follows the incident management process. Thus, the same Incident Management SLA criteria applies. The advantages of the case handling in the new Case Management system are:

- Much faster evaluation of a process error,
- More specific enrichment of further details to analyze and solve a case,
- Faster information to customers and trading partners if issues are detected which needs to be solved on their site,
- Provides new options to further automate error and incident handling.

<b>Result</b>	
---------------	---

A report was reviewed that contains a log of identified errors and details on how these errors were forwarded to the case management system. The evidence confirms that identified errors are reliably recorded and systematically forwarded to the case management system. The audit found that the error identification and escalation process is effectively implemented and ensures that processing errors are handled in a timely manner.

**By inspecting the documentation prepared by SEEBURGER INFORMATIK EOOD and through our IT-supported audit procedures, we were able to satisfy ourselves that this process is implemented and operated effectively and complies with the requirements of ISAE 3402 SOC 1 Type 2.**

## 6. Incident Management

Control Objective
<p><b>IM - Incident Management</b></p> <p>Controls provide reasonable assurance that operational procedures are monitored, SLA-deviations are identified and incidents are handled quickly to recover service availability.</p>
Management Practice
<p><b>IM_01 - Service Level Agreements and priorities in Incident Management</b></p> <p>Contractually agreed Service Level Agreements for each specific customer are stored in the SEEBURGER INFORMATIK EOOD Service Desk.</p> <p><b>IM_02 - Escalation of the IRT</b></p> <p>For priority level 1 (emergency) and 2 (critical) incidents, an escalation process is initiated after 80 % of the response time elapses.</p>
Test to be performed by BFMT
<p><b>Test of Design</b></p> <p>It is checked whether the controls in incident management are appropriately designed to achieve the control objectives. To this end, the description of the incident management process is reviewed to determine whether a procedure for processing incident tickets in accordance with the contractually defined service level agreements has been documented. In addition, it is checked whether an escalation procedure for incidents of priority levels 1 and 2 has been defined and documented.</p> <p><b>Test of Operating Effectiveness</b></p> <p>An assessment is made as to whether the controls designed in incident management have functioned effectively over the audit period. To this end, the “Helpline” ticketing tool and the system configuration are monitored to determine whether configurations for response and processing times have been implemented in accordance with the contractually agreed service level agreements. In addition, customer contracts and master data from customer classification are inspected for a selection of customers to determine whether the agreed service level agreements and operating times have been correctly transferred to the system. Finally,</p>

incident tickets and SLA reports are reviewed for a selection of critical and emergency incidents that triggered the escalation process to determine whether incidents were escalated and handled in accordance with the incident management process description.

**Management Practice by SEEBURGER INFORMATIK EOOD**

**IM\_01 - Service Level Agreements and priorities in Incident Management**

The SLAs and service times contractually agreed with the customer form the basis for processing incidents. These form part of the service and performance description for each specific customer and are stored in the SEEBURGER INFORMATIK EOOD Service Desk.

When a contract is concluded with the customer, the signed documents are digitalized and stored in the SEEBURGER INFORMATIK EOOD master data system. The Service Level Agreement modules relevant for incident processing are transferred to the SEEBURGER INFORMATIK EOOD Service Desk. The MDM system is also a data source here. An automated comparison is performed on a daily basis to ensure data consistency between both systems. If any discrepancies are identified, a ticket is generated and a manual follow-up inspection is initiated.

**Result**



A report containing a list of customers and their contractually agreed SLAs was reviewed. The evidence confirms that the SLAs for all customers are stored in the service desk and can be traced at any time. The review found that the documentation of the SLAs is complete and consistent. In addition, an assessment was made of whether compliance with the agreed SLAs is regularly monitored and reported.

**By inspecting the documentation prepared by SEEBURGER INFORMATIK EOOD and through our IT-supported audit procedures, we were able to satisfy ourselves that this process is implemented and operated effectively and complies with the requirements of ISAE 3402 SOC 1 Type 2.**


**Management Practice by SEEBURGER INFORMATIK EOOD**

**IM\_02 - Escalation of the IRT**

Response times for incidents form part of “Premium” quality Service Level Agreements contractually agreed with the customer. The escalation process handles the prioritization of levels 1 (emergency) and 2 (critical) because related faults can have a severe impact on the customer’s EDI business processes. The processing of such faults has to start within the defined response times, which is why an escalation process is initiated once 80 % of the respective response time has elapsed.

When a ticket is opened, it is assigned an entry time stamp, the SLA of the customer and prioritization information. The response times agreed contractually with the customer are stored in the ticket system.

When a priority 1 or 2 incident reaches 80 % of the agreed response time and an advisor has not yet started to process the incident, the ticket system sends an escalation mail to a defined target group automatically. Members of the group then initiate the actions required to ensure the ticket is processed in compliance with SLA.

<b>Result</b>	
---------------	---

A report containing a log of high-priority incidents and the associated escalation times was reviewed. The evidence confirms that the escalation process for emergency and critical incidents is reliably triggered after the defined times. The review found that high-priority incidents are monitored in a timely manner and escalated in accordance with the guidelines.

**By inspecting the documentation prepared by SEEBURGER INFORMATIK EOOD and through our IT-supported audit procedures, we were able to satisfy ourselves that this process is implemented and operated effectively and complies with the requirements of ISAE 3402 SOC 1 Type 2.**

## 7. System-Based Change Management

Control Objective
<p><b>CM - System-Based Change Management</b></p> <p>Controls provide reasonable assurance that system-based changes (including emergency changes) to applications are authorized, tested, approved and documented.</p>
Management Practice
<p><b>CM_01 - Documented Change Management process</b></p> <p>Changes are managed in a formal process.</p> <p><b>CM_02 - Testing and quality assurance of changes</b></p> <p>As part of System-Based Change Management, only software updates and service packs approved by QA are imported. A QA approval for Emergency Changes can also be issued at a later time.</p> <p><b>CM_03 - Documentation of implemented changes</b></p> <p>Each change is checked to determine whether all mandatory information has been provided.</p> <p><b>CM_04 - Change Advisory Approval</b></p> <p>CAB approval is obtained for normal changes.</p> <p><b>CM_05 - Approval and documentation in emergency cases</b></p> <p>ECAB approval is required for emergency changes, but this can be obtained at a later time.</p> <p><b>CM_06 - Final approval and documentation of changes</b></p> <p>Function tests must be conducted once the change is implemented. The test results are documented in the change.</p>

### Test to be performed by BFMT

#### Test of Design

The focus is on whether the controls in system-based change management are appropriately designed to achieve the control objectives. To this end, the description of the system-based change management process is inspected to determine whether procedures for documenting, authorizing, and validating changes to production have been defined and documented. Furthermore, it is checked whether procedures for testing and quality assurance of changes have been defined and documented, including the approval of emergency changes by quality assurance. In addition, it is checked whether procedures for documenting all necessary information after the implementation of changes have been defined and documented. Finally, it is checked whether procedures for approving changes by the CAB and for approving emergency changes by the ECAB have been defined and documented. This also takes into account subsequent approval for emergency changes. It is also checked whether procedures for performing functional tests and for documenting the test results have been defined and documented.



#### Test of Operating Effectiveness



An assessment is made as to whether the controls designed in system-based change management have functioned effectively over the audit period. To this end, change requests and corresponding tickets for a selection of changes are inspected to determine whether the changes were authorized and documented prior to processing. For a further selection of changes, the change requests and tickets are reviewed to ensure that only software updates and service packs approved by quality assurance have been imported. For a selection of emergency changes, the corresponding tickets and quality assurance documentation are reviewed to determine whether quality assurance approved the changes. Finally, for a selection of changes, the corresponding tickets are inspected to determine whether all required information has been provided. For a selection of normal changes, the corresponding tickets are reviewed to determine whether the changes were approved by the CAB. For a selection of emergency changes, a check is performed to determine whether the emergency changes have been approved by the ECAB. Finally, for a selection of implemented changes, the corresponding tickets are checked to determine whether functional tests have been performed and the test results documented.



### Management Practice by SEEBURGER INFORMATIK EOOD

#### CM\_01 - Documented Change Management process

The procedure for handling system-based changes is described in central documentation. The document is managed centrally in a document management system. A history of changes to the document is kept. New main versions of the document are checked and released in a formal approval process carried out by the head of Cloud Services. The relevant valid version is stored centrally in the SEEBURGER INFORMATIK EOOD intranet and can be accessed by all employees.

<b>Result</b>	
<p>A report was reviewed that contains a record of the changes, their status, and the change process that was carried out. The evidence confirms that changes are managed according to a defined, formal process. The audit found that the change management process is applied consistently and that all changes are documented in a traceable manner.</p> <p><b>By inspecting the documentation prepared by SEEBURGER INFORMATIK EOOD and through our IT-supported audit procedures, we were able to satisfy ourselves that this process is implemented and operated effectively and complies with the requirements of ISAE 3402 SOC 1 Type 2.</b></p>	
<b>Management Practice by SEEBURGER INFORMATIK EOOD</b>	
<p><b>CM_02 - Testing and quality assurance of changes</b></p> <p>The QA department at SEEBURGER INFORMATIK EOOD stores software elements (releases, service packs, hotfixes) approved by QA in a central location (HadDock). For system-based Changes, only software elements from HadDock are imported.</p> <p>Exception: Development may also provide a hotfix directly in particularly critical cases (Emergency Changes). This must either be approved by QA at a later time, or an official hotfix / service pack must be implemented in an additional system-based change.</p>	
<b>Result</b>	
<p>A report was reviewed that contains a log of imported software updates and service packs, as well as documentation of QA approval. The documentation confirms that only approved updates and service packs are transferred to the production systems. The review found that the QA-driven release process is reliably implemented and that changes are only made after formal approval.</p> <p><b>By inspecting the documentation prepared by SEEBURGER INFORMATIK EOOD and through our IT-supported audit procedures, we were able to satisfy ourselves that this process is implemented and operated effectively and complies with the requirements of ISAE 3402 SOC 1 Type 2.</b></p>	
<b>Management Practice by SEEBURGER INFORMATIK EOOD</b>	
<p><b>CM_03 - Documentation of implemented changes</b></p> <p>In the CSP mandatory fields are defined that require the input of necessary information. Without the correct indication of the information, the change request cannot be forwarded for approval. It is the responsibility of the CAB to check the Change Request for completeness and reject approval, if necessary.</p>	

<b>Result</b>	
<p>A report was reviewed that documents a log of changes and the checks performed. The evidence confirms that each change is checked for completeness of mandatory information. The audit found that the process for ensuring complete change information is consistently implemented and that changes are only processed with all necessary information.</p> <p><b>By inspecting the documentation prepared by SEEBURGER INFORMATIK EOOD and through our IT-supported audit procedures, we were able to satisfy ourselves that this process is implemented and operated effectively and complies with the requirements of ISAE 3402 SOC 1 Type 2.</b></p>	
<b>Management Practice by SEEBURGER INFORMATIK EOOD</b>	
<p><b>CM_04 - Change Advisory Approval</b></p> <p>In the SEEBURGER INFORMATIK EOOD CSP the complete change process is implemented. The approval of changes is firmly implemented in the CSP and must always take place before a change can be implemented.</p> <p>The approval can only be given by members of the CAB. Those CAB members are defined and documented in the related work instruction.</p>	
<b>Result</b>	
<p>A report containing a log of normal changes and their CAB approval status was reviewed. The evidence confirms that CAB approval is obtained for all normal changes. The review found that the approval process is reliably implemented and that changes are only implemented after formal approval by the CAB.</p> <p><b>By inspecting the documentation prepared by SEEBURGER INFORMATIK EOOD and through our IT-supported audit procedures, we were able to satisfy ourselves that this process is implemented and operated effectively and complies with the requirements of ISAE 3402 SOC 1 Type 2.</b></p>	
<b>Management Practice by SEEBURGER INFORMATIK EOOD</b>	
<p><b>CM_05 - Approval and documentation in emergency cases</b></p> <p>In the CSP, the approval step is stored permanently in the Change process. In emergency situations, the Change Owner of an Emergency Change can implement the change without written approval and instead obtain verbal confirmation from an ECAB member. The Change Owner documents the verbal approval from the ECAB member in the change (separate service unit in the change).</p> <p>A CAB member can provide written approval the next working day in the CSP.</p>	

<b>Result</b>	
<p>A report containing a log of emergency changes and their ECAB approval status was reviewed. The evidence confirms that ECAB approval is obtained for all emergency changes, even if this is done retrospectively. The review found that the emergency change process is effectively implemented and that changes are only completed after formal approval by the ECAB.</p> <p><b>By inspecting the documentation prepared by SEEBURGER INFORMATIK EOOD and through our IT-supported audit procedures, we were able to satisfy ourselves that this process is implemented and operated effectively and complies with the requirements of ISAE 3402 SOC 1 Type 2.</b></p>	
<b>Management Practice by SEEBURGER INFORMATIK EOOD</b>	
<p><b>CM_06 - Final approval and documentation of changes</b></p> <p>A PIR (Post Implementation Review) section in the Change Request specifies the tests required following a change (mandatory fields). The Change Owner must conduct these tests after a change is implemented and then enter the test results in the Change Form.</p>	
<b>Result</b>	
<p>A report containing a log of changes and the corresponding functional test results was reviewed. The evidence confirms that functional tests are performed after each change and the results are documented. The review found that the process for ensuring functional testing is implemented consistently and that changes are only completed after successful test documentation.</p> <p><b>By inspecting the documentation prepared by SEEBURGER INFORMATIK EOOD and through our IT-supported audit procedures, we were able to satisfy ourselves that this process is implemented and operated effectively and complies with the requirements of ISAE 3402 SOC 1 Type 2.</b></p>	

## 8. Backup & Recovery

Control Objective
<p><b>BR - Backup &amp; Recovery</b></p> <p>Controls provide reasonable assurance that back-up is accurate, available, complete, monitored and readability of media is ensured through regular tests.</p>
Management Practice
<p><b>BR_01 - Formal process</b></p> <p>The backup and restoration of data is regulated in a formal process. The finer details are outlined in management manuals and the service catalog.</p> <p><b>BR_02 - Specifying the backup data</b></p> <p>All EDI systems are implemented according to a backup set-up guideline, which defines the directories and database schemata that need to be backed up. The implementation is documented in a ticket.</p> <p><b>BR_03 - Verification of successful data backup</b></p> <p>The successful implementation of the backup is verified by:</p> <ul style="list-style-type: none"> <li>• Regular reviews of the log files written during the backup.</li> <li>• Monitoring and notification from the manufacturer in the case of irregularities.</li> </ul> <p><b>BR_04 - Actuality and regulations</b></p> <p>The interval and storage periods of the backups are defined and described in the service catalog.</p> <p><b>BR_05 - Restoration tests</b></p> <p>Restoration tests are conducted and documented at regular intervals.</p>
Test to be performed by BFMT
<p><b>Test of Design</b></p>

We check whether the controls in backup and recovery management are appropriately designed to achieve the control objectives. To this end, we review the description of the backup and recovery process to determine whether procedures for preparing all systems for a regulated backup process have been defined and documented. In addition, it is checked whether procedures for implementing and documenting the standard backup configuration as well as for directories and database schemas have been defined and documented. Furthermore, it is checked whether a schedule for performing backups and documenting them has been defined and documented. Finally, the description of the backup service catalog is inspected to determine whether procedures for backup intervals and storage periods have been defined and documented. The description of the backup and recovery process is also inspected to determine whether procedures for regular recovery and recovery testing of backed-up data have been defined and documented.

**Test of Operating Effectiveness**

An assessment is made as to whether the controls designed for backup and recovery management have functioned effectively over the audit period. To this end, the system configuration is inspected for a selection of newly installed EDI systems and the corresponding status is checked to determine whether implementation was carried out in accordance with the backup setup policy. The backup log files are monitored to verify that the backups were documented automatically. Incident tickets are reviewed for all failed backups to determine whether errors were confirmed and follow-up actions were initiated and documented. For a selection of quarterly reviews, the review documentation is examined to determine whether regular reviews have been performed and tracked. In addition, the system configuration of the backup management tool is checked to determine whether the system has been configured in accordance with the description of the backup and recovery process and the backup service catalog. Finally, the test logs of all recovery tests performed are inspected to determine whether they have been performed regularly.

**Management Practice by SEEBURGER INFORMATIK EOOD**

**BR\_01 - Formal process**

The data backup and restoration process are described in a formal process and published in management manuals within the IT organization.

**Result**







A report containing the documented process for data backup and recovery was reviewed. The evidence confirms that the backup and recovery measures are formally regulated and documented in a comprehensible manner. The audit revealed that the process is implemented consistently and that data backup and recovery are controlled and carried out according to plan.



SEEBURGER

**By inspecting the documentation prepared by SEEBURGER INFORMATIK EOOD and through our IT-supported audit procedures, we were able to satisfy ourselves that this process is implemented and operated effectively and complies with the requirements of ISAE 3402 SOC 1 Type 2.**

<b>Management Practice by SEEBURGER INFORMATIK EOOD</b>	
<p><b>BR_02 - Specifying the backup data</b></p> <p>The following data is backed up during the standard data backup:</p> <ul style="list-style-type: none"> <li>• EDI system configuration data,</li> <li>• Database and EDI runtime data and</li> <li>• Communication master data of trading partners.</li> </ul>	
<b>Result</b>	
<p>A report containing a list of EDI systems and their respective security configurations was reviewed. The evidence confirms that all EDI systems have been implemented and secured in accordance with the policy. The review found that the security configurations are consistently implemented and that the data security measures comply with the established standards.</p> <p><b>By inspecting the documentation prepared by SEEBURGER INFORMATIK EOOD and through our IT-supported audit procedures, we were able to satisfy ourselves that this process is implemented and operated effectively and complies with the requirements of ISAE 3402 SOC 1 Type 2.</b></p>	
<b>Management Practice by SEEBURGER INFORMATIK EOOD</b>	
<p><b>BR_03 - Verification of successful data backup</b></p> <p>Data backup logs are examined and any faults that occur are analyzed and managed.</p>	
<b>Result</b>	
<p>A report containing logs of the backup processes and their successful completion was reviewed. The evidence confirms that the implementation of the backup is regularly reviewed and that the backups are performed successfully. The review found that the backup reviews are performed consistently and that the integrity of the backups is ensured.</p> <p><b>By inspecting the documentation prepared by SEEBURGER INFORMATIK EOOD and through our IT-supported audit procedures, we were able to satisfy ourselves that this process is implemented and operated effectively and complies with the requirements of ISAE 3402 SOC 1 Type 2.</b></p>	

<b>Management Practice by SEEBURGER INFORMATIK EOOD</b>	
<b>BR_04 - Actuality and regulations</b>	
All EDI productive data from the EDI Cloud Service is backed up incrementally once a day and fully once a week (referred to as “standard data backup” in the following). The relevant data backups are stored for ten days. The configuration data of the EDI system (SEEBURGER INFORMATIK EOOD Business Integration Server) in the data center, the EDI database and the runtimes of the EDI system are backed up.	
<b>Result</b>	
A report documenting the defined backup intervals and retention periods was reviewed. The evidence confirms that the intervals and retention periods are clearly defined and described in a comprehensible manner. The audit found that the backup strategy is implemented consistently and that data is backed up and retained in accordance with the established guidelines.	
<b>By inspecting the documentation prepared by SEEBURGER INFORMATIK EOOD and through our IT-supported audit procedures, we were able to satisfy ourselves that this process is implemented and operated effectively and complies with the requirements of ISAE 3402 SOC 1 Type 2.</b>	
<b>Management Practice by SEEBURGER INFORMATIK EOOD</b>	
<b>BR_05 - Restoration tests</b>	
Regular restoration tests are conducted to guarantee the usability of the data backup systems.	
<b>Result</b>	
A report containing records of the recovery tests performed and their results was reviewed. The evidence confirms that recovery tests are planned, performed, and documented on a regular basis. The audit found that the effectiveness of backup and recovery measures is systematically reviewed and that data can be reliably recovered when needed.	
<b>By inspecting the documentation prepared by SEEBURGER INFORMATIK EOOD and through our IT-supported audit procedures, we were able to satisfy ourselves that this process is implemented and operated effectively and complies with the requirements of ISAE 3402 SOC 1 Type 2.</b>	

## 9. Business Continuity Management

Control Objective
<p><b>BC - Business Continuity Management</b></p> <p>Controls provide reasonable assurance that Business Continuity measures are established and applied.</p>
Management Practice
<p><b>BC_01 - SEEBURGER INFORMATIK EOOD emergency plan</b></p> <p>The organization is prepared for defined crisis scenarios and there are set procedures for assembling the emergency operation organization. These procedures are reviewed on a regular basis.</p> <p><b>BC_02 - Handling unforeseen events like force majeure or critical Cyber Security attack</b></p> <p>In the event of an unforeseen event like force majeure or critical cyber security attack with a potential to affect many systems and/or staff and/or customers, BCM ensures that the SEEBURGER INFORMATIK EOOD organization and SEEBURGER INFORMATIK EOOD business processes continue to operate, e.g. functions are assumed by other locations.</p> <p><b>BC_03 - Safety of equipment</b></p> <p>The relevant company values for the scope of the ISAE 3402 audit are included in an asset management system. Information about:</p> <ul style="list-style-type: none"> <li>• Identification,</li> <li>• Software,</li> <li>• Employees,</li> <li>• Spatial assignment and</li> <li>• saved or processed information</li> </ul> <p>is related to one another in this asset management system.</p> <p><b>BC_04 - Protection requirements analysis</b></p> <p>The criticality and restoration sequence of the systems are determined during the protection requirements analysis.</p>

### **BC\_05 - Evidence of the effectiveness of measures**

The replication of the data is configured in accordance with the contractually agreed DR option.

#### **Test to be performed by BFMT**

#### **Test of Design**

The focus is on whether the controls in business continuity management are appropriately designed to achieve the control objectives. To this end, the business continuity process is analyzed to determine whether procedures and responsibilities for business continuity have been defined and documented for a variety of crisis scenarios. The cyber crisis management plan is inspected to verify that specific assessment and activity procedures have been defined and implemented for SEEBURGER INFORMATIK EOOD subsidiaries. In addition, the description of the business continuity process is inspected to determine whether procedures have been defined and documented to ensure business continuity in the event of force majeure scenarios. The description of the business continuity process is also inspected to determine whether procedures for integrating asset management and business continuity management have been defined and documented. The inspection of the protection needs analysis tool verifies whether a procedure for assessing the criticality and recovery sequence of systems has been implemented. Finally, the description is inspected to determine whether a procedure for restoring backed-up data has been defined and documented.

#### **Test of Operating Effectiveness**

An assessment is made as to whether the controls designed in the business continuity management system have functioned effectively over the audit period. This includes reviewing the annual crisis management exercise to determine whether the organization has conducted specific training on possible crisis scenarios. For a selection of business processes, the emergency plan for force majeure scenarios and the countermeasures are inspected to determine whether procedures have been defined to ensure business continuity. The asset management system is reviewed to determine whether a central asset database has been defined and implemented that documents the criticality of each asset for business continuity. Furthermore, the protection needs analysis report is reviewed to determine whether procedures for analyzing the criticality of relevant systems have been defined and implemented and whether consequences for the recovery sequence have been derived from this. Finally, the test logs of all recovery tests performed are inspected to determine whether they have been carried out regularly.

#### **Management Practice by SEEBURGER INFORMATIK EOOD**

#### **BC\_01 - SEEBURGER INFORMATIK EOOD emergency plan**

SEEBURGER INFORMATIK EOOD maintains a crisis plan that covers major crisis scenarios such as building damage, loss of personnel and damage to IT infrastructure due to e.g. fire, natural disasters, pandemics or cyber-attacks.

The crisis plan defines the crisis team, internal and external communication as well as initial measures and the organization in the emergency run and restart phase. In addition, each critical area maintains and tests concrete emergency run and recovery plans of its business processes.

**Result**



Interviews were conducted and a report was reviewed that contains the documented crisis scenarios and the corresponding procedures for convening the emergency response organization. The evidence confirms that the organization is prepared for defined crisis scenarios and that the emergency response organization can be structured and set up in a comprehensible manner. The audit found that the procedures are consistently documented and can be implemented.

**By inspecting the documentation prepared by SEEBURGER INFORMATIK EOOD and through our IT-supported audit procedures, we were able to satisfy ourselves that this process is implemented and operated effectively and complies with the requirements of ISAE 3402 SOC 1 Type 2.**

**Management Practice by SEEBURGER INFORMATIK EOOD**

**BC\_02 - Handling unforeseen events like force majeure or critical Cyber Security attack**

Based on defined criteria either a specific disaster situation or a major crisis situation will be detected and the crisis plan activated. The crisis team immediately is activated and will work according the defined procedures.

In case of a technical disaster situation the disaster recovery procedures will be initiated and infrastructure and systems activated on the disaster recovery location.


In case of a major crisis situation the departments activate their emergency procedures and work according to the defined emergency plans. Recovery teams are activated and start the recovery of the infrastructure according the recovery plans. The recovery plans contain the recovery of critical business processes, supporting processes and assets from day 0 of a crisis situation.

**Result**



Interviews were conducted and a report was reviewed that contains details on the BCM processes and evidence of their implementation. The evidence confirms that the organization has effective BCM processes in place to ensure business continuity even in the event of unforeseen incidents. The audit found that the BCM measures are consistently implemented and practicable within the organization.

**By inspecting the documentation prepared by SEEBURGER INFORMATIK EOOD and through our IT-supported audit procedures, we were able to satisfy ourselves that this process is implemented and operated effectively and complies with the requirements of ISAE 3402 SOC 1 Type 2.**


<b>Management Practice by SEEBURGER INFORMATIK EOOD</b>	
<b>BC_03 - Safety of equipment</b>	
<p>The relevant company values for the scope of the ISAE 3402 audit are stored in an inventory system managed by the IT infrastructure. They are uniquely identified by a sequential number. “Employee” and “hardware” information is included in this inventory system. The “employee” and “unique SEEBURGER INFORMATIK EOOD number” information included in an asset management system maintained by Information Security Management forms the basis for a protection requirements analysis. In this system, the assets are supplemented with “spatial assignment” and “saved” information.</p>	
<b>Result</b>	
<p>A report containing a list of the company assets recorded in the asset management system was reviewed. The evidence confirms that all company assets relevant to the ISAE 3402 audit have been fully recorded. The review found that the asset management system reliably supports the documentation and traceability of the relevant company assets.</p> <p><b>By inspecting the documentation prepared by SEEBURGER INFORMATIK EOOD and through our IT-supported audit procedures, we were able to satisfy ourselves that this process is implemented and operated effectively and complies with the requirements of ISAE 3402 SOC 1 Type 2.</b></p>	
<b>Management Practice by SEEBURGER INFORMATIK EOOD</b>	
<b>BC_04 - Protection requirements analysis</b>	
<p>The protection requirements for information stem from the possible consequences of a security incident. This is illustrated by the classification of information as per IS guideline “Classifying information”. The task of determining the protection requirements is the responsibility of specialist and/or technical information managers.</p> <p>All information must be assessed in relation to the information security objectives of:</p> <ul style="list-style-type: none"> <li>• Availability,</li> <li>• Confidentiality and</li> <li>• Integrity</li> </ul> <p>in the five defined protection requirement classes (damage classes):</p> <ul style="list-style-type: none"> <li>• low,</li> </ul>	

- medium,
- high and
- very high

in the categories

- Violation of laws,
- Negative impact on task fulfilment,
- Negative external effect and
- Financial damage.

The protection requirements of information values are aggregated along the hierarchy and define the protection requirements for the next stage.  
The connection between “Asset” and “Information” is established in the SEEBURGER INFORMATIK EOOD asset management system.

<b>Result</b>	
---------------	---

A report was reviewed that contains details on the analysis of protection requirements and the defined criticality and recovery sequence of the systems. The evidence confirms that the systems are prioritized according to their criticality and that an orderly recovery sequence has been defined. The review found that the analysis of protection requirements is systematic and that recovery priorities are consistently documented.

**By inspecting the documentation prepared by SEEBURGER INFORMATIK EOOD and through our IT-supported audit procedures, we were able to satisfy ourselves that this process is implemented and operated effectively and complies with the requirements of ISAE 3402 SOC 1 Type 2.**

**Management Practice by SEEBURGER INFORMATIK EOOD**

**BC\_05 - Evidence of the effectiveness of measures**

SEEBURGER INFORMATIK EOOD offers a range of optional disaster recovery services for restoring the availability of EDI Managed Services within a reasonable time frame in the event of a disaster situation. A “disaster situation” arises if the entire data center in which SEEBURGER INFORMATIK EOOD provides and operates the EDI IT infrastructure for CUSTOMERS fails (e.g. as a result of an explosion or flooding). SEEBURGER INFORMATIK EOOD offers this disaster recovery service in different performance classes.

Description	Disaster Recovery Options (“DR Options”)		
	DR BASIC	DR ADVANCED	DR PREMIUM
<b>Procedure</b>	Only backup services in a second <b>SEEBURGER INFORMATIK EOOD</b> data center	Backup services and replication of the system in a second <b>SEEBURGER INFORMATIK EOOD</b> data center	Backup services and replication of the system in a second <b>SEEBURGER INFORMATIK EOOD</b> data center
<b>Standard data backup</b>	Data backup 1x per day incrementally, 1x per week in full		
<b>Backup of configuration data of System</b>	Same as standard data backup	Replication every 20 minutes	Replication every 10 minutes
<b>Backup of database and runtime data</b>	Same as standard data backup	Replication every 24 hours	Replication every 12 hours
<b>Backup of master communication data for trading partners</b>	Same as standard data backup	Replication every 24 hours	Replication every 12 hours
<b>System recovery</b>	Within 48 hours	Within 24 hours	Within 8 hours
<b>Recovery of data from backup</b>	Within 96 hours	Within 24 hours	Within 8 hours

The following data is backed up during the standard data backup (see also BR\_0x controls):

- Configuration data of system
- Database and runtime data
- Master communication data of trading partners.

Within the context of this service certificate, “replication” means that the EDI system used by the CUSTOMER is mirrored in a second SEEBURGER INFORMATIK EOOD data center. The system and configuration data required for the restoration of the entire EDI Cloud Services as well as the database and EDI runtime data in the relevant cycle presented in the above table are replicated in the second SEEBURGER INFORMATIK EOOD data center.

The following services are included in the different forms.

“DR BASIC” option

In the “DR BASIC” DR Option, the recovery of the Cloud Services after a Disaster Event has occurred shall be carried out in accordance with the following procedure:

- Recovery and configuration of the system at the SEEBURGER INFORMATIK EOOD data center;
- Importing the last data backup; and
- Resumption of operation of the agreed Cloud Service.

“DR ADVANCED” and “DR PREMIUM” options

With the DR-Options “DR ADVANCED” and “DR PREMIUM” the recovery of the Cloud Services after a Disaster Event has occurred shall be carried out in accordance with the following procedure:

- Re-configuration of the external IP-Addresses to the second SEEBURGER INFORMATIK EOOD data center
- Re-configuration of the customer connection to the second SEEBURGER INFORMATIK EOOD data center
- Resumption of operation of the agreed Cloud Service.

**Implementation of the replication**

SEEBURGER INFORMATIK EOOD uses Oracle Data Guard to replicate data to a redundant system in another data center location. Replication of data is typically done immediately. EDI systems are configured in a way that the data base connection is switched within less than ten minutes in case of a disaster.

Restoration of systems is done according to the Recovery settings as described in the BR\_05 controls.

<b>Result</b>	
---------------	---

A report containing details on the configuration of data replication was reviewed. The evidence confirms that data replication is set up in accordance with the contractually agreed DR option. The review found that replication is implemented consistently and that data is reliably available when needed.

**By inspecting the documentation prepared by SEEBURGER INFORMATIK EOOD and through our IT-supported audit procedures, we were able to satisfy ourselves that this process is implemented and operated effectively and complies with the requirements of ISAE 3402 SOC 1 Type 2.**

# General Engagement Terms

## for

### Wirtschaftsprüferinnen, Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften

#### [German Public Auditors and Public Audit Firms]

#### as of January 1, 2024

**This is an English translation of the German text, which is the sole authoritative version.**

#### 1. Scope and application

(1) These engagement terms apply to contracts between German Public Auditors (Wirtschaftsprüferinnen/Wirtschaftsprüfer) or German Public Audit Firms (Wirtschaftsprüfungsgesellschaften) – hereinafter collectively referred to as "German Public Auditors" – and their engaging parties for assurance services, tax advisory services, advice on business matters and other engagements except as otherwise agreed in writing (Textform) or prescribed by a mandatory rule.

(2) Third parties may derive claims from contracts between German Public Auditors and engaging parties only when this is agreed or results from mandatory rules prescribed by law. In relation to such claims, these engagement terms also apply to these third parties. A German Public Auditor is also entitled to invoke objections (Einwendungen) and defences (Einreden) arising from the contractual relationship with the engaging party to third parties.

#### 2. Scope and execution of the engagement

(1) Object of the engagement is the agreed service – not a particular economic result. The engagement will be performed in accordance with the German Principles of Proper Professional Conduct (Grundsätze ordnungsmäßiger Berufsausübung). The German Public Auditor does not assume any management functions in connection with his services. The German Public Auditor is not responsible for the use or implementation of the results of his services. The German Public Auditor is entitled to make use of competent persons to conduct the engagement.

(2) Except for assurance engagements (betriebswirtschaftliche Prüfungen), the consideration of foreign law requires an express agreement in writing (Textform).

(3) If circumstances or the legal situation change subsequent to the release of the final professional statement, the German Public Auditor is not obligated to refer the engaging party to changes or any consequences resulting therefrom.

#### 3. The obligations of the engaging party to cooperate

(1) The engaging party shall ensure that all documents and further information necessary for the performance of the engagement are provided to the German Public Auditor on a timely basis, and that he is informed of all events and circumstances that may be of significance to the performance of the engagement. This also applies to those documents and further information, events and circumstances that first become known during the German Public Auditor's work. The engaging party will also designate suitable persons to provide information.

(2) Upon the request of the German Public Auditor, the engaging party shall confirm the completeness of the documents and further information submitted as well as the explanations and statements provided in statement as drafted by the German Public Auditor or in a legally accepted written form (gesetzliche Schriftform) or any other form determined by the German Public Auditor.

#### 4. Ensuring independence

(1) The engaging party shall refrain from anything that endangers the independence of the German Public Auditor's staff. This applies throughout the term of the engagement, and in particular to offers of employment or to assume an executive or non-executive role, and to offers to accept engagements on their own behalf.

(2) Where the performance of the engagement to impair the independence of the German Public Auditor, of related firms, firms within his network, or such firms associated with him, to which the independence requirements apply in the same way as to the German Public Auditor in other engagement relationships, the German Public Auditor is entitled to terminate the engagement for good cause.

#### 5. Reporting and oral information

To the extent that the German Public Auditor is required to present results in a legally accepted written form (gesetzliche Schriftform) or in writing (Textform) as part of the work in executing the engagement, only that presentation is authoritative. Draft of such presentations are non-binding. Except as otherwise provided for by law or contractually agreed, oral statements and explanations by the German Public Auditor are binding only when they are confirmed in writing (Textform). Statements and information of the German Public Auditor outside of the engagement are always non-binding.

#### 6. Distribution of, a German Public Auditor's professional statement

(1) The distribution to a third party of professional statements of the German Public Auditor (results of work or extracts of the results of work whether in draft or in a final version) or information about the German Public Auditor acting for the engaging party requires the German Public Auditor's consent be issued in writing (Textform), unless the

engaging party is obligated to distribute or inform due to law or a regulatory requirement.

(2) The use by the engaging party for promotional purposes of the German Public Auditor's professional statements and of information about the German Public Auditor acting for the engaging party is prohibited.

#### 7. Deficiency rectification

(1) In case there are any deficiencies, the engaging party is entitled to specific subsequent performance by the German Public Auditor. The engaging party may reduce the fees or cancel the contract for failure of such subsequent performance, for subsequent non-performance or unjustified refusal to perform subsequently, or for unconscionability or impossibility of subsequent performance. If the engagement was not commissioned by a consumer, the engaging party may only cancel the contract due to a deficiency if the service rendered is not relevant to him due to failure of subsequent performance, to subsequent non-performance, to unconscionability or impossibility of subsequent performance. No. 9 applies to the extent that further claims for damages exist.

(2) The engaging party must assert a claim for subsequent performance (Nacherfüllung) in writing (Textform) without delay. Claims for subsequent performance pursuant to paragraph 1 not arising from an intentional act expire after one year subsequent to the commencement of the time limit under the statute of limitations.

(3) Apparent deficiencies, such as clerical errors, arithmetical errors and deficiencies associated with technicalities contained in a German Public Auditor's professional statement (long-form reports, expert opinions etc.) may be corrected – also versus third parties – by the German Public Auditor at any time. Misstatements which may call into question the results contained in a German Public Auditor's professional statement entitle the German Public Auditor to withdraw such statement – also versus third parties. In such cases the German Public Auditor should first hear the engaging party, if practicable.

#### 8. Confidentiality towards third parties, and data protection

(1) Pursuant to the law (§ [Article] 323 Abs 1 [paragraph 1] HGB [German Commercial Code: Handelsgesetzbuch], § 43 WPO [German Law regulating the Profession of Wirtschaftsprüfer: Wirtschaftsprüferordnung], § 203 StGB [German Criminal Code: Strafgesetzbuch]) the German Public Auditor is obligated to maintain confidentiality regarding facts and circumstances confided to him or of which he becomes aware in the course of his professional work, unless the engaging party releases him from this confidentiality obligation.

(2) When processing personal data, the German Public Auditor will observe national and European legal provisions on data protection.

#### 9. Liability

(1) For legally required services by German Public Auditors, in particular audits, the respective legal limitations of liability, in particular the limitation of liability pursuant to § 323 Abs. 2 HGB, apply.

(2) Insofar neither a statutory limitation of liability is applicable, nor an individual contractual limitation of liability exists, claims for damages due to negligence arising out of the contractual relationship between the engaging party and the German Public Auditor, except for damages resulting from injury to life, body or health as well as for damages that constitute a duty of replacement by a producer pursuant to § 1 ProdHaftG [German Product Liability Act: Produkthaftungsgesetz], are limited to € 4 million pursuant to § 54 a Abs. 1 Number 2 WPO. This applies equally to claims against the German Public Auditor made by third parties arising from, or in connection with, the contractual relationship.

(3) When multiple claimants assert a claim for damages arising from an existing contractual relationship with the German Public Auditor due to the German Public Auditor's negligent breach of duty, the maximum amount stipulated in paragraph 2 applies to the respective claims of all claimants collectively.

(4) The maximum amount under paragraph 2 relates to an individual case of damages. An individual case of damages also exists in relation to a uniform damage arising from a number of breaches of duty. The individual case of damages encompasses all consequences from a breach of duty regardless of whether the damages occurred in one year or in a number of successive years. In this case, multiple acts or omissions based on the same source of error or on a source of error of an equivalent nature are deemed to be a single breach of duty if the matters in question are legally or economically connected to one another. In this event the claim against the German Public Auditor is limited to € 5 million.

(5) A claim for damages expires if a suit is not filed within six months subsequent to the written statement (Textform) of refusal of

# General Engagement Terms

## for

### Wirtschaftsprüferinnen, Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften

#### [German Public Auditors and Public Audit Firms]

#### as of January 1, 2024

**This is an English translation of the German text, which is the sole authoritative version.**

acceptance of the indemnity and the engaging party has been informed of this consequence. This does not apply to claims for damages resulting from scienter, a culpable injury to life, body or health as well as for damages that constitute a liability for replacement by a producer pursuant to § 1 ProdHaftG. The right to invoke a plea of the statute of limitations remains unaffected. (6) § 323 HGB remains unaffected by the rules in paragraphs 2 to 5.

#### 10. Supplementary provisions for audit engagements

(1) If the engaging party subsequently amends the financial statements or management report audited by a German Public Auditor and accompanied by an auditor's report (Bestätigungsvermerk), he may no longer use this auditor's report.

If the German Public Auditor has not issued an auditor's report, a reference to the audit conducted by the German Public Auditor in the management report or any other public reference is permitted only with the German Public Auditor's consent, issued in a legally authorized by him.

(2) If the German Public Auditor revokes the auditor's report, it may no longer be used. If the engaging party has already made use of the auditor's report, then upon the request of the German Public Auditor he must give notification of the revocation.

(3) The engaging party has a right to five official copies of the report. Additional official copies will be charged separately.

#### 11. Supplementary provisions for assistance in tax matters

(1) When advising on an individual tax issue as well as when providing ongoing tax advice, the German Public Auditor is entitled to use as a correct and complete basis the facts provided by the engaging party – especially numerical disclosures; this also applies to bookkeeping engagements. Nevertheless, he is obligated to indicate to the engaging party any material errors he has identified.

(2) The tax advisory engagement does not encompass procedures required to observe deadlines unless the German Public Auditor has explicitly accepted a corresponding engagement. In this case the engaging party must provide the German Public Auditor with all documents required to observe deadlines – in particular tax assessments – on such a timely basis that the German Public Auditor has an appropriate lead time.

(3) Except as agreed otherwise in writing (Textform), ongoing tax advice encompasses the following work during the contract period:

- a) preparation and electronic transmission of annual tax returns, including financial statements for tax purposes in electronic format, for income tax, corporate tax and business tax, namely on the basis of the annual financial statements, and on other schedules and evidence documents required for the taxation, to be provided by the engaging party
- b) examination of tax assessments in relation to the taxes referred to in (a)
- c) negotiations with tax authorities in connection with the returns and assessments mentioned in (a) and (b)
- d) support in tax audits and evaluation of the results of tax audits with respect to the taxes referred to in (a)
- e) participation in petition or protest and appeal procedures with respect to the taxes mentioned in (a).

In the aforementioned tasks the German Public Auditor takes into account material published legal decisions and administrative interpretations.

(4) If the German Public auditor receives a fixed fee for ongoing tax advice, the work mentioned under paragraph 3 (d) and (e) is to be

remunerated separately, except as agreed otherwise in writing (Textform).

(5) Insofar the German Public Auditor is also a German Tax Advisor and the German Tax Advice Remuneration Regulation (Steuerberatungsvergütungsverordnung) is to be applied to calculate the remuneration, a greater or lesser remuneration than the legal default remuneration can be agreed in writing (Textform).

(6) Work relating to special individual issues for income tax, corporate tax, business tax and valuation assessments for property units as well as all issues in relation to sales tax, payroll tax, other taxes and dues requires a separate engagement. This also applies to:

- a) work on non-recurring tax matters, e.g. in the field of estate tax and real estate sales tax;
- b) support and representation in proceedings before tax and administrative courts and in criminal tax matters;
- c) advisory work and work related to expert opinions in connection with changes in legal form and other re-organizations, capital increases and reductions, insolvency related business reorganizations, admission and retirement of owners, sale of a business, liquidations and the like, and
- d) support in complying with disclosure and documentation obligations.

(7) To the extent that the preparation of the annual sales tax return is undertaken as additional work, this includes neither the review of any special accounting prerequisites nor the issue as to whether all potential sales tax allowances have been identified. No guarantee is given for the complete compilation of documents to claim the input tax credit.

#### 12. Electronic communication

Communication between the German Public Auditor and the engaging party may be via e-mail. In the event that the engaging party does not wish to communicate via e-mail or sets special security requirements, such as the encryption of e-mails, the engaging party will inform the German Public Auditor in writing (Textform) accordingly.

#### 13. Remuneration

(1) In addition to his claims for fees, the German Public Auditor is entitled to claim reimbursement of his expenses; sales tax will be billed additionally. He may claim appropriate advances on remuneration and reimbursement of expenses and may make the delivery of his services dependent upon the complete satisfaction of his claims. Multiple engaging parties are jointly and severally liable.

(2) If the engaging party is not a consumer, then a set-off against the German Public Auditor's claims for remuneration and reimbursement of expenses is admissible only for undisputed claims or claims determined to be legally binding.

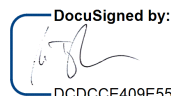
#### 14. Dispute Settlement

The German Public Auditor is not prepared to participate in dispute settlement procedures before a consumer arbitration board (Verbraucherschlichtungsstelle) within the meaning of § 2 of the German Act on Consumer Dispute Settlements (Verbraucherstreitbeilegungsgesetz).

#### 15. Applicable law

The contract, the performance of the services and all claims resulting there from are exclusively governed by German law.

Bretten, January 12, 2026

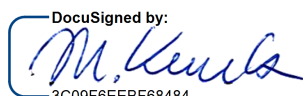
DocuSigned by:  
  
DCDCCE409E554AD

Matthias Feßenbecker

Director, Executive Board

SEEBURGER INFORMATIK EOOD

Bretten, January 12, 2026

DocuSigned by:  
  
3C09E6EEBE68484

Dr. Martin Kuntz

Director, Executive Board

SEEBURGER INFORMATIK EOOD

Viechtach, January 12, 2026



Dr. Martin Trost

Wirtschaftsprüfer

BFMT Audit GmbH

Wirtschaftsprüfungsgesellschaft

## Additional Agreements

to the general terms and conditions of BFMT Audit GmbH

In addition to the general terms and conditions for auditors and accounting firms, the Client **SEEBURGER INFORMATIK EOOD** and the accounting firm (**BFMT Audit GmbH Wirtschaftsprüfungsgesellschaft**) agree to limit the **maximum liability to € 1.5 million**.

We confirm that we have been advised of the possibility of **increasing the limitation of liability (higher insurance)** against payment of the corresponding fee.

Furthermore, we confirm that we are aware of the risks underlying this order or have been informed of this by the contractor.

The limitation of liability also applies in relation to third parties; the Client is obliged to inform third parties who wish to rely on the results of our activity.

**Bretten, January 12, 2026**

**Bretten, January 12, 2026**

**Viechtach, January 12, 2026**

DocuSigned by:



DCDCCE409E554AD

Matthias Feßenbecker

Director, Executive Board

SEEBURGER INFORMATIK EOOD

DocuSigned by:



3C09F6FEBF68484

Dr. Martin Kuntz

Director, Executive Board

SEEBURGER INFORMATIK EOOD



Dr. Martin Trost

Wirtschaftsprüfer

BFMT Audit GmbH

Wirtschaftsprüfungsgesellschaft