Independent Assurance Report on Axient Pty Ltd's Description of its System and on the Suitability of the Design of its Controls Relevant to the Security, Availability and Confidentiality Trust Services Criteria (SOC 2)

Prepared in accordance with the following:

AT-C section 105: Concepts Common to All Attestation Engagements

AT-C section 205: Assertion-Based Examination Engagements

Contents

Section I

ASSERTION OF AXIENT PTY LTD MANAGEMENT

ASSERTION OF AXIENT PTY LTD MANAGEMENT

16 October 2024

We have prepared the accompanying description of Axient Pty Ltd's ('Axient') Xfax Software as Service system for the purposes of the independent assurance report. We have prepared the Description in accordance with the following description criteria ('Description Criteria'):

- SOC 2: the criteria for a description of a service organization's system in DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (AICPA, Description Criteria) with regards to the Description.

The Description is intended to provide report users with information about the Axient Xfax Software as Service system (the 'System') that may be useful when assessing the risks arising from interactions with Axient's system. This includes the controls that Axient has designed and implemented to provide reasonable assurance that its service commitments and system requirements were achieved based on the following agreed criteria ('Agreed Criteria'):

- SOC 2: the trust services criteria relevant to Common Criteria/Security, Availability, and Confidentiality (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).

Axient uses Microsoft Azure ('Microsoft Azure' or 'subservice organization') to provide cloud hosting services. The Description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Axient, to achieve Axient's service commitments and system requirements based on the Agreed Criteria. The Description presents Axient's controls, the Agreed Criteria, and the types of complementary subservice organization controls assumed in the design of Axient'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 are necessary, along with controls at Axient, to achieve Axient's service commitments and system requirements based on the Agreed Criteria. The Description presents Axient's controls, the Agreed Criteria, and the complementary user entity controls assumed in the design of Axient's controls.

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

a. the Description presents Axient's Xfax that was designed and implemented as of 10 October 2024, in accordance with the Description Criteria; and
b. the controls stated in the Description were suitably designed as of 10 October 2024, to provide reasonable assurance that Axient's service commitments and system requirements would be achieved based on the Agreed Criteria, if the controls operated effectively as of that date, and if the subservice organization and user entities applied the complementary controls assumed in the design of Axient's controls as of that date.

Mark Howarth
Managing Director
Axient Pty Ltd

Section II

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Axient Pty Ltd

Scope

We have examined Axient Pty Ltd's ('Axient') accompanying description of its Xfax Software as Service system (the 'Description') which has been prepared for the purposes of the independent assurance report.

Axient prepared the Description based on the following description criteria ('Description Criteria'):

- SOC 2: the criteria for a description of a service organization's system in DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (AICPA, Description Criteria) with regards to the Description.

The Description is intended to provide report users with information about Axient's Xfax Software as Service system (the 'System') that may be useful when assessing the risks arising from interactions with Axient's system. This includes the controls that Axient has designed and implemented to provide reasonable assurance that its service commitments and system requirements were achieved based on the following agreed criteria ('Agreed Criteria'):

- SOC 2: the trust services criteria relevant to Common Criteria/Security, Availability, and Confidentiality (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).

Axient uses Microsoft Azure ('Azure' or 'subservice organization') to provide cloud hosting services. The Description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Axient, to achieve Axient's service commitments and system requirements based on the Agreed Criteria. The complementary subservice organization controls have been reviewed by Axient management. 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 includes complementary user entity controls that are necessary, along with controls at Axient, to achieve Axient's service commitments and system requirements based on the Agreed Criteria. The Description presents Axient's controls, the Agreed Criteria, and the complementary user entity controls assumed in the design of Axient's controls. The complementary user entity controls have not been assessed by our examination and remain the responsibility of those related entities to complete their own review.

Service Organization's Responsibilities

Axient is responsible for its service commitments and system requirements and for designing and implementing effective controls within the system to provide reasonable assurance that Axient's service commitments and system requirements were achieved. Axient has provided the accompanying assertion titled "Assertion of Axient Management" (the 'Assertion') about the Description and the suitability of the design of the controls described therein to provide reasonable assurance that the service commitments and system requirements would be achieved based on the Agreed Criteria. Axient is also responsible for preparing the Description and Assertion, including the completeness, accuracy, and method of presentation of the Description and Assertion; providing the services covered by the Description; selecting the applicable Agreed Criteria and stating the related controls in the Description; and identifying the risks that threaten the achievement of the Axient's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the Description and on the suitability of the design of controls stated in the Description based on our examination. Our examination was conducted in accordance with AT-C 105 and AT-C 205 put forth by the Auditing Standards Board (ASB) of the American Institute of Certified Public Accountants (AICPA). Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects:

- The Description is presented in accordance with the Description Criteria.
- The controls stated in the Description were suitably designed.

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

An examination of the Description of Axient's system and the suitability of the design of controls involves the following:

- Obtaining an understanding of the system and Axient's service commitments and system requirements.
- Assessing the risks that the Description is not presented in accordance with the Description Criteria and that controls were not suitably designed.
- Performing procedures to obtain evidence about whether the Description is presented in accordance with the Description Criteria.
- Performing procedures to obtain evidence about whether controls stated in the Description were suitably designed to provide reasonable assurance that Axient achieved its service commitments and system requirements based on Agreed Criteria.
- Evaluating the overall presentation of the Description.

Inherent Limitations

The Description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual report users may consider important to meet their informational needs.

Because of the inherent limitations of any internal control structure it is possible that, even if the controls are suitably designed and implemented as designed, once the controls are in operation the control objectives may not be achieved so that fraud, error, or non-compliance with laws and regulations may occur and not be detected.

An assurance engagement on the implementation of controls at a specified date does not provide assurance on whether the controls operated effectively as designed or will operate effectively in the future. Any projection of the outcome of the evaluation of the suitability of the design of controls to future periods is subject to the risk that the controls may become unsuitable because of changes in conditions.

Opinion

In our opinion, in all material respects,

1) the Description presents Axient's Xfax Software as Service system that was designed and implemented as of 10 October 2024, in accordance with the Description Criteria; and
2) the controls stated in the Description were suitably designed as of 10 October 2024, to provide reasonable assurance that Axient's service commitments and system requirements would be achieved based on the Agreed Criteria, if its controls operated effectively throughout that period and if the subservice organization and user entities applied the complementary controls assumed in the design of Axient's controls as of that date.

Restricted Use

This report is intended solely for the information and use of Axient, user entities of Axient's Xfax, business partners of Axient subject to risks arising from interactions with the Xfax, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators 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, business partners, subservice organizations, and other parties
- Internal control and its limitations
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services
- The Agreed Criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements 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

AssuranceLab CPAs LLC
Austin, Texas
United States
16 October 2024

Section III

AXIENT PTY LTD'S DESCRIPTION OF ITS SYSTEM

OVERVIEW OF OPERATIONS

Company Background

Axient Pty Ltd ('Axient') was founded in January 2000 providing digital fax software, technical services including presales, implementation, and ongoing service desk support. In 2000, Axient's vision for the business was to give customers value by automating the sending and receiving of documents.

In 2024, Axient's vision is to be a global provider of document exchange software for business-critical, time-sensitive documents, connecting businesses with their peers in finance, banking, insurance and health. Axient's clients include medium to large organisations, software vendors and partners.

Description of Services Provided

The Axient range of Cloud Computing Services is built on the Microsoft Azure platform and the Microsoft .NET Framework technology stack, ensuring security, compliance, and reliability. This includes Xfax, a secure solution for cloud-based document exchange; Xconnect, facilitating seamless connectivity between customers and the Xfax service; SendMail, provides secure and efficient email communication with built in tracking capabilities ensuring reliable delivery and event monitoring; and DocumentXchange , designed for secure, encrypted, document sharing among peers on the Xfax network.

Principal Service Commitments and System Requirements

Axient has established processes, policies, and procedures to meet its objectives related to its Xfax (the 'System'). Those objectives are based on the purpose, vision, and values of Axient as well as commitments that Axient makes to user entities, the requirements of laws and regulations that apply to Axient's activities, and the operational requirements that Axient has established.

Commitments are documented, and communicated in customer agreements, as well as in public descriptions of the System. The operational requirements are communicated in Axient's processes, policies and procedures, system design documentation, and customer agreements. This includes policies around how the System is designed and developed, how the System is operated, how the system components are managed, and how employees are hired, developed, and managed to support the System.

Components of the System

Infrastructure

Axient's primary infrastructure used to provide the System includes the cloud hosted networking, compute and database components of Microsoft Azure.

System	Type	Description
Azure Virtual Machines	Cloud Compute	Service to run virtual machines.
Azure SQL Database	Data Storage	Storage of client data.
Azure Firewall	Network Firewall	A cloud-native network firewall security service that provides threat protection for cloud workloads running in Azure.
Cloudflare	Network Services	DNS, load balancing, DDOS protection, web firewall and TLS encryption.

System	Type	Description
Azure Key Vault	Encryption	A cloud service to securely store keys, passwords, certificates, and other secrets.

Software

Primary software is used to support Axient's system.

Software	Purpose
Xfax	The Software as Service system provided to Axient customers.
Azure Defender	Cloud security posture management (CSPM) and cloud workload protection (CWP) that finds weak spots across cloud configurations.
Microsoft Entra ID	Authentication software used to identify and authenticate users for access control to the systems.
Azure Security Center	Monitoring and managing the security of virtual machines and other cloud computing resources within the Microsoft Azure public cloud.
LastPass	Enterprise password manager used to store authentication secrets and strengthen password security.
Intune	Mobile device management software used to track and manage security policies on endpoint devices.
Sentinel One, Cylance	Anti-virus software used to protect endpoint devices from malware.
Bitbucket	Source code repository used to manage the software code and version control.
Nessus	Vulnerability scanning software to identify, log and resolve technical vulnerabilities.
ConnectWise Manage	Ticketing software used to log events and requirements to support the internal controls.
Office 365	Microsoft's suite of enterprise productivity, collaboration, and communication tools.

People

Axient has 5 people that are organized into the following functional areas:

- Leadership: The executive level is responsible for corporate governance.
- Product: Responsible for managing the roadmap of requirements and balancing the Engineering team priorities.
- Engineering: Responsible for building and maintaining the infrastructure and software.
- Customer Success: Responsible for the customer experience, support and services.
- Implementations: Responsible for enterprise implementations and integrations to onboard and set up new customers.

- Project Management: Responsible for enterprise delivery of programs and projects to support the objectives.
- Operations: Responsible for monitoring and supporting robust and effective company and system operations.
- Risk and Compliance: Responsible for identification, assessment, treatment and monitoring to manage risks and support compliance.
- Partnerships: Responsible for managing partnerships with complementary service providers.
- Sales: Responsible for onboarding new customers and aligning requirements.
- Marketing: Responsible for branding, market positioning and attracting customers.

Data

The data collected and processed by Axient includes the following types:

- Basic personal details: name, email, contact details
- User activity: user activity within the software
- Financial account information: account balances, transactions
- Business information: proprietary data of business activities and property
- Medical data: personal health information

Processes, Policies and Procedures

Processes, policies, and procedures are established that set the standards and requirements of the System. All personnel are expected to comply with Axient's policies and procedures that define how the System should be managed. The documented policies and procedures are shared with all Axient's employees and can be referred to as needed.

Physical Security

The critical infrastructure and data of the Systems are hosted by Azure. There are no trusted local office networks. As such, Azure is responsible for the key physical security controls that support the System.

Logical Access

Axient's logical access processes restrict access to the infrastructure, software, and data to only those that are authorized for access. Access is based on the concept of least privilege that limits the system components and access privileges to the minimum level required to fulfil job responsibilities.

The in-scope systems require approval and individual authentication practices prior to gaining access. Microsoft Entra ID authentication software is used for identity management and single sign-on. Access management processes are followed to ensure new and modified access is approved, terminated users access is removed, and access rights are quarterly reviewed and adjusted when no longer required. Additional information security policies and procedures require Axient employees to use the systems and data in an appropriate and authorized manner.

Automated and manual security practices are used to protect the perimeter security and network to prevent unauthorized access attempts and tampering from third-party actors with malicious intent. Those include applying encryption of data and communications, annual testing for and remediation of technical vulnerabilities and applying network controls like firewalls and event monitoring to prevent and detect unauthorized activity.

Axient employee workstations are required to follow defined security practices to mitigate the risks of data leakage and malware that may compromise the devices, system access and sensitive data. Microsoft InTune mobile device management software is used to monitor, systematically enforce device requirements, and provide remote management capabilities for the workstations.

System Operations

Backup and restoration procedures for the System are defined and followed. The System is monitored through a combination of automated and manual processes to prevent and detect any issues with the infrastructure, software, and data. Alerts and logs are monitored with incident management processes defined for handling and resolving adverse events.

Axient's critical infrastructure and data are hosted by Microsoft Azure with multiple availability zones to provide failover capability in the event of an outage of one of the data centers. Redundancy and disaster recovery in continuity considerations are built into the system design of Microsoft Azure to support Axient's availability objectives. These are supported by the system monitoring, incident management processes and defined recovery and continuity plans.

Change Control

Backup and restoration procedures for the System are defined and followed. The System is monitored through a combination of automated and manual processes to prevent and detect any issues with the infrastructure, software, and data. Alerts and logs are monitored with incident management processes defined for handling and resolving adverse events.

Axient's critical infrastructure and data are hosted by Azure with multiple availability zones to provide failover capability in the event of an outage of one of the data centers. Redundancy, disaster recovery, and continuity considerations are built into the system design of Azure to support Axient's availability objectives. These are supported by the system monitoring, incident management processes and defined recovery and continuity plans.

Data Governance

Axient uses data to support the System's objectives and services. An approach to effective data governance has been established to understand and communicate the data that are used in the System, the objectives and requirements of that data, and the commitments of Axient.

Established processes, policies, and procedures define the operational requirements for data governance, including how data is classified, handled, and used by the System in supporting the objectives and services.

Boundaries of the System

The scope of this report includes the Xfax (the 'System'). This report does not include the cloud hosting services provided by Microsoft Azure.

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, INFORMATION AND COMMUNICATION, AND MONITORING

Control Environment

Integrity and Ethical Values

The effectiveness of controls is dependent on the integrity and ethical values of the people who implement, manage, and monitor them. Integrity and ethical values are important foundations of Axient's control environment, affecting the design, implementation, and monitoring of the controls. Integrity and ethical behavior are supported by Axient's culture, governance, hiring and onboarding practices, ethical and behavioral standards, the way those are communicated, and how they are reinforced in practice. 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.

Commitment to Competence

Axient's competence of employees includes the knowledge and skills necessary to accomplish employees' roles and responsibilities, in support of Axient's objectives and commitments. Management's commitment to competence includes careful consideration of the competence levels required for each role, the requisite skills, knowledge, and experience, and the actual performance of individuals, teams and the company as a whole.

Management's Philosophy and Operating Style

Axient's management philosophy and operating style is a purpose-driven, risk-based approach to pursuing the company objectives and satisfying Axient's commitments. Risk taking is an essential part of pursuing the objectives. A formal approach is taken to understanding those risks and being deliberate about which risks are acceptable, and where risk mitigation actions are required.

Organizational Structure and Assignment of Authority and Responsibility

Axient's organizational structure provides the framework within which its activities for achieving the objectives are planned, executed, managed, and monitored. An organizational structure has been developed to suit Axient's needs and is revised over time as the company grows and requirements change.

Roles and responsibilities are further established and communicated through documented policies, and job descriptions, as part of individual performance review processes, reviewing and communicating team and functional performance, and the various operational team and governance meetings.

Human Resource Policies and Practices

Axient's employees are the foundation for achieving the objectives and commitments. Axient's hiring, onboarding and human resource practices are designed to attract, develop, and retain high-quality employees. That includes training and development, performance evaluations, compensation, and promotions, providing personal support and perks for individuals, recognizing team and company success, and building a culture of alignment to a shared purpose and vision. It also includes disciplinary processes and business planning to avoid single-person dependencies to ensure the objectives and commitments are not reliant on individuals.

Risk Assessment Process

Risk Assessments

Axient's risk assessment process identifies and manages risks that threaten achievement of the objectives and commitments. This includes risks that may affect the security, reliability or integrity of the services provided to user organizations and other interested stakeholders.

A formal process is followed to identify, assess, treat, and monitor the risks to ensure the risks are aligned to the risk appetite and objectives of Axient, and mitigated or avoided where appropriate. Risks identified in this process include but is not limited to:

- Operational risk – changes in the environment, staff, or management personnel, reliance on third parties, and threats to security, reliability, and integrity of Axient's operations.
- Strategic risk – new technologies, changing business models, and shifts within the industry.
- Compliance – legal and regulatory obligations and changes.
- Financial – the sustainability of Axient and resources supporting the objectives.

These risks are identified by Axient management, employees, and third-party stakeholders, and updated in the risk register as a single source of monitoring the risks. The formal risk assessments ensure the ongoing commitment of management, and support completeness and an evolving view of the risk landscape in Axient's context.

Integration with Risk Assessment

Established internal controls include Axient's policies, procedures, automated system functions and manual activities. The controls are designed and implemented to address the identified risks, and to meet the obligations and criteria set by laws, regulations, customer commitments and other compliance obligations. The controls follow a continual improvement methodology in consideration of the costs and benefits of such control improvements and recognizing the changing landscape and requirement of those controls as Axient grows, and the associated risks change

Information and Communications Systems

Information and communication are a core part of Axient's 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 Axient's operations effectively. The information and communication systems consider the internal control requirements, operating requirements, and the needs of interested parties including employees, customers, third-party vendors, regulators, and shareholders.

The information and communication systems include central tracking systems that support Axient's established processes, as well as various meetings, and documented policies, procedures, and organizational knowledge.

Monitoring Controls

Management monitors the controls to ensure that they are operating as intended and that controls are modified and continually improved over time. Leadership, culture, and communication of the controls are important enablers to the effectiveness of the controls in practice. This ensures buy-in amongst the employees and empowers Axient's team and individuals to prioritize the performance and continual improvement of the controls. Evaluations are performed during the course of business, in management reviews, and by independent auditors to assess the design and operating effectiveness of the controls. Deficiencies that are identified are communicated to responsible control owners to agree remediation actions or re-enforce the control requirements and importance. Corrective actions are tracked with agreed

timelines and ownership for remediation with ownership of management and the Board, for ensuring appropriate actions are completed in a timely manner.

Changes to the System in the Last 12 Months

No significant changes have occurred to the services provided to user entities in the 12 months preceding the end of the examination date.

Incidents in the Last 12 Months

No significant incidents have occurred to the services provided to user entities in the 12 months preceding the end of the examination date.

Criteria Not Applicable to the System

All Common Criteria/Security, Availability, and Confidentiality Trust Services Criteria were applicable to Axient's Xfax.

COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS

This report does not include the cloud hosting services provided by Microsoft Azure.

Subservice Description of Services

Microsoft Azure, commonly referred to as Azure, is a cloud computing service created by Microsoft for building, testing, deploying, and managing applications and services through Microsoft-managed data centers.

Complementary Subservice Organization Controls

Axient's services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the Agreed Criteria related to Axient's services to be solely achieved by Axient control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of Axient.

The following subservice organization controls should be implemented by Azure to provide additional assurance that the Agreed Criteria described within this report are met.

Subservice Organization – Microsoft Azure		
Category	**Criteria**	**Control**
Common Criteria/ Security	CC6.1-CC6.8	Logical access measures are established and followed to ensure access to systems and data is restricted to authorized personnel with technical safeguards and ongoing assessments to reduce the risk of system and data breaches.
	CC6.4	Procedures have been established to restrict physical access to the data center to authorized employees, vendors, contractors, and visitors.
		Physical access mechanisms (e.g., access card readers, biometric devices, man traps / portals, cages, locked cabinets) have been implemented and are administered to restrict access to authorized individuals.
		Security verification and check-in are required for personnel requiring temporary access to the interior data center facility including tour groups or visitors.
		The data center facility is monitored 24x7 by security personnel.
		Physical access to the data center is reviewed quarterly and verified by the data center management team.
	CC7.1-CC7.5	Incident management and response policies and procedures are established and followed to identify, analyze, classify, respond to and resolve adverse events.
	CC8.1	Formal processes are established and followed to ensure system changes are documented, tracked, prioritized, developed, tested and approved prior to deployment into production.
Availability	A1.2	Azure has developed a Business Continuity and Disaster Recovery (BC / DR) Standard Operating Procedure and documentation that includes the defined information security and availability requirements.

Subservice Organization – Microsoft Azure		
Category	**Criteria**	**Control**
		The BCP team conducts testing of the business continuity and disaster recovery plans established for Azure services, per the defined testing schedule for different loss scenario. Each loss scenario is tested at least annually. Issues identified during testing are resolved and plans are updated accordingly.
		Backups of key Azure service components and secrets are performed regularly and stored in fault-tolerant (isolated) facilities. Backups are monitored and backup errors are investigated and followed-up on appropriately.
		Critical Azure components have been designed with redundancy to sustain isolated faults and minimize disruptions to customer services.
		Data Protection Services (DPS) backs up data for properties based on a defined schedule and upon request of the properties. Data is retained according to the data type identified by the property. DPS investigates backup errors and skipped files and follows up appropriately.
		Customer data is automatically replicated within Azure to minimize isolated faults. Customers are able to determine geographical regions of the data processing and storage, including data backups.
		Azure services are configured to automatically restore customer services upon detection of hardware and system failures.
		Data center Management team maintains and tests data center-managed environmental equipment within the facility according to documented policy and maintenance procedures.
		Environmental controls have been implemented to protect systems inside data center facilities, including temperature and heating, ventilation, and air conditioning (HVAC) controls, fire detection and suppression systems, and power management systems.

Axient management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the relevant Agreed Criteria through written contracts and published terms of service. In addition, Axient performs monitoring of the subservice organization controls by reviewing attestation reports and monitoring the performance of the subservice organization controls.

COMPLEMENTARY USER ENTITY CONTROLS

Axient's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the Agreed Criteria related to Axient's services to be solely achieved by Axient control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Axient's.

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

User entities are responsible for:

- Understanding and complying with Axient's terms of service.
- Notifying Axient of changes made to technical or administrative contact information.
- Providing and maintaining an approvers list for changes to the services, configurations, or access.
- Administering their users' access rights including approval, removal, and periodic review to ensure access is appropriate.
- Performing any required risk assessments and approvals when using pre-built integrations available with Axient's services.
- Performing any required risk assessments and approvals for using Axient's open application programming interface (API), and notifying Axient of any identified vulnerabilities, security breaches or system failures when using the APIs.
- Ensuring the supervision, management, and control of the use of Axient's services by their personnel.
- Developing their own disaster recovery and business continuity plans that address the inability to access or utilize Axient services for any critical reliance on these services.
- Immediately notifying Axient of any actual or suspected information security breaches or system failures.

SOC 2 TRUST SERVICES CRITERIA

Trust Services Categories Selected by Axient

Common Criteria (*to all Categories*)
Security refers to the protection of i. information during its collection or creation, use, processing, transmission, and storage and ii. systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

Availability
Availability refers to the accessibility of information used by the entity's systems, as well as the products or services provided to its customers. The availability objective does not, in itself, set a minimum acceptable performance level; it does not address system functionality (the specific functions a system performs) or usability (the ability of users to apply system functions to the performance of specific tasks or problems). However, it does address whether systems include controls to support accessibility for operation, monitoring, and maintenance.

Confidentiality
Confidentiality addresses the entity's ability to protect information designated as confidential from its collection or creation through its final disposition and removal from the entity's control in accordance with management's objectives. Information is confidential if the custodian (for example, an entity that holds or stores information) of the information is required to limit its access, use, and retention and restrict its disclosure to defined parties (including those who may otherwise have authorized access within its system boundaries). Confidentiality requirements may be contained in laws or regulations or in contracts or agreements that contain commitments made to customers or others. The need for information to be confidential may arise for many different reasons. For example, the information may be proprietary, intended only for entity personnel. Confidentiality is distinguished from privacy in that privacy applies only to personal information, whereas confidentiality applies to various types of sensitive information. In addition, the privacy objective addresses requirements regarding collection, use, retention, disclosure, and disposal of personal information. Confidential information may include personal information as well as other information, such as trade secrets and intellectual property.

Section IV

CRITERIA AND RELATED CONTROLS

SOC 2 TRUST SERVICES CRITERIA

Trust Services Criteria for the Security Category

Common Criteria 1: Control Environment

CC1.0	Criteria	Control Activity
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	Background checks are conducted for new hires prior to onboarding.
		The security policies set out the requirements for managing information security across the organisation's operations.
		The code of conduct establishes workforce conduct standards of integrity, ethical values, and appropriate behaviour to support a secure and effective working environment.
		The acceptable use policy sets out the roles, responsibilities and requirements to maintain the security of systems, data and endpoint devices.
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Axient's board of directors meets at least semi-annually and maintains meeting minutes.
		The board of directors maintains oversight and provides support for the information security program with briefings at least annually.
		Axient's board of directors has a documented charter that outlines its oversight responsibilities for internal control and information security.
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	The documented organization chart outlines the roles, functional responsibilities and reporting lines for Axient personnel.
		Job descriptions are documented to support the hiring of suitable candidates and to communicate the key job responsibilities of each individual.
		Axient's set of information security policies cover the roles, responsibilities and requirements to support effective internal control that support the information security objectives.

CC1.0	Criteria	Control Activity
		Management has established defined roles and responsibilities to oversee implementation of the information security policy across the organization.
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Background checks are conducted for new hires prior to onboarding.
		Axient's set of information security policies cover the roles, responsibilities and requirements to support effective internal control that support the information security objectives.
		The code of conduct establishes workforce conduct standards of integrity, ethical values, and appropriate behaviour to support a secure and effective working environment.
		Security awareness training is conducted for Axient employees at least annually.
		Axient evaluates the performance of all employees through a formal, annual performance review.
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	The documented organization chart outlines the roles, functional responsibilities and reporting lines for Axient personnel.
		Job descriptions are documented to support the hiring of suitable candidates and to communicate the key job responsibilities of each individual.
		The code of conduct establishes workforce conduct standards of integrity, ethical values, and appropriate behaviour to support a secure and effective working environment.
		Management has established defined roles and responsibilities to oversee implementation of the information security policy across the organization.
		The acceptable use policy sets out the roles, responsibilities and requirements to maintain the security of systems, data and endpoint devices.
		Axient evaluates the performance of all employees through a formal, annual performance review.

Common Criteria 2: Information and Communication

CC2.0	Criteria	Control Activity
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	The network security policy establishes the roles, responsibilities and requirements for securing the network with cryptographic controls, security hardening and network monitoring.
		Axient performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are logged and planned where weaknesses or potential improvements are identified.
		Axient maintains an architecture diagram to document the system boundaries and support the functioning of internal control.
		The asset management policy establishes Axient's scope of information assets and requirements for how those are tracked and managed accordingly.
		The information assets are identified, classified and centrally logged for ongoing monitoring and governance.
CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Axient's set of information security policies cover the roles, responsibilities and requirements to support effective internal control that support the information security objectives.
		The security policies set out the requirements for managing information security across the organisation's operations.
		Security awareness training is conducted for Axient employees at least annually.
		Established incident response plans document the potential events, pre-planned response steps and communication requirements to ensure incidents are handled effectively.
		The acceptable use policy sets out the roles, responsibilities and requirements to maintain the security of systems, data and endpoint devices.
		The incident management policy defines the contacts and methods for employees to report security-related incidents and concerns.

CC2.0	Criteria	Control Activity
		The incident management policy defines the roles, responsibilities and requirements for identifying, classifying and resolving incidents, including devising lessons learned to prevent recurrence.
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	Terms of service are agreed with Axient's customers and users of the services to communicate their responsibilities and terms of use.
		The vendor management policy sets out the roles, responsibilities and requirements for managing the risks associated with third-party providers.
		Axient follows a formal incident management process that includes logging, classifying, and tracking incidents through to resolution with lessons learned devised to prevent recurrence.
		Established incident response plans document the potential events, pre-planned response steps and communication requirements to ensure incidents are handled effectively.
		The incident management policy defines the roles, responsibilities and requirements for identifying, classifying and resolving incidents, including devising lessons learned to prevent recurrence.
		The vulnerability management program defines the approach to identifying, assessing and resolving security vulnerabilities, including defined timeframes based on severity.
		The vendor register includes material third-party software and service providers with tracking of the vendor agreements, risk ratings and vendor governance activities.

Common Criteria 3: Risk Assessment

CC3.0	Criteria	Control Activity
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	Axient has defined a formal risk management process for evaluating risks based on identified threats, assessment criteria, existing internal controls and the risk tolerance.
		Axient's set of information security policies cover the roles, responsibilities and requirements to support effective internal control that support the information security objectives.
		The security policies set out the requirements for managing information security across the organisation's operations.
CC3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	Axient has defined a formal risk management process for evaluating risks based on identified threats, assessment criteria, existing internal controls and the risk tolerance.
		Axient conducts risk assessments at least annually to identify new and emerging risks, revise the existing risks, and devise risk mitigation actions.
		Axient's management prepares a remediation plan to formally manage the resolution of findings identified in the risk assessment activities.
		The vendor management policy sets out the roles, responsibilities and requirements for managing the risks associated with third-party providers.
		An annual vendor risk assessment is completed to ensure the identification and treatment of risks remains accurate and appropriate.
		The vendor register includes material third-party software and service providers with tracking of the vendor agreements, risk ratings and vendor governance activities.
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	Axient has defined a formal risk management process for evaluating risks based on identified threats, assessment criteria, existing internal controls and the risk tolerance.
		Axient conducts risk assessments at least annually to identify new and emerging risks, revise the existing risks, and devise risk mitigation actions.

CC3.0	Criteria	Control Activity
		Axient's management prepares a remediation plan to formally manage the resolution of findings identified in the risk assessment activities.
		The risk assessment process considers the potential for fraud including malicious acts of employees or other users of the system.
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	The risk assessment process identifies and assesses changes that could significantly impact the system of internal control.
		Axient has defined a formal risk management process for evaluating risks based on identified threats, assessment criteria, existing internal controls and the risk tolerance.
		Axient conducts risk assessments at least annually to identify new and emerging risks, revise the existing risks, and devise risk mitigation actions.
		The documented organization chart outlines the roles, functional responsibilities and reporting lines for Axient personnel.
		The vendor management policy sets out the roles, responsibilities and requirements for managing the risks associated with third-party providers.

Common Criteria 4: Monitoring Activities

CC4.0	Criteria	Control Activity
CC4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and / or separate evaluations to ascertain whether the components of internal control are present and functioning.	The information security policies are reviewed by management at least annually and updated where required.
		Axient performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are logged and planned where weaknesses or potential improvements are identified.
		Backup and restoration tests are performed at least annually to ensure the recovery controls are effective.
		Axient follows a formal incident management process that includes logging, classifying, and tracking incidents through to resolution with lessons learned devised to prevent recurrence.
		Vulnerability scans are conducted on a quarterly basis.
		Independent penetration tests are conducted annually.
		Management is assigned ownership of ongoing monitoring of the effectiveness of controls and that key policy and process requirements are being adhered to.
		An annual vendor risk assessment is completed to ensure the identification and treatment of risks remains accurate and appropriate.
CC4.2	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	Axient's workstations operating system security patches are applied automatically.
		Axient's board of directors meets at least semi-annually and maintains meeting minutes.
		The board of directors maintains oversight and provides support for the information security program with briefings at least annually.
		Axient's board of directors has a documented charter that outlines its oversight responsibilities for internal control and information security.
		Management tracks whether control failures, breaches of policies and procedures, customer complaints and other issues are assessed, tracked and monitored through to resolution, as applicable.

CC4.0	Criteria	Control Activity
		The information security policies are reviewed by management at least annually and updated where required.
		Vulnerability scans are conducted on a quarterly basis.
		The incident management policy defines the roles, responsibilities and requirements for identifying, classifying and resolving incidents, including devising lessons learned to prevent recurrence.
		Independent penetration tests are conducted annually.
		Management is assigned ownership of ongoing monitoring of the effectiveness of controls and that key policy and process requirements are being adhered to.

Common Criteria 5: Control Activities

CC5.0	Criteria	Control Activity
CC5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Axient conducts risk assessments at least annually to identify new and emerging risks, revise the existing risks, and devise risk mitigation actions.
		Axient's management prepares a remediation plan to formally manage the resolution of findings identified in the risk assessment activities.
		Axient performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are logged and planned where weaknesses or potential improvements are identified.
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	The network security policy establishes the roles, responsibilities and requirements for securing the network with cryptographic controls, security hardening and network monitoring.
		Axient conducts risk assessments at least annually to identify new and emerging risks, revise the existing risks, and devise risk mitigation actions.
		Axient's set of information security policies cover the roles, responsibilities and requirements to support effective internal control that support the information security objectives.
		The security policies set out the requirements for managing information security across the organisation's operations.
		Backup and restoration tests are performed at least annually to ensure the recovery controls are effective.
		Axient conducts annual business continuity and disaster recovery tests to ensure the response plans are effective.
		Vulnerability scans are conducted on a quarterly basis.
		Security awareness training is conducted for Axient employees at least annually.
		The incident management policy defines the contacts and methods for employees to report security-related incidents and concerns.
		Independent penetration tests are conducted annually.

CC5.0	Criteria	Control Activity
CC5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Job descriptions are documented to support the hiring of suitable candidates and to communicate the key job responsibilities of each individual.
		The information security policies are reviewed by management at least annually and updated where required.
		Axient's set of information security policies cover the roles, responsibilities and requirements to support effective internal control that support the information security objectives.
		The security policies set out the requirements for managing information security across the organisation's operations.
		Backup and restoration tests are performed at least annually to ensure the recovery controls are effective.
		The incident management policy defines the contacts and methods for employees to report security-related incidents and concerns.

Common Criteria 6: Logical and Physical Access Controls

CC6.0	Criteria	Control Activity
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	User accounts are individually assigned with a unique user ID to support system logging and accountability.
		Multi-factor authentication is required for access to sensitive systems.
		The security policies set out the requirements for managing information security across the organisation's operations.
		Axient stores sensitive data, including customer data, in databases that are encrypted at rest.
		The access control policy requires role-based access control where access rights are limited to the requirements of each role.
		The asset management policy establishes Axient's scope of information assets and requirements for how those are tracked and managed accordingly.
		Axient has established formal guidelines for passwords to govern the management and use of authentication mechanisms.
		The access control policy establishes the requirements for authentication including strong passwords, multi-factor and single sign-on as applicable to Axient's systems.
		The information assets are identified, classified and centrally logged for ongoing monitoring and governance.
		Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed	The access control policy requires appropriate access approvals, quarterly user access reviews, and revocation of access in a timely manner upon termination, to ensure access is restricted to authorised personnel.
		User accounts are individually assigned with a unique user ID to support system logging and accountability.
		New hire access privileges to critical systems are approved by management prior to provisioning.

CC6.0	Criteria	Control Activity
	when user access is no longer authorized.	A defined terminations process is followed including revocation of user access from systems in a timely manner.
		Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, considering the concepts of least privilege and segregation of duties, to meet the entity's objectives.	The access control policy requires appropriate access approvals, quarterly user access reviews, and revocation of access in a timely manner upon termination, to ensure access is restricted to authorised personnel.
		User access reviews are performed at least quarterly to confirm Axient user access to critical systems is appropriate.
		User accounts are individually assigned with a unique user ID to support system logging and accountability.
		New hire access privileges to critical systems are approved by management prior to provisioning.
		The access control policy requires role-based access control where access rights are limited to the requirements of each role.
		A defined terminations process is followed including revocation of user access from systems in a timely manner.
		Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	This criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no	User access reviews are performed at least quarterly to confirm Axient user access to critical systems is appropriate.
		The disposal of sensitive information assets follows a defined process to ensure sensitive data is effectively erased before the safeguards over the information assets are removed.

CC6.0	Criteria	Control Activity
	longer required to meet the entity's objectives.	The asset management policy establishes Axient's scope of information assets and requirements for how those are tracked and managed accordingly.
		A defined terminations process is followed including revocation of user access from systems in a timely manner.
		The information assets are identified, classified and centrally logged for ongoing monitoring and governance.
		Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Axient uses firewall configurations that ensure only approved networking ports and protocols can be used.
		Systematically applied security restrictions are used to protect against data leakage.
		Vulnerability scans are conducted on a quarterly basis.
		Security awareness training is conducted for Axient employees at least annually.
		The acceptable use policy sets out the roles, responsibilities and requirements to maintain the security of systems, data and endpoint devices.
		Connections and data flows to System and the supporting infrastructure are encrypted in transit.
		Independent penetration tests are conducted annually.
		Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	Systematically applied security restrictions are used to protect against data leakage.
		Axient stores sensitive data, including customer data, in databases that are encrypted at rest.
		The acceptable use policy sets out the roles, responsibilities and requirements to maintain the security of systems, data and endpoint devices.

CC6.0	Criteria	Control Activity
		Connections and data flows to System and the supporting infrastructure are encrypted in transit.
		Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	The network security policy establishes the roles, responsibilities and requirements for securing the network with cryptographic controls, security hardening and network monitoring.
		Axient's workstations operating system security patches are applied automatically.
		Antivirus software is installed on workstations to protect against malware.
		Infrastructure logging is configured to monitor web traffic and suspicious activity with automated alerts raised for anomalous activity.
		Systematically applied security restrictions are used to protect against data leakage.
		Vulnerability scans are conducted on a quarterly basis.
		Security awareness training is conducted for Axient employees at least annually.
		The acceptable use policy sets out the roles, responsibilities and requirements to maintain the security of systems, data and endpoint devices.
		Independent penetration tests are conducted annually.
		Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.

Common Criteria 7: System Operations

CC7.0	Criteria	Control Activity
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	Infrastructure logging is configured to monitor web traffic and suspicious activity with automated alerts raised for anomalous activity.
		Axient uses a version control system to manage source code, documentation, release labelling, and other change management tasks.
		Vulnerability scans are conducted on a quarterly basis.
		Independent penetration tests are conducted annually.
		Vulnerabilities identified from the penetration tests, vulnerability scans, and any other sources, are centrally logged, classified and followed through to resolution in a timely manner based on their severity.
		Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	Axient uses logging software that sends alerts to appropriate personnel.
		Infrastructure logging is configured to monitor web traffic and suspicious activity with automated alerts raised for anomalous activity.
		Vulnerabilities identified from the penetration tests, vulnerability scans, and any other sources, are centrally logged, classified and followed through to resolution in a timely manner based on their severity.
		Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	Axient follows a formal incident management process that includes logging, classifying, and tracking incidents through to resolution with lessons learned devised to prevent recurrence.
		Established incident response plans document the potential events, pre-planned response steps and communication requirements to ensure incidents are handled effectively.

CC7.0	Criteria	Control Activity
		The incident management policy defines the roles, responsibilities and requirements for identifying, classifying and resolving incidents, including devising lessons learned to prevent recurrence.
		Vulnerabilities identified from the penetration tests, vulnerability scans, and any other sources, are centrally logged, classified and followed through to resolution in a timely manner based on their severity.
		Axient has appointed an emergency response team to mobilise and manage incidents through to resolution.
		Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	The incident response plans are reviewed at least annually to confirm they provide an effective response to potential incidents.
		Axient follows a formal incident management process that includes logging, classifying, and tracking incidents through to resolution with lessons learned devised to prevent recurrence.
		Established incident response plans document the potential events, pre-planned response steps and communication requirements to ensure incidents are handled effectively.
		The incident management policy defines the roles, responsibilities and requirements for identifying, classifying and resolving incidents, including devising lessons learned to prevent recurrence.
		Axient has appointed an emergency response team to mobilise and manage incidents through to resolution.
		Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	The business continuity plans document the scenarios, impacts, key stakeholders, response plans, escalation points and communication channels to effectively manage critical events.

CC7.0	Criteria	Control Activity
		Daily backups are performed and monitored to support recoverability of the production data.
		The incident response plans are reviewed at least annually to confirm they provide an effective response to potential incidents.
		The established disaster recovery plan outlines roles, responsibilities and detailed procedures for the recovery of critical systems.
		Established incident response plans document the potential events, pre-planned response steps and communication requirements to ensure incidents are handled effectively.
		Vulnerabilities identified from the penetration tests, vulnerability scans, and any other sources, are centrally logged, classified and followed through to resolution in a timely manner based on their severity.
		Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.

Common Criteria 8: Change Management

CC8.0	Criteria	Control Activity
CC8.1	The entity authorizes, designs, develops, or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Separate environments are used for testing and production for Axient's System.
		Axient uses a version control system to manage source code, documentation, release labelling, and other change management tasks.
		The change management policy governs the software development lifecycle including tracking, testing, approving and validating changes to the source code.
		Change releases are independently reviewed and approved prior to deployment.
		System changes are tested based on the type of change prior to implementation.
		Code developments require a system enforced peer review prior to merging with the master code branch.
		Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.

Common Criteria 9: Risk Mitigation

CC9.0	Criteria	Control Activity
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	The business continuity plans document the scenarios, impacts, key stakeholders, response plans, escalation points and communication channels to effectively manage critical events.
		Axient utilizes multiple availability zones to replicate production data across different zones to support the systems availability and recovery objectives.
		Daily backups are performed and monitored to support recoverability of the production data.
		The backup policy establishes the requirements for backups and recoverability.
		The established disaster recovery plan outline roles, responsibilities and detailed procedures for the recovery of critical systems.
		Backup and restoration tests are performed at least annually to ensure the recovery controls are effective.
		Axient conducts annual business continuity and disaster recovery tests to ensure the response plans are effective.
		Axient follows a formal incident management process that includes logging, classifying, and tracking incidents through to resolution with lessons learned devised to prevent recurrence.
		Established incident response plans document the potential events, pre-planned response steps and communication requirements to ensure incidents are handled effectively.
		Axient maintains cybersecurity insurance to mitigate the impact of potential data breaches and disruptions.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	The vendor management policy sets out the roles, responsibilities and requirements for managing the risks associated with third-party providers.
		An annual vendor risk assessment is completed to ensure the identification and treatment of risks remains accurate and appropriate.

CC9.0	Criteria	Control Activity
		The vendor register includes material third-party software and service providers with tracking of the vendor agreements, risk ratings and vendor governance activities.

Trust Services Criteria for the Availability Category

A1.0	Criteria	Control Activity
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	Axient utilizes multiple availability zones to replicate production data across different zones to support the systems availability and recovery objectives.
		A load balancer automatically distributes incoming application traffic across multiple instances and availability zones.
		Auto-scaling configuration is used to automatically provision additional capacity when predefined thresholds are met.
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	Axient utilizes multiple availability zones to replicate production data across different zones to support the systems availability and recovery objectives.
		Axient uses logging software that sends alerts to appropriate personnel.
		A load balancer automatically distributes incoming application traffic across multiple instances and availability zones.
		Daily backups are performed and monitored to support recoverability of the production data.
		The backup policy establishes the requirements for backups and recoverability.
		The established disaster recovery plan outline roles, responsibilities and detailed procedures for the recovery of critical systems.
		Axient conducts annual business continuity and disaster recovery tests to ensure the response plans are effective.
		Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	Daily backups are performed and monitored to support recoverability of the production data.
		Backup and restoration tests are performed at least annually to ensure the recovery controls are effective.
		Axient conducts annual business continuity and disaster recovery tests to ensure the response plans are effective.

Trust Services Criteria for the Confidentiality Category

C1.0	Criteria	Control Activity
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	A register of the types and sources of confidential data collected and processed is maintained to track assets and storage locations of confidential data.
		The data classification, handling and retention policy establishes the method of data classification to ensure appropriate protections are applied based on its sensitivity.
		Confidential data is maintained within the system boundaries at all times where security controls are applied to restrict access to authorized individuals.
		The access control policy requires role-based access control where access rights are limited to the requirements of each role.
		The acceptable use policy sets out the roles, responsibilities and requirements to maintain the security of systems, data and endpoint devices.
		Employment contracts are formed with Axient employees including a non-disclosure agreement (NDA) for confidential information.
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	The disposal of sensitive information assets follows a defined process to ensure sensitive data is effectively erased before the safeguards over the information assets are removed.
		The acceptable use policy sets out the roles, responsibilities and requirements to maintain the security of systems, data and endpoint devices.
		A defined terminations process is followed including revocation of user access from systems in a timely manner.

GUIDANCE REGARDING INFORMATION PROVIDED BY THE SERVICE AUDITOR

AssuranceLab's examination of the controls of Axient was limited to the related Agreed Criteria and control activities specified by the management of Axient and did not encompass all aspects of Axient's operations or operations at user entities. Our examination was performed in accordance with AT-C section 105: Concepts Common to All Attestation Engagements and AT-C section 205: Assertion-Based Examination Engagements.

Our examination of the control activities was performed using the following testing methods:

TEST	DESCRIPTION
Inquiry	The service auditor made inquiries of service organization personnel. Inquiries were made to obtain information and representations from the client to determine that the client's knowledge of the control and corroborate policy or procedure information.
Observation	The service auditor observed application of the control activities by client personnel.
Inspection	The service auditor inspected among other items, source documents, reports, system configurations to determine performance of the specified control activity and in some instances the timeliness of the performance of control activities.
Re-performance	The service auditor independently executed procedures or controls that were originally performed by the service organization as part of the entity's internal control.

In determining whether the report meets the criteria, the user auditor should perform the following procedures:

- Understand the aspects of the service organization's controls that may affect the service commitments and system requirements based on the Agreed Criteria
- Understand the infrastructure, software, procedures, and data that are designed, implemented, and operated by the service organization
- Determine whether the Agreed Criteria are relevant to the user entity's assertions
- Determine whether the service organization's controls are suitably designed to provide reasonable assurance that its service commitments and system were achieved based on the Agreed Criteria

Office Locations

AUSTRALIA
Level 3/11 York Street
Sydney NSW 2000

UNITED STATES
1400 Lavaca Street, Suite 700
Austin, Texas 78701

EMEA
Block 2 Charlemont Street, Charlemont Row
Saint Kevin's, Dublin, D01 F6X6