Sofy SOC2 Report

Service Organization Control-report (SOC 2)
based on Trust Services Principles and Criteria
Security, Processing Integrity, Availability and
Confidentiality

KPMG Advisory N.V.
14 December 2018
This report contains 43 pages

Executive Summary

Scope	Sofy Platform
Period of Examination	January 1, 2018 to November 30, 2018
Applicable Trust Principle(s)	Security, Availability, Processing Integrity and Confidentiality
Subservice Providers	Microsoft Azure
Opinion Result	unqualified
Testing Exceptions	0

Contents

1. Management Statement

1. Management statement

We have prepared the attached description titled Description of Sofy system as of January 1, 2018 (the description), based on the criteria in items (a)(i)–(ii) below (the description criteria). The description is intended to provide users with information about the Sofy system, particularly system controls intended to meet the criteria for the security, availability, confidentiality and processing integrity principles set forth in TSP section 100, Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy issued by the Assurance Services Executive Committee of the AICPA (applicable trust services criteria).

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

A. the description fairly presents the Sofy system throughout the period 1 January 2018 to 30 November 2018 (the 'specified period'), based on the following description criteria::
   i. The description contains the following information:
      1. The types of services provided;
      2. The components of the system used to provide the services, which are the following:
         a. Infrastructure. The physical and hardware components of a system (facilities, equipment, and networks);
         b. Software. The programs and operating software of a system (systems, applications, and utilities);
         c. People. The personnel involved in the operation and use of a system (developers, operators, users, and managers);
         d. Procedures. The automated and manual procedures involved in the operation of a system;
         e. Data. The information used and supported by a system (transaction streams, files, databases, and tables);
      3. The boundaries or aspects of the system covered by the description;
      4. If information is provided to, or received from, subservice organizations or other parties, how such information is provided or received; the role of the subservice organization and other parties; and the procedures performed to determine that such information and its processing, maintenance, and storage are subject to appropriate controls;
      5. For each category being reported on, the applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, the following:
         a. Complementary user-entity controls contemplated in the design of the service organization's system;
         b. For subservice organizations presented using the carve-out method, the nature of the services provided by the subservice organization; each of the applicable trust services criteria that are intended to be met by controls at the subservice organization, alone or in combination with controls at the service organization, and the types of controls expected to be implemented at carved-out subservice organizations to meet those criteria;
      6. Any applicable trust services criteria that are not addressed by a control and the reasons therefore;
      7. Relevant details of changes to the service organization's system during the period covered by the description.

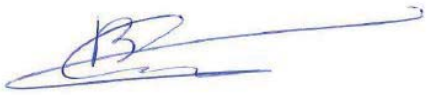
ii. The description does not omit or distort information relevant to the service organization's system while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs.

iii. The controls stated in the description were suitably designed to meet the applicable trust services criteria provided user entities applied the complementary user-entity controls contemplated in the design of the system throughout the specified period; and

iv. The controls stated in the description operated effectively throughout the period 1 January 2018 to 30 November 2018 to meet the applicable trust services criteria.

KPMG Advisory N.V.

Amstelveen, December 14, 2018



Bram Coolen
Partner

2. Independent service auditor's report

2. Independent service auditor's report

To the Management of KPMG Sofy,

2.1 Scope

We have been engaged to obtain reasonable assurance and report on the attached description titled "Description of Sofy system" for the period 1 January 2018 to 30 November 2018 (the description) and the suitability of the design and operating effectiveness of controls to meet the trust services criteria relevant to security, availability, confidentiality and processing integrity set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy issued by the American Institute of Certified Public Accountants and the Chartered Professional Accountants of Canada (applicable trust services criteria) throughout the period 1 January 2018 to 30 November 2018 (the 'specified period').

The description indicates that certain applicable trust services criteria specified in the description can be achieved only if complementary user-entity controls contemplated in the design of KPMG Sofy's ("Service Entity") 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.

KPMG Sofy uses service organizations (subservice organization) Microsoft Azure and Argusoft ("Subservice Entity") to perform hosting and development. The description indicates that certain applicable trust services criteria can only be met if controls at the subservice organization are suitably designed and operating effectively. For its description KPMG Sofy uses the carve-out method. The description of the system therefore does not include any of the controls implemented at the subservice organization. Our engagement did not extend to the controls provided by the subservice organization.

The applicable categories are identified in KPMG Sofy's statement in combination with the applicable trust service criteria.

2.2 Service organization's responsibilities

In section 1, KPMG Sofy has provided the attached statement titled "Management Statement" which is based on the criteria identified in management's statement. KPMG Sofy is responsible for (1) preparing the description and statement; (2) the completeness, accuracy, and method of presentation of both the description and statement; (3) providing the services covered by the description; (4) specifying the controls that meet the applicable trust services criteria and stating them in the description; and (5) designing, implementing, and documenting the controls to meet the applicable trust services criteria.

2.3 Service auditor's responsibilities

Our responsibility is to express an opinion on the:

- fairness of the presentation of the description based on the description criteria set forth in KPMG Sofy's statement;
- suitability of the design and operating effectiveness of the controls to meet the applicable trust services criteria, based on our procedures to obtain reasonable assurance.

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

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

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

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

2.4 Inherent limitations

KPMG Sofy's description is prepared to meet the common needs of a broad range of customers and their auditors and may not, therefore, include every aspect of the system that each individual customer may consider important in its own particular environment. Also, because of their nature and inherent limitations, controls at a service organization may not always operate effectively to meet the applicable trust services criteria. Also, the projection to the future of any evaluation of the fairness of the presentation of the description or conclusions about the suitability of the design of the controls to meet the applicable trust services criteria is subject to the risks that the system may change or that controls at a service organization may become inadequate or fail.

2.5 Opinion

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

a) The description fairly presents the Sofy system as designed and implemented throughout the period from 1 January 2018 to 30 November 2018;

a) The controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated effectively throughout the period 1 January 2018, to 30 November 2018 and user entities applied the complementary user-entity controls contemplated in the design of klantnaam's controls throughout the period 1 January 2018, to 30 November 2018; and

b) The controls tested, which together with the complementary user-entity controls referred to in the scope paragraph of this report, if operating effectively, were those necessary to provide reasonable assurance that the applicable trust services criteria were met, operated effectively throughout the period 1 January 2018, to 30 November 2018.

2.6 Description of Tests of Controls

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

2.7 Restricted use

This report and the description of tests of controls and results thereof are intended solely for the information and use of KPMG Sofy; user entities of the Sofy system during some or all of the period 1 January 2018 to 30 November 2018; and independent auditors and practitioners providing services to such user entities who have sufficient knowledge and understanding of the following:

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

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

Amstelveen, December 14, 2018

BDO Audit & Assurance B.V.
On behalf,

SIGNED

J. van Schajik RE CISA
Partner

KPMG

3. Description of Sofy system

3.1 Introduction

Sofy is an innovative enterprise application platform focused on analytics and feedback. It provides business insights based on the real time analysis of master and transactional data. These insights are presented to users via notifications, social feeds and dashboards. The simulation and root cause analysis features provide a powerful toolset to explain why things are happening. The platform engines are out of the box, fueled by KPMG better practices and industry standards. The insights provided by Sofy are actionable, relevant and focused on sustainable improvement.

Based on emerging and innovative technology (e.g. Microsoft Azure, SAP HANA), Sofy is a secure application that is accessible from any device.

Sofy offers its customers an extensive set of solutions, including:

— Process Monitoring and Control;
— Spend Analytics;
— Access Control;
— Governance, Risk and Compliance;
— Data Quality;
— Tax;
— Sanction List Monitoring.

3.2 Services provided and scope of SOC2 report

Sofy provides its services to customers in the form of a software-as-a-service (SaaS) solution hosted on Microsoft Azure. All Sofy solutions are based on the Sofy platform, as illustrated in the figure below:

The scope of this SOC2 report covers the Sofy platform as well as the Sofy solutions provided to customers. Sofy is hosted on Microsoft Azure, which means that hardware, physical infrastructure and datacenters are provided by the Microsoft Azure environment. The services that Microsoft Azure provides to Sofy are covered by a SOC2 report from Microsoft, and boundary controls have been put in place.

3.3 The components of the system

3.3.1 Infrastructure

Sofy has a cloud-based system landscape with a shared architecture used by multiple clients. Sofy is built on top of Microsoft Azure and uses Azure IaaS and PaaS services. Within this environment there is a production, acceptance, test and development landscape, all based on the same landscape components which are shared to some extent. The Sofy environment has three main components:

— Azure Webapp to host the application;
— SQL Server to host the databases;
— SFTP server which is used to upload data to the Sofy environment.

The environments are managed through the Azure portal. Access to this portal is restricted to specific users and requires multi-factor authentication.

3.3.2 Software

The Sofy platform and the Sofy solutions are developed by Sofy and offered to customers. Strict development and release management procedures are used to ensure high quality standards.

To support Sofy in delivering its applications, several Azure services are used:

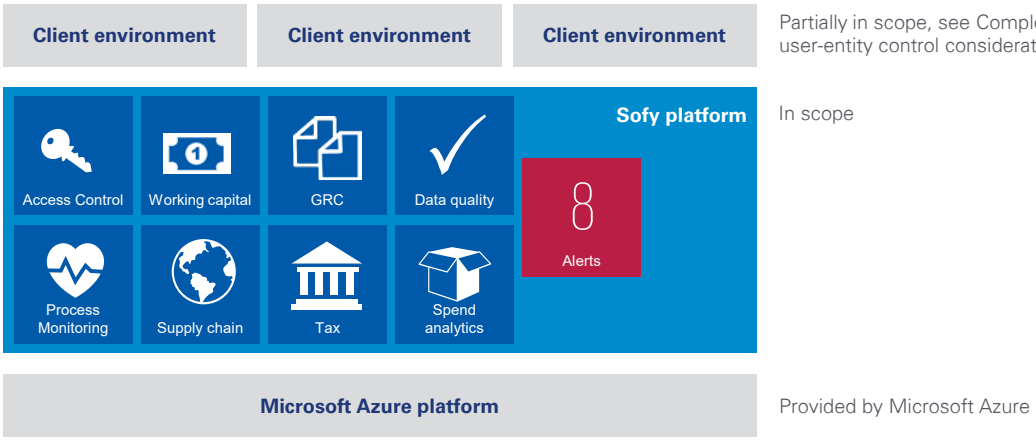


Fig. 1 Overview of the Sofy platform

— Active Directory to provide directory services and role-based access control;
— Azure Security Center for vulnerability scanning and monitoring;
— Microsoft Operations Management suite for various tasks including security monitoring;
— Visual Studio Team Services for continuous integration and delivery.

Furthermore, the Sofy platform itself offers various tools to support and maintain the Sofy platform, including:

— Tenant manager to manage client environments;
— Ticketing solution for change and incident management;
— Service Level Agreement and Reporting solution;
— GRC solution to manage all Sofy risks and controls;
— Wiki for documentation.

3.3.3 People

The figure below shows the organizational structure of Sofy which consists of a management team with six different divisions: Platform Development; Operations; Portfolio Management, Client Delivery, Marketing & Sales and Back Office.

Each team member has defined responsibilities and accountabilities with regard to the security, availability, processing integrity and confidentiality of the Sofy system.

3.3.3.1 Management team

Sofy management is responsible for developing the company strategy and successfully managing the Sofy processes and team. Sofy management includes a KPMG partner who has the authority to sign formal agreements and make financial decisions. Operational management is delegated by the KPMG partner to other Sofy management employees. Periodical Sofy management updates are organized to ensure that management has sufficient information to fulfil their responsibilities.

3.3.3.2 Operations and Client Delivery

Sofy team members that are active for Sofy customers are responsible for implementing, supporting and optimizing customer environments. The Service Desk is the main point of contact with the clients. It owns and manages clients' requests, incidents, and bugs, and answers clients' inquiries. Customer activities are performed by KPMG Sofy team members and can be supported by other KPMG personnel.

Infrastructure Management is responsible for managing, maintaining, improving and optimizing the infrastructure and middleware components including databases, web servers, virtual machines, storage, Azure subscriptions, and backups.

Implementation Project Management is responsible for ensuring successful Sofy implementation for individual customers. This team collects requirements, manages the budget and manages changes to environments. Furthermore the authority of the Implementation Project Manager includes the initiation of changes on behalf of the client, as well as the overall management of the client environment. The Implementation Project Manager reports to the Sofy Management Team and the KPMG Engagement Partner.

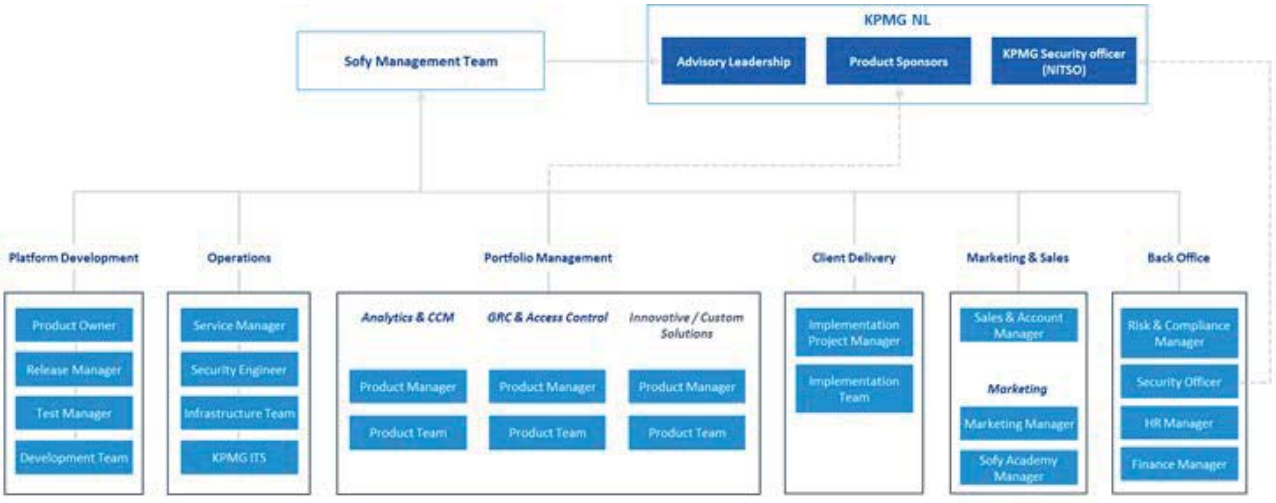


Fig. 2 Organizational structure of Sofy

3.3.3.3 Platform Development & Portfolio Management

The Sofy team members that are responsible for researching new possibilities and improvements for both the platform and the applications are active in the Portfolio Management area.

Portfolio Management is responsible for developing and executing the product roadmap, making products sales ready and positioning the product in the market.

Platform Development is responsible for managing active development on the platform level, releases and release cycles including promotion of functionality between environments, and managing, optimizing and improving the development lifecycle.

3.3.3.4 Marketing & Sales

The Sofy team members that are active in the Marketing & Sales area are responsible for marketing and sales activities. These activities are not in scope for SOC2.

3.3.3.5 Back Office

The Sofy team members that are active in the Back Office area are responsible for maintaining and improvement of risk mitigation, security, HR and learning and development.

Risk & Compliance Management is responsible for all risk- and compliance-related activities, to ensure that the control framework remains up to date, new risks are detected promptly and appropriate mitigating controls are implemented. Further responsibilities include the periodical sign-off of the controls and managing all external audits.

Security Management is responsible for maintaining a safe and secure environment for customers and employees by establishing and enforcing security policies and procedures; supervising the security of the system and overseeing the operations of Sofy's security solutions.

Sofy Human Resources Management is responsible for all Sofy-specific HR processes including onboarding, performance development and off-boarding. This is organized in close conformity with KPMG HR processes which include hiring and performance development.

Sofy Academy Manager includes knowledge management and maintenance and improvement of the Sofy training academy.

3.3.4 Procedures

Policies and procedures form the basis of the services provided by Sofy. The policies and procedures define the requirements to meet the security controls. Policies and procedures are documented and accessible to Sofy employees. The policies and procedures include, but are not limited to:

Sofy Control Framework – Describes the controls that Sofy puts in place to meet the security, availability, processing integrity and confidentiality requirements of the system;

Organizational Structure – Describes the Sofy organization structure, roles and responsibilities;

Role Descriptions – Describes the roles and responsibilities as well as the requirements and skills for Sofy candidates;

Sofy HR Guide – Describes the HR processes such as onboarding, off-boarding, training and development;

Sofy Security Policy – The security policy is applicable to all information and IT systems at Sofy and is based on industry standards;

Sofy Acceptable Use Policy – Acceptable Use Policy establishes the minimum standards for the acceptable and appropriate use of Sofy's information and IT assets by users;

Information Classification – Describes the classification of information within Sofy to meet the system requirements regarding availability, processing integrity, and confidentiality;

Risk Management – The Risk Management session is conducted on a yearly basis to identify and assess business and IT risks and determine risk management strategies;

User Guides, Process Documentation and Work Instructions – Describes operational processes and work instructions for Sofy employees to follow;

Security Design – Describes the security architecture and security hardening mechanism for Sofy;

Change Management – Describes the Change Management process within Sofy, which ensures that changes are registered, evaluated, reviewed and approved accordingly. The purpose of this document is to give all people involved an overview of the entire process, and describe how activities are to be performed;

Incident Management – Describes the Incident Management process within Sofy, which ensures that incidents are registered, evaluated and tracked until resolution. The purpose of this document is to give all stakeholders involved an overview of the entire process, their roles and their responsibilities in the process;

Release Management – The Release Management process is designed to maintain consistency of processes and standards in all software and infrastructure deployments into controlled environments;

Software Development Work Instruction – Describes the development process including tools, and development methods;

Patch Management – Describes the process of patching system components including automated and manual patching;

Service Level Management – The Service Level Management (SLM) process is applied for negotiating Service Level Agreements (SLAs), and ensuring that the SLAs are met. The process includes several controls to ensure that these goals are met, including monitoring service levels, reporting and periodic reviews;

Monitoring – Describes the operational monitoring of Sofy and monitoring the Azure environment, as well as security monitoring;

Role-based Access Control and Password Policy – Contains the role-based access control policy for Sofy. It contains a description of the policies, procedures and tools related to role-based access control;

Backup and recovery procedures – Describes the backup policy and backup work instructions ;

Business continuity plan and disaster recovery – Describes the Sofy business continuity and disaster recovery plan for Sofy including potential disaster scenarios.

In addition, Sofy relies on generic KPMG policies and procedures with regard to the management of mobile devices and HR processes. Sofy's policies and procedures are designed to be both complementary to and compliant with KPMG's policies and procedures.

Sofy uses the SOC2 framework for baseline control procedures which is documented in the Sofy control framework. The control framework of Sofy covers the following areas:

- Organization, Governance and Management;
- Human Resource Management;
- Communication;
- Logical and Physical Access Controls;
- Risk Management and Design and Implementation of Controls;
- Availability;
- Confidentiality;
- Incident Management;
- Change Management;
- Release Management;
- Monitoring of Controls;
- Processing Integrity;
- Security;
- System Operations.

The control framework includes control activities for managing the security, availability, processing integrity and confidentiality of Sofy.

3.3.5 Data

Data in Sofy can be divided into three main categories, customer data, confidential data and public data. Customer data includes all application databases, files, tables, customer system configurations, documentation and transactions that are stored and processed as part of a customer environment.

Confidential data includes all other confidential non-customer -specific data including procedures, documentation, configurations and Sofy operations process transactions (such as incident and change tickets). Public data is, as the name suggests, publicly accessible data such as information that is provided on the public website or in marketing material.

Most of Sofy's data is stored in SQL Server databases. Direct access to these databases is restricted and protected through the use of logical access mechanisms.

Sofy provides several mechanisms to ensure that data is processed consistently and processing integrity can be maintained. These mechanisms include validation of data imports, mechanisms to validate user input and error handling mechanisms.

3.3.6 System Boundaries and Complementary User-entity Control Considerations

This section describes the boundaries of Sofy's system and the control considerations that should be taken into account by user entities. As customers are able to configure and maintain their own customer environments, Sofy cannot take full responsibility for the security, availability, confidentiality and processing integrity of the services provided.

3.3.6.1 System Boundaries

Users of Sofy's system should take the following boundaries into account:

— System development;
— Limitations with respect to customer environments and data.

3.3.6.1.1 System Development

The development of the Sofy platform is outsourced to a third-party organization. The development of the Sofy platform including the development environment and the developers are not in scope. Sofy has put several controls in place in order to ensure that software releases are compliant with Sofy's commitments and requirements with regards to security, availability, confidentiality and processing integrity. These controls include:

— The segregation of development, test, acceptance and production environments;
— A strict role-based access control process and logical access controls that ensure that only Sofy employees can access production data and environments;
— Customer data may only be used in production environments;
— A strict release management process which includes testing procedures, security reviews and enforced approval mechanisms;
— A contract with the development organization that includes a confidentiality agreement.

Through the use of these controls, the development process, environment and third-party development organization are not in scope for this SOC2 report.

Note: The development of (client-specific) Sofy applications on top of the platform that use the Sofy configuration capabilities is within the scope of this SOC2 report.

3.3.6.2 Complementary User-entity Control Considerations

Controls that should be considered by user entities:

- User entities are responsible for data confidentiality controls at user organizations, such as segregation of duties, (non-)disclosure of information at the user organization;
- User entities are responsible for the integrity of customer data, as customers themselves are responsible for processing their data using the Sofy application. Sofy does apply controls to validate data inputs and outputs and employs strict release management and testing procedures to ensure that the Sofy system is able to process data correctly;
- User entities are responsible for logical access management of non-Sofy users;
- The management of users, their accounts, associated access devices, authentication, authorization mechanisms and associated policies as well as guidelines for non-Sofy users, are not covered in the SOC2 scope;
- User entities are responsible for user reviews for non-Sofy users;
- The access for Sofy users is controlled through role-based access controls and is subject to periodic reviews by management. The process for performing these checks is part of the system description. However, the customers' user reviews are out of the scope of this description;
- User entities are responsible for timely reporting of (security) incidents.

3.4. Relevant Aspects of the Control Environment, Risk Assessment Process, Monitoring, and Information and Communication

3.4.1 Control Environment

Sofy's control environment has been designed with an emphasis given to controls in its policies, procedures, methods, and organizational structure. The following is a description of key elements of the control environment related to Sofy:

- Sofy's Organizational Structure;
- Integrity, Ethics and Codes of Conduct;
- HR Policies and Practices;
- Responsibility for Internal Control and Risk Management;
- Information Security.

Because of the limitations that are inherent in any system of internal control, this system is designed to manage, rather than eliminate, the risk of failure to achieve corporate objectives. Accordingly, it can only provide reasonable but not absolute assurance against material misstatements or loss.

3.4.1.1 Organizational Structure

KPMG Sofy's Organizational Structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. KPMG Sofy's management believes that establishing a relevant organizational structure includes consideration of key areas of authority and responsibility and appropriate lines of reporting. KPMG Sofy has developed an organizational structure suited to its needs. Roles and responsibilities for designing, developing, implementing, operating, monitoring, and maintaining the system are defined within job descriptions, policies, and procedures. An overview of the organizational structure is provided in the section "People".

3.4.1.2 KPMG Sofy in relation to KPMG

KPMG Sofy is part of the larger KPMG organization and therefore KPMG processes with regard to HR, performance management, ethics and independence are followed. KPMG Sofy has introduced several additional processes that are specific to the KPMG Sofy system. Together these processes form the basis for the Sofy system of control.

KPMG exercises oversight over the Sofy system through financial reporting, periodical management meetings and the quality and risk management department

3.4.1.3 Integrity, Ethics and Codes of Conduct

KPMG has a dedicated ethics and independence program as well as defined professional standards and a code of conduct. The Code of Conduct is intended for use:

- By our leadership and senior management teams, to establish "tone from the top" by underpinning their responsibility for ethical decision-making, reinforcing their position as positive role models and upholding universal compliance with the KPMG Values;
- By new and prospective employees as a guide to the firm they are considering joining;

— By our clients, suppliers, external consultants and contacts, as they seek to understand the nature of the organisation with which they are dealing;

— Most importantly, by all our people, to recognise what is expected of them and the responsibilities resting on each of them to make sure we all adhere to the KPMG Values, for the benefit of each other, our firm, our clients and the wider communities in which we operate.

Upon hiring and each year subsequently, all employees and hired contractors are required to complete an ethics and independence questionnaire and follow the required training. In addition, a whistleblowing hotline has been established by KPMG. The whistleblowing hotline has been setup to offers employees and others to report matters including unethical behavior, fraud, shortcomings in quality systems or any other concerns in an anonymous and confidential matter.

3.4.1.4 HR Policies and Practices

KPMG Sofy has a clearly defined organizational structure in place, supported with regular oversight by supervisory and management personnel. In addition, KPMG and KPMG Sofy have shared formal HR policies and behavioral standards that clearly communicate organizational values, expectations, and ethical standards. Processes include:

— Formal hiring processes that include screening, background checks and skill assessments;

— Onboarding and off-boarding processes;

— Development management processes;

— Training and development processes specifically designed for Sofy.

Development management

Development is one of our main priorities. We devote a great deal of time and attention to the development of our people, to make sure our clients also recognize the expertise and skills of our employees.

The Development Conversation (DC) starts in July or as early as possible. The PDC contains the following:

— A look back over the past year;

— Determining the direction for the coming year;

— An overview of the development needs.

The performance development conversation includes an evaluation of the annual development plan, long term development path, business goals and KPMG's behavioral values.

3.4.1.5 Responsibility for Internal Controls and Risk Management

The Sofy control framework is designed to control the KPMG Sofy system as well as controlling access and managing risk. It establishes the strategic approach, helps ensure that the necessary controls and HR policies and procedures are in place for the organization to meet its objectives, and facilitates performance reviews. Under the responsibility of KPMG Sofy management there are a couple of key roles and governance bodies with regard to internal controls and risk management.

3.4.1.5.1 Sofy Management Team

Sofy management is responsible for developing the company strategy and successfully managing the Sofy processes and team. Sofy management includes a KPMG partner who has the authority to sign formal agreements and make financial decisions.

Sofy management is responsible for exercising oversight over the Sofy system and performance of internal controls.

Operational management is delegated by the KPMG partner to other Sofy management employees.

3.4.1.5.2 Security Manager

The Security Manager is responsible for maintaining a safe and secure environment for customers and employees by establishing and enforcing security policies and procedures; supervising the security of the system and overseeing the operations of Sofy's security solutions. The Security Manager has the authority to manage the infrastructure assets from a security perspective as well as authorizing security-related changes. The Security Manager reports to the Management Team and the Risk and Compliance Manager.

3.4.1.5.3 Risk and Compliance Manager

The Risk and Compliance Manager is responsible for all risk- and compliance-related activities, ensuring that the control framework remains up to date, that new risks are detected promptly and that appropriate mitigating controls are implemented.

His/her responsibilities furthermore include the periodical sign-off of the controls and managing all external audits. The Risk and Compliance Manager has the authority to monitor all risk-related activities and determine risk mitigating actions when required.

3.4.2 Risk Assessment

Sofy Risk Management processes are designed to identify preventive actions and to ensure related measures are implemented. Sofy performs several processes in relation to Risk Management to ensure compliance with all security, confidentiality, availability and processing integrity commitments, including:

— A periodic strategic session where strategic, operational and financial objectives are discussed;
— A periodic risk management session where relevant business and IT risks are discussed;
— The controls as described in the Sofy control framework;
— Continuous monitoring of security and service levels;
— Control self-assessments using the Sofy risk management solution;
— A yearly external audit performed by an independent auditor;
— A periodic external vulnerability scan/penetration test.

Results of these assessments are communicated with management.

The yearly risk management session is performed to identify, assess, and prioritize risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events. Risk Management's objective is to ensure that uncertainty does not deflect the organization's focus away from the business goals. Sofy Risk Management processes are designed to identify preventive actions and to ensure that related measures are implemented. Sofy performs several processes in relation to Risk Management to ensure compliance with all security, confidentiality, availability and processing integrity commitments:

— Identification of potential risk scenarios in relation to both business and IT;
— Assessment of risks (probability and business impact);
— Determination of mitigation strategies;
— Definition of risk response actions for each risk and assignment to a risk owner;
— Changes to and adaption of the Sofy Control Framework.

3.4.3 Monitoring

The management and supervisory personnel of KPMG Sofy monitor the performance and quality of control operations as a normal part of their activities.

3.4.3.1 Periodic Control Reviews

Control self-assessments and reviews of processes are performed by operating units on a periodic basis using the Sofy Risk Management solution. This process includes reviews of system configurations as well as process reviews such as incident management and change management. In addition, a periodic review for each control is performed by the control owner to ensure the effectiveness of the controls.

Results of these reviews are shared with management and actions are taken when required.

3.4.3.2 Service Level Review Board

Sofy has a dedicated Service Level Review Board that is responsible for reviewing the quality of service level management processes to ensure that current and future obligations are met, and that any potential risks are mitigated accordingly. The Service Level Review Board meets regularly to discuss these topics.

3.4.3.3 Evaluation of the system of control

The system of control is evaluated on a periodic basis to ensure that control activities are aligned with the processes and goals of Sofy. This includes an evaluation of the information required to support the functional requirements.

3.4.4 Information and Communication

3.4.4.1 Communication with Employees

Communication with employees is established in several ways. First of all, Sofy is a relatively small team and employees are located in the same office. In terms of formal communication, weekly team meetings are held and periodic newsletters are sent out.

These channels are also used to communicate about changing objectives, changes and operations.

Information regarding the system of control, way of working and processes is shared as part of the onboarding process and the yearly security awareness session.

3.4.4.2 Information provided to User Entities

Information provided to user entities includes Service Level Reports that are prepared and delivered as part of the service level management process. The frequency and level of reporting detail depends on SLA agreements. Generally, Service Level Reports are distributed on a periodic basis and include details about:

— Service Availability;
— Incident Overview;
— Change Overview.

As part of the onboarding process, clients are informed how to report incidents, request changes and ask questions. Confidentiality agreements, service descriptions and service levels are shared during the contracting phase.

3.4.4.3 Whistle-blowing hotline

KPMG has a whistle-blowing hotline in place to allow for anonymous reporting of incidents, unethical behavior or other concerns.

3.5 Subservice organizations

Sofy utilizes Microsoft Azure for its infrastructure including but not limited to computing services, storage, and networks as well as platform services. Microsoft Azure has a SOC2 report for the trust service principles security, availability, processing integrity and confidentiality.

We have implemented monitoring controls at Sofy that are designed to monitor that the SOC2 criteria can be achieved and that any risks related to the effectiveness of Azure controls are managed. These controls include:

— Related party and vendor systems are subject to review as part of the vendor risk management process. Attestation reports (SOC 2 reports) are obtained and evaluated when available. Site visits and other procedures are performed based on the entity's vendor management criteria;
— SOC2 attestation reports of the cloud hosting provider are reviewed periodically as part of the vendor risk management process. Specifically, controls with regards to physical access are evaluated;
— Availability monitoring.

3.6 Significant changes to the system during the year

- Additional controls because of SOC 2 2017 TSP introduction. The following controls are added:
    - Control 101
    - Control 103
    - Control 104
    - Control 105
    - Control 107
    - Control 108
    - Control 120
    - Control 121
- The organisational structure of Sofy has been changed in 2018 to handle further growth of the platform and organisation.
- We keep improving our platform and its architecture. As Sofy is expanding on a global level, we are further automating and standardizing our infrastructure. This allows us to grow while keeping the environment under control.
- Introduced the distinction between Platinum, Gold and Standard contracts. The difference for these contracts is reflected in a different release management frequency. The procedures and safeguards remain the same.