SOC 3 Report
For Split Payments S.L.

An Independent Service Auditor's Report
on Controls Relevant to Security, Confidentiality,
and Privacy

January 03, 2025, to January 30, 2026

AUDIT AND ATTESTATION BY

PRESCIENT
ASSURANCE

Prescient Assurance LLC.
1900 Church Street, Suite 300
Nashville, TN, 37203

CPA

www.prescientassurance.com
info@prescientassurance.com
+1 646 209 7319

Table of Contents

Management's Assertion **4**
Independent Service Auditor's Report **7**
Scope 7
Service Organization's Responsibilities 7
Inherent Limitations 8
Opinion 8
Attachment A **10**
Company Overview and Types of Products and Services Provided 11
The principal service commitments and system requirements 11
The components of the system used to provide the services 12
People 12
System Boundaries 13
The Applicable Trust Services Criteria and the Related Controls Designed to Provide Reasonable Assurance That the Service Organization's Service Commitments and System Requirements Were Achieved 13
Integrity and Ethical Values 13
Commitment to Competence 13
Management's Philosophy and Operating Style 14
Organizational Structure and Assignment of Authority and Responsibility 14
Human Resource Policies and Practices 15
Risk Assessment Process 15
Integration with Risk Assessment 15
Information and Communication Systems 15
Monitoring Controls 16
On-going Monitoring 16
Reporting Deficiencies 16
Complementary Subservice Organization Controls (CSOCs) 16
Any Specific Criterion of the Applicable Trust Services Criteria That is Not Relevant to the System and the Reasons it is Not Relevant 18

SECTION 1

Management's Assertion

Flanks

Restricted Use & Distribution

Management's Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within Split Payments S.L.'s Flanks systems (the system) throughout the period January 03, 2025, to January 30, 2026, to provide reasonable assurance that Split Payments S.L.'s service commitments and system requirements relevant to Security ,Confidentiality, and Privacy were achieved. Our description of the boundaries of the system is presented in Attachment A [A] and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of controls within the system throughout the period January 03, 2025, to January 30, 2026, to provide reasonable assurance that Split Payments S.L.'s service commitments and system requirements were achieved based on the trust services criteria relevant to Security ,Confidentiality, and Privacy (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, in AICPA Trust Services Criteria (With Revised Points of Focus - 2022) (2017 applicable trust services criteria). Split Payments S.L. 's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Attachment A [A].

Split Payments S.L. uses a subservice organization for cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Split Payments S.L., to achieve Split Payments S.L. 's service commitments and system requirements based on the applicable trust services criteria. The description presents Split Payments S.L.'s controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Split Payments S.L.'s controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Split Payments S.L., to achieve Split Payments S.L. 's service commitments and system requirements based on the applicable trust services criteria. The description presents Split Payments S.L.'s controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Split Payments S.L.'s controls.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period January 03, 2025, to January 30, 2026, to provide reasonable assurance that Split Payments S.L. 's service commitments and system requirements were achieved based on the applicable trust services criteria.

DocuSigned by:

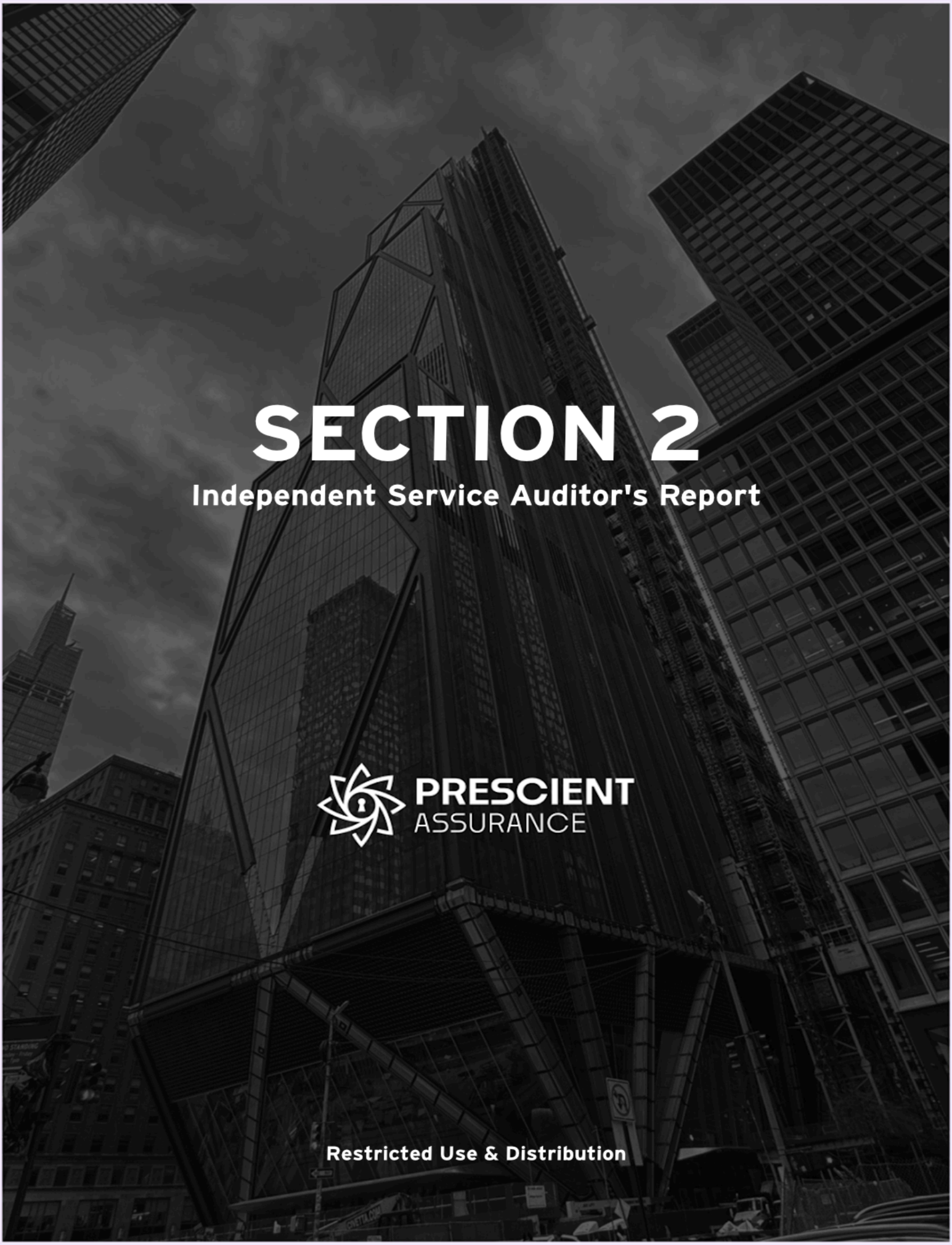
Joaquim de la Cruz

2F39EB3B7DA6464...

Joaquim De La Cruz

CEO

Split Payments S.L.



SECTION 2

Independent Service Auditor's Report

PRESCIENT ASSURANCE

Restricted Use & Distribution

Independent Service Auditor's Report

To: Management of Split Payments S.L.

Scope

We have examined Split Payments S.L.'s ("Split Payments S.L.") accompanying assertion in Section I, titled "Management's Assertion" (the assertion) that the controls within Split Payments S.L.'s Flanks systems (the system) were effective throughout the period January 03, 2025, to January 30, 2026, to provide reasonable assurance that Split Payments S.L.'s service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Confidentiality, and Privacy (applicable trust services criteria) set forth in TSP Section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria) (With Revised Points of Focus - 2022) (2017 applicable trust services criteria).

Split Payments S.L. uses a subservice organization for cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Split Payments S.L. , to achieve Split Payments S.L. 's service commitments and system requirements based on the applicable trust services criteria. The description presents Split Payments S.L.'s controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Split Payments S.L.'s controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that certain complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Split Payments S.L., to achieve Split Payments S.L. 's service commitments and system requirements based on the applicable trust services criteria. The description presents Split Payments S.L.'s controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Split Payments S.L.'s controls. Our examination did not include such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls

Service Organization's Responsibilities

Split Payments S.L. is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Split Payments S.L. 's service commitments and system requirements were achieved. In Section I, Split Payments S.L. has provided the accompanying assertion about the effectiveness of the controls within the system. When preparing its assertion, Split Payments S.L. is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the controls are not effective to achieve Split Payments S.L. service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Split Payments S.L. service commitments and system requirements based on the applicable trust services criteria

Our examination also included performing such other procedures as we considered necessary in the circumstances.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risks that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Split Payments S.L.'s Flanks system was effective throughout the period January 03, 2025, to January 30, 2026, to provide reasonable assurance that Split Payments S.L. service commitments and system requirements were achieved based on the applicable trust services criteria and is fairly stated, in all material respects.

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

Signed by:
Prescient Assurance
3903D025383246D...

Prescient Assurance LLC

March 30, 2026


SECTION 3
Attachment A
flanks
Restricted Use & Distribution

Company Overview and Types of Products and Services Provided

Flanks is a wealth management technology company redefining the advisory services industry. Its solution, Flanks LUME, automates manual tasks and transforms complex wealth data into actionable insights that help advisors get a holistic view of their clients' wealth to make faster, more informed investment and risk management decisions. Flanks was founded in 2019 in Barcelona by software engineers Joaquim de la Cruz and Sergi Lao alongside former Santander Private Banking Global Head Álvaro Morales, and combines advanced technology with deep financial expertise to serve companies like banks, family offices, and tech companies. To date, the company has raised a total of 23.5 million euros from investors.

Flanks provides a SaaS-based wealth management platform that aggregates and processes customer financial data. The system is hosted on Google Cloud Platform, with customer data encrypted at rest and in transit. Access is controlled through role-based permissions and monitored under documented security policies.

The principal service commitments and system requirements

Flanks designs its processes and procedures related to the system to meet its objectives. Those objectives are based on the service commitments that Flanks makes to user entities, the laws, and regulations that govern the provision of the services, and the financial, operational, and compliance requirements that Flanks has established for the services. The system services are subject to the Security, Confidentiality, and Privacy commitments established internally for its services.

Flanks' commitments to users are communicated through Service Level Agreements (SLAs) or Master Subscription Agreements (MSAs), online Privacy Policy and Terms & Conditions, and in the description of the service offering provided online.

Flank's security commitments include (but are not limited to) the following:

- System features and configuration settings designed to authorize user access while restricting unauthorized users from accessing information not needed for their role
- Use of intrusion detection systems to prevent and identify potential security attacks from users outside the boundaries of the system
- Regular vulnerability scans over the system and network, and penetration tests over the production environment
- Operational procedures for managing security incidents and breaches, including notification procedures
- Use of encryption technologies to protect customer data both at rest and in transit
- Use of data retention and data disposal procedures.

Flank's confidentiality commitments include (but are not limited to) the following:

- The use of encryption technologies to protect system data both at rest and in transit
- Confidentiality and non-disclosure agreements with employees, contractors, and third parties
- Confidential information must be used only for the purposes explicitly stated in agreements between the company and user entities

Flank's confidentiality commitments include (but are not limited to) the following:

- Adherence to relevant privacy laws and regulations, to ensure that personal data is collected, processed, and stored in compliance with legal requirements.
- Implementation of data minimization practices to ensure that only the necessary personal data is collected and retained for the intended purposes.
- Obtaining explicit consent from data subjects for the collection, use, and sharing of their personal information, where applicable.
- Implementation of data subject rights management processes, including the ability to access, correct, or delete personal information upon request.
- Regular privacy impact assessments to identify and mitigate risks to personal data and ensure ongoing compliance with privacy regulations.
- Secure data transfer mechanisms and strict data-sharing agreements with third parties to protect personal information during transfers

The components of the system used to provide the services

People

The company employs dedicated team members to handle major product functions, including operations, and support. The IT/Engineering Team monitors the environment, as well as manages data backups and recovery. The Company focuses on hiring the right people for the right job as well as training them both on their specific tasks and on the ways to keep the company and its data secure.

This report does not include the Cloud Hosting Services provided by GCP at multiple facilities.

Flanks has a staff organized in the following functional areas:

Management: Individuals who are responsible for enabling other employees to perform their jobs effectively and for maintaining security and compliance across the environment.

Operations: Responsible for maintaining the availability of production infrastructure, and managing access and security for production infrastructure. Only members of the Operations team have access to the production environment. Members of the Operations team may also be members of the Engineering team.

Information Technology: Responsible for managing laptops, software, and other technology involved in employee productivity and business operations.

Product Development: Responsible for the development, testing, deployment, and maintenance of the source code for the system. Responsible for the product life cycle, including adding additional product functionality.

System Boundaries

The boundaries of the Flanks are the specific aspects of the Company's infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of the Flanks.

This report does not include the Cloud Hosting Services provided by GCP at multiple facilities.

The Applicable Trust Services Criteria and the Related Controls Designed to Provide Reasonable Assurance That the Service Organization's Service Commitments and System Requirements Were Achieved

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of Flanks control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Flanks ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

Specific control activities that the service organization has implemented in this area are described below:

- The company requires employees to acknowledge a code of conduct at the time of hire. Employees who violate the code of conduct are subject to disciplinary actions in accordance with a disciplinary policy.
- The company requires employees to sign a confidentiality agreement during onboarding.
- The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.

Commitment to Competence

Flanks management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for jobs and how those levels translate into the requisite skills and knowledge.

Specific control activities that the service organization has implemented in this area are described below:

- Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.
- The company requires employees to complete security awareness training within thirty days of hire and at least annually thereafter.

Management's Philosophy and Operating Style

Flanks management team must balance two competing interests: continuing to grow and develop in a cutting edge, rapidly changing technology space while remaining excellent and conservative stewards of the highly sensitive data and workflows our customers entrust to us.

The management team meets frequently to be briefed on technology changes that impact the way Flanks can help customers build data workflows, as well as new security technologies that can help protect those workflows, and finally any regulatory changes that may require Flanks to alter its software to maintain legal compliance. Major planned changes to the business are also reviewed by the management team to ensure they can be conducted in a way that is compatible with our core product offerings and duties to new and existing customers.

Specific control activities that the service organization has implemented in this area are described below:

- The company's Board of Directors or a relevant subcommittee is briefed by senior management at least annually on the state of the company's cybersecurity and privacy risk. The leadership provides feedback and direction to management as needed.
- The company's Board of Directors has sufficient expertise to oversee management's ability to design, implement, and operate information security controls. The leadership engages third-party information security experts and consultants as needed.

Organizational Structure and Assignment of Authority and Responsibility

Flanks' organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

Flanks' assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

Specific control activities that the service organization has implemented in this area are described below:

- The company maintains an organizational chart that describes the organizational structure and reporting lines.
- The company's information security policies and procedures are documented and reviewed at least annually.

Human Resource Policies and Practices

Flanks' success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. Flanks human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

Specific control activities that the service organization has implemented in this area are described below:

- The company requires employees to acknowledge a code of conduct at the time of hire. Employees who violate the code of conduct are subject to disciplinary actions in accordance with a disciplinary policy.
- The company requires employees to sign a confidentiality agreement during onboarding.
- The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.

Risk Assessment Process

Flanks' risk assessment process identifies and manages risks that could potentially affect Flanks ability to provide reliable and secure services to our customers. As part of this process, Flanks maintains a risk register to track all systems and procedures that could present risks to meeting the company's objectives. Risks are evaluated by likelihood and impact, and management creates tasks to address risks that score highly on both dimensions. The risk register is reevaluated annually, and tasks are incorporated into the regular Flanks product development process so they can be dealt with predictably and iteratively.

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of Flanks system; as well as the nature of the components of the system result in risks that the criteria will not be met. Flanks addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the criteria are met. Because each system and the environment in which it operates are unique, the combination of risks to meeting the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the system, Flanks management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

Information and Communication Systems

Information and communication are an integral component of Flanks internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations.

Flanks uses several information and communication channels internally to share information with management, employees, and customers. Flanks uses chat systems and email as the primary internal and external communications channels.

Structured data is communicated internally via SaaS applications and project management tools. Finally, Flanks uses in-person and video “all hands" meetings to communicate company priorities and goals from management to all employees.

Monitoring Controls

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. Flanks management performs monitoring activities to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Employee activity and adherence to company policies and procedures is also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

On-going Monitoring

Flanks management conducts quality assurance monitoring on a regular basis and additional training is provided based upon results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications.

Management's close involvement in Flanks operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing any control's weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of Flanks personnel.

Reporting Deficiencies

Our internal risk management tracking tool is utilized to document and track the results of on-going monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks, and instructions for escalation are supplied to employees in company policy documents. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool.

Complementary Subservice Organization Controls (CSOCs)

The description does not extend to the services provided by GCP (the subservice organization). Section 4 of this report and the description of the system only cover the relevant trust services criteria and related controls in support of the achievement of Split Payments S.L. service commitments and system requirements and exclude the related controls of the subservice organization.

Although the subservice organization has been carved out for the purposes of this report, Split Payments S.L. 's management has assumed, in the design of the system, that certain complementary subservice organization controls (CSOCs) would be implemented by the subservice organization. Such controls are necessary, in combination with controls at Split Payments S.L. to provide reasonable assurance that Split Payments S.L.'s service commitments and system requirements were achieved. Because the related service commitments and system requirements can only be achieved if the CSOCs are suitably designed and operating effectively during the period January 03, 2025 to January 30, 2026, each user entity must evaluate Split Payments S.L.'s controls, related tests of controls, and results of tests described in section 4 of this report, considering the types of related CSOCs expected to be implemented at the subservice organization as shown below.

Subservice Organization	Services Provided	Criteria	Expected CSOCs
GCP	Infrastructure Hosting	CC6.4	Physical access to data centers is approved by an authorized individual.
		CC6.4	Physical access rights are revoked in a timely manner when no longer required.
		CC6.4	Physical access to data centers is reviewed periodically by appropriate personnel.
		CC6.4	Data center facilities are monitored using physical security monitoring controls, including video surveillance.
		CC6.4	Access to server locations is managed by electronic access control devices.
		CC7.2	Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.
		CC7.5	Backup and recovery capabilities are maintained to support restoration of systems following security incidents or system failures.
		CC8.1	Changes are reviewed for business impact and approved by authorized personnel prior to migration to production.
		C1.2	Production media is securely decommissioned, physically destroyed, and verified prior to leaving the data center.

Management of Split Payments S.L. receives and reviews independent third-party assessment reports of its subservice organization annually. In addition, Split Payments S.L. Management monitors the services performed by the subservice organization to determine whether operations and controls expected to be implemented at the subservice organization are suitably designed and operating effectively. Management monitors the subservice organization status page to stay informed of any changes in the services performed and has a customer support portal to relay any issues or concerns to subservice organization management.

Any Specific Criterion of the Applicable Trust Services Criteria That is Not Relevant to the System and the Reasons it is Not Relevant

There were no specific Security, Confidentiality, and Privacy Trust Services Criteria as set forth in TSP Section 100 that were not relevant to the Flanks system as presented in this report.