
ISAE 3402 Report Type 2

SKIDATA AG,
Grödig, Austria

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

for the Period from November 1, 2019 to April 30, 2020

Table of Contents

1	Independent Service Auditor's Assurance Report	1
2	SKIDATA's Assertion	7
3	Description of the System Provided by SKIDATA	13
3.1	General Information on SKIDATA and Services Provided	15
3.1.1	Overview of SKIDATA.....	15
3.1.2	Solutions and Products	15
3.1.3	Customers	16
3.2	Scope of this Report	16
3.2.1	SDAZ	16
3.2.2	DTA	16
3.2.3	SDRDM	16
3.3	Control Environment	16
3.3.1	Integrity and Ethical Values	16
3.3.2	Commitment to Competence.....	17
3.3.3	Executive Board and Supervisory Board.....	17
3.3.4	Management's Philosophy and Operating Style.....	17
3.3.5	Organizational Structure.....	17
3.3.6	Human Resource Policies and Practices	18
3.3.7	Risk Management.....	18
3.3.8	Information and Communication	19
3.3.9	Monitoring	19
3.3.10	Control Objectives and Description of Related Controls ...	19
3.3.11	Changes since Last Report	21
3.4	Verbal Process Description	27
3.4.1	System Architecture SDAZ	27
3.4.2	System Architecture DTA.....	28
3.4.3	Acquisition and Maintenance of Technology Infrastructure	28
3.4.4	Incident & Problem Management	28
3.4.5	Product Creation Process Software	29
3.4.6	Product Release Process	30
3.4.7	Hotfix and Patch Procedure.....	30
3.4.8	Definition and Management of Service Levels	30
3.4.9	System Security	31
3.4.10	Management of the Configuration	32
3.4.11	Management of Data and Backups.....	32
3.4.12	Management of Physical Access	32
3.4.13	Enable and Manage Operations	32
3.4.14	Monitor and Evaluate Internal Control	33
3.5	User Control Considerations	33
4	Information Provided by the Independent Service Auditor.....	35
4.1	Control Objectives, Related Controls and PwC's Tests of Operating Effectiveness	37
4.1.1	System / Controls Overview	39
4.1.2	Acquire and Maintain Technology Software.....	41
4.1.3	Acquire and Maintain Technology Infrastructure.....	42
4.1.4	Enable Operation and Use	43
4.1.5	Procure IT Resources	45
4.1.6	Manage Changes.....	46
4.1.7	Install and Accredite Solutions and Changes	47
4.1.8	Define and Manage Service Levels	48
4.1.9	Manage Third-party Services.....	49
4.1.10	Ensure Systems Security	50
4.1.11	Manage Service Desk and Incidents.....	52
4.1.12	Manage the Configuration	53

4.1.13	Manage Data	54
4.1.14	Manage the Physical Environment	55
4.1.15	Manage Operations.....	56
4.1.16	Monitor and Evaluate Internal Control.....	57
4.1.17	Communicate Management Aims and Directions	58
4.1.18	Manage IT Human Resources.....	59
4.1.19	Manage Quality	60

Index of Appendices

General Conditions of Contract for the Public Accounting Professions

1 Independent Service Auditor's Assurance Report

Independent Service Auditor's Assurance Report on Controls at SKIDATA AG

To the
Management of
SKIDATA AG
Untersbergstraße 40
5083 Grödig, Austria

Scope and Terms of Engagement

We have been engaged to report on SKIDATA AG's, Grödig, Austria (subsequently called "SKIDATA") description on pages 13 to 33 of its system of IT general controls related to the solutions SDAZ and DTA provided at the housing centers of its contractor in Wels, Austria, throughout the period November 1, 2019 to April 30, 2020 (the description) and on the suitability of the design and operating effectiveness 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 customer controls contemplated in the design of SKIDATA's controls are suitably designed and operating effectively, along with related controls at the service organization. We have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

SKIDATA uses a subservice organization for the data center in Wels, Austria, where its IT infrastructure components are housed. The description on pages 13 to 33 includes only the controls and related control objectives of SKIDATA and excludes the control objectives and related controls of the subservice organization. Our examination did not extend to controls of the subservice organization (use of carve-out method).

Our assignment and professional liability for this engagement is governed by the General Conditions of Contract for the Public Accounting Professions (AAB 2018) attached to this report. By reading and using the information contained in this report, the recipient confirms acceptance (including the limitation of our liability as stipulated in clause 7) with respect to us.

SKIDATA's Responsibilities

SKIDATA is responsible for: preparing the description and the accompanying assertion on pages 7 to 33 including the completeness, accuracy and method of presentation of the description and the assertions; providing the services covered by the description; specifying the control objectives and stating them in the description; identifying the risks that threaten the achievement of the control objectives; identifying the criteria and designing, implementing and effectively operating controls to achieve the stated control objectives.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on SKIDATA'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 the 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 were suitably designed and operating effectively.

An assurance engagement to report on the description of a service organization's system and the suitability of the design and operating effectiveness of controls at a service organization involves performing procedures to obtain evidence about the description, and the suitability of design and operating effectiveness of controls. The procedures selected depended on the service auditor's judgment, including the assessment of the risks that the description is not fairly presented, and that the controls were not suitably designed or operating effectively. Our procedures also 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 control objectives stated therein, and the suitability of the criteria specified by the service organization and described on pages 7 to 11.

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

Independence and Quality Control of the Auditor

We have complied with the Code of Ethics for Professional Accountants issued by the International Ethics Standards Board for Accountants, which includes independence and other requirements founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behavior.

The audit firm applies the International Standard on Quality Control 1 (“ISQC 1”) and accordingly maintain a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Inherent Limitations

SKIDATA’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 and correct all errors or omissions in the system of IT general controls related to the solutions SDAZ and DTA provided at the housing centers of its contractor in Wels, Austria. Also, the projection to future periods of any evaluation of the fairness of the presentation of the description, or opinions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives is subject to the risk that controls at a service organization may become inadequate or fail.

Opinion

Our opinion has been formed on the basis of the matters outlined in this report. The criteria we used in forming our opinion are those described on pages 7 to 11. In our opinion, in all material respects:

- a) the description fairly presents the system as designed and implemented throughout the period November 1, 2019 to April 30, 2020;
- b) the controls related to the control objectives stated in the description were suitably designed throughout the period November 1, 2019 to April 30, 2020, and

- c) the controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period November 1, 2019 to April 30, 2020.

Description of Tests of Controls

The specific controls tested and the nature, timing, and results of those tests are detailed on pages 35 to 60.

Intended Users and Purpose

We were engaged to report by SKIDATA and, therefore, this report and the description of tests of controls and results thereof on pages 35 to 60 are intended for the use of SKIDATA.

We permit the disclosure of this report, in full only, including the description of tests of controls and results thereof by SKIDATA, at its discretion, to customers who have used SKIDATA’s system of specific controls related to the solutions SDAZ and DTA provided at the housing centers of its contractor in Wels, Austria, and their auditors, who have a sufficient understanding to consider it, along with other information about controls operated by customers themselves, when assessing the risks of material misstatements of customers’ financial statements, without assuming or accepting any responsibility or liability to customers or their auditors on our part.

Salzburg, June 17, 2020

PwC Salzburg
Wirtschaftsprüfung und
Steuerberatung GmbH



p.p. Rainer Ziehaus



Anton Pichler
Austrian Certified Public Accountant

2 SKIDATA's Assertion

SKIDATA's Assertion

SKIDATA AG
Untersbergstraße 40
5083 Grödig
Austria

We have prepared the accompanying description of SKIDATA's system of specific controls related to the solutions SDAZ and DTA provided at the housing centers of its contractor in Wels, Austria. This description is intended for user entities of the system and their auditors, who have a sufficient understanding to consider the description, along with other information, when assessing the risks of material misstatements of user entities' financial statements.

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

1. The accompanying description on pages 13 to 33 fairly presents the system of IT general controls related to the solutions SDAZ and DTA provided at the housing centers of its contractor in Wels, Austria. The description is relevant for processing user entities' transactions throughout the period November 1, 2019 to April 30, 2020.

The criteria used in making this assertion were that the accompanying description:

- a) presents how the system was designed and implemented, including:
 - the types of services provided including, as appropriate, classes of transactions processed;
 - the procedures, within both information technology and manual systems, by which those transactions, as appropriate, were initiated, recorded, processed, corrected as necessary, and transferred to the reports prepared for user entities of the system;

- how the system dealt with significant events and conditions, other than transactions;
 - the process used to prepare reports to user entities of the system;
 - relevant control objectives and controls designed to achieve those objectives including, as applicable, complementary user entity controls contemplated in the design of the service organization's controls;
 - 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 transactions of user entities of the system.
- b) includes relevant details of changes to the service organization's system during the period November 1, 2019 to April 30, 2020.
 - c) 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 user entities of the system and their auditors, and therefore may not include every aspect of the system that each individual user entity of the system and its auditor may consider important in its own particular environment.

2. the controls related to the control objectives stated in the description were suitably designed and operated effectively throughout the period November 1, 2019 to April 30, 2020.

The criteria used in making this assertion were that:

- a) the risks that threatened the achievement of the control objectives stated in the description were identified;
- b) the controls identified in the description would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved;
- c) the controls were consistently applied as designed, including that manual controls were applied by individuals who have the appropriate competence and authority, throughout the period November 1, 2019 to April 30, 2020.

Grödig, June 17, 2020

Alexander Vouk

Michael Gradnitzer

Members of the Executive Board of SKIDATA AG

3 Description of the System Provided by SKIDATA

3.1 General Information on SKIDATA and Services Provided

3.1.1 Overview of SKIDATA

SKIDATA AG is an Austrian company, founded in 1997 and is ranked among the worldwide leading providers of access solutions and visitor management. Today, SKIDATA AG is the parent company of the SKIDATA Group represented by 26 subsidiaries worldwide. Almost 10,000 SKIDATA systems guarantee quick and secure access for people and vehicles in: ski regions, shopping centers, major airports, cities, sport stadiums, fair and amusement parks.

The SKIDATA Group offers turnkey solutions from a single source:

- Access and visitor management
- System controlling
- Monitoring and maintenance
- Cost control
- Administration
- Services

The foundation of SKIDATA's success is on the one hand based on the more than 1,000 dedicated and skilled employees and the clear focus on research and development. On the other hand, the company stands for responsibility and sustainability and benefits from the global network of its parent company, the Swiss Kudelski Group. SKIDATA AG and its 26 subsidiaries and countless partners are present in over 90 countries.

3.1.2 Solutions and Products

SKIDATA's systems provide the operators with optimal efficiency, highest security and profitable options to maximize the return on investment. The production of SKIDATA's hardware is outsourced whereas the development, sales, marketing and after sales services of SKIDATA products (hardware & software) and solutions are core competencies of SKIDATA.

SKIDATA offers its clients a wide range of solutions and services for controlled access of persons and vehicles. SKIDATA's know-how and products are designed to help its customers to maximize their benefits. SKIDATA's range of solutions and products comprise:

- Management Software
 - Parking.Logic for professional parking access and revenue control
 - Handshake.Logic for access management at event venues and stadiums
 - Summit.Logic (formerly Freemotion.Logic) for access management at mountain sport resorts
 - DTA for all the above segments as a hosted service
- Access Components
 - Barrier.Gate, Power.Gate and Lite.Gate ,the access solution devices for access with cars
 - Vario.Gate for professional and smooth mass entrance of persons
 - Freemotion.Gate and Easy.Gate for professional and smooth access check at ski resorts
 - Handheld.Gate, the mobile reader and admission devices for flexible access control
- POS Solutions
 - Manual.Cash, the workstation for operators
 - Power.Cash for easy and convenient automated cash and credit card payment
 - EasyTicket.Cash for convenient ticket sale via ticket vending machines
 - OPOS.Cash for selling ski passes at the hotel reception
- Data carriers such as RFID cards, barcode tickets or magnetic stripe cards
- Business Services
- System Interfaces for smooth and easy integration of third-party systems

3.1.3 Customers

With its wide range of sophisticated solutions and cutting-edge products, the SKIDATA Group serves the needs of customers in various segments. SKIDATA has therefore tailored its solutions to the specific needs of the following customer segments:

- Ski Resort Operators
- Airport Cities & Hubs
- Regional & City Airports
- Off Airport
- Hospitals or Health Centers
- Residential Car Parks
- City Parking
- Spa & Wellness
- Office, Business Parks & Multifunctional Buildings
- Park & Ride
- Retail
- Hotels
- Shopping Centers
- Public Transport
- Fairs & Exhibition Centers
- Stadiums & Arenas
- Attraction & Amusement Parks
- Festivals
- Universities & Educational Institutions
- Urban & Tourism Destinations

3.2 Scope of this Report

3.2.1 SDAZ

The mountain destination market in Europe is characterized by numerous independent ski lift operators. However, these ski lift operators collaborate in terms of marketing and by providing slope miles for skiers together with other ski lift operators (ski pools). These alliances enable skiers to enjoy slopes of different ski lift operators without buying various, different tickets. From a technical point of view, this situation leads to two challenges:

- Tickets need to be valid beyond the single ski lift operator; skiers should be able to use all slopes within the entire ski pool
- Whenever two or more independent ski lift operators collaborate, revenue must be allocated

SKIDATA SDAZ enables ski lift operators to offer ski pool-wide valid tickets, monitoring functions and management information by recording and processing the ticket data in databases operated centrally by SKIDATA. Moreover, SKIDATA provides services that deliver the basis for revenue allocation.

3.2.2 DTA

DTA is a hosted service at SKIDATA AG which allows customers to connect their locally installed access control and sales system with cloud-based sales and access systems. This cloud can be hosted at SKIDATA AG or being installed as an on-premise installation.

For this purpose, DTA offers basically 2 different interfaces which are used for interacting with the service:

1. Contractor interface: This is used for connecting systems which fulfill a contract, e.g. a Summit.Logic access control system. This interface is restricted for internal use at SKIDATA and its products
2. Sales Channel interface: This is the public interface which is used to operate web shops and cash desks

DTA contains data for tickets and which customer they belong to, but does not contain sales or revenue data.

3.2.3 SDRDM

SDRDM is a reporting tool for Freemotion.Logic and Summit.Logic. It provides numerous reports related to sales data and access data. User permissions can be defined on report level and row level (limit access to specific companies or pools). Schedules for automatic report generation can be defined. The tool provides a set of reports for allocation of revenues to specific companies within a pool according to defined allocation rules.

3.3 Control Environment

3.3.1 Integrity and Ethical Values

The effectiveness of controls is determined by the integrity and ethical values of the company's management as well as by those people who implement, conduct and monitor them. Hence, integrity and ethical values are the core elements of SKIDATA's control environment and are included in the Kudelski/SKIDATA code of conduct. This code of conduct is designed to achieve a common understanding by all employees of the group concerning appropriate ethical behavior and includes – but is not limited to – steps to mitigate and remove incentives that might prompt employees to engage in dishonest, illegal or unethical acts. Besides the role model function of senior

management, controls are in place in order to ensure and maintain employee integrity and ethical behavior.

- The Kudelski/SKIDATA code of conduct includes the guiding principles
- Ethical and behavioral standards are part of the employee handbook, which is published on the intranet and therefore available on a group-wide level
- Contracts of employment include a confidentiality agreement. The contract of employment is signed by all employees.
- If employees acknowledge a failure to comply with behavioral standards, a formal resolution process is in place, which is distributed together with the code of conduct.

3.3.2 Commitment to Competence

For every new job to be filled, management must determine technical and social / behavioral requirements and document them in a formal job description. This job description forms the basis for candidate screening during the recruiting process.

In addition, the supervisors have to review their employees' competencies and skills annually based on a standardized and corporate-wide methodology. The appraisal must be approved by the employee, the responsible manager and the manager's supervisor. It is also reviewed by HR.

The key competencies and technical skills for the employees that need to be developed are mutually defined among the superiors and the employees during the annual performance appraisal. In order to address the demand for development, a plan is agreed upon, which contains on-the-job actions (e.g. coaching and feedback) and/or off-the-job actions such as internal and/or external trainings. Employees who have attended an external training are obliged to share the acquired knowledge by holding internal trainings.

SKIDATA is aware that sustainable success is based on its employees. Therefore, SKIDATA attracts highly qualified personnel through its presence at career fairs, cooperation with universities and colleges of engineering, provision of master thesis collaborations, fringe benefits, etc.

3.3.3 Executive Board and Supervisory Board

Corporate commitment to efficient controls is largely determined by SKIDATA AG's executive board and the supervisory board, which oversees management activities. The executive board understands its responsibility with regard to financial reporting and internal control.

Executive Board	Supervisory Board
• David Luken (CEO) • Alexander Vouk • Robert Weiskopf	• Charles Egli (Chairman) • Mauro Saladini (Vice Chairman) • André Kudelski • Patrick Foetisch • Laurent Dassault

Due to the importance of adequate and efficient controls, SKIDATA AG has implemented control activities, which are described below:

- Review of the code of conduct by the executive board on a regular basis
- Performance, strategy and recent topics are discussed monthly at the executive management meeting and quarterly at supervisory board meetings
- The monthly reporting of key performance indicators is reviewed by the executive management and the executive board
- Review of significant deviations by the executive board
- Regular reporting of key performance indicators to members of the supervisory board

3.3.4 Management's Philosophy and Operating Style

Risk awareness, emphasis on process requirements, due diligence regarding assigned tasks and the importance of accurate financial reporting are some of the characteristics of the executive boards' philosophy and operating style. Therefore strategy workshops and board meetings are held on a regular basis.

3.3.5 Organizational Structure

SKIDATA's value chain comprises R&D, marketing & sales and after-sales services as well as supporting activities such as finance and HR. In order to ensure best-in-class operations and an efficient reporting structure as well as

to provide a framework for planning, directing and controlling of operations, SKIDATA AG is organized in several units – Sales, Business Line Management and Innovation, Operations, Research and Development, Business Development, Human Resources and Finance. These units are supervised by business unit managers. In the case of Sales and Finance, the unit managers are part of the executive board. This assignment of responsibilities fosters appropriate communication and efficient reporting to the executive management, executive board and the supervisory board. The units are again subdivided into departments.

SKIDATA AG has established an organizational chart that communicates key areas of authority, responsibility and reporting structure as well as the people in charge of the key areas. The organizational chart is distributed among employees through the intranet. Moreover, the organizational chart is part of the employee handbook.

3.3.6 Human Resource Policies and Practices

The Human Resource (HR) process covers hiring and orientation, evaluation, training and promotion as well as compensation, social benefits and resignation. Thereby, the HR department is mainly responsible for the recruiting and screening of job applicants and also the administration and coordination of the entry and exit process, annual evaluation activities, training programs and compensation and benefits. SKIDATA AG's management is responsible for the review of employees' job performance together with the operational implementation of HR practices and policies. The specific control activities with respect to the HR processes are:

- All new hires require an upfront approval by CEO and CFO.
- The monthly HR reporting gives an overview about all employee changes by business unit to ensure that only approved positions are filled.
- Job applicants are interviewed by HR and the responsible supervisor. For all key / management positions, an assessment center is established to evaluate social and technical skills in detail.
- An electronic entry checklist must be completed for each new employee. A copy is maintained in the employee file.
- An electronic exit checklist must be completed for each employee leaving. A copy is maintained in the employee file.

- The SKIDATA Group has implemented an annual review and appraisal process. Management performs evaluations for each employee based on a common corporate methodology.
- The SKIDATA Group applies a compensation model that includes a fixed and a variable part for all employees. The variable pay is defined by financial targets that are defined by the executive board as well as non-financial goals that are individually agreed upon between the employees and the responsible superior. The target achievement is reviewed annually by the responsible manager and approved by supervisors before payment.
- All permanent employees are required to acknowledge the code of conduct and IT security policy during their 90-day onboarding period, which includes all important regulations regarding the use and handling of the IT infrastructure, email and internet. A copy of the signed 90-day onboarding checklist is filed in the employee file.

3.3.7 Risk Management

Risk management at SKIDATA AG is about the identification, analysis and management of risks, which could potentially affect SKIDATA's business and its ability to provide reliable customer transactions. SKIDATA AG considers risk management as a process for both downside risks and upside potentials.

In order to address different uncertainties, risk management is performed on several levels of the organization, which are described below. These risk management activities are centrally supervised by the head of controlling & risk management.

As mentioned before, SKIDATA's risk management is a multi-step approach at three distinctive levels – high-level, mid-level and on a detailed level. At the highest level, SKIDATA addresses all relevant events that could affect the company's overall business model and its success on the market. This level of risk management encompasses threats related, e.g., to the economic environment, product range, strategic position and geographic expansion. The mid-level section comprises all detailed and non-detailed aspects of the risk management for a specific element of SKIDATA (e.g., finance-related risks) that are standardized. On the lowest level of risk management, SKIDATA focuses on specific processes and the relevant key risks and controls.

This basic approach is documented in SKIDATA's risk management policy.

3.3.8 Information and Communication

SKIDATA AG's management has established several communication channels in order to inform employees about significant events, initiatives and organizational topics. Furthermore, SKIDATA AG ensures that employees understand their individual roles and their contribution to the performance of the SKIDATA Group. SKIDATA's communication channels encompass:

- Intranet that informs the workforce of recent events or organizational topics. It is also used as a platform for the communication of policies.
- Periodic staff meetings
- Training programs for employees
- Mail messaging system
- Periodic employee performance appraisal

SKIDATA AG's management has also introduced communication channels to gather information for the determination of relevant risks. Each department head must report recent events periodically to the superior according to the line of command, which is part of the job description. There are regular staff meetings of the department heads and the respective business unit manager, executive board meetings, and meetings of the business unit managers and the executive board that address current events and strategic developments.

3.3.9 Monitoring

The executive board oversees the operating performance of the company and its strategic objectives. Furthermore, the executive board conducts control activities such as the monthly review of key performance indicators and variance analysis (e.g. budget-to-actuals). In addition, there are regular examinations of accounting and finance-related processes by the CFO and the controlling and risk management department. Moreover, controllers investigate deviations to the budget and the prior year (detailed variance analysis) and report their findings to the CFO. Monitoring tools (e.g. compliance monitor) for sales, costs and investments are provided to management; major deviations must be justified to the CFO. At Kudelski Group level, COSO (Committee of Sponsoring Organizations of the Treadway Commission) has been implemented. In order to comply with the parent company's group policies major principles have been implemented at SKIDATA AG, SKIDATA's Control Objectives and Description of Related Controls.

3.3.10 Control Objectives and Description of Related Controls

SKIDATA AG has implemented a set of control objectives, which are relevant to the services in scope of this report and to its customers. Furthermore, SKIDATA AG has applied the respective procedures and controls to mitigate potential risks in each area. The control objectives are largely oriented on the following COBIT 4.1 topics:

- Management aims and directions are communicated to safeguard IT security. (PO6)
- Human Resources are managed, including permission management to IT resources. (PO7)
- Quality of software development is managed by defined practices and processes. (PO8)
- Acquisition and maintenance of software is regulated by quality test plans. (AI2)
- Infrastructure acquisitions are approved to ensure the required security and stability. (AI3)
- Knowledge about new software, which is necessary for successful operation and support, is transferred. (AI4)
- Changes to the existing system software and hardware are authorized, tested, approved, properly implemented and documented (change procedures). (AI6)
- Installation of solution and changes are performed according to agreed release planning after evaluating test result. (AI7)
- Service level agreements (SLAs) are established. (DS1)
- Support of third-party providers is established by maintenance agreements which are reviewed with respect to effectiveness and completeness. (DS2)
- Access to hosted systems and the network infrastructure devices is appropriately restricted to authorized users only. (DS5)
- Incidents are tracked, resolved and escalated in a timely manner. (DS8)
- Integrity of system with respect to hardware and application compliance as well as security compliance is managed by defined and regularly updated guidelines. These guidelines are the basis for the review of the integrity of the hardware and software configuration. (DS9)
- Backups are performed reliably, accurately and completely in accordance with the established backup plan. (DS11)

- Physical access to the data centers is appropriately restricted to authorized individuals only. (DS12)
- High availability of the service is provided by monitoring performance parameters of the configurations. Processes in place assure coverage of the monitoring system. Based on a review of monitoring parameters the required capacity is allocated for IT services. (DS13)
- Monitoring and evaluation of controls based on internal and external audits safeguard the effectiveness of defined controls. (ME2)

SKIDATA's control objectives and a detailed description of the derived control activities are provided in the control matrix, which is part of section 3.

For hosted software in scope, SDAZ and DTA, the data center is hosted in Wels by eww ag | ITandTEL.

The backup location is at the same location but in a different room, separated by fire resistant walls and doors. A further backup for the storage system is in a different location and hosted by eww ag | ITandTEL.

eww ag | ITandTEL is the housing partner for the data center for DTA and SDAZ. The subservice organization's control objectives and related controls are omitted from the description. The control objectives in the report include only the objectives that the service organization's controls are intended to achieve.

3.3.11 Changes since Last Report

The control matrix of SKIDATA AG and SKIDATA AUSTRIA GmbH was reviewed in a multi-disciplinary approach by representatives from multiple departments within SKIDATA AG and a SKIDATA subsidiary. The controls have been evaluated with respect to coverage of IT risks to better support customer and business requirements.

Effective controls already in place have been described in more detail with respect to process, controls and responsibilities. Controls which could not cover the IT risk appropriately have been replaced by more effective controls. Additionally, a higher coverage with respect to COBIT- 4 has been achieved. The new control matrix is effective as of November 1, 2019.

Control ID	Control Description	Description of Change
PO_o6a	It is verified that the IT Security Rule is updated on a yearly basis. A new version on the intranet is the related evidence. Additionally, it is verified that employees have been informed by checking availability of related newsletter.	Replaces DS5_a; Proactive information to users
PO_o7a	For each new employee a track record / acknowledgment of IT Security guideline on the learning platform is available. This report is checked regarding completeness.	Replaces DS5_b; Process improvement to provide coverage for temporary employees
PO_o7c	For each permanent employee leaving the company a workflow is to be executed which contains the tasks to disable his active directory account.	New
PO_o8a	The SW development process documents must be	Replaces AI6_a; Editorial changes

	available for R&D and must be reviewed once a year.	
AI_o2a	The test plan (which includes test cases with expected results) must exist for each release and service pack. Hotfixes are excluded.	New
AI_o3a	A list of all new deployments is regularly reviewed to assure that deployment tickets exist.	Replaces AI3_b; Editorial changes
AI_o3b	A list of all network devices and installed firmware versions is created and compared to the latest available firmware version.	Replaces AI3_f
AI_o3c	The update plan is annually reviewed and approved.	Replaces AI3_h; Improvement of tracking
AI_o3d	A Nessus patch report is generated after each update session. The reports are reviewed monthly to check if any patches have been left out and if the frequency matches the update plan.	Replaces AI3_d and AI3_i; Process improvement by better definition of specific update requirements.
AI_o4a, AI_o4b, AI_o4c	Check timely availability of release documentation (release notes / hotfix notes).	Replaces AI4_a; Evidences specifically defined for SAAS & on-premise SW
AI_o4d, AI_o4e AI_o4f,	Check availability and date of "release" email to stakeholders before release (excluding hotfixes) is published on repository.	New
AI_o4f	Verify that documentation for customer about new functionality (Release Highlights) is published on intranet.	Replaces AI6_f; New document set defined

AI_05a	Check annual approval of rule ASP (Authorization & Signatory Powers)	Replaces AI3_a; Split to different responsible persons
AI_05b	For all demands requested by employees of the hosting department (identified by cost center) it is verified if the acquisition has been approved according to the approval matrix.	Replaces AI3_a; Split to different responsible persons
AI_06a	Hotfixes are requested in a separate field by technical support. A verification task is created/verified and closed. The field "hotfix" available in the HF version is updated by Development.	Replaces AI6_e; Editorial changes
AI_06b	Check availability of hotfix release document (hotfix notes) for each published hotfix. The approval date is to be before/equal to availability date on server.	New
AI_06c	For transparent tracking of changes each software change has to be recorded in the issue tracking tool (e.g. JIRA). A verification task for defects needs to exist. A testing task for features needs to exist. A fixversion needs to be set.	Replaces AI6_b and AI6_c for on-premise software
AI_06d	For transparent tracking of changes each software change has to be recorded in the issue tracking tool (e.g. JIRA). Standard issue types are user stories and bugs. A testing task for each	Replaces AI6_b and AI6_c for SAAS software

	standard issue type (e.g. user story, bug) needs to exist. The fixversion(s) in the standard issue type need(s) to be set. The testing task and the standard issue type need to be "closed".	
AI_07a	Verify that the release plan for Summit.Logic is published on the PMO intranet site.	New
AI_07b	A QA environment needs to exist where SW changes can be verified before they are released.	Replaces AI6_g; Editorial changes
AI_07c	For each deployment of DTA, which is tracked by the hosting team, release notes have to be available with an approval date before deployment date.	Replaces AI6_d for SAAS software; Adjustment of control to process
AI_07d	SDAZ software (Summit.Logic) is provided on repository only after release notes have been published by QA.	Replaces AI6_d for on-premise software; Adjustment of control to process
DS_01a	It is verified that required documents are available on the intranet, consisting of the hosted service agreement and fact sheets for the hosted service.	Editorial changes on DS1_a
DS_01b	Each year a review takes place whether the hosted service agreements template has to be adjusted. If updates are required, it is checked whether the related documents have	Editorial changes on DS1_b

	been updated and published on the intranet.	
DS_o2a	Once a year, the list of maintenance agreements is reviewed for correctness and completeness. The basis of this review is the hardware inventory carried out in DS9_a. During the review, decisions are made whether a piece of hardware needs a maintenance agreement and if yes, what kind of maintenance is most appropriate.	Replaces DS2_a; More detailed description
DS_o5d	The list of firewall tickets is reviewed monthly for consistency.	Replaces DS5_d; Description adjusted to new way of tracking
DS_o5e	Once a year, all firewall rules are being reviewed and discussed in a review meeting by the relevant parties. Unnecessary or obsolete rules will be removed, as well as rule simplifications will be carried out. The result of the review is a ticket that includes all proposed changes. This ticket needs to be reviewed and approved.	Replaces DS5_e; Description adjusted to new way of tracking
DS_o5h	For each new employee an entry checklist has to be available. Within the checklist the access permissions have to be defined by the superior. Permissions to hosting environment are subject to further control DS_5i.	Replaces DS5_h; Description adjusted to new way of tracking

DS_o5i	The list of user request tickets is reviewed monthly for consistency.	Replaces DS5_i; Editorial changes
DS_o5k	A review of all operating system users is performed regularly. All users and their permissions are checked for validity and rationality. Users that are obviously obsolete are deactivated. Irregularities in permissions are discussed with the users and/or their superiors. The result of the review is a ticket that includes all proposed changes. This ticket needs to be approved.	Replaces DS5_k; More detailed description
DS_o5o	The results of the pentest are evaluated together with Development and architects and actions are derived and planned for.	Replaces DS5_o; Process improvement
DS_o8a	Show that mandatory fields must be filled to be able to forward the issue to CTS.	Replaces DS8_a; Editorial changes
DS_o8b	Responsible person checks via dashboard problem management that issues are answered within a defined period. (OLA)	Replaces DS8_c; Improvement of tracking procedure
DS_8b	Skipped	Control only described tool, risk covered by DS8_b.
DS_o8d	The responsible person checks via dashboard problem management that issues forwarded to R&D are linked with change request tool by R&D	Replaces DS8_d; Editorial Changes only

DS_o8e	All incident tickets at Hosting are regularly reviewed for irregularities, especially tickets that are older than 30 days and tickets that have not yet been assigned to a person.	Replaces DS8_e; Editorial changes
DS_o8f	Verify if OLA document has been approved within the last 12 months.	New
DS_o9a	Once a year, the hardware inventory is reviewed by comparing the documentation with the actual data center. This review is documented in a ticket.	Replaces DS9_a; Adjustment of tracking procedure
DS_o9b	Check whether all DTA application updates are based on OTRS ticket.	Replaces DS9_b; Adjustment of tracking procedure
DS_o9c	An annual review is conducted to review changes to the baseline and to assure conformity with security industry best practices.	Replaces DS5_l; Process improvement
DS_o9d	Compliance of servers with the hardening baseline is checked regularly. The result is a report with comments and mitigation efforts of potential non-compliance via tickets.	Replaces DS5_m; Process improvement
DS_11a	The backup strategy plan is reviewed for consistency and continuous improvement once a year.	Replaces DS11_a; Editorial changes
DS_11b	Once a month, all backup summary tickets are reviewed to check if any backup faults have been overlooked.	Replaces DS11_b; Editorial changes

DS_11e	Restore tests are done regularly in order to guarantee operational capability of backups. This is done by testing various restore scenarios like VM restore, database schema restore and single file restore. If restore tests fail, the reason will be investigated and corrections will be made. Details are being documented in the ticket.	Replaces DS11_e; More detailed description of control
DS_12a	Once a year, a test of all rack door alerts is conducted. The test is documented and approved.	Replaces DS_12j; Process improvement
DS_12b	The list of users with rack access is reviewed regularly.	Replaces DS_12k; Editorial changes
DS_13a	To assure that no asset is forgotten, an annual review is conducted. The list of known assets is compared to the list of assets configured in the monitoring system.	New
DS_13b	To assure availability and redundancy of resources, the capacity of the infrastructure is reviewed yearly. Investment decisions are based on this review.	New
DS_13c	To assure availability of individual services, all services are monitored via the monitoring system on a five-minute basis. The achieved SLAs are being	New

	reviewed every month and reported to Operations.	
ME_o2a	Check that an ISAE core team meeting is held, following up on periodical checks, ISAE related process improvements and remedial actions from previous ISAE reports.	New
ME_o2b	Check availability and status of list for periodical tasks	New
ME_o2c	Deviations found by external auditor are noted in the minutes of the ISAE core team meeting and remedial actions are taken.	New
DS3_a	Prior to the clearing process, the transaction data is verified for completeness and consistency by a programmed routine. As a result, a list of detected errors is displayed for further investigation and manual correction by the pool clearing personnel.	This control has been moved to the controls of the subsidiary.
DS3_b	A tool for customers and technicians of SKIDATA for verifying data consistency is installed on the SDAZ and can be used prior to pool clearing.	This control has been moved to the controls of the subsidiary.

DS8_a	Incidents are systematically recorded through capturing them in JIRA by the service technicians. Such a record is called "fault record". An entry of a fault record in JIRA requires certain mandatory fields which must be filled in by the service technicians.	This control is still applicable for SKIDATA AG and additionally for the subsidiary.
AI3_c	In the area of MS-OS the update procedure provided by MS (WSUS server) is used. Security updates on application servers are installed automatically. A report is sent to OTRS.	Replaced: AI3_c, AI3_g, AI3_d are replaced by AI3_h and AI3_i
AI3_g	Linux OS security updates of application servers are deployed at least monthly (<30 days).	Replaced: AI3_c, AI3_g, AI3_d are replaced by AI3_h and AI3_i
AI3_d	OS security updates of database servers (Oracle and MSSQL), domain controllers and backup servers are deployed at least 3 times a year.	Replaced: AI3_c, AI3_g, AI3_d are replaced by AI3_h and AI3_i
AI3_h	An update plan is established for each server. The update plan is regularly reviewed.	New: AI3_h and AI3_i replace AI3_c, AI3_g, AI3_d
AI3_i	OS updates are applied according to the update plan. Different update tools and logs are used for Windows and Linux.	New: AI3_h and AI3_i replace AI3_c, AI3_g, AI3_d
AI3_f	Firmware of network devices (switches and firewalls) is checked at least for security updates. Findings on those other devices are documented.	Common tool for documentation, Removed section on automatic check with Nessus.

DS5_c	Changes of firewall configuration are based on customer requirements which are placed via phone or email.	Replaced by DSD5_d: This control applicable for SDAZ only is now covered by DS5_d.
DS5_d	Firewall rule change requests can be placed by TS or from within hosted services. All requests have to be captured by OTRS, must contain a description of the rule and the use case.	This control is now additionally applicable for SDAZ (before only for DTA). Four eyes principle, which had not been applied for SDAZ, has been skipped for DTA.
DS5_l	Security parameters on OS level are set to achieve an appropriate security standard. The baseline security parameters are defined in a Confluence page. Configuration samples are checked on a regular basis.	Frequency has been changed from continuously to quarterly. Added: "Configuration samples are checked on a regular basis."
DS5_m	Security parameters on network infrastructure devices (routers and switches) level are set to achieve an appropriate security standard. The baseline settings are defined on a Confluence page. Configuration samples are checked on a regular basis.	Frequency has been changed from continuously to quarterly. Added: "Configuration samples are checked on a regular basis."
DS9_a	Each piece of hardware is captured in workflow and document management tools used by SKIDATA. It is identifiable by its serial number. Changes are documented within the documents and workflow tools.	Frequency has been changed from continuously to event-driven.

AI4_a	For all changes of software provided by SKIDATA - except hotfixes (see control AI6_e for the procedure for hotfixes) – release notes are prepared primarily for the support (incident and problem management) but for the sales force as well. Details regarding the changes are available through a link in JIRA.	Editorial changes. "A four eyes principle is in place" has been omitted from description, since this applies to the testing process and not the release process.
DS5_b	New SKIDATA AG and SKIDATA Austria GmbH employees confirm that they are aware of the IT security policy within the 90-day onboarding plan. The signed 90-days plan is kept in the personnel records.	Approval of IT security policy is now covered by the 90-day onboarding checklist.
DS5_h	Based on a signed contract of employment HR sets up an entry checklist. The checklist contains all necessary tasks to set up the employee's working environment such as workstation, 90-day onboarding plan, IT access rights, etc. Based on this checklist, the IT sets up a user account for the SDNET domain. The respective superior grants the specific access rights based on the user's function. In case of SDAZ the additional user accounts are approved and set up by the team leader CC/NSA.	Approval of IT security policy is now covered by 90-day onboarding checklist. Tool for onboarding changed.

3.4 Verbal Process Description

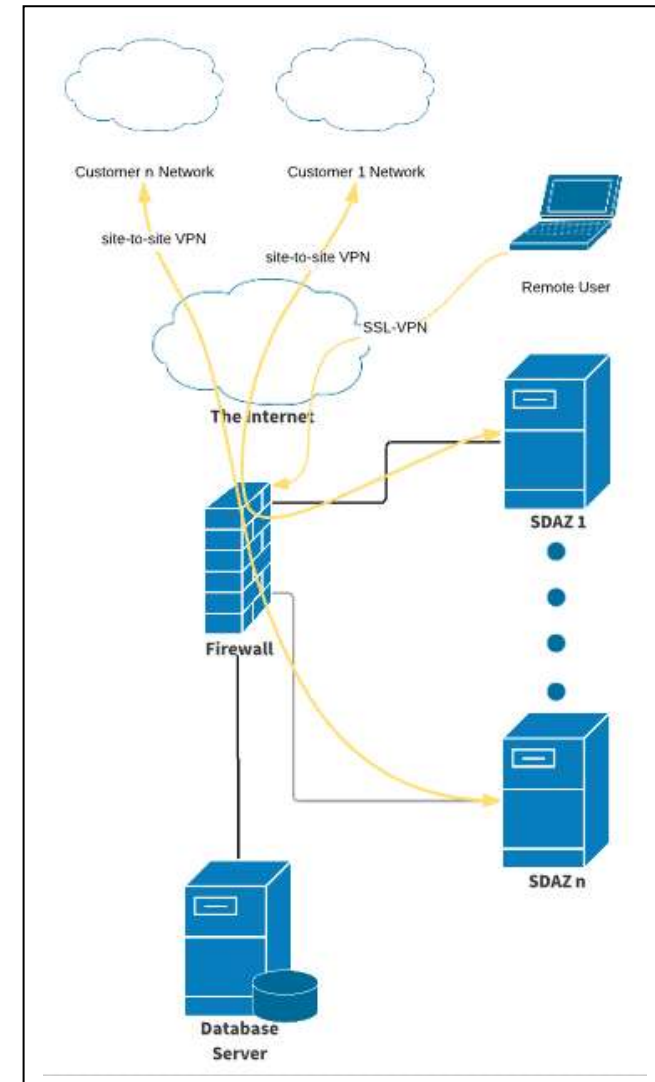
3.4.1 System Architecture SDAZ

The system architecture is represented by a network and servers, secured by firewalls. The devices from the customer are connected via a configured site-to-site VPN tunnel connection to the SDAZ server. Only necessary ports are allowed on the firewall to access the SDAZ server.

Each SDAZ hosts the required applications and has its own network/VLAN, which separates the server from other servers. The corresponding database(s) are on dedicated database servers in a different network/VLAN.

The customer gains access only through the configured site-to-site VPN tunnel or a personalized two-factor SSL-VPN authentication

SKIDATA technicians obtain access through the core firewall. Accessing the system is secured by the usage of personalized user credentials on the servers and personalized two-factor SSL-VPN authentication on the firewalls.



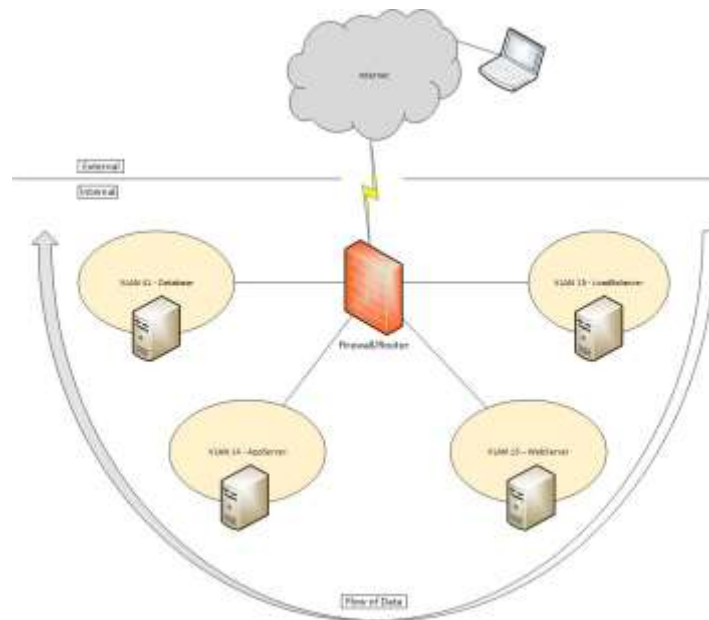
3.4.2 System Architecture DTA

In the environment of DTA every single component of the hosted stack is connected to each other via a firewall. After a request for the system passed the firewall, it is presented to a load balancer, which is then distributing the request to a webserver.

The webserver then passes the request via another firewall layer to the respective application server. The data needed for handling the application server is requested from the database via another firewall layer.

All parts of the service are at least N+1 redundant. This means that the failure of any one component will not result in any service degradation.

DTA provides cloud-based sales and access system functionality within a SKIDATA access system which is built from components described in 2.1.2.



3.4.3 Acquisition and Maintenance of Technology Infrastructure

Procurement of IT resources (hardware and software) follows the standard company procedures. Authorization is regulated by defined signatory powers and updated yearly. (AI_05a)

The Acquisition and Maintenance of Technology infrastructure is approved according rules displayed in the signatory powers document and provides the stability for the business. (AI_05b)

The deployment of new servers (physical or virtual server) is documented in a related deployment ticket. This ticket contains information about the purpose of the server and assures that necessary follow-up steps are taken care of. (AI_03a)

Network devices are listed with the currently installed firmware versions. The list is regularly compared against the latest available versions. If a new version is available, a decision is taken whether to update to the new firmware version. (AI_03b)

A server update plan is maintained to address the issue of different update cycles for different classes of servers. The update plan contains a list of server categories and the frequency in which OS updates are applied to them. (AI_03c)

OS updates are applied to servers according to the frequencies defined in the update plan (AI_03d).

3.4.4 Incident & Problem Management

The customer support at SKIDATA is managed in a two-layer approach – the incident management and the problem management.

Incident management is performed by the local market organizations. The service technician of the local market organization is the first contact point for the customer in the case of both hardware and software related incidents occurred. The objective of incident management is to restore any impaired or failed functionality reported by the customer as soon as possible. Central technical support is engaged in the incident process if special expertise is required. The removal of the root cause is subordinated for the incident management. A workaround establishing the service from the user perspective is a valid option for the resolution of the incident.

Problem management is performed centrally by the central technical support at the SKIDATA headquarters. The engineers at the central technical support have advanced knowledge and great experience with the SKIDATA products. The problem management supports the incident management by analyzing the root cause of incidents and their resolution. Problem management submits recognized product deficiencies to the development department for correction by creating a *Defect* ticket in JIRA.

JIRA supports the processes incident management, problem management, product creation, documentation and product release procedure within SKIDATA.

The following part is dedicated to the process of the handling of customer issues related to software. In the case an incident is reported to the local market organization, the service technician captures the incident in JIRA and creates a fault record. This entry requires certain mandatory fields (DS_o8a) as well as prioritizing the fault record. If the service technician is able to restore the functionality, the fault record will be closed. In the case a resolution cannot be achieved, the service technician will forward the fault record to the central technical support at the headquarters.

Technicians at central technical support review the prioritization. If the engineer does not agree with it, the service technician will be contacted in order to find a common prioritization. Problem management analyzing the incident tries to provide a temporary or permanent resolution for the issue which is documented in the related JIRA fault record.

Incidents which cannot be permanently resolved by problem management are transferred to a change request for development tracked as JIRA defect issue. Problems pending for resolution by a software change are linked to the related defect issue. Consistent linking between problem records (Fault records) and change requests (Defect records) is verified regularly. (DS_o8d)

Central technical support processes reported incidents according to defined priority. An OLA document defines priorities and response times. The OLA document is reviewed and approved by the head of CTS on yearly basis. (DS_o8f). Performance with respect to defined OLA is displayed in JIRA dashboards, tracked by responsible persons and in a bi-weekly status meeting. (DS_o8d)

3.4.5 Product Creation Process Software

In the product creation process, changes are triggered either from defects, which are forwarded by the central technical support unit, or feature requests, which are handed over by Product Line Management.

The product creation process is adjusted to the nature of the product. DTA is a SAAS product only, hosted by SKIDATA, delivering access and sales services to multiple customers from a single instance. Freemotion.Logic, Summit.Logic and SDRDM are on-premise software products. Hosting of SDAZ (part of Summit.Logic/Freemotion.Logic functionality) is provided to customers. However, basic principles are shared in the development process.

For new releases (except hotfixes) a test plan is generated which defines the testing tasks to be performed before releasing the software to production. (AI_o2a)

Each change (feature, defect, user story, bug) is recorded and tracked with JIRA. A testing task related to the change is created for each change record. The testing task has to be closed before the change is released. The release number is identified with the change record. (AI_o6c, AI_o6d).

Testing is performed by a specialized testing department (Quality Assurance). All changes (excluding hotfixes) are tested in a defined QA test environment. (Hotfixes often address issues only emerging within very specific configurations.) (AI_o7b)

Prior to the release, regression tests are conducted in order to ensure a high level of quality. Thereby, not just the single bug-fix or feature is tested but the entire software where the latest changes are implemented. The quality engineer thus runs the software in a test environment and verifies whether the major functionalities are working.

On-premise software is released/ published at the product repository after formal release notification from Quality Assurance. (AI_o7d)

SSAS Software (DTA) is deployed at the production server only after formal release notification from Quality Assurance. (AI_o7c)

3.4.6 Product Release Process

The objective of the release process is to control the release of SKIDATA branded products. The release process is intended to ensure that (a) SKIDATA products fulfill customer requirements, (b) SKIDATA can provide suitable support for installation and operation of the products, and (c) production delivers products with continuously high quality.

A rough release schedule for versions and service packs is defined by the product management. (AI_07a) When a product release is planned, the head of Quality Assurance defines the release criteria for the product release subject to the consent of Product Line Management and Software Development. The release criteria are defined in a check sheet based on a template. A quality test plan is generated for major releases and service packs. (AI_02a).

The sales department provides a document about new functionality within a major release. The document set contains prepared presentation material (PowerPoint) and pdf documentation (Release Highlights), which can be used as hand-out to customers. (AI_04g)

The head of Quality Assurance verifies the new version or service packs against the predefined release criteria. If the release criteria are met the head of product quality management approves the new version or the service packs with a signature on the previously prepared release notes. A notification about the release is sent to stakeholders of SKIDATA. (AI_04d-f)

The release notes provide documentation and knowhow transfer on changes (features and defects) implemented with the release as well as information on known deficiencies. The document is based on issues tracked in JIRA. (AI_04a-c)

3.4.7 Hotfix and Patch Procedure

Change procedures for defects and features are defined and documented. Those procedures are reviewed if they are up to date and accordingly approved. Changes of the procedures are traceably documented in a document management system. The latest version is available on the intranet. (PO_08a)

A patch is a fix for a hosted system. Since the change affects all customers immediately after deployment test requirements are higher than with on-premise software. For a patch, in addition to the testing tasks specific for the resolved issue, an automated regression test has to be passed. (AI_06d)

The objective of the hotfix procedure is to provide an accelerated approach to recover the customers' system. A hotfix is therefore processed with priority in central technical support, Quality Assurance and Software Development. If an incident at the customer's site shows a major impact on the operation, the service technician will call for a hotfix at the central technical support. The service technician therefore prioritizes the fault record accordingly and additionally ticks off the checkbox for hotfixes in JIRA. The activation of this checkbox triggers an accelerated recovery process. The engineer at the central technical support reviews the request for a hotfix according to its justification. (AI_06a) If the incident cannot be solved by the engineer at the central technical support, the fault record is forwarded to the product creation process. The process for hotfixes deviates in two points from the standard product creation process: (a) The defect is a preferred process and (b) the verification of the hotfix is carried out by the engineer at the central technical support. The engineer approves the hotfix through a signature on the hotfix notes of the respective hotfix (AI6_e) and sends it to the service technician for the reason of system recovery. Each hotfix is documented by hotfix notes. If hotfixes shall be made available for other customers, the hotfix and the related hotfix note is published at the product repository. (AI_06b)

3.4.8 Definition and Management of Service Levels

The contract, which is concluded with each new customer, comprises the sales contract, the hosted service agreement and the fact sheet about the product/service. The sales contract and the hosted service agreement are templates which are administrated by and available from the legal department. The fact sheets are available in the repository on the intranet and are administrated by the respective sales support organization. Service levels are stated in the hosted service agreement and further specified on the fact sheet for group-wide valid service levels such as system availability and backup procedure. (DS_01a) The template for the sales contract covers the most critical areas:

- Service availability
- Support time
- Response time

On an annual basis, the contract template is reviewed according to validity and subsequently approved by the legal department and the Central Hosting department. Changes to the contract template are marked and recorded in a traceable manner. (DS_01b)

Actual support and response times are defined according to selected service packages depending on customer requirements. These service levels are defined by the local service organization since they deliver these services.

With third-party suppliers maintenance agreements are in place to minimize downtimes with critical failures. Once a year, the list of maintenance agreements is reviewed for correctness and completeness. During the review, decisions are made whether a piece of hardware needs a maintenance agreement and if yes, what kind of support is most appropriate. (DS_2a)

3.4.9 System Security

The SKIDATA office security standards are defined in the IS policy which is available on the intranet for all SKIDATA employees. It is reviewed and approved by the head of IT infrastructure on an annual basis. (PO_06a) New employees are informed about the IT Security Rule and they have to perform and acknowledge a related online training. (PO_07a)

Based on a signed contract of employment, HR sets up an entry checklist in a web based tool. The checklist contains all the tasks necessary to set up the employee's working environment such as a workstation, IT access rights, etc. Based on this checklist, the IT infrastructure department sets up a user account (DS_05h). The respective department head grants specific access rights based on the employee's function.

If employees are leaving the company HR/Payroll invokes a workflow which triggers various tasks to be performed within the SKIDATA transition. To the IT department a task is assigned to disable the user account at the defined exit date. For employees with limited engagement the exit date is defined already with the entry checklist. (PO_07c)

The computer center network (SDAZ) is physically separated from the SKIDATA operational network (SDNET) and is in an external location. System access by privileged user accounts on the mountain servers is restricted and reviewed for validity. (DS5_e) Connections/access to the SDNET network and internet are managed and controlled by firewalls.

Access to SDAZ can be gained via SSL-VPN with two-factor authentication from external locations or via site-to-site VPN. All users need an account in the SDNET active directory and assigned permissions to access the server. SKIDATA employees need a valid token from the IT department.

In the case of SDAZ, the additional user accounts on the SDAZ are approved and set up by Central Hosting. In the case of termination of employment, SDNET, SDAZ and Summit.Logic access permissions are deactivated and in the case of department changes Summit.Logic access permissions are adapted.

Based on the sales contract, the SKIDATA application engineer sets up a unique limited OS user account for the respective SDAZ and a privileged user account on Summit.Logic for each ski pool member. Additionally, the SKIDATA application engineer sets up Summit.Logic user accounts where requested in writing by the ski pool member. (DS_05k) The application engineer deactivates user accounts on Summit.Logic where requested in writing by the ski pool member. With these privileged Summit.Logic user accounts, the ski pool members administer their own application and user accounts. Closing the management application screen immediately results in logoff from the server. This setting cannot be modified by the customer.

The following user groups generally have access to SDAZ with regard to Summit.Logic:

- Application engineers (SKIDATA employee)
The application engineers are responsible for the configuration of the Summit.Logic application according to ski pool member requirements. The application engineers have privileged access rights.
- Central hosting engineers (SKIDATA employee)
Central hosting engineers have privileged user accounts on every infrastructure device in this environment. These users are the architects and operators of the server system and have the highest level of access privileges. They are responsible for the server, infrastructure devices and firewall configurations.
- Service technicians (SKIDATA employee)
The service technicians are responsible for the Summit.Logic configuration. They have privileged user accounts on the SDAZ servers and are responsible for configuration, maintenance and support of the SKIDATA Summit.Logic application.
- Ski pool members (Non-SKIDATA)
The ski pool member is the customer. He gains access to the system via a VPN tunnel between the customer's local network and the

SKIDATA core firewall. He has a limited user account on the SDAZ server to which his ski resort belongs and can start the Summit.Logic management application with a privileged user account for configuration purposes.

- Pool clearing engineers (SKIDATA employee)
The pool clearing engineer is responsible for the pool clearing process. He has a privileged user account on the SDAZ server and the DB server.

3.4.10 Management of the Configuration

A hardware inventory of all equipment in our data center is maintained. Each piece of hardware is documented and identified by serial number (when possible). When hardware is added or removed, the documentation has to be updated. (DS_09a)

Changes of application software are tracked within the hosting departments ticketing system. Important information about the update is documented within the ticket. (DS_09b)

Security hardening baselines are maintained for Windows and Linux servers. An annual review is conducted to review changes to the baseline and to assure conformity with security industry best practices. (DS_09c)

Baselines defined in the security hardening baseline document are applied for Windows and Linux servers. Compliance of servers with the hardening baseline is checked regularly. The result is a report with comments and mitigation efforts of potential non-compliance via tickets. (DS_09d)

3.4.11 Management of Data and Backups

A backup strategy plan is maintained for different categories of servers. A strategy contains parameters like backup interval, retention time and backup type. The strategy plan also contains a guideline on how to identify a successful backup report. (DS_11a)

Daily backup summaries tickets are created by our backup software. Central Hosting personnel checks the summaries for irregularities and inconsistencies. The criteria for successful summaries are defined in the backup strategy plan. (DS_11b).

Central Hosting's backup systems are set up in a way that they allow various restore methods. Restore tests are done regularly in order to guarantee operational capability of backups. This is done by testing various restore scenarios like VM restore, database schema restore and single file restore. If restore tests fail, the reason will be investigated and corrections will be made. Details are being documented in the ticket. (DS_11c)

3.4.12 Management of Physical Access

Access to the shared data center is controlled by our suppliers and covered by the ISO 27001 certificate provided.

Individual racks at the third-party server housing are secured with door alerts. Whenever a rack door is opened, an SMS alert is generated and sent to the Central Hosting member who is on call duty. Once a year, a test of all rack door alerts is conducted. The test is documented and approved. (DS_12a)

The access to individual server racks at the third-party server housing is secured by additional rack locks to guarantee access only for Central Hosting employees and persons cleared by Central Hosting. The list of users with rack access is reviewed regularly. (DS_12b)

3.4.13 Enable and Manage Operations

Central Hosting monitors all their networked assets 24/7 for critical indicators like availability and resource utilization. The deployment ticket from control AI_03a is the trigger to configure a new target in the monitoring system. (DS_13a)

Central Hosting monitors its infrastructure usage (memory, CPU, storage) on a daily basis. To assure availability and redundancy of resources, the capacity of the infrastructure is reviewed yearly. Investment decisions are based on this review. (DS_13b)

To assure availability of individual services, all services are monitored via the monitoring system on a five-minute basis. The achieved SLAs are being reviewed every month and reported to Operations (DS_13c).

3.4.14 Monitor and Evaluate Internal Control

Internal controls for IT are observed by delegates (management or specialists) from multiple departments monitoring and evaluating processes and effectiveness of controls. In regular team meetings the status and potential improvement actions are elaborated. (ME_o2a), (ME_o2b)

Remedial actions are identified, initiated and implemented for issues raised by external auditors. (ME_o2c)

3.5 User Control Considerations

The processing of transactions performed by SKIDATA for clients and the controls at SKIDATA cover only a part of the overall client internal control of the SDAZ and DTA at SKIDATA. Concerning the control objectives of the processing, it is not reasonable to focus solely on the control activities of SKIDATA. Each client's internal organization controls must be evaluated in conjunction with the controls of the company and the testing that are summarized in section 4 (information provided by the independent service auditor section of this report).

This section highlights some of those control responsibilities that SKIDATA believes should be carried out by each client's organization. It is the customer's responsibility to evaluate its own internal controls with regard to the controls given below. Furthermore, the following list of controls is intended to address only those controls related to the interface and communication between each user organization and SKIDATA. Accordingly, this list does not purport to be and is not a complete listing of the controls that provide a basis for the assertions underlying the financial statements of client organizations.

The client is responsible for ensuring that:

- Only authorized client personnel can execute critical functions and appropriate segregation of duties is implemented.
 - Only authorized client personnel can submit configuration changes to Summit.Logic and SDAZ as well as the respective network components such as firewalls.
 - Only authorized client personnel can submit change requests.
 - An appropriate review of clearing data is provided by SKIDATA with regard to accuracy and completeness.
 - Events that may affect operations are reported to SKIDATA in a timely, comprehensive manner.
 - Administration of the user accounts for the employees of the client.
 - Evaluate if the scope (systems) of the report is appropriate to derive an overall conclusion for the intended use.
-
- Appropriate logical access is provided to servers, routers and other network components that are not under the control of SKIDATA personnel.
 - Appropriate system security and user account management are provided on Summit.Logic.
 - Appropriate physical security and environmental controls are provided at the client's facility.

4 Information Provided by the Independent Service Auditor

4.1 Control Objectives, Related Controls and PwC's Tests of Operating Effectiveness

This section has been prepared by SKIDATA to identify the control objectives related to SKIDATA's system of IT general controls for the solutions SDAZ and DTA provided at the housing centers of its contractor in Wels, Austria. In addition, management has identified those activities in place that have been designed to satisfy these objectives.

This report, when combined with an understanding of the internal controls in place at user organizations, is intended to assist in an evaluation of the total control environment of SKIDATA customers.

These control objectives do not encompass all aspects of the services provided or procedures followed by SKIDATA. Tests of controls were not extended to procedures in effect at customer locations or other control procedures that may be described in section 2, but not listed in the matrix of section 3.

This description of controls has been examined and tested by PwC in accordance with the International Standard on Assurance Engagements 3402, "Assurance reports on controls at a service organization", issued by the International Auditing and Assurance Standards Board, which provides guidance for an auditor who issues reports on the processing of transactions for a service organization. It is each interested party's responsibility to evaluate this information in relation to the internal controls in place at each customer location in order to assess control risk. If an effective customer internal control structure is not in place, SKIDATA's internal controls may not compensate for such weaknesses.

Each control objective stated is followed by the corresponding control activities that have been established by SKIDATA. Following the description of the control activities, a summary of tests performed by PwC is provided to determine whether the controls in place operated effectively during the period November 1, 2019 to April 30, 2020.

SKIDATA uses a subservice organization for the data center in Wels, Austria, where its IT infrastructure components are housed. The description on pages 15 to 60 includes only the controls and related control objectives of SKIDATA and excludes the control objectives and related controls of the subservice organization. Our examination did not extend to controls of the subservice organization (use of carve-out method).

Test of Controls

Tests of operating effectiveness of SKIDATA's controls included such tests as were considered necessary to evaluate whether those internal controls were in place and the extent of compliance with those controls.

Tests performed of the operational effectiveness of controls detailed in the matrix are described below:

Inquiry	Making inquiries with appropriate SKIDATA personnel to obtain: – Understanding and additional information regarding control – Corroborating evidence of the control
Observation	Viewing the application or existence of specified controls.
Inspection	Examining documents and records indicating performance of the control. Includes among other things: – Inspection of source documentation and authorizations to verify propriety of transactions processed – Inspection of documents or records for evidence of performance, such as existence of initials and signatures – Inspection of company documentation, such as procedure manuals – Inspection of system configuration
Reperformance	Repeating control activities as they have been performed by SKIDATA and comparing results.

4.1.1 System / Controls Overview

Controls		Affected systems		
Control ID	Control Name	SDAZ	DTA	SDRDM
PO_06a	Guideline for general IT security	✓	✓	✓
PO_07a	Implementation of general IT security	✓	✓	✓
PO_07c	Job termination	✓	✓	✓
PO_08_a	Software process	✓	✓	✓
AI_02a	Quality test plan	✓	✓	✓
AI_03a	Server deployment	✓	✓	
AI_03b	Network device updates	✓	✓	
AI_03c	Server update plan	✓	✓	
AI_03d	Server update execution	✓	✓	
AI_04a	Document release content - DTA	✓		
AI_04b	Document release content - SDAZ		✓	
AI_04c	Document release content - SDRDM			✓
AI_04d	Inform stakeholders - DTA	✓		
AI_04e	Inform stakeholders - SDAZ		✓	
AI_04f	Inform stakeholders - SDRDM			✓
AI_04g	Inform customer on new functionality		✓	
AI_05a	Authorization & Signatory Powers	✓	✓	
AI_05b	Approval of infrastructure acquisition	✓	✓	
AI_06a	Hotfix - Authorization, change & testing		✓	✓
AI_06b	Release of hotfixes		✓	✓
AI_06c	JIRA handling - SDAZ		✓	✓
AI_06d	JIRA handling - DTA	✓		
AI_07a	Release planning		✓	✓
AI_07b	Test environment	✓	✓	✓
AI_07c	Release of SAAS	✓		
AI_07d	Release of on-premise software		✓	✓
DS_01a	Hosted service agreement available	✓	✓	
DS_01b	Hosted service agreement review	✓	✓	

Controls		Affected systems		
Control ID	Control Name	SDAZ	DTA	SDRDM
DS_02a	Maintenance agreements	✓	✓	
DS_05d	Firewall changes	✓	✓	
DS_05e	Firewall review	✓	✓	
DS_05h	Manage access permission to IT resources	✓	✓	
DS_05i	User account requests	✓	✓	
DS_05k	User account reviews	✓	✓	
DS_05o	External penetration tests	✓		
DS_08a	Service desk -Assurance that incidents are tracked, resolved and escalated in a defined manner	✓	✓	✓
DS_08b	Service desk - Show that recorded incidents are handled within the OLA	✓	✓	✓
DS_08d	Service desk - Assure that issues forwarded to 3rd level are linked within ticketing system	✓	✓	✓
DS_08e	Hosting - Incident management	✓	✓	
DS_08f	Service desk - Priorities for incident handling and lead time are defined	✓	✓	✓
DS_09a	Inventory management	✓	✓	
DS_09b	Application updates	✓		
DS_09c	Maintenance of security baseline	✓	✓	
DS_09d	Implementation of security baseline	✓	✓	
DS_11a	Backup strategy plan	✓	✓	
DS_11b	Backup job reviews	✓	✓	
DS_11e	Restore tests	✓	✓	
DS_12a	Rack door alerts	✓	✓	
DS_12b	Rack access control	✓	✓	
DS_13a	Infrastructure monitoring review	✓	✓	
DS_13b	Provide required resources	✓	✓	
DS_13c	Monitor SLAs	✓	✓	
ME_02a	Continuous monitoring of controls	✓	✓	
ME_02b	Monitoring of periodical checks	✓	✓	
ME_02c	Measures on exception noted in external audit	✓	✓	

4.1.2 Acquire and Maintain Technology Software

Control Objective by SKIDATA: Controls provide reasonable assurance that changes to software and systems in the production environment are properly authorized, tested, documented, released, implemented and segregation of duties is adhered to.

Control ID	Control Description by SKIDATA	Automation Category	Frequency	Tests Performed by PwC	Results of Testing
AI2_a	The test plan (which includes test cases with expected results) must exist for each release and service pack. Hotfixes are excluded.	IT-dependent manual	Event-driven	Inquiry and Inspection Inquiry of the control owner and inspected the test plan for new releases and service pack.	No exceptions noted

4.1.3 Acquire and Maintain Technology Infrastructure

Control Objective by SKIDATA: Controls provide reasonable assurance that infrastructure acquisitions are approved and provide the security and stability required by business.

Control ID	Control Description by SKIDATA	Automation Category	Frequency	Tests Performed by PwC	Results of Testing
AI3_a	A list of all new deployments is regularly reviewed to assure that deployment tickets exist.	IT-dependent manual	Annually	Inquiry and Inspection Inquiry of the control owner and inspected the new deployments and the corresponding tickets.	No exceptions noted
AI3_b	A list of all network devices and installed firmware versions is created and compared to the latest available firmware version.	IT-dependent manual	Annually	Inquiry and Inspection Inquiry of the control owner and inspected firmware states of the network infrastructure devices for DTA and SDAZ and the corresponding documentation of the firmware check. Selected a sample of devices to see if the documented firmware version is installed.	No exceptions noted
AI3_c	The update plan is annually reviewed and approved.	IT-dependent manual	Annually	Inquiry and Inspection Inquiry of the control owner and inspected the reviewed update plan and the corresponding ticket.	No exceptions noted
AI3_d	A Nessus patch report is generated after each update session. The reports are reviewed monthly to check if any patches have been left out and if the frequency matches the update plan.	IT-dependent manual	Monthly	Inquiry and Inspection Inquiry of the control owner and inspected a sample of the Nessus patch reports and the corresponding tickets.	No exceptions noted

4.1.4 Enable Operation and Use

Control Objective by SKIDATA: Controls provide reasonable assurance that knowledge about new software which is necessary for successful support is transferred.

Control ID	Control Description by SKIDATA	Automation Category	Frequency	Tests Performed by PwC	Results of Testing
AI4_a	Check timely availability of release documentation (release notes / hotfix notes). DTA	IT-dependent manual	Event-driven	Inquiry and Inspection Inquiry of the control owner and inspected a sample of the documentation for the new DTA releases.	No exceptions noted
AI4_b	Check timely availability of release documentation (release notes / hotfix notes). SDAZ	IT-dependent manual	Event-driven	Inquiry and Inspection Inquiry of the control owner and inspected a sample of the documentation for the new SDAZ releases.	No exceptions noted
AI4_c	Check timely availability of release documentation (release notes / hotfix notes). SDRDM	IT-dependent manual	Event-driven	Inquiry and Inspection Inquiry of the control owner and inspected a sample of the documentation for the new SDRDM releases.	No exceptions noted
AI4_d	Check availability and date of "release" email to stakeholders before release is deployed on production system. DTA	IT-dependent manual	Event-driven	Inquiry and Inspection Inquiry of the control owner and inspected a sample of new DTA releases and noted that the stakeholders were informed before the release was deployed.	No exceptions noted
AI4_e	Check availability and date of "release" email to stakeholders before release (excluding hotfixes) is published on repository. SDAZ	IT-dependent manual	Event-driven	Inquiry and Inspection Inquiry of the control owner and inspected a sample of new SDAZ releases to ensure that the stakeholders were informed before the release was deployed.	No exceptions noted

Control ID	Control Description by SKIDATA	Automation Category	Frequency	Tests Performed by PwC	Results of Testing
AI4_f	Check availability and date of "release" email to stakeholders before release (excluding hotfixes) is published on repository. SDRDM	IT-dependent manual	Event-driven	Inquiry and Inspection Inquiry of the control owner and inspected the new SDRDM releases to ensure that the stakeholders were informed before the release was deployed.	No exceptions noted
AI4_g	Verify that documentation for customer about new functionality (Release Highlights) is published on intranet.	IT-dependent manual	Event-driven	Inquiry Inquiry of the control owner and noted that there was no new release during the period under review.	No testing

4.1.5 Procure IT Resources

Control Objective by SKIDATA: Controls provide reasonable assurance that the procurement processes are handled in a structured and well-organized form and that a professional ERP solution is used for the acquisition of products.

Control ID	Control Description by SKIDATA	Automation Category	Frequency	Tests Performed by PwC	Results of Testing
AI5_a	Check annual approval of rule ASP (Authorization & Signatory Powers)	IT-dependent manual	Annually	Inquiry and Inspection Inquiry of the control owner and inspected the approved ASP policy.	No exceptions noted
AI5_b	For all demands requested by employees of the hosting department (identified by cost center) it is verified if the acquisition has been approved according to the approval matrix.	IT-dependent manual	Event-driven	Inquiry and Inspection Inquiry of the control owner and inspected a sample of the acquisition according to the approval matrix.	No exceptions noted

4.1.6 Manage Changes

Control Objective by SKIDATA: Controls provide reasonable assurance that changes to existing system software and hardware are authorized, tested, approved, properly implemented, and documented.

Control ID	Control Description by SKIDATA	Automation Category	Frequency	Tests Performed by PwC	Results of Testing
AI6_a	Hotfixes are requested in a separate field by technical support. A verification task is created/verified and closed. The field "hotfix" available in the HF version is updated by Development.	IT-dependent manual	Event-driven	Inquiry and Inspection Inquiry of the control owner and inspected a sample of requested hotfixes, their verification and the corresponding tickets.	No exceptions noted
AI6_b	Check availability of hotfix release document (hotfix notes) for each published hotfix. The approval date is to be before/equal to the availability date on server.	IT-dependent manual	Event-driven	Inquiry and Inspection Inquiry of the control owner and inspected a sample of hotfixes whether the approval date is before/equal to the availability date.	No exceptions noted
AI6_c	A verification task for defects needs to exist. A testing task for features needs to exist. A fixversion needs to be set.	IT-dependent manual	Event-driven	Inquiry and Inspection Inquiry of the control owner and inspected a sample of defects if the verification task and test task is documented and completed in a corresponding JIRA ticket and a fixversion is set.	No exceptions noted
AI6_d	A testing task for each standard issue type (e.g. user story, bug) needs to exist. The fixversion(s) in the standard issue type need(s) to be set. The testing task and the standard issue type need to be "closed".	IT-dependent manual	Event-driven	Inquiry and Inspection Inquiry of the control owner and inspected a sample auf tickets if a test task exists and the standard issue type is released and "closed".	No exceptions noted

4.1.7 Install and Accredited Solutions and Changes

Control Objective by SKIDATA: Control provide reasonable assurance that changes are properly tested before and after implementation in the live system, and a test environment has been established that allows systematic tests for changes.

Control ID	Control Description by SKIDATA	Automation Category	Frequency	Tests Performed by PwC	Results of Testing
AI7_a	Verify that the release plan for Summit.Logic is published on the PMO intranet site.	IT-dependent manual	Annually	Inquiry and Inspection Inquiry of the control owner and inspected the that the release plan of Summit.Logic is published on the PMO intranet site.	No exceptions noted
AI7_b	A QA environment needs to exist where SW changes can be verified before they are released.	IT-dependent manual	Event-driven	Inquiry and Inspection Inquiry of the control owner and inspected the existence of QA environment for testing and verifying SW changes.	No exceptions noted
AI7_c	For each deployment of DTA which is tracked by the hosting team release notes have to be available with an approval date before the deployment date.	IT-dependent manual	Event-driven	Inquiry and Inspection Inquiry of the control owner and inspected a sample of DTA deployments.	No exceptions noted
AI7_d	SDAZ Software (Summit.Logic) is provided on repository only after release notes have been published by QA.	IT-dependent manual	Event-driven	Inquiry and Inspection Inquiry of the control owner and inspected a sample of published release notes.	No exceptions noted

4.1.8 Define and Manage Service Levels

Control Objective by SKIDATA: Controls provide reasonable assurance that service level agreements, which formalize the performance criteria, are established.

Control ID	Control Description by SKIDATA	Automation Category	Frequency	Tests Performed by PwC	Results of Testing
DS1_a	It is verified that required documents are available on the intranet, consisting of the hosted service agreement and fact sheets for the hosted service.	IT-dependent manual	Event-driven	Inquiry and Inspection Inquiry of the control owner and inspected the availability of the hosted service agreement and fact sheets on the intranet.	No exceptions noted
DS1_b	Each year a review takes place whether the hosted service agreements template has to be adjusted. If updates are required, it is checked whether the related documents have been updated and published on the intranet.	IT-dependent manual	Annually	Inquiry and Inspection Inquiry of the control owner and inspected the approval of hosted service agreements templates by the legal department. Inspected if changes have been documented and approved.	No exceptions noted

4.1.9 Manage Third-party Services

Control Objective by SKIDATA: Controls provide reasonable assurance that services provided by third parties are managed in a professional way.

Control ID	Control Description by SKIDATA	Automation Category	Frequency	Tests Performed by PwC	Results of Testing
DS2_a	Once a year, the list of maintenance agreements is reviewed for correctness and completeness. The basis of this review is the hardware inventory carried out in DS9_a. During the review, decisions are made whether a piece of hardware needs a maintenance agreement and if yes, what kind of maintenance is most appropriate.	IT-dependent manual	Annually	Inquiry and Inspection Inquiry of the control owner and inspected the maintenance agreement review documentation and if follow-up steps have been taken.	No exceptions noted

4.1.10 Ensure Systems Security

Control Objective by SKIDATA: Controls provide reasonable assurance that access to operating system, Freemotion.Logic and network infrastructure devices is appropriately restricted to authorized users.

Control ID	Control Description by SKIDATA	Automation Category	Frequency	Tests Performed by PwC	Results of Testing
DS5_d	The list of firewall tickets is reviewed monthly for consistency.	IT-dependent manual	Monthly	Inquiry and Inspection Inquiry of the control owner and inspected a sample of monthly reviews and the corresponding tickets.	No exceptions noted
DS5_e	Once a year, all firewall rules are being reviewed and discussed in a review meeting by the relevant parties. Unnecessary or obsolete rules will be removed, as well as rule simplifications will be carried out. The result of the review is a ticket that includes all proposed changes. This ticket needs to be reviewed and approved.	IT-dependent manual	Annually	Inquiry and Inspection Inquiry of the control owner and inspected the reviews of all firewall rules and the corresponding tickets.	No exceptions noted
DS5_h	For each new employee an entry checklist has to be available. Within the checklist the access permissions have to be defined by the superior. Permissions to hosting environment are subject to further control DS5_i.	IT-dependent manual	Event-driven	Inquiry and Inspection Inquiry of the control owner and inspected the checklists from the superiors for a sample of new employees.	No exceptions noted
DS5_i	The list of user request tickets is reviewed monthly for consistency.	IT-dependent manual	Monthly	Inquiry and Inspection Inquiry of the control owner and inspected a sample of monthly reviews and the corresponding tickets.	No exceptions noted

Control ID	Control Description by SKIDATA	Automation Category	Frequency	Tests Performed by PwC	Results of Testing
DS5_k	A review of all operating system users is performed regularly. All users and their permissions are checked for validity and rationality. Users that are obviously obsolete are deactivated. Irregularities in permissions are discussed with the users and/or their superiors. The result of the review is a ticket that includes all proposed changes. This ticket needs to be approved.	IT-dependent manual	Annually	Inquiry and Inspection Inquiry of the control owner and inspected the user reviews of all OS, the corresponding tickets and their approval for changes.	No exceptions noted
DS5_o	The results of the pentest are evaluated together with Development and architects and actions are derived and planned for.	IT-dependent manual	Annually	Inquiry and Inspection Inquiry of the control owner and inspected the evaluation of the pentest and the corresponding tickets for changes if needed.	No exceptions noted

4.1.11 Manage Service Desk and Incidents

Control Objective by SKIDATA: Controls provide reasonable assurance that incidents are tracked, resolved and escalated in a timely manner.

Control ID	Control Description by SKIDATA	Automation Category	Frequency	Tests Performed by PwC	Results of Testing
DS8_a	Show that mandatory fields must be filled to be able to forward the issue to CTS.	IT-dependent manual	Annually	Inquiry and Inspection Inquiry of the control owner and inspected the purpose of mandatory fields in JIRA tool for forwarding the issues to CTS.	No exceptions noted
DS8_b	Responsible person checks via dashboard problem management that issues are answered within a defined period. (OLA)	IT-dependent manual	Bi-weekly	Inquiry and Inspection Inquiry of the control owner and inspected the tracking of issues in JIRA tool dashboard and the response time to it.	No exceptions noted
DS8_d	Responsible person checks via dashboard problem management that issues forwarded to R&D are linked with change request tool by R&D.	IT-dependent manual	Event-driven	Inquiry and Inspection Inquiry of the control owner and inspected the link of the tickets between issues forwarded to R&D and change request tool by R&D in JIRA tool dashboard.	No exceptions noted
DS8_e	All incident tickets at Hosting are regularly reviewed for irregularities, especially tickets that are older than 30 days and tickets that have not yet been assigned to a person.	IT-dependent manual	Monthly	Inquiry and Inspection Inquiry of the control owner and inspected a sample of monthly reports and the corresponding tickets.	No exceptions noted
DS8_f	Verify if OLA document has been approved within the last 12 months.	IT-dependent manual	Annually	Inquiry and Inspection Inquiry of the control owner and inspected the approval of OLA documents.	No exceptions noted

4.1.12 Manage the Configuration

Control Objective by SKIDATA: Controls provide reasonable assurance that adequate operating procedures are undertaken in order to ensure sound operations.

Control ID	Control Description by SKIDATA	Automation Category	Frequency	Tests Performed by PwC	Results of Testing
DS9_a	Once a year, the hardware inventory is reviewed by comparing the documentation with the actual data center. This review is documented in a ticket.	IT-dependent manual	Annually	Inquiry and Inspection Inquiry of the control owner and inspected the review of HW inventory and the corresponding ticket for it.	No exceptions noted
DS9_b	Check whether all DTA application updates are based on OTRS ticket.	IT-dependent manual	Monthly	Inquiry and Inspection Inquiry of the control owner and inspected a sample of monthly checks of DTA application updates and the corresponding OTRS tickets.	No exceptions noted
DS9_c	An annual review is conducted to review changes to the baseline and to assure conformity with security industry best practices.	IT-dependent manual	Annually	Inquiry and Inspection Inquiry of the control owner and inspected the review of the baseline to assure conformity with security industry best practices.	No exceptions noted
DS9_d	Compliance of servers with the hardening baseline is checked regularly. The result is a report with comments and mitigation efforts of potential non-compliance via tickets.	IT-dependent manual	Annually	Inquiry and Inspection Inquiry of the control owner and inspected the report and the corresponding tickets.	No exceptions noted

4.1.13 Manage Data

Control Objective by SKIDATA: Controls provide reasonable assurance that backups are performed reliably, accurately and completely in accordance with the established backup plan.

Control ID	Control Description by SKIDATA	Automation Category	Frequency	Tests Performed by PwC	Results of Testing
DS11_a	The backup strategy plan is reviewed for consistency and continuous improvement once a year.	IT-dependent manual	Annually	Inquiry and Inspection Inquiry of the control owner and inspected the backup plans (relevant for DTA and SDAZ) to ensure that reviewed backup procedures exist.	No exceptions noted
DS11_b	Once a month, all backup summary tickets are reviewed to check if any backup faults have been overlooked.	IT-dependent manual	Monthly	Inquiry and Inspection Inquiry of the control owner and inspected a sample of monthly reports and the corresponding tickets.	No exceptions noted
DS11_e	Restore tests are done regularly in order to guarantee operational capability of backups. This is done by testing various restore scenarios like VM restore, database schema restore and single file restore. If restore tests fail, the reason will be investigated and corrections will be made. Details are being documented in the ticket.	IT-dependent manual	Annually	Inquiry and Inspection Inquiry of the control owner and inspected the documentation of the annual restore tests and their corresponding tickets.	No exceptions noted

4.1.14 Manage the Physical Environment

Control Objective by SKIDATA: Controls provide reasonable assurance that physical access to the data center is appropriately restricted to authorized individuals.

Control ID	Control Description by SKIDATA	Automation Category	Frequency	Tests Performed by PwC	Results of Testing
DS12_a	Once a year, a test of all rack door alerts is conducted. The test is documented and approved.	IT-dependent manual	Annually	Inquiry and Inspection Inquiry of the control owner and inspected the documented test of the rack door alert and sent "Rack Door Alert SMS's".	No exceptions noted
DS12_b	The list of users with rack access is reviewed regularly.	IT-dependent manual	Annually	Inquiry and Inspection Inquiry of the control owner and inspected the reviewed list of users with rack access and the corresponding ticket for it.	No exceptions noted

4.1.15 Manage Operations

Control Objective by SKIDATA: Controls provide reasonable assurance that the provided infrastructure and services are available and work properly by performing appropriate monitoring and maintenance activities.

Control ID	Control Description by SKIDATA	Automation Category	Frequency	Tests Performed by PwC	Results of Testing
DS13_a	To assure that no asset is forgotten, an annual review is conducted. The list of known assets is compared to the list of assets configured in the monitoring system.	IT-dependent manual	Annually	Inquiry and Inspection Inquiry of the control owner and inspected the review of the list with known and configured assets.	No exceptions noted
DS13_b	To assure availability and redundancy of resources, the capacity of the infrastructure is reviewed yearly. Investment decisions are based on this review.	Manual	Annually	Inquiry and Inspection Inquiry of the control owner and inspected the availability and redundancy of resources, the capacity of infrastructure and investment decisions.	No exceptions noted
DS13_c	To assure availability of individual services, all services are monitored via the monitoring system on a five-minute basis. The achieved SLAs are being reviewed every month and reported to Operations.	Manual	Monthly	Inquiry and Inspection Inquiry of the control owner and inspected a sample of monthly reports and SLA reviews.	No exceptions noted

4.1.16 Monitor and Evaluate Internal Control

Control Objective by SKIDATA: Controls provide reasonable assurance that a process is established allowing the ICS to cover organizational and legal requirements and that the effectiveness of controls is monitored and acted upon.

Control ID	Control Description by SKIDATA	Automation Category	Frequency	Tests Performed by PwC	Results of Testing
ME2_a	Check that an ISAE core team meeting is held, following up on periodical checks, ISAE related process improvements and remedial actions from previous ISAE reports.	Manual	Annually	Inquiry and Inspection Inquiry of the control owner and inspected the checks related to improvements of the ISAE Audit.	No exceptions noted
ME2_b	Check availability and status of list for periodical tasks.	Manual	Annually	Inquiry and Inspection Inquiry of the control owner and inspected the availability and status of periodical tasks.	No exceptions noted
ME2_c	Deviations found by external auditor are noted within minutes of ISAE core team meeting and remedial actions are taken.	Manual	Annually	Inquiry and Inspection Inquiry of the control owner and inspected the documented meeting minutes relevant for the ISAE audit.	No exceptions noted

4.1.17 Communicate Management Aims and Directions

Control Objective by SKIDATA: Controls provide reasonable assurance that appropriate IT security measures are implemented and tested within the data center organization.

Control ID	Control Description by SKIDATA	Automation Category	Frequency	Tests Performed by PwC	Results of Testing
PO6_a	It is verified that the IT Security Rule is updated on a yearly basis. A new version on the intranet is the related evidence. Additionally it is verified that employees have been informed by checking availability of related newsletter.	Manual	Annually	Inquiry and Inspection Inquiry of the control owner and inspected the review of IT Security Rule and the email information for the employees.	No exceptions noted

4.1.18 Manage IT Human Resources

Control Objective by SKIDATA: Controls provide reasonable assurance that access to operating system, Freemotion.Logic and network infrastructure devices is appropriately restricted to authorized users.

Control ID	Control Description by SKIDATA	Automation Category	Frequency	Tests Performed by PwC	Results of Testing
PO7_a	For each new employee a track record / acknowledgment of the IT Security guideline on the learning platform is available. This report is checked regarding completeness.	IT-dependent manual	Monthly	Inquiry and Inspection Inquiry of the control owner and inspected the newsletter about the new IT Security Rule and its track record for completing it.	No exceptions noted
PO7_c	For each permanent employee leaving the company a workflow is to be executed which contains the tasks to disable his active directory account.	IT-dependent manual	Event-driven	Inquiry and Inspection Inquiry of the control owner and inspected a sample of employees that left the company.	No exceptions noted

4.1.19 Manage Quality

Control Objective by SKIDATA: Controls provide reasonable assurance that changes to software and systems in the production environment are properly authorized, tested, documented, released, implemented and segregation of duties is adhered to.

Control ID	Control Description by SKIDATA	Automation Category	Frequency	Tests Performed by PwC	Results of Testing
PO8_a	The SW development process documents must be available for R&D and must be reviewed once a year.	Manual	Annually	Inquiry and Inspection Inquiry of the control owner and inspected the review of the SW development process and its availability on the intranet.	No exceptions noted

Appendix

General Conditions of Contract for the Public Accounting Professions (AAB 2018)

Recommended for use by the Board of the Chamber of Tax Advisers and Auditors, last recommended in its decision of April 18, 2018

Preamble and General Items

(1) Contract within the meaning of these Conditions of Contract refers to each contract on services to be rendered by a person entitled to exercise profession in the field of public accounting exercising that profession (de facto activities as well as providing or performing legal transactions or acts, in each case pursuant to Sections 2 or 3 Austrian Public Accounting Professions Act (WTBG 2017). The parties to the contract shall hereinafter be referred to as the "contractor" on the one hand and the "client" on the other hand).

(2) The General Conditions of Contract for the professions in the field of public accounting are divided into two sections: The Conditions of Section I shall apply to contracts where the agreeing of contracts is part of the operations of the client's company (entrepreneur within the meaning of the Austrian Consumer Protection Act. They shall apply to consumer business under the Austrian Consumer Protection Act (Federal Act of March 8, 1979 / Federal Law Gazette No. 140 as amended) insofar as Section II does not provide otherwise for such business.

(3) In the event that an individual provision is void, the invalid provision shall be replaced by a valid provision that is as close as possible to the desired objective.

SECTION I

1. Scope and Execution of Contract

(1) The scope of the contract is generally determined in a written agreement drawn up between the client and the contractor. In the absence of such a detailed written agreement, (2)-(4) shall apply in case of doubt:

(2) When contracted to perform tax consultation services, consultation shall consist of the following activities:

a) preparing annual tax returns for income tax and corporate tax as well as value-added tax (VAT) on the basis of the financial statements and other documents and papers required for taxation purposes and to be submitted by the client or (if so agreed) prepared by the contractor. Unless explicitly agreed otherwise, documents and papers required for taxation purposes shall be produced by the client.

b) examining the tax assessment notices for the tax returns mentioned under a).

c) negotiating with the fiscal authorities in connection with the tax returns and notices mentioned under a) and b).

d) participating in external tax audits and assessing the results of external tax audits with regard to the taxes mentioned under a).

e) participating in appeal procedures with regard to the taxes mentioned under a).

If the contractor receives a flat fee for regular tax consultation, in the absence of written agreements to the contrary, the activities mentioned under d) and e) shall be invoiced separately.

(3) Provided the preparation of one or more annual tax return(s) is part of the contract accepted, this shall not include the examination of any particular accounting conditions nor the examination of whether all relevant concessions, particularly those with regard to value added tax, have been utilized, unless the person entitled to exercise the profession can prove that he/she has been commissioned accordingly.

(4) In each case, the obligation to render other services pursuant to Sections 2 and 3 WTBG 2017 requires for the contractor to be separately and verifiably commissioned.

(5) The aforementioned paragraphs (2) to (4) shall not apply to services requiring particular expertise provided by an expert.

(6) The contractor is not obliged to render any services, issue any warnings or provide any information beyond the scope of the contract.

(7) The contractor shall have the right to engage suitable staff and other performing agents (subcontractors) for the execution of the contract as well as to have a person entitled to exercise the profession substitute for him/her in executing the contract. Staff within the meaning of these Conditions of Contract refers to all persons who support the contractor in his/her operating activities on a regular or permanent basis, irrespective of the type of underlying legal transaction.

(8) In rendering his/her services, the contractor shall exclusively take into account Austrian law; foreign law shall only be taken into account if this has been explicitly agreed upon in writing.

(9) Should the legal situation change subsequent to delivering a final professional statement passed on by the client orally or in writing, the contractor shall not be obliged to inform the client of changes or of the consequences thereof. This shall also apply to the completed parts of a contract.

(10) The client shall be obliged to make sure that the data made available by him/her may be handled by the contractor in the course of rendering the services. In this context, the client shall particularly but not exclusively comply with the applicable provisions under data protection law and labor law.

(11) Unless explicitly agreed otherwise, if the contractor electronically submits an application to an authority, he/she acts only as a messenger and this does not constitute a declaration of intent or knowledge attributable to him/her or a person authorized to submit the application.

(12) The client undertakes not to employ persons that are or were staff of the contractor during the contractual relationship, during and within one year after termination of the contractual relationship, either in his/her company or in an associated company, failing which he/she shall be obliged to pay the contractor the amount of the annual salary of the member of staff taken over.

2. Client's Obligation to Provide Information and Submit Complete Set of Documents

(1) The client shall make sure that all documents required for the execution of the contract be placed without special request at the disposal of the contractor at the agreed date, and in good time if no such date has been agreed, and that he/she be informed of all events and circumstances which may be of significance for the execution of the contract. This shall also apply to documents, events and circumstances which become known only after the contractor has commenced his/her work.

(2) The contractor shall be justified in regarding information and documents presented to him/her by the client, in particular figures, as correct and complete and to base the contract on them. The contractor shall not be obliged to identify any errors unless agreed separately in writing. This shall particularly apply to the correctness and completeness of bills. However, he/she is obliged to inform the client of any errors identified by him/her. In case of financial criminal proceedings he/she shall protect the rights of the client.

(3) The client shall confirm in writing that all documents submitted, all information provided and explanations given in the context of audits, expert opinions and expert services are complete.

(4) If the client fails to disclose considerable risks in connection with the preparation of financial statements and other statements, the contractor shall not be obliged to render any compensation insofar as these risks materialize.

(5) Dates and time schedules stated by the contractor for the completion of the contractor's products or parts thereof are best estimates and, unless otherwise agreed in writing, shall not be binding. The same applies to any estimates of fees: they are prepared to best of the contractor's knowledge; however, they shall always be non-binding.

(6) The client shall always provide the contractor with his/her current contact details (particularly the delivery address). The contractor may rely on the validity of the contact details most recently provided by the client, particularly have deliveries made to the most recently provided address, until such time as new contact details are provided.

3. Safeguarding of Independence

(1) The client shall be obliged to take all measures to prevent that the independence of the staff of the contractor be jeopardized and shall himself/herself refrain from jeopardizing their independence in any way. In particular, this shall apply to offers of employment and to offers to accept contracts on their own account.

(2) The client acknowledges that his/her personal details required in this respect, as well as the type and scope of the services, including the performance period agreed between the contractor and the client for the services (both audit and non-audit services), shall be handled within a network (if any) to which the contractor belongs, and for this purpose transferred to the other members of the network including abroad for the purpose of examination of the existence of grounds of bias or grounds for exclusion and conflicts of interest. For this purpose the client expressly releases the contractor in accordance with the Data Protection Act and in accordance with Section 80 (4) No. 2 WTBG 2017 from his/her obligation to maintain secrecy. The client can revoke the release from the obligation to maintain secrecy at any time.

4. Reporting Requirements

(1) (Reporting by the contractor) In the absence of an agreement to the contrary, a written report shall be drawn up in the case of audits and expert opinions.

(2) (Communication to the client) All contract-related information and opinions, including reports, (all declarations of knowledge) of the contractor, his/her staff, other performing agents or substitutes ("professional statements") shall only be binding provided they are set down in writing. Professional statements in electronic file formats which are made, transferred or confirmed by fax or e-mail or using similar types of electronic communication (that can be stored and reproduced but not oral, i.e. e.g. text messages but not telephone) shall be deemed as set down in writing; this shall only apply to professional statements. The client bears the risk that professional statements may be issued by persons not entitled to do so as well as the transfer risk of such professional statements.

(3) (Communication to the client) The client hereby consents to the contractor communicating with the client (e.g. by e-mail) in an unencrypted manner. The client declares that he/she has been informed of the risks arising from the use of electronic communication (particularly access to, maintaining secrecy of, changing of messages in the course of transfer). The contractor, his/her staff, other performing agents or substitutes are not liable for any losses that arise as a result of the use of electronic means of communication.

(4) (Communication to the contractor) Receipt and forwarding of information to the contractor and his/her staff are not always guaranteed when the telephone is used, in particular in conjunction with automatic telephone answering systems, fax, e-mail and other types of electronic communication. As a result, instructions and important information shall only be deemed to have been received by the contractor provided they are also received physically (not by telephone, orally or electronically), unless explicit confirmation of receipt is provided in individual instances. Automatic confirmation that items have been transmitted and read shall not constitute such explicit confirmations of receipt. This shall apply in particular to the transmission of decisions and other information relating to deadlines. As a result, critical and important notifications must be sent to the contractor by mail or courier. Delivery of documents to staff outside the firm's offices shall not count as delivery.

(5) (General) In writing shall mean, insofar as not otherwise laid down in Item 4. (2), written form within the meaning of Section 886 Austrian Civil Code (ABGB) (confirmed by signature). An advanced electronic signature (Art. 26 eIDAS Regulation (EU) No. 910/2014) fulfills the requirement of written form within the meaning of Section 886 ABGB (confirmed by signature) insofar as this is at the discretion of the parties to the contract.

(6) (Promotional information) The contractor will send recurrent general tax law and general commercial law information to the client electronically (e.g. by e-mail). The client acknowledges that he/she has the right to object to receiving direct advertising at any time.

5. Protection of Intellectual Property of the Contractor

(1) The client shall be obliged to ensure that reports, expert opinions, organizational plans, drafts, drawings, calculations and the like, issued by the contractor, be used only for the purpose specified in the contract (e.g. pursuant to Section 44 (3) Austrian Income Tax Act 1988). Furthermore, professional statements made orally or in writing by the contractor may be passed on to a third party for use only with the written consent of the contractor.

(2) The use of professional statements made orally or in writing by the contractor for promotional purposes shall not be permitted; a violation of this provision shall give the contractor the right to terminate without notice to the client all contracts not yet executed.

(3) The contractor shall retain the copyright on his/her work. Permission to use the work shall be subject to the written consent by the contractor.

6. Correction of Errors

(1) The contractor shall have the right and shall be obliged to correct all errors and inaccuracies in his/her professional statement made orally or in writing which subsequently come to light and shall be obliged to inform the client thereof without delay. He/she shall also have the right to inform a third party acquainted with the original professional statement of the change.

(2) The client has the right to have all errors corrected free of charge if the contractor can be held responsible for them; this right will expire six months after completion of the services rendered by the contractor and/or – in cases where a written professional statement has not been delivered – six months after the contractor has completed the work that gives cause to complaint.

(3) If the contractor fails to correct errors which have come to light, the client shall have the right to demand a reduction in price. The extent to which additional claims for damages can be asserted is stipulated under Item 7.

7. Liability

(1) All liability provisions shall apply to all disputes in connection with the contractual relationship, irrespective of the legal grounds. The contractor is liable for losses arising in connection with the contractual relationship (including its termination) only in case of willful intent and gross negligence. The applicability of Section 1298 2nd Sentence ABGB is excluded.

(2) In cases of gross negligence, the maximum liability for damages due from the contractor is tenfold the minimum insurance sum of the professional liability insurance according to Section 11 WTBG 2017 as amended.

(3) The limitation of liability pursuant to Item 7. (2) refers to the individual case of damages. The individual case of damages includes all consequences of a breach of duty regardless of whether damages arose in one or more consecutive years. In this context, multiple acts or failures to act that are based on the same or similar source of error as one consistent breach of duty if the matters concerned are legally and economically connected. Single damages remain individual cases of damage even if they are based on several breaches of duty. Furthermore, the contractor's liability for loss of profit as well as collateral, consequential, incidental or similar losses is excluded in case of willful damage.

(4) Any action for damages may only be brought within six months after those entitled to assert a claim have gained knowledge of the damage, but no later than three years after the occurrence of the (primary) loss following the incident upon which the claim is based, unless other statutory limitation periods are laid down in other legal provisions.

(5) Should Section 275 Austrian Commercial Code (UGB) be applicable (due to a criminal offense), the liability provisions contained therein shall apply even in cases where several persons have participated in the execution of the contract or where several activities requiring compensation have taken place and irrespective of whether other participants have acted with intent.

(6) In cases where a formal auditor's report is issued, the applicable limitation period shall commence no later than at the time the said auditor's report was issued.

(7) If activities are carried out by enlisting the services of a third party, e.g. a data-processing company, any warranty claims and claims for damages which arise against the third party according to law and contract shall be deemed as having been passed on to the client once the client has been informed of them. Item 4. (3) notwithstanding, in such a case the contractor shall only be liable for fault in choosing the third party.

(8) The contractor's liability to third parties is excluded in any case. If third parties come into contact with the contractor's work in any manner due to the client, the client shall expressly clarify this fact to them. Insofar as such exclusion of liability is not legally permissible or a liability to third parties has been assumed by the contractor in exceptional cases, these limitations of liability shall in any case also apply to third parties on a subsidiary basis. In any case, a third party cannot raise any claims that go beyond any claim raised by the client. The maximum sum of liability shall be valid only once for all parties injured, including the compensation claims of the client, even if several persons (the client and a third party or several third parties) have sustained losses; the claims of the parties injured shall be satisfied in the order in which the claims have been raised. The client will indemnify and hold harmless the contractor and his/her staff against any claims by third parties in connection with professional statements made orally or in writing by the contractor and passed on to these third parties.

(9) Item 7. shall also apply to any of the client's liability claims to third parties (performing agents and vicarious agents of the contractor) and to substitutes of the contractor relating to the contractual relationship.

8. Secrecy, Data Protection

(1) According to Section 80 WTBG 2017 the contractor shall be obliged to maintain secrecy in all matters that become known to him/her in connection with his/her work for the client, unless the client releases him/her from this duty or he/she is bound by law to deliver a statement.

(2) Insofar as it is necessary to pursue the contractor's claims (particularly claims for fees) or to dispute claims against the contractor (particularly claims for damages raised by the client or third parties against the contractor), the contractor shall be released from his/her professional obligation to maintain secrecy.

(3) The contractor shall be permitted to hand on reports, expert opinions and other written statements pertaining to the results of his/her services to third parties only with the permission of the client, unless he/she is required to do so by law.

(4) The contractor is a data protection controller within the meaning of the General Data Protection Regulation ("GDPR") with regard to all personal data processed under the contract. The contractor is thus authorized to process personal data entrusted to him/her within the limits of the contract. The material made available to the contractor (paper and data carriers) shall generally be handed to the client or to third parties appointed by the client after the respective rendering of services has been completed, or be kept and destroyed by the contractor if so agreed. The contractor is authorized to keep copies thereof insofar as he/she needs them to appropriately document his/her services or insofar as it is required by law or customary in the profession.

(5) If the contractor supports the client in fulfilling his/her duties to the data subjects arising from the client's function as data protection controller, the contractor shall be entitled to charge the client for the actual efforts undertaken. The same shall apply to efforts undertaken for information with regard to the contractual relationship which is provided to third parties after having been released from the obligation to maintain secrecy to third parties by the client.

9. Withdrawal and Cancellation („Termination“)

(1) The notice of termination of a contract shall be issued in writing (see also Item 4, (4) and (5)). The expiry of an existing power of attorney shall not result in a termination of the contract.

(2) Unless otherwise agreed in writing or stipulated by force of law, either contractual partner shall have the right to terminate the contract at any time with immediate effect. The fee shall be calculated according to Item 11.

(3) However, a continuing agreement (fixed-term or open-ended contract on – even if not exclusively – the rendering of repeated individual services, also with a flat fee) may, without good reason, only be terminated at the end of the calendar month by observing a period of notice of three months, unless otherwise agreed in writing.

(4) After notice of termination of a continuing agreement and unless otherwise stipulated in the following, only those individual tasks shall still be completed by the contractor (list of assignments to be completed) that can (generally) be completed fully within the period of notice insofar as the client is notified in writing within one month after commencement of the termination notice period within the meaning of Item 4, (2). The list of assignments to be completed shall be completed within the termination period if all documents required are provided without delay and if no good reason exists that impedes completion.

(5) Should it happen that in case of a continuing agreement more than two similar assignments which are usually completed only once a year (e.g. financial statements, annual tax returns, etc.) are to be completed, any such assignments exceeding this number shall be regarded as assignments to be completed only with the client's explicit consent. If applicable, the client shall be informed of this explicitly in the statement pursuant to Item 9, (4).

10. Termination in Case of Default in Acceptance and Failure to Cooperate on the Part of the Client and Legal Impediments to Execution

(1) If the client defaults on acceptance of the services rendered by the contractor or fails to carry out a task incumbent on him/her either according to Item 2, or imposed on him/her in another way, the contractor shall have the right to terminate the contract without prior notice. The same shall apply if the client requests a way to execute (also partially) the contract that the contractor reasonably believes is not in compliance with the legal situation or professional principles. His/her fees shall be calculated according to Item 11. Default in acceptance or failure to cooperate on the part of the client shall also justify a claim for compensation made by the contractor for the extra time and labor hereby expended as well as for the damage caused, if the contractor does not invoke his/her right to terminate the contract.

(2) For contracts concerning bookkeeping, payroll accounting and administration and assessment of payroll-related taxes and contributions, a termination without prior notice by the contractor is permissible under Item 10, (1) if the client verifiably fails to cooperate twice as laid down in Item 2, (1).

11. Entitlement to Fee

(1) If the contract fails to be executed (e.g. due to withdrawal or cancellation), the contractor shall be entitled to the negotiated compensation (fee), provided he/she was prepared to render the services and was prevented from so doing by circumstances caused by the client, whereby a merely contributory negligence by the contractor in this respect shall be excluded; in this case the contractor need not take into account the amount he/she obtained or failed to obtain through alternative use of his/her own professional services or those of his/her staff.

(2) If a continuing agreement is terminated, the negotiated compensation for the list of assignments to be completed shall be due upon completion or in case completion fails due to reasons attributable to the client (reference is made to Item 11, (1)). Any flat fees negotiated shall be calculated according to the services rendered up to this point.

(3) If the client fails to cooperate and the assignment cannot be carried out as a result, the contractor shall also have the right to set a reasonable grace period on the understanding that, if this grace period expires without results, the contract shall be deemed ineffective and the consequences indicated in Item 11, (1) shall apply.

(4) If the termination notice period under Item 9, (3) is not observed by the client as well as if the contract is terminated by the contractor in accordance with Item 10, (2), the contractor shall retain his/her right to receive the full fee for three months.

12. Fee

(1) Unless the parties explicitly agreed that the services would be rendered free of charge, an appropriate remuneration in accordance with Sections 1004 and 1152 ABGB is due in any case. Amount and type of the entitlement to the fee are laid down in the agreement negotiated between the contractor and his/her client. Unless a different agreement has verifiably been reached, payments made by the client shall in all cases be credited against the oldest debt.

(2) The smallest service unit which may be charged is a quarter of an hour.

(3) Travel time to the extent required is also charged.

(4) Study of documents which, in terms of their nature and extent, may prove necessary for preparation of the contractor in his/her own office may also be charged as a special item.

(5) Should a remuneration already agreed upon prove inadequate as a result of the subsequent occurrence of special circumstances or due to special requirements of the client, the contractor shall notify the client thereof and additional negotiations for the agreement of a more suitable remuneration shall take place (also in case of inadequate flat fees).

(6) The contractor includes charges for supplementary costs and VAT in addition to the above, including but not limited to the following (7) to (9):

(7) Chargeable supplementary costs also include documented or flat-rate cash expenses, traveling expenses (first class for train journeys), per diems, mileage allowance, copying costs and similar supplementary costs.

(8) Should particular third party liabilities be involved, the corresponding insurance premiums (including insurance tax) also count as supplementary costs.

(9) Personnel and material expenses for the preparation of reports, expert opinions and similar documents are also viewed as supplementary costs.

(10) For the execution of a contract wherein joint completion involves several contractors, each of them will charge his/her own compensation.

(11) In the absence of any other agreements, compensation and advance payments are due immediately after they have been requested in writing. Where payments of compensation are made later than 14 days after the due date, default interest may be charged. Where mutual business transactions are concerned, a default interest rate at the amount stipulated in Section 456 1st and 2nd Sentence UGB shall apply.

(12) Statutory limitation is in accordance with Section 1486 of ABGB, with the period beginning at the time the service has been completed or upon the issuing of the bill within an appropriate time limit at a later point.

(13) An objection may be raised in writing against bills presented by the contractor within 4 weeks after the date of the bill. Otherwise the bill is considered as accepted. Filing of a bill in the accounting system of the recipient is also considered as acceptance.

(14) Application of Section 934 ABGB within the meaning of Section 351 UGB, i.e. rescission for laesio enormis (lesion beyond moiety) among entrepreneurs, is hereby renounced.

(15) If a flat fee has been negotiated for contracts concerning bookkeeping, payroll accounting and administration and assessment of payroll-related taxes and contributions, in the absence of written agreements to the contrary, representation in matters concerning all types of tax audits and audits of payroll-related taxes and social security contributions including settlements concerning tax assessments and the basis for contributions, preparation of reports, appeals and the like shall be invoiced separately. Unless otherwise agreed to in writing, the fee shall be considered agreed upon for one year at a time.

(16) Particular individual services in connection with the services mentioned in Item 12, (15), in particular ascertaining whether the requirements for statutory social security contributions are met, shall be dealt with only on the basis of a specific contract.

(17) The contractor shall have the right to ask for advance payments and can make delivery of the results of his/her (continued) work dependent on satisfactory fulfillment of his/her demands. As regards continuing agreements, the rendering of further services may be denied until payment of previous services (as well as any advance payments under Sentence 1) has been effected. This shall analogously apply if services are rendered in installments and fee installments are outstanding.

(18) With the exception of obvious essential errors, a complaint concerning the work of the contractor shall not justify even only the partial retention of fees, other compensation, reimbursements and advance payments (remuneration) owed to him/her in accordance with Item 12.

(19) Offsetting the remuneration claims made by the contractor in accordance with Item 12. shall only be permitted if the demands are uncontested and legally valid.

13. Other Provisions

(1) With regard to Item 12, (17), reference shall be made to the legal right of retention (Section 471 ABGB, Section 369 UGB); if the right of retention is wrongfully exercised, the contractor shall generally be liable pursuant to Item 7. or otherwise only up to the outstanding amount of his/her fee.

(2) The client shall not be entitled to receive any working papers and similar documents prepared by the contractor in the course of fulfilling the contract. In the case of contract fulfillment using electronic accounting systems the contractor shall be entitled to delete the data after handing over all data based thereon – which were prepared by the contractor in relation to the contract and which the client is obliged to keep – to the client and/or the succeeding public accountant in a structured, common and machine-readable format. The contractor shall be entitled to an appropriate fee (Item 12. shall apply by analogy) for handing over such data in a structured, common and machine-readable format. If handing over such data in a structured, common and machine-readable format is impossible or unfeasible for special reasons, they may be handed over in the form of a full print-out instead. In such a case, the contractor shall not be entitled to receive a fee.

(3) At the request and expense of the client, the contractor shall hand over all documents received from the client within the scope of his/her activities. However, this shall not apply to correspondence between the contractor and his/her client and to original documents in his/her possession and to documents which are required to be kept in accordance with the legal anti-money laundering provisions applicable to the contractor. The contractor may make copies or duplicates of the documents to be returned to the client. Once such documents have been transferred to the client, the contractor shall be entitled to an appropriate fee (Item 12. shall apply by analogy).

(4) The client shall fetch the documents handed over to the contractor within three months after the work has been completed. If the client fails to do so, the contractor shall have the right to return them to the client at the cost of the client or to charge an appropriate fee (Item 12. shall apply by analogy) if the contractor can prove that he/she has asked the client twice to pick up the documents handed over. The documents may also further be kept by third parties at the expense of the client. Furthermore, the contractor is not liable for any consequences arising from damage, loss or destruction of the documents.

(5) The contractor shall have the right to compensation of any fees that are due by use of any available deposited funds, clearing balances, trust funds or other liquid funds at his/her disposal, even if these funds are explicitly intended for safekeeping, if the client had to have anticipated the counterclaim of the contractor.

(6) To secure an existing or future fee payable, the contractor shall have the right to transfer a balance held by the client with the tax office or another balance held by the client in connection with charges and contributions, to a trust account. In this case the client shall be informed of the transfer. Subsequently, the amount secured may be collected either after agreement has been reached with the client or after enforceability of the fee by execution has been declared.

14. Applicable Law, Place of Performance, Jurisdiction

(1) The contract, its execution and the claims resulting from it shall be exclusively governed by Austrian law, excluding national referral rules.

(2) The place of performance shall be the place of business of the contractor.

(3) In absence of a written agreement stipulating otherwise, the place of jurisdiction is the competent court of the place of performance.

SECTION II

15. Supplementary Provisions for Consumer Transactions

(1) Contracts between public accountants and consumers shall fall under the obligatory provisions of the Austrian Consumer Protection Act (KSchG).

(2) The contractor shall only be liable for the wilful and grossly negligent violation of the obligations assumed.

(3) Contrary to the limitation laid down in Item 7. (2), the duty to compensate on the part of the contractor shall not be limited in case of gross negligence.

(4) Item 6. (2) (period for right to correction of errors) and Item 7. (4) (asserting claims for damages within a certain period) shall not apply.

(5) Right of Withdrawal pursuant to Section 3 KSchG:

If the consumer has not made his/her contract statement in the office usually used by the contractor, he/she may withdraw from the contract application or the contract proper. This withdrawal may be declared until the contract has been concluded or within one week after its conclusion; the period commences as soon as a document has been handed over to the consumer which contains at least the name and the address of the contractor as well as instructions on the right to withdraw from the contract, but no earlier than the conclusion of the contract. The consumer shall not have the right to withdraw from the contract

1. if the consumer himself/herself established the business relationship concerning the conclusion of this contract with the contractor or his/her representative,

2. if the conclusion of the contract has not been preceded by any talks between the parties involved or their representatives, or

3. in case of contracts where the mutual services have to be rendered immediately, if the contracts are usually concluded outside the offices of the contractors, and the fee agreed upon does not exceed €15.

In order to become legally effective, the withdrawal shall be declared in writing. It is sufficient if the consumer returns a document that contains his/her contract declaration or that of the contractor to the contractor with a note which indicates that the consumer rejects the conclusion or the maintenance of the contract. It is sufficient if this declaration is dispatched within one week.

If the consumer withdraws from the contract according to Section 3 KSchG,

1. the contractor shall return all benefits received, including all statutory interest, calculated from the day of receipt, and compensate the consumer for all necessary and useful expenses incurred in this matter,

2. the consumer shall pay for the value of the services rendered by the contractor as far as they are of a clear and predominant benefit to him/her.

According to Section 4 (3) KSchG, claims for damages shall remain unaffected.

(6) Cost Estimates according to Section 5 Austrian KSchG:

The consumer shall pay for the preparation of a cost estimate by the contractor in accordance with Section 1170a ABGB only if the consumer has been notified of this payment obligation beforehand.

If the contract is based on a cost estimate prepared by the contractor, its correctness shall be deemed warranted as long as the opposite has not been explicitly declared.

(7) Correction of Errors: Supplement to Item 6.:

If the contractor is obliged under Section 932 ABGB to improve or complement his/her services, he/she shall execute this duty at the place where the matter was transferred. If it is in the interest of the consumer to have the work and the documents transferred by the contractor, the consumer may carry out this transfer at his/her own risk and expense.

(8) Jurisdiction: Shall apply instead of Item 14. (3)

If the domicile or the usual residence of the consumer is within the country or if he/she is employed within the country, in case of an action against him/her according to Sections 88, 89, 93 (2) and 104 (1) Austrian Court Jurisdiction Act (JN), the only competent courts shall be the courts of the districts where the consumer has his/her domicile, usual residence or place of employment.

(9) Contracts on Recurring Services:

(a) Contracts which oblige the contractor to render services and the consumer to effect repeated payments and which have been concluded for an indefinite period or a period exceeding one year may be terminated by the consumer at the end of the first year, and after the first year at the end of every six months, by adhering to a two-month period of notice.

(b) If the total work is regarded as a service that cannot be divided on account of its character, the extent and price of which is determined already at the conclusion of the contract, the first date of termination may be postponed until the second year has expired. In case of such contracts the period of notice may be extended to a maximum of six months.

(c) If the execution of a certain contract indicated in lit. a) requires considerable expenses on the part of the contractor and if he/she informed the consumer about this no later than at the time the contract was concluded, reasonable dates of termination and periods of notice which deviate from lit. a) and b) and which fit the respective circumstances may be agreed.

(d) If the consumer terminates the contract without complying with the period of notice, the termination shall become effective at the next termination date which follows the expiry of the period of notice.