**hoch.rein IT Solutions GmbH**
Kolitzheim

Report on the description of HITS systems and services and on the design of controls related to the control objectives stated in the description as of 31 December 2024.

## Table of Contents



## Appendix

# I. Independent Service Auditor's Report [provided by Baker Tilly]

To hoch.rein IT Solutions GmbH, Kolitzheim, Germany

### Scope

We have been engaged by hoch.rein IT Solutions GmbH (the "Service Organization" or "HITS") to report on HITS description (Section II and III) of HITS systems and services (the "System") titled "HITS Description of Systems and Services as of 31 December 2024" and on the design of controls related to the control objectives stated in the description.

The Description indicates that certain control objectives specified in the Description can be achieved only if complementary user entity controls assumed in the design of HITS controls are suitably designed, along with the Service Organization's related controls. Our procedures did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design of such complementary user entity controls.

### HITS Responsibilities

HITS is responsible for: preparing the description (Section III) and accompanying statement (Section II) including the completeness, accuracy and method of presentation of the description and the assertion; providing the services covered by the description; stating the control objectives; and designing, implementing and effectively operating controls to achieve the stated control objectives.

### Our Independence and Quality Management

We have complied with the independence and other ethical requirements of the Code of Professional Conduct established by the International Auditing and Assurance Standards Board. We applied the statements on quality management standards established by the International Auditing and Assurance Standards Board and accordingly maintain a comprehensive system of quality management.

### Service Auditor's Responsibilities

Our responsibility is to express an opinion on HITS description and on the design of controls related to the control objectives stated in that description, based on our procedures. We conducted our engagement in accordance with International Standard on Assurance Engagements (ISAE) 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 in all material respects.

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

tion is not fairly presented, and that controls are not suitably designed. An assurance engagement of this type also includes evaluating the overall presentation of the description, the suitability of the control objectives stated therein, and the suitability of the criteria specified by the service organization and described. As noted above, we did not perform any procedures regarding the operating effectiveness of controls included in the description and, accordingly, do not express an opinion thereon.

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

**Limitations of Controls at a Service Organization**

HITS description is prepared to meet the common needs of a broad range of user entities and their auditors and may not, therefore, include every aspect of the "System" that each individual customer may consider important in its own particular environment. Also, because of their nature, controls at a service organization may not prevent or detect all errors or omissions in processing or reporting transactions.

**Opinion**

Our opinion has been formed on the basis of the matters outlined in this report. The criteria we used in forming our opinion are those described in HITS Statement in Section II. In our opinion, in all material respects:

- The description fairly presents HITS System as designed and implemented as of 31 December 2024 and
- The controls related to the control objectives stated in the description were suitably designed and implemented as of 31 December 2024.

**Intended Users and Purpose**

This report is intended only for customers who have used HITS 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 obtaining an understanding of customers' information systems relevant to financial reporting. This report is not intended for, and should not be used by, anyone other than these parties.

**General Engagement Terms (GET)**

The terms governing this engagement are set out in the "General Engagement Terms" (General Engagement Terms for Wirtschaftsprüferinnen, Wirtschaftsprüfer and Wirtschaftsprüfungsgesellschaften [German Public Auditors and Public Audit Firms] as of January 1, 2024), which are attached to this report as Appendix 1 and referred to as "GET".

The limitation of liability within the GET covers all Addresses as a whole (defined as hoch.rein IT Solutions GmbH and any other third party receiving the report) and will have to be allocated between the Addressees (§ 428 German Civil Code). It is agreed that such allocation will be entirely a matter for the Addresses, who will be under no obligation to inform Baker Tilly of the

agreement reached. If for whatever reason, no such allocation is agreed, no Addressee will dispute the validity, enforceability, or operation of the limitation of liability on the grounds that no such allocation was agreed.

By reading and using the information contained in this report, the recipient confirms notice of the GET (including the limitation of our liability as stipulated in Sec. 9 (2)) and accepts validity of the attached GET.

Düsseldorf, 31 January 2025

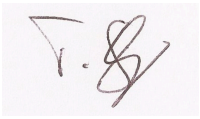
Baker Tilly GmbH & Co. KG

Wirtschaftsprüfungsgesellschaft

Martin Uebelmann

Certified Information Systems Auditor (CISA)

Partner



Thorsten Scharpenberg

Certified Information Systems Auditor (CISA)

Director

# II. Management Assertion [provided by HITS]

The accompanying description of hoch.rein IT Solutions GmbH (HITS) has been prepared for user entities of the “System” and their auditors who have a sufficient understanding to consider the description, along with other information including information about controls operated by customers them-selves, when obtaining an understanding of customers’ information systems relevant to financial reporting. HITS confirms, to the best of knowledge and belief, that:

a) The accompanying description fairly presents the system for processing customers’ transactions as at 31.12.2024. The criteria we used in making this assertion were that the Description:
   i) Presents how the system was designed and implemented, including, if applicable:
      - 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 in-correct information and how information is transferred to the reports prepared customers.
      - How the system dealt 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) 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.

b) The controls related to the control objectives stated in the accompanying description were suitably designed as at 31.12.2024. The criteria used in making this assertion were that:
   i) The risks that threatened achievement of the control objectives stated in the description were identified; and
   ii) The identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved.

Kolitzheim, 31.01.2025

André Simon

Management

hoch.rein IT Solutions GmbH, Gräsleinsgasse 1, 97509 Kolitzheim-OT Zeilitzheim
Telefon: +49 (0) 9 385 / 9 804 – 0
Fax: +49 (0) 9 385 / 9 804 – 590
E-Mail. support.it@hoch-rein.com
Website: www.hoch-rein.com

# III. HITS Description of Systems and Services [provided by HITS]

## 1 Overview of the Service Organization

hoch.rein IT Solutions GmbH is a hybrid provider of a traditional system house portfolio and comprehensive managed services offerings. The company operates its own data center in the INNOPARK Kitzingen, running mostly independent of the public network and thus keeping its own IT infrastructure, as well as that of its customers, in-house. This ensures that the IT infrastructure of both hoch.rein IT Solutions and its customers remains secure and reliable.

## 2 Scope of Description

hoch.rein IT Solutions is specialized in delivering comprehensive IT services and solutions. Their business revolves around helping companies optimizing and securing their IT infrastructure, ensuring performance and compliance with industry standards. The company offers managed services which cover everything from workplace management (for local and mobile environments) to data center management, where they ensure high availability, security, and efficient performance. They also manage applications, networks, and security infrastructure, providing proactive solutions to maintain the integrity and security of corporate networks.

Through these services, hoch.rein IT Solutions enables clients to focus on their core business while ensuring their IT infrastructure is secure, efficient, and future oriented.

IT security is of central importance at hoch.rein IT Solutions and is part of every planning and measure in IT and is fundamental for the compliance of a company.

This description covers the physical and logical security measures required for the secure operation of the data center. It includes structural safeguards, access control systems, the security of servers and network components, as well as processes for maintenance and inspection. In addition, the description includes backup and restore strategies, change management, the use of an incident management system, data protection measures, and an IT emergency plan to ensure the operation of the data center. The objective is to guarantee the security of systems and data while maximizing the availability of IT services.

## 3 Scope of this ISAE 3402 Report

This report focuses particularly on the implementation and monitoring of security measures across all outlined areas (HITS guidelines). The documented measures ensure that all security-related aspects meet current requirements and are regularly reviewed. The risk control matrix (hoch.rein_Risiko-Kontroll-Matrix_2024_EN.xlsx) serves as the foundation and an integral part of these guidelines.

# 4 Control Environment

hoch.rein IT Solutions GmbH demonstrates its commitment to security by implementing an internal control system that adheres to the requirements of ISAE 3402 and is continuously optimized. This includes regular inspections, maintenance, and the use of cutting-edge technology to ensure the security of the data center. Responsibility for overseeing the security measures lies with the IT department.

# 5 Risk assessment

Risk management involves the identification and assessment of potential risks in the following areas:

- Physical risks: Access controls and structural protective measures reduce the risk of physical threats.
- Logical risks: Firewalls and antivirus software protect against cyberattacks.
- Emergency planning: The IT emergency plan addresses risks such as cyberattacks, hardware failures, and natural disasters, and defines clear recovery processes.
- Change management risks: Changes to IT systems are systematically reviewed to minimize operational risks.
- Data protection: Data protection measures safeguard personal data from loss or misuse.

HITS has implemented a Risk-Control-Matrix aligned with its business model and its overall strategic orientation.

# 6 Information and Communications

**The internal and external communication processes of** hoch.rein **IT Solutions GmbH ensure that security policies and procedures are regularly communicated and implemented. The incident management system documents all security-related incidents and ensures that changes are recorded and reviewed.**

# 7 Monitoring Activities

The monitoring measures include regular physical inspections and audits of IT systems. Backups are routinely monitored and tested to ensure they are successfully executed and can be restored. All incidents and changes are thoroughly documented to ensure the integrity of the security measures.

To support general operation (data center and specialist advice), the following special functions take action:

- Information security officer
- Data protection officer

# 8 Control Activities

The control activities of hoch.rein IT Solutions GmbH include comprehensive physical and logical security measures. Physical measures involve access controls, video surveillance, and fire protection systems. Logical security measures, such as firewalls, access controls, regular backups, and encryption, safeguard the IT systems. Change management ensures the secure implementation of system changes, while incident management enables quick responses to IT disruptions. Additionally, regular restore tests and strict data protection policies ensure data security and recoverability in the event of an emergency.

By implementing and consistently applying these steps, we ensure that the policies and controls required for ISAE 3402 certification for the data center are adhered to and continuously monitored.

**Physical security**
Physical security and procedural measures in handling access, maintenance, and monitoring of individual components to ensure availability at the data center in Kitzingen.

**Logical Security**
Logical security of the data center is divided into the sections "Firewall and AV," the handling of "Unique Users (user identification across all levels) and group accounts," as well as "Remote access and access rights" in general.

**Backup and Restore**
The backup and restore concepts contain all technical and organisational measures to protect IT systems and data from loss or misuse as well as the procedure for data backup and data recovery in the event of a disaster.

**Change Management**
IT change management includes procedures to ensure the successful prioritisation, approval, planning and implementation of changes to IT systems.

**Problem- & Incident Management**
The incident management process aims to quickly identify and resolve IT disruptions to maintain business operations. It involves identifying and resolving incidents that threaten the IT services of a company. As part of HITS IT Service Management, the problem & incident management focuses on maintaining or restoring operations and security.

**Data Protection**
Data protection measures include, among others: hcoh.rein IT Solutions has implemented strict data protection policies to ensure compliance with the General Data Protection Regulation (GDPR). This includes appointing an external data protection officer.

**Business Continuity Planning**
To ensure business continuity, hcoh.rein IT Solutions has implemented an IT emergency plan. This serves as a tool for responding to extraordinary IT events that could lead to the failure of critical business processes. The objective is to maintain operational capacity and restore all IT processes swifts.

# 9 Complementary Controls

Complementary Controls are designed with the assumption that certain controls will be implemented by user and subservice organizations. It is not feasible for all of the control objectives related to HITS services to be solely achieved by the control procedures from HITS. Accordingly, user and subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of HITS.

The following user entity controls should be implemented by user entities to provide additional assurance that the control objectives described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

**Control Activities**

- Control Objective: Controls provide reasonable assurance that systems are adequately physically protected.
  - Customers are responsible to inform HITS about visits and authorize them. Approvers communicated to HITS need to be up to date.
- Control Objective: Controls provide reasonable assurance that access to relevant data is adequately secured.
  - Customers are responsible to define security requirements for those systems, which are only implemented after authorization from customers. Approvers communicated to HITS need to be up to date.
  - The customer has responsibility for specially housed systems.
  - Customers are responsible to cooperate in the administration of changes and communication.
  - Customers are responsible to review the reasonableness of all customer firewall rules.
  - Customers are responsible for the password specifications of the customer systems.
  - Customers are responsible for restriction to change passwords to the systems administered by the customer at all levels.
  - Customers are responsible for the appropriately configuration of the system parameters of the customer systems.
  - Customers are responsible for restriction to change the configuration of the parameters for the systems administered by the customer at all levels.
- Control Objective: Controls provide reasonable assurance that users can be uniquely identified.
  - Customers are responsible for the assurance that users can be uniquely identified for the systems administered by the customer at all levels.

- Control Objective: Controls provide reasonable assurance that authorizations are appropriately assigned and monitored so that accounting-relevant data is protected against unauthorized access and changes.
  - Customers are responsible for defining the specifications of remote access accounts for the customer systems.
  - Customers are responsible for the remote access accounts of client employees to the customer systems. Customers are responsible for the systems administered by the customer at all levels.
  - Customers are responsible for the approval of client employees to the customer systems and to keep the key user/approver information up to date.
  - Customers are responsible for the reporting of users leaving.
- Control Objective: Controls provide reasonable assurance that changes to programs, applications, databases, operating systems, network, network components, hardware and systems are adequately tested and authorized.
  - Customers are responsible to inform HITS about up to date approvers / key contacts.
  - Customers are responsible for internal approval processes (e.g. data owner).
  - Customers are responsible for the commissioning of test environment and the execution of functional tests.
  - Customers are responsible for releasing the change where required. Customers are responsible to report indications to HITS in case of customer specific dependencies.
  - Customers are responsible for the systems administered by the customer.
- Control Objective: Controls provide reasonable assurance that relevant data is fully backed up so that it can be restored if necessary.
  - Customers are responsible for requirements and communication in case of need for change.
- Control Objective: Controls provide reasonable assurance that, in the event of a disaster, full operations can be restored in a reasonable time and relevant data is not damaged or lost.
  - Customers are responsible for the communication of relevant information for the preparation of the emergency plan.
  - Customers are responsible for the assignment of maximum downtime.
- Control Objective: Controls provide reasonable assurance that incidents, problems and major incidents are identified, recorded and resolved at an early stage.
  - Customers are responsible for requirements and communication in the event of a need for change.
  - Customers are responsible for commissioning response times (contractually agreed).
  - Customers are responsible for commissioning solution times.

- Customers are responsible for reviewing solutions and reopening tickets as necessary.

- Control Objective: Controls provide reasonable assurance that continuous IT operations can be ensured.
  - Customers are responsible for the systems administered by the customer.

## 10 Appendix and applicable documents

| Short description | Title | Version |
|---|---|---|
| ICS control matrix | hoch.rein_Risiko-Kontroll-Matrix_2024_EN.xlsx | 12.07.2024 |

# IV. HITS Control Objectives, Related Controls and the Results of Baker Tilly's Procedures [provided by Baker Tilly]

## Tests of control environment and results thereof

The control environment represents the collective effect of various factors on establishing of enhancing the design of the controls specified by HITS. In planning the nature, timing and extent of our testing of the controls specified by HITS, we considered the following aspects of HITS control environment:

- Organizational structure
- Policies and Procedures
- Risk assessment processes
- Management monitoring procedures

## Description of control objectives, controls, tests and results of tests

On the pages that follow, the description of control objectives and the controls to achieve the objectives have been specified by and are in the responsibility of HITS. They are documented in the description of the system, as mentioned above and have only been included in the tables below to avoid redundancy. The description of testing performed, and the results of tests are the responsibility of the service auditor.

HITS has defined the control objectives and controls per process in the control framework in this chapter. We have included our testing procedures as well as the test results in this control framework (column „Test procedures performed by Baker Tilly“ and „Conclusion“).

## Physical Security and Environmental Protection

| **Control Objective** | | | |
|---|---|---|---|
| **1** | Controls provide reasonable assurance that systems are adequately physically protected. | | |
| **#** | **Control description** | **Test procedures performed by Baker Tilly** | **Conclusion** |
| **1.1** | There is a policy regarding physical security that is annually reviewed. | Inspected the policy and procedures regarding physical security for appropriateness and determined that they were approved by management, reviewed and updated annually. | No relevant exceptions noted. |
| **1.2** | The server or technical rooms are adequately equipped to ensure the operation and availability of the essential IT systems, depending on their risk assessment, in the event of a loss. | Inspection of data center by physical examination to determine that appropriate measures are taken according to the policies. | No relevant exceptions noted. |
| **1.3** | A procedure for granting access authorizations to the data center/server room is implemented:<br>• Permanent access is authorized,<br>• (Temporary) access cards are issued on a personalized basis,<br>• Access cards and authorizations are revoked promptly when employees leave the company or department. | Determined through inquiry with management and inspection of policies. Access to the server room was restricted to authorized personnel. Changes to access codes were documented. Visitor and technician access to the data center was limited to those who had been preapproved by an authorized employee. Inspected the access log to determine that it was implemented. | No relevant exceptions noted. |

| **Control Objective** | | | |
|---|---|---|---|
| **1** | Controls provide reasonable assurance that systems are adequately physically protected. | | |
| **#** | **Control description** | **Test procedures performed by Baker Tilly** | **Conclusion** |
| **1.4** | The access authorizations are checked at regular intervals. | Inquired whether access authorizations to the data center are reviewed at least once a year. Inspected the documentation of the last review to determine that it was performed. | No relevant exceptions noted. |
| **1.5** | Entrances to the data center/server room are secured by alarmed doors, code cards, and security guards if necessary. | Observed protection of the INNOPARK campus and buildings, and that access to restricted areas was secured using RFID-cards and PIN Pads. | No relevant exceptions noted. |
| **1.6** | The server or technical rooms are adequately equipped to ensure the operation and availability of the essential IT systems, depending on their risk assessment, in the event of a claim. | Inspected the data center by physical examination. Examined physical hardware and power schematics and determined air conditioning, UPS, and an emergency generator were deployed. Regular inspection checks are also conducted to ensure the physical protection of the systems Inspected the documentation of the last inspection to determine that it was performed. | No relevant exceptions noted. |
| **1.7** | The technical equipment is maintained and checked regularly (usually once a year). | Inquired whether technical equipment is maintained and checked at least once a year. Inspected the documentation of the last inspection to determine that it was performed. | No relevant exceptions noted. |

## Logical Security I

| **Control Objective** | | | |
|---|---|---|---|
| **2** | Controls provide reasonable assurance that access to relevant data is adequately secured. | | |
| **#** | **Control description** | **Test procedures performed by Baker Tilly** | **Conclusion** |
| **2.1** | There is a security policy that is annually reviewed. It contains rules how access rights are limited, granted, reviewed and revoked; how security settings like passwords have to be set and how the overall system security is ensured. | Inspected the policy and procedures regarding logical security for appropriateness and determined that they were approved by management, reviewed and updated annually. | No relevant exceptions noted. |
| **2.2** | Relevant firewall and network parameters for security configuration must be regularly checked for updates, evaluated and implemented. | Inquired whether firewall and network parameters for security configuration are reviewed regularly. Inspected the documentation of the last review in accordance with the policy to determine that it was performed. | No relevant exceptions noted. |
| **2.3** | The administration of firewall rules is to be assigned on a restricted basis. Changes are to be implemented and documented only after approval. | Inquired whether the procedure for the secure use of administrator authorizations of firewall rules at HITS is established and documented in a traceable manner. Inspected the documentation of a change to determine that it was implemented after proper approval was granted | No relevant exceptions noted. |

| **Control Objective** | | | |
|---|---|---|---|
| **2** | Controls provide reasonable assurance that access to relevant data is adequately secured. | | |
| **#** | **Control description** | **Test procedures performed by Baker Tilly** | **Conclusion** |
| **2.4** | The deposited firewall rules are reviewed regularly. | Inquired whether firewall rules are reviewed regularly. Inspected the documentation of the last review to determine that it was performed. | No relevant exceptions noted. |
| **2.5** | Password guidelines have been defined and implemented to prevent unauthorized access.<br>The policy regulates the permitted handling of identifiers and passwords by the identifier holders (including the secrecy of personal passwords, the prohibition of using other people's personal identifiers), the criteria for assigning identifiers with administrative rights, the password obligation, password complexity, password lifetime and password history.<br>The rules on passwords are set up in the relevant system in each case. | Inquired whether guidelines for passwords are established and documented in a traceable manner. Inspected the parameters to determine that parameters were implemented in accordance with the policy. | No relevant exceptions noted. |

| **Control Objective** | | | |
|---|---|---|---|
| **2** | Controls provide reasonable assurance that access to relevant data is adequately secured. | | |
| **#** | **Control description** | **Test procedures performed by Baker Tilly** | **Conclusion** |
| **2.6** | Permissions to change passwords must be restricted. | Inquired whether a procedure for the secure use of authorizations to change passwords at HITS is established and documented in a traceable manner. Inspected and verified that the authorization to change passwords is restricted. | No relevant exceptions noted. |
| **2.7** | Critical system parameters are implemented according to defined specifications. | Inspected the system whether critical system parameters are implemented according to defined specifications in accordance with the policy. | No relevant exceptions noted. |
| **2.8** | The administration of critical system parameters is to be assigned and logged in a restricted manner. | Inquired whether the procedure for the secure use of administrator authorizations of critical system parameters at HITS is defined and verified that the authorization to adjust critical system parameters is restricted. | No relevant exceptions noted. |

## Logical Security II

| **Control Objective** | | | |
|---|---|---|---|
| **3** | Controls provide reasonable assurance that users can be uniquely identified. | | |
| **#** | **Control description** | **Test procedures performed by Baker Tilly** | **Conclusion** |
| **3.1** | User accounts are only set up on a personalized basis. | Inspected whether the policy and procedures for HITS users are in place and appropriate. We inspected whether the procedure aligns with typical guidelines for managing user access on a personalized basis. | No relevant exceptions noted. |
| **3.2** | There are clear rules for using non-personalized user accounts. | Inspected whether the policy and procedures how non-personalized user accounts can be used by several people are defined. We also inspected measures being used to systematically record who has used the users and when. | No relevant exceptions noted. |

## Logical Security III

| **Control Objective** | | | |
|---|---|---|---|
| **4** | Controls provide reasonable assurance that authorizations are appropriately assigned and monitored so that accounting-relevant data is protected against unauthorized access and changes. | | |
| **#** | **Control description** | **Test procedures performed by Baker Tilly** | **Conclusion** |
| **4.1** | Access by external service providers is only enabled after approval and activities are monitored. | Inquired whether the procedure for the secure use of remote access at HITS is established and documented in a traceable manner. Inspected the documentation and review of a log to determine that it was implemented. | No relevant exceptions noted. |
| **4.2** | The activation of external service providers is only possible for a restricted group of people and must be documented. | Inquired whether the procedure for the activation of remote access at HITS is established for a restricted group of people and documented in a traceable manner. Inspected the documentation of an approval to determine that it was implemented. | No relevant exceptions noted. |
| **4.3** | A procedure for setting up, changing and deactivating users is established and documented. | Inquired whether the policy and procedures regarding the access approval process are defined and determined that they were approved by management, reviewed and updated annually. | No relevant exceptions noted. |
| **4.4** | User authorizations are set up and changed only after being requested and approved by the data or system owner. | Inquired whether the procedure for the approval of an authorization request at HITS is established and documented in a traceable manner. Inspected the documentation of an approval to determine that the approval follows the documented procedure. | No relevant exceptions noted. |

| **Control Objective** | | | |
|---|---|---|---|
| **4** | Controls provide reasonable assurance that authorizations are appropriately assigned and monitored so that accounting-relevant data is protected against unauthorized access and changes. | | |
| **#** | **Control description** | **Test procedures performed by Baker Tilly** | **Conclusion** |
| **4.5** | The defined procedures for changing access rights due to a job change are adhered to and are documented in a comprehensible manner. | Inquired whether the procedure for the approval of an authorization request due to a job change at HITS is established and documented in a traceable manner. Inspected the documentation of an approval to determine that it was implemented. | No relevant exceptions noted. |
| **4.6** | In the case of departing employees, rights are revoked promptly and, if necessary, known group account passwords are changed. | Inquired whether the policy and procedures to deactivate users promptly after leaving the company are defined. Inspected the documentation of a departing employee to determine that it was implemented. | No relevant exceptions noted. |
| **4.7** | The assigned authorizations are reviewed annually for appropriateness. The user review must be documented in a comprehensible manner. | Inquired whether user accounts and permissions are reviewed regularly. Inspected the documentation of the last review to determine that it was performed. | No relevant exceptions noted. |
| **4.8** | The assigned administrative authorizations are limited and reviewed quarterly for appropriateness. The user review is documented in a traceable manner. | Inquired whether administrative user accounts and permissions are reviewed regularly. Inspected the documentation of the last review to determine that it was performed. | No relevant exceptions noted. |

| **Control Objective** | | | |
|---|---|---|---|
| **4** | Controls provide reasonable assurance that authorizations are appropriately assigned and monitored so that accounting-relevant data is protected against unauthorized access and changes. | | |
| **#** | **Control description** | **Test procedures performed by Baker Tilly** | **Conclusion** |
| **4.9** | A comprehensible authorization concept is in place, appropriate separation of functions is in place and implemented on the system side. | Inquired to ascertain that a comprehensible concept for user authorizations is in place and is reviewed annually to ensure that it is up to date; an appropriate separation of functions is in place and implemented in the system. Inspected the documentation of the last review. | No relevant exceptions noted. |
| **4.10** | Data of different customers is logically separated from each other. | Inquired whether the policy and procedures regarding logical separation of data for different customers are in place and inspected whether it is implemented in the system. | No relevant exceptions noted. |
| **4.11** | Logs are created and archived on a regular basis in order to perform analysis when needed. | Inspected whether logs are created and archived. | No relevant exceptions noted. |
| **4.12** | The relevant systems are permanently monitored for operationally dangerous or relevant occurrences, and any malfunctions or problems are promptly rectified. | Inquired regarding the policy and procedures for system monitoring and inspected an example event ensuring that the productive environment was monitored and events were published if predefined thresholds were reached. | No relevant exceptions noted. |

## Change Management

| **Control Objective** | | | |
|---|---|---|---|
| **5** | Controls provide reasonable assurance that changes to programs, applications, databases, operating systems, network, network components, hardware and systems are adequately tested and authorized.<br><br>Note: No system development is done at HITS, so that program and application changes only refer to patching | | |
| **#** | **Control description** | **Test procedures performed by Baker Tilly** | **Conclusion** |
| **5.1** | A procedure for the commissioning, development, testing and release of changes as well as the transfer to productive operation has been established and documented. | Inspected the policy and procedures regarding change management for appropriateness and determined that they were approved by management, reviewed and updated annually. | No relevant exceptions noted. |
| **5.2** | For new change requests by customers, HITS checks whether the change was initiated by the defined key contact person.<br><br>Changes initiated by HITS follow the standard change process documented in tickets. | Inquired whether the policy and procedures for commissioning, developing, testing, and releasing changes and for transferring them to productive operations have been established. Inspected the documentation of a change to determine that it was handled accordingly. | No relevant exceptions noted. |

| **Control Objective** | | | |
|---|---|---|---|
| **5** | Controls provide reasonable assurance that changes to programs, applications, databases, operating systems, network, network components, hardware and systems are adequately tested and authorized.<br><br>Note: No system development is done at HITS, so that program and application changes only refer to patching | | |
| **#** | **Control description** | **Test procedures performed by Baker Tilly** | **Conclusion** |
| **5.3** | Changes are evaluated in terms of their criticality and relevance in a traceable manner. | Inquired whether the policy and procedures for evaluating the criticality of changes have been established and documented. Inspected the documentation of a change to determine that it was handled accordingly. | No relevant exceptions noted. |
| **5.4** | Changes are evaluated in terms of their criticality and relevance and tested in a traceable manner. | Inquired whether the policy and procedures for evaluating the criticality and testing of changes have been established and documented. Inspected the documentation of a change to determine that it was handled accordingly. | No relevant exceptions noted. |
| **5.5** | Program changes are released by the client before being transferred to the productive system. | Inquired whether the policy and procedures for realizing the program changes by the client have been established. Inspected the documentation of a change to determine that it was handled accordingly. | No relevant exceptions noted. |
| **5.6** | A procedure for identifying relevant patches, including assessment and testing, has been defined and implemented. | Inquired regarding the policy and procedures for receiving notification from the vendor when new patches are available. Inspected the verification documentation that relevant patches were deployed after confirmation. Inspected the documentation of a change to determine that it was accurately captured. | No relevant exceptions noted. |

| **Control Objective** | | | |
|---|---|---|---|
| **5** | Controls provide reasonable assurance that changes to programs, applications, databases, operating systems, network, network components, hardware and systems are adequately tested and authorized.<br><br>Note: No system development is done at HITS, so that program and application changes only refer to patching | | |
| **#** | **Control description** | **Test procedures performed by Baker Tilly** | **Conclusion** |
| **5.7** | A procedure for identifying relevant patches, including assessment and testing, has been defined and implemented. | n/a - covered by overall change management (controls 5.1 to 5.5) | No relevant exceptions noted. |
| **5.8** | Patches are released by the client before being transferred to the production system. | n/a - covered by overall change management (controls 5.1 to 5.5) | No relevant exceptions noted. |

## Backup and Restore

| Control Objective | | | |
|---|---|---|---|
| **6** | Controls provide reasonable assurance that relevant data is backed up according to the defined extend so that it can be restored if necessary. | | |
| **#** | **Control description** | **Test procedures performed by Baker Tilly** | **Conclusion** |
| **6.1** | The established procedures for data backup and recovery are documented.<br>The process and procedures for data backup and recovery as well as the handling of archived data are described and known to the relevant employees. | Inspected the policy and procedures regarding backup and restore for appropriateness and determined that they were approved by management, reviewed and updated annually. | No relevant exceptions noted. |
| **6.2** | Data backups are performed to an appropriate extent within the scope of the defined service levels and tolerable downtimes (usually daily differential, weekly and monthly full backup). | Inspected the procedure regarding scheduling, defining and performing backups within defined service levels and tolerable downtimes and ascertained it is adapted as required. | No relevant exceptions noted. |

| **Control Objective** | | | |
|---|---|---|---|
| **6** | Controls provide reasonable assurance that relevant data is backed up according to the defined extend so that it can be restored if necessary. | | |
| **#** | **Control description** | **Test procedures performed by Baker Tilly** | **Conclusion** |
| **6.3** | The data backups are continuously monitored by an ongoing monitoring system that automatically detects faulty backup processes and automatically generates corresponding notifications. | Inquired regarding the policy and procedures for monitoring and error handling and ascertained that they were reviewed, updated and approved. | No relevant exceptions noted. |
| **6.4** | Data backups are stored at a secure external location in accordance with a defined procedure. | Inquired whether the policy and procedures for the handling of archived data are described and known to the employees concerned. We ascertained that the yearly review of the storage location was properly documented. | No relevant exceptions noted. |
| **6.5** | The backups are regularly checked for recoverability. | Inquired regarding the policy and procedures whether the recovery / restore of backups were checked regularly. Inspected the documentation of a restore test to determine that it was performed. | No relevant exceptions noted. |
| **6.6** | Data backups are stored in accordance with a defined procedure for a specified period of time. | Inquired whether the policy and procedures for the handling of archived data are described and known to the employees concerned. Inspected for one instance whether the data was stored accordingly. | No relevant exceptions noted. |

## Business Continuity Planning

| **Control Objective** | | | |
|---|---|---|---|
| **7** | Controls provide reasonable assurance that, in the event of a disaster, full operations can be restored in a time defined by the customer and relevant data is not damaged or lost. | | |
| **#** | **Control description** | **Test procedures performed by Baker Tilly** | **Conclusion** |
| **7.1** | An emergency plan is in place that documents<br>- the necessary availability and tolerable downtimes,<br>- possible damage events with probability of occurrence and amount of damage,<br>- measures to be initiated in the event of damage,<br>- contact persons (client, service provider) and<br>- responsibilities<br>- emergency tests to be carried out documented.<br><br>The emergency plan is updated as necessary. | Inspected the policy and procedures regarding disaster recovery for appropriateness and determined that they were approved by management, reviewed and updated annually. | No relevant exceptions noted.<br><br>**Note:**<br>The emergency management framework is currently being revised by the client. An overall Business Continuity Plan will be documented. |

| **Control Objective** | | | |
|---|---|---|---|
| **7** | Controls provide reasonable assurance that, in the event of a disaster, full operations can be restored in a time defined by the customer and relevant data is not damaged or lost. | | |
| **#** | **Control description** | **Test procedures performed by Baker Tilly** | **Conclusion** |
| **7.2** | The emergency plan is tested regularly according to the defined regulations in the emergency plan (at least 1x per year). | Inquired whether the emergency plan was checked regularly. Inspected the documentation of a test to determine that it was performed. | No relevant exceptions noted. |

## Problem- & Incident Management

| Control Objective | | | |
|---|---|---|---|
| **8** | Controls provide reasonable assurance that incidents, problems and major incidents are identified, recorded and resolved at an early stage. | | |
| **#** | **Control description** | **Test procedures performed by Baker Tilly** | **Conclusion** |
| **8.1** | A problem- & incident management system has been defined and implemented to record, analyse and promptly resolve faults and report them to management. | Inspected the policy and procedures regarding problem- & incident management for appropriateness and determined that they were approved by management, reviewed and updated annually. | No relevant exceptions noted. |
| **8.2** | There is a reporting process for security incidents that supports a prompt response and investigation of unauthorized system incidents. | Inquired whether major incidents or problems are identified, tracked, and monitored, and escalation mechanisms are defined. Inspected the documentation of a major incident to determine that it was handled in accordance with the policy. | No relevant exceptions noted. |
| **8.3** | Incidents and problems are dealt with in a timely manner. | Inquired whether incidents or problems are identified, tracked, and monitored, and escalation mechanisms are defined. Inspected the documentation of an incident to determine that it was dealt with in a timely manner. | No relevant exceptions noted. |
| **8.4** | The problem management system provides for appropriate documentation that enables problems or faults to be traced back to their cause. | Inquired whether incidents or problems are documented in a traceable manner. Inspected the documentation of an incident to determine that it was documented as defined. | No relevant exceptions noted. |

## Operations

| Control Objective | | | |
|---|---|---|---|
| **9** | Controls provide reasonable assurance that continuous IT operations can be ensured. | | |
| **#** | **Control description** | **Test procedures performed by Baker Tilly** | **Conclusion** |
| **9.1** | Standardized procedures are defined and documented for IT operations (e.g., operating procedures) to ensure process integrity and continuous operation. | Inspected the policy and procedures regarding IT operations (e.g. 1.1) for appropriateness and determined that they were approved by management, reviewed and updated annually. | No relevant exceptions noted. |
| **9.2** | Tools are in place to monitor system availability and capacity. Incident tickets are created automatically and follow the standard incident management process. | Inspected the policy and procedures whether they contained details about how continuous IT operations can be ensured. Inspected the configuration whether these measures are implemented, and tickets are created automatically. | No relevant exceptions noted. |

| **Control Objective** | | | |
|---|---|---|---|
| **9** | Controls provide reasonable assurance that continuous IT operations can be ensured. | | |
| **#** | **Control description** | **Test procedures performed by Baker Tilly** | **Conclusion** |
| **9.3** | The relevant IT infrastructure is permanently monitored for incidents that pose a threat to operations or are relevant, and faults or problems are rectified promptly.<br>The monitoring of the IT infrastructure is automated using tools in which the relevant critical threshold values and performance and capacity criteria for the relevant IT components are stored. | Inquired the procedure whether active, tool-supported monitoring is in use to identify errors in data processing, which result in incident tickets. Inspected the documentation of an incident to determine that it was handled accordingly. | No relevant exceptions noted. |

## Data Protection

| Control Objective | | | |
|---|---|---|---|
| **10** | Controls provide reasonable assurance that data confidentiality can be maintained. | | |
| **#** | **Control description** | **Test procedures performed by Baker Tilly** | **Conclusion** |
| **10.1** | There is a data protection concept implemented, which is reviewed at least annually. Review is documented. | Inspected the policy and procedures regarding data protection for appropriateness and determined that they were approved by management, reviewed and updated annually. | No relevant exceptions noted. |
| **10.2** | A data protection officer is appointed, who regularly reports to management. | Ascertained that a data protection officer has been appointed and reports to management on a regular basis. | No relevant exceptions noted. |
| **10.3** | Technical and organizational measures are implemented and observed in line with the data protection concept. This includes confidentiality requirements for employs and service providers. The data protection officer regularly checks whether the TOMs are appropriate. | Ascertained whether employees are bound to secrecy and to compliance with data protection regulations. Inspected whether the TOMs are checked regularly. | No relevant exceptions noted. |

# Appendix 1: General Engagement Terms

[Translator's notes are in square brackets]

## General Engagement Terms

for

**Wirtschaftsprüferinnen, Wirtschaftsprüfer and Wirtschaftsprüfungsgesellschaften**
**[German Public Auditors and Public Audit Firms]**

as of January 1, 2024

### 1. Scope of 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) Were 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





50342
01/2024

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 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 accepted written form (gesetzliche Schriftform), and with a wording 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 therefrom are exclusively governed by German law.