



**XERO LIMITED**

**SOC 2 REPORT**

FOR

CLOUD BASED ACCOUNTING

A TYPE 2 INDEPENDENT SERVICE AUDITOR'S REPORT ON CONTROLS  
RELEVANT TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY

NOVEMBER 1, 2023, TO OCTOBER 31, 2024

Attestation and Compliance Services



**Proprietary & Confidential**

Unauthorized use, reproduction, or distribution of this report, in whole or in part, is strictly prohibited.

This report is intended solely for use by the management of Xero Limited, user entities of Xero Limited's services, and other parties who have sufficient knowledge and understanding of Xero Limited's services covered by this report (each referred to herein as a "specified user").

If the report recipient is not a specified user (herein referred to as a "non-specified user"), use of this report is the non-specified user's sole responsibility and at the non-specified user's sole and exclusive risk. Non-specified users may not rely on this report and do not acquire any rights against Schellman & Company, LLC as a result of such access. Further, Schellman & Company, LLC does not assume any duties or obligations to any non-specified user who obtains this report and/or has access to it.

Unauthorized use, reproduction, or distribution of this report, in whole or in part, is strictly prohibited.

# TABLE OF CONTENTS

SECTION 1	INDEPENDENT SERVICE AUDITOR'S REPORT .....	1
SECTION 2	MANAGEMENT'S ASSERTION .....	5
SECTION 3	DESCRIPTION OF THE SYSTEM .....	7
SECTION 4	TESTING MATRICES .....	26
SECTION 5	OTHER INFORMATION PROVIDED BY XERO .....	76

# **SECTION I**

## **INDEPENDENT SERVICE AUDITOR'S REPORT**

## INDEPENDENT SERVICE AUDITOR'S REPORT

To Xero Limited:

### Scope

We have examined Xero Limited's ("Xero" or the "service organization") accompanying description of its Cloud Based Accounting system, in Section 3, throughout the period November 1, 2023, to October 31, 2024, (the "description"), based on 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*) ("description criteria"), and the suitability of the design and operating effectiveness of controls stated in the description throughout the period November 1, 2023, to October 31, 2024, to provide reasonable assurance that Xero's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality ("applicable trust services criteria") set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Xero 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 Xero, to achieve Xero's service commitments and system requirements based on the applicable trust services criteria. The description presents Xero's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Xero'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 information included in Section 5, "Other Information Provided by Xero" is presented by Xero management to provide additional information and is not a part of the description. Information about Xero's response to testing exceptions has not been subjected to the procedures applied in the examination of the description, the suitability of the design of controls, and the operating effectiveness of the controls to achieve Xero's service commitments and system requirements based on the applicable trust services criteria.

### Service Organization's Responsibilities

Xero 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 Xero's service commitments and system requirements were achieved. Xero has provided the accompanying assertion, in Section 2, ("assertion") about the description and the suitability of design and operating effectiveness of controls stated therein. Xero 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 trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization'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 design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA) and in accordance with International Standard on Assurance Engagements 3000 (Revised), Assurance Engagements Other Than Audits or Reviews of Historical Financial Information, issued by the International Auditing and Assurance Standards Board. 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 and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our qualified opinion.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and the service organization'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 or did not operate effectively.
- 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 the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- Evaluating the overall presentation of the description.

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

#### *Service Auditor's Independence and Quality Control*

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement, including the Code of Professional Conduct established by the AICPA and the International Ethics Standards Board for Accountants' Code of Ethics for Professional Accountants.

We applied the Statements on Quality Control Standards established by the AICPA and, accordingly, maintain a comprehensive system of quality control.

#### *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 users may consider important to meet their informational needs.

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 are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

#### *Description of Test of Controls*

The specific controls we tested, and the nature, timing, and results of those tests are presented in Section 4 of our report titled "Testing Matrices."

#### *Explanatory Paragraph*

The accompanying description of the Cloud Based Accounting system in Section 3 states that version control branch protections are enabled to restrict users from circumventing the change management process and that access privileges to implement changes into the production environment are restricted to user accounts accessible by authorized personnel who do not have administrative access to the version control software. However, controls related to restricting change implementation to personnel who did not have administrative access to the version control software were not consistently performed during the period, and therefore were not operating effectively throughout the period November 1, 2023, to October 31, 2024. As a result, controls did not provide reasonable assurance that Xero's service commitments and system requirements were achieved based on trust services

criterion CC8.1, which states, “The entity authorizes, designs, develops, or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.”

*Opinion*

In our opinion, except for the effects of the matters giving rise to the modification, in all material respects:

- the description presents Xero’s Cloud Based Accounting system that was designed and implemented throughout the period November 1, 2023, to October 31, 2024, in accordance with the description criteria;
- the controls stated in the description were suitably designed throughout the period November 1, 2023, to October 31, 2024, to provide reasonable assurance that Xero’s service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organization applied the complementary controls assumed in the design of Xero’s controls throughout that period; and
- the controls stated in the description operated effectively throughout the period November 1, 2023, to October 31, 2024, to provide reasonable assurance that Xero’s service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls assumed in the design of Xero’s controls operated effectively throughout that period.

*Restricted Use*

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of Xero, user entities of Xero’s Cloud Based Accounting system during some or all of the period of November 1, 2023, to October 31, 2024, business partners of Xero subject to risks arising from interactions with the Cloud Based Accounting system, 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 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 applicable trust services criteria; and
- 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.

*SCHILLMAN & COMPANY, LLC*

Columbus, Ohio  
November 25, 2024

# **SECTION 2**

## **MANAGEMENT'S ASSERTION**



## MANAGEMENT'S ASSERTION

We have prepared the accompanying description of Xero's Cloud Based Accounting system, in Section 3, throughout the period November 1, 2023, to October 31, 2024, (the "description") based on 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)*, ("description criteria"). The description is intended to provide report users with information about the Cloud Based Accounting system that may be useful when assessing the risks arising from interactions with Xero's system, particularly information about system controls that Xero has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality ("applicable trust services criteria") set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*.

Xero 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 Xero, to achieve Xero's service commitments and system requirements based on the applicable trust services criteria. The description presents Xero's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Xero's controls. The description does not disclose the actual controls at the subservice organization.

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

- the description presents Xero's Cloud Based Accounting system that was designed and implemented throughout the period November 1, 2023, to October 31, 2024, in accordance with the description criteria;
- the controls stated in the description were suitably designed throughout the period November 1, 2023, to October 31, 2024, to provide reasonable assurance that Xero's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization applied the complementary controls assumed in the design of Xero's controls throughout that period; and
- except for the effects of the matter described in the following paragraph, the controls stated in the description operated effectively throughout the period November 1, 2023, to October 31, 2024, to provide reasonable assurance that Xero's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls assumed in the design of Xero's controls operated effectively throughout that period.

Our accompanying description of the Cloud Based Accounting system in Section 3 states that version control branch protections are enabled to restrict users from circumventing the change management process and that access privileges to implement changes into the production environment are restricted to user accounts accessible by authorized personnel who do not have administrative access to the version control software. However, controls related to restricting change implementation to personnel who did not have administrative access to the version control software were not consistently performed during the period, and therefore were not operating effectively throughout the period November 1, 2023, to October 31, 2024. As a result, controls did not provide reasonable assurance that our service commitments and system requirements were achieved based on trust services criterion CC8.1, which states, "The entity authorizes, designs, develops, or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives."

# **SECTION 3**

## **DESCRIPTION OF THE SYSTEM**

## OVERVIEW OF OPERATIONS

### Company Background

Founded in 2006 and domiciled in New Zealand, Xero is one of the fastest growing software as a service companies globally. For accountants and bookkeepers, Xero helps build a relationship of trust with small business clients through online collaboration. Xero is a leader in the New Zealand, Australian, and United Kingdom cloud accounting markets, employing a world-class team of more than 4,000 people in 15 offices across the globe. Xero is listed on the Australian Securities Exchange.

### Description of Services Provided

Xero is a cloud-based accounting software platform for small businesses and their advisors that allows users to track and pay bills on time, manage spending, and submit or reimburse expense claims with expense management tools, set up bank connections of the secure flow of transactions into Xero, bank reconciliation, financial reporting and more. Xero small business accounting software is a subscription service with more than four million subscribers worldwide. Customers are able to choose a pricing plan for their subscription and may choose to add optional add-ons such as payroll, project tracking, expense claiming, and advanced analytics to their plan. Xero is accessible from web browsers as well as from mobile devices.

Service	Products
Xero Business Platform	<p>Xero small business accounting software used by small business, bookkeepers and accounting partners including the following features:</p> <ul style="list-style-type: none"> <li>• Invoicing</li> <li>• e-invoicing</li> <li>• Inventory</li> <li>• Payroll</li> <li>• Banking and Bank Reconciliation</li> <li>• General Ledger</li> <li>• Journals</li> <li>• Analytics Plus</li> <li>• Contacts &amp; Smart Lists</li> <li>• Bills</li> <li>• Expense claims</li> <li>• Projects</li> <li>• Quotes</li> <li>• Reporting</li> <li>• Accept Payments</li> <li>• Purchase Orders</li> <li>• Fixed assets</li> <li>• Files</li> <li>• Transactional Taxes</li> </ul>
Xero Partner Products	<p>Xero Partner products which are used by accountants and bookkeepers are in scope including the following products:</p> <ul style="list-style-type: none"> <li>• Xero HQ</li> <li>• Practice Manager</li> <li>• Workpapers</li> <li>• Xero Tax</li> </ul>
Hubdoc	<p>Real-time document capture and auto-fetching of bank statements, bills and receipts from financial institutions, utilities, telecom providers and online vendors.</p>
Developer API platform	<p>The developer API platform which provides the ability for customers to integrate with private and certified apps through the app marketplace.</p>
Mobile applications	<p>Applications which provide a limited set of features for Xero products on mobile devices.</p>

---

## PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Xero commits to customers that it will conduct certain objectives in relation to the services provided. These commitments are documented and reviewed by management to ensure that the operations, reporting, and compliance objectives are aligned with the company's mission to achieve commitments. Xero documents commitments in customer agreements, terms of use, and security documentation that are available to customers via Xero's public-facing website.

Specific security, availability, and confidentiality commitments include the following:

- Maintain technical and organizational measures, internal controls, and data security routines to protect customer data.
- Protection of data at rest and in transit.
- Protection of information systems from unauthorised access, use, modification, disclosure, destruction, threats, or hazards.
- Continuous communication of the Xero platform service availability.
- Ability to recover and restore customer data in the event of a business disruption or disaster.
- Maintain customer data as confidential and not disclose information to any unauthorised party.
- Customer data is removed from Xero systems upon customer request or at the end of the seven-year retention period following customer termination.
- Customer data is retained for a period of seven years following the termination of the customer agreement.

Xero has also established system requirements that support the achievement of the principal service commitments relevant to the security, availability, and confidentiality trust services categories and relevant laws and regulations. These requirements are communicated internally via the information security policies and procedures and regular security awareness training documentation, and externally via the Xero public-facing website.

These requirements include, but are not limited to, defined processes around the following:

- Employees undergo background checks prior to employment.
- Employees undergo mandatory security awareness training upon hire, and annually thereafter.
- Roles and responsibilities for Xero employees who have access to confidential data and the responsibility for protecting the information and information systems.
- Access control policies for employees with access to Xero's production environment and source code such that access levels are approved prior to credentials being issued, reviewed at predefined intervals, and based on legitimate business need based on the principle of least privilege.
- Software development lifecycle (SDLC) policies for any changes to the production environment to ensure that key processes and security checks are consistently performed from change initiation through release.
- Risk assessment practices to assist in identifying and managing potential internal or external risks that could negatively affect Xero's critical business processes and their ability to provide reliable services to their customers.
- Incident management process to address data breaches and security events related to Xero's products and services in an efficient and timely manner.
- Disaster recovery and business continuity plans to prepare Xero in the event of extended service outages caused by factors beyond their control and to restore services to the widest extent possible in a minimal timeframe.

Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed; how the system is operated; how the internal business systems and networks are managed; and how employees are hired, trained, and managed. In addition

to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the Cloud Based Accounting system.

In accordance with our assertion, and the description criteria, the aforementioned service commitments and requirements are those principal service commitments and requirements common to the broad base of users of the system and may therefore not fully address the specific service commitments and requirements made to all system users, in each individual case.

---

## COMPONENTS OF THE SYSTEM USED TO PROVIDE THE SERVICE

### System Boundaries

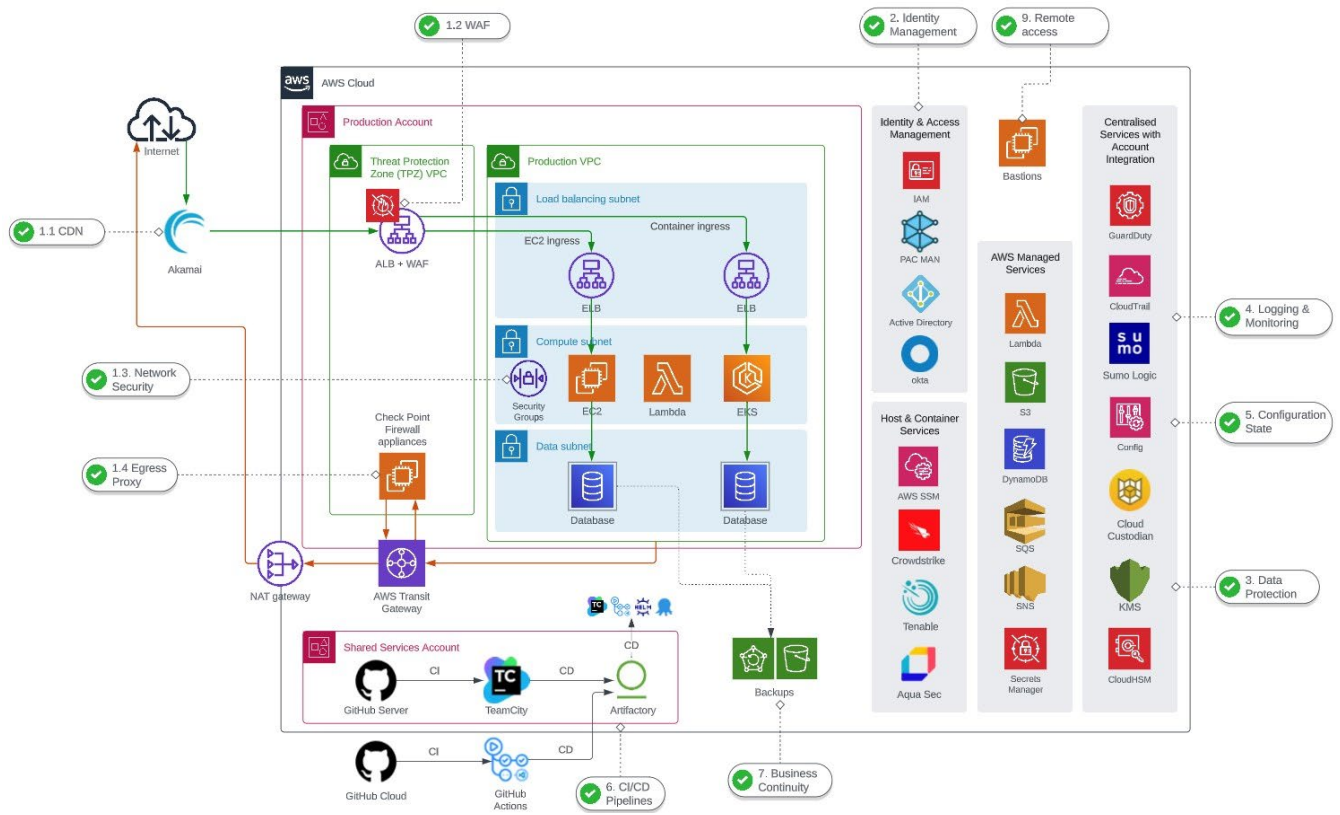
A system is designed, implemented, and operated to achieve specific business objectives in accordance with management-specified requirements. The purpose of the system description is to delineate the boundaries of the system, which includes the services outlined above and the five components described below: infrastructure, software, people, procedures, and data.

### Infrastructure and Software

Xero's production infrastructure resides in the Amazon Web Services, Inc. (AWS) Elastic Cloud Compute (EC2) Virtual Private Cloud (VPC) environment. For high availability and infrastructure resilience, the AWS production infrastructure is distributed across availability zones in the United States (US) East (N. Virginia) (us-east-1) AWS region with a secondary site located in the US West (Oregon) (us-west-2) AWS region. Xero also uses the Canada Central availability zone (ca-central-1) for storing backups of base configurations and Canadian accounting data.

Production data is stored in MySQL database engines managed by Amazon Relational Database Service (Amazon RDS). Xero has deployed database engines as a cluster where the cluster volume spans multiple availability zones, with each availability zone having a copy of the database cluster data. The database cluster consists of two database instances: primary database instance and replica. The primary database supports read and write operations and performs data modifications to the cluster volume. The replica connects to the same storage as the primary database instance and supports only read operations. Replicas are maintained in separate availability zones from the primary database instance for high availability.

Amazon EC2 virtual server instances running on Linux operating systems are utilized to support Xero's cloud-based accounting system. Amazon RDS datastores are backed up and stored as objects within Amazon Simple Storage Service (Amazon S3) buckets. RDS backups stored within Amazon S3 buckets are replicated to a separate AWS data center region to provide redundancy and data availability.



The in-scope infrastructure consists of multiple applications, operating system platforms and databases, as shown in the table below:

Primary Infrastructure			
Production Application	Business Function Description	Operating System Platform	Physical Location
Active Directory	Network domain supporting Single Sign-On (SSO) to the in-scope systems.	Microsoft Windows	AWS (US-East-1)
Amazon EC2	Virtual instances that provide scalable computing capacity supporting the system.	Amazon Linux Amazon Machine Image (AMI) – Ubuntu	
Servers	Virtualized compute infrastructure to support Xero's Cloud-Based Accounting System.	MySQL	
Bastion Hosts	Provide access to Amazon EC2 instances and database engines within the AWS production environment.	Microsoft Windows	
Block Storage	Block storage volumes used as datastores for the Xero's Cloud-Based Accounting System.	Amazon Elastic Block Store (EBS)	
Security Groups	Act as virtual firewalls for associated Amazon EC2 instances, controlling both inbound and outbound traffic at the instance level.	Amazon Proprietary	
Amazon S3	Object storage service utilized to store and protect backup data across multiple availability zones.		

Primary Infrastructure			
Production Application	Business Function Description	Operating System Platform	Physical Location
Firewall System	Virtual firewall system configured to protect the network perimeter and limit inbound and outbound access.	Amazon Proprietary	AWS (US-East-1)

### Secondary Infrastructure and Supporting Software

- Okta – identity management solution integrated with Active Directory utilized to provide SSO services to corporate and production applications and systems.
- Sumo Logic – cloud-based security information and event management (SIEM) tool utilized for security, operations, and business intelligence use cases providing log management and analytics services that leverage machine-generated big data to deliver real-time information technology (IT) operations and security insights.
- GitHub – version control repository utilized to provide version control and source code management.
- Amazon GuardDuty – threat / intrusion detection system (IDS) utilized to continuously monitor and analyse account and network events for possible or actual malicious activity, unauthorised behavior, and/or security breaches.
- Jamf Mobile Device Management (MDM) – Apple device management solution utilized to centrally manage Apple devices and deploy configuration profiles, encryption, and send remote commands to Apple devices.
- Jenkins – open-source automation server utilized to build and deploy change pipelines to the production environment.
- OctopusDeploy – open-source automated deployment and release management tool utilized to deploy change pipelines to the production environment.
- TeamCity – open-source continuous integration/continuous delivery (CI/CD) tool utilized to build and deploy change pipelines to the production environment as well as a version control tool.
- OneTrust Platform – risk management software utilized to document, track, and monitor security, availability, and confidentiality risks as well as vendor audits.
- Atlassian Jira (Jira) – workflow management system utilized for issue tracking and project management.
- Slack – communications platform utilized to facilitate daily conversations related to various aspects of the business.
- Windows Defender – endpoint security software utilized to centrally manage antivirus and anti-malware for Windows workstations.
- FortiClient Zero Trust Fabric Agent – endpoint security software utilized to centrally manage antivirus and anti-malware for MacOS workstations.
- FileVault / BitLocker – built-in disk encryption feature utilised for providing full disk encryption for employee workstations.
- Nessus Tenable.io (Tenable) – cloud-based endpoint security and asset scanning platform utilized to identify and analyze threats and vulnerabilities.
- Zendesk – management system utilized for customer issues and support tracking as well as user access procedures.

## People

The following groups are responsible for providing services related to Xero's cloud-based accounting system:

- Executive Management – responsible for overseeing operations are the Chief Product and Technology Officer, Chief Financial Officer, Chief People Officer, Chief Business Operations & Strategy Officer, Chief Legal Officer & Company Secretary, Chief Marketing Officer, Chief Revenue Officer and Chief Executive Officer.
- Product Engineering – the team is embedded within product and other platform services teams. Engineers are responsible for providing consulting services for AWS architectural design decisions and for product alignment with AWS infrastructure services and capabilities.
- Architecture & Integration – responsible for the overall architectural leadership and practice across Xero. Architects are embedded in teams across Xero and work as an enabling and aligning function and lead the technical engagement in M&A (mergers and acquisitions) due diligence and integration planning.
- Engineering Delivery – responsible for the overall engineering practices and standards across Xero, technology delivery practice, and the technical lead for the Xero application modernization programme of work.
- Delivery and Operations – responsible for the overall technology strategy development and leadership; ensuring smooth operations of technology, delivery of major programmes and strategically important projects, performance, planning and monitoring of Technology's work portfolio and the overall agile delivery practices of Technology teams.
- Platform as a Service (PaaS) – responsible for building and maintaining infrastructure. PaaS products and services bridge the gap between AWS's building blocks and having a fully available, secure, backed-up environment from which Xero can be operated. PaaS oversees networks, SQL infrastructure and backups, compute, and CI/CD.
- Commercial Operations/Technology – responsible for tracking and optimizing Xero's spending on its cloud platform.
- Reliability – responsible for the reliability and commercial operations of the Xero cloud platform.
- Enterprise Technology:
  - Customer Platforms and Solutions: Product management/ownership, business analysis, development and testing resource providing enhancement and support to Xero's sales, marketing, customer service and systems.
  - People Systems: Product management/ownership, business analysis, development and testing resources providing enhancement and support to Xero's corporate IT, i.e., HR, Finance, Legal, Facilities, and core internal IT.
  - Engineering, Subscription and Billing: Development, testing and DevOps resource provided to the above two teams in a matrix fashion. This team also supports Enterprise Technology's environments, monitoring, integration solutions and engineering practice (in conjunction with the broader technology function). This team also does the product management/ownership, business analysis, development and testing to enhance and support Xero's integration, and subscription and billing systems.
- Ecosystem – responsible for building and growing Xero's open API, working with app and developer partners around the world to connect Xero subscribers with apps to run their entire business operations.
- Product – the team is divided into two major product portfolios, the business product portfolio, and the partner product portfolio.
- Sales and Marketing – these divisions spearhead the marketing and sales initiatives at Xero and are responsible for positioning its services in the global market.
- Finance – responsible for meeting financial reporting compliance requirements. Reports to Xero's Chief Financial Officer.

- Workplace Experience (Facilities) – responsible for office accommodation and the in-house services that make the workplace run smoothly for Xero employees.
- Legal – responsible for corporate compliance and risk management. The legal team is global, with members of the team based in New Zealand, Australia, the United Kingdom, Canada, and the United States of America.
- Risk and Assurance – responsible for providing independent and objective assurance and advice on Xero’s organizational governance, risk management, and internal control processes.
- Security – responsible for the security of Xero systems and data, and compliance with regulations and industry standards.
- Data – team reports into the security team and covers four key functional areas – data platforms, data enrichment, data applications, and data strategy, governance, and evangelism.
- People Experience (PX) – Xero’s HR team. Responsible for managing hiring and onboarding.

## Procedures

### Access, Authentication and Authorization

Xero maintains a wireless corporate network in corporate office locations which requires domain authentication and is tied to a user’s lightweight directory access protocol (LDAP) credentials and a trusted certificate. Users access the corporate network using their LDAP credentials, which consists of a unique username and password. Remote access to the internal network is also available over VPN and requires the user to connect using their LDAP credentials and a trusted certificate. Connecting to the VPN requires the user to connect using their domain credentials and multi-factor authentication (MFA). To ensure that passwords adhere to strong security control in accordance with the access control standard, the following password requirements have been established:

- Set a minimum password length for the number of password characters based on account type.
- Set a maximum password age, after which the user will be required to change their password.
- Set a password history to prevent users from repeating passwords. Where possible, the history will be set to 24 passwords before allowing a password to be reused.
- Enforce password complexity standards.
- Lock user accounts after a set number of unsuccessful login attempts:
  - For Xero's systems, accounts will be locked after 6 unsuccessful login attempts; the account will remain locked until a 15-minute period has passed or is unlocked by the respective access management team for that system.
  - For privileged accounts or Xero's production and development systems, accounts will be locked after 6 unsuccessful login attempts where supported; the account will remain locked until it is unlocked by an authorised administrator.
- Lock computers after 5 minutes of inactivity, requiring users to re-enter their passwords.
- Disconnect sessions after 30 minutes of inactivity or upon receiving a request from a user (requiring re-authentication by the user).
- Terminate disconnected sessions (which have no user connected to it) after 30 minutes.
- Use of approved password management systems permitted to store passwords securely.

A unique username, password, and MFA code are utilized to restrict front-end access to the production environment via the AWS management console. Active Directory and Okta are utilized to restrict backend access to the production environment via SSO. Backend access to the production environment via AWS session manager service (SSM) requires users to first authenticate to Okta, including MFA, and a bastion host prior to accessing production instances. Backend access to the production environment via Remote Desktop Gateways requires users to first authenticate with Active Directory located on AWS, Duo MFA, and the bastion host prior to accessing production instances. For bastion access, the bastion hosts are unique to each VPC and use a separate network

username and password (Active Directory located on AWS). Users must first be connected to the network either by being in the office or remotely connected to the VPN to access the production environment.

Access to production databases is restricted to authorised personnel based on their job description. A formal process is established for provisioning access to the production databases. All access requests are documented and approved by the manager of the employee requesting access or the database owner.

### Access Requests and Access Revocation

Permissions to individual accounts are restricted based on role and job requirements. Requests to grant and revoke access, change access permission, create new accounts and roles are documented and tracked via the ticketing system for action by the security identity and access team.

Access requests to the corporate network access and AWS systems are handled by the internal IT team and security identity and access team, respectively, via ticketing system for tracking and documentation purposes. Access to AWS systems and data is restricted to users who are required to work on specific projects requiring access. Approval of access is documented within the tickets and requires approval from the user's manager and member of the internal IT team or security identity and access team dependent on the type of access requested.

For employees or contractors leaving Xero, the user's manager must provide an end date in the HR workflow application which triggers the termination process. The HR workflow application system generates a checklist of action points for the manager which includes recovery of any assets and a list of access revocations for systems the individual had access to. A notification ticket is automatically generated and sent to the internal IT and security identity and access teams to revoke access to the network, production systems, infrastructure, and data systems.

Xero performs quarterly user access reviews, including administrative access, for access to the production network and platform to ensure access rights are appropriate. A ticket is created to document and track the review. Any access which is deemed inactive or no longer required is identified and disabled.

### *Security Groups and Firewall Systems*

Xero utilizes AWS security groups which act as virtual firewalls for associated Amazon EC2 instances. Rules are configured for each security group that controls the inbound and outbound traffic to EC2 instances. Security groups are managed within the AWS management console. Additionally, a web application firewall (WAF) is in place and configured to monitor and allow or deny network traffic flowing in and out of the AWS environment from internal and external targets. A default rule is configured for the firewall to deny any traffic from a public source to internal targets, and additional rules are applied to allow for the flow of traffic between specified sources and destinations within the AWS environment.

### *Antivirus and Full Disk Encryption*

Workstations are protected with full disk encryption and configured with antivirus software that has been configured to automatically update virus signatures and scan registered clients daily. Workstations are centrally managed via a mobile device management application.

### *Change Management*

Xero has established change management policies, standards, and guidelines to define the process for managing changes to systems and applications in production that include assessing the impact of changes, testing, approvals, and rollback of unsuccessful changes. Changes are documented within a ticketing system to track the change through to implementation and for managing the change process. The tickets include information such as the change request description, target release, priority levels, and approval.

Each change must be packaged into an artifact which is deployed through at least one pre-production environment before production. Each change must be peer reviewed before being deployed to subsequent environments. Changes are verified and documented in pre-production using automated and manual testing. Development and testing occur in development, test, and user acceptance testing (UAT) environments. Production data resides only in the segregated production environment to ensure that confidential customer data is not used for testing purposes. A CI/CD pipeline is created to move packages to the live stage and production environments. Upon completion of testing and verification passes, the artifact is deployed to production. Xero generates synthetic data for use in test environments. Product teams create their test data using predefined scripts.

Changes to production are in two categories: security/application changes and infrastructure changes. The security engineering team is responsible for implementing and monitoring security changes to production via the ticketing system.

Infrastructure changes are monitored and implemented by the platform teams who log and track changes within the ticketing system. Infrastructure changes include the following:

- Standard change – change which is considered low risk and impact. Each change requires a peer review to be completed prior to being actioned.
- Non-standard change – change which is non-standard in nature and is categorized by its risk and impact (including financial). Each change requires a peer review to be completed and approval prior to being actioned.
- Emergency change – change that needs to be implemented with urgency to resolve or prevent a degradation in service. Each change requires a review prior to being applied.
- Notification change (pre-approved) – change which is considered low risk and low impact, follows a well-documented procedure, and has been pre-approved by site reliability engineering.

Xero uses a build management and CI/CD service to manage, track and provide control over versions of source code for release. Each release is uniquely identifiable and contains the changes which are recorded in source control, which allows for a recovery plan to be applied to remediate any issue with the release if necessary (rollback or roll forward). Access privileges to develop code and implement changes into the production environment are restricted to user accounts accessible by authorised personnel who do not have administrative access to the version control software. All software is required to have a proven recovery plan. Release versions are retained and mapped within the version control, build/release management, or CI/CD software. The ability to make changes to source code during development from the version control software is restricted to authorised personnel.

Logging of actions taken during development, including details about the change, timestamp, and user information, is recorded automatically within the CI/CD systems. Teams are also notified automatically of changes which occur to their project through the internal communication system which is integrated with the release management software.

Production and non-production environments are segregated, with separate AWS accounts and VPCs for each environment. Access to the environments is provisioned and managed by the security identity and access team via AWS identity and access management (IAM).

Patching software or hardware is a required part of IT operations to address threats in a timely and controlled manner. Patch management strategies are in place for and applied to desktops and endpoints, network systems, and platform systems and include virus patch management and operations systems deployment patching and services (e.g., firewall or network device). The remediation strategy is based on a 'pets' and 'cattle' model of systems management. Remediation of vulnerabilities on 'pets' is generally a patch in place method that applies to systems that generally cannot be recycled without significant service disruption or risk of data loss. Remediation of vulnerabilities on 'cattle' focuses on recycling of the system, meaning a new system is deployed that is fully up to date, and the old system is terminated and not reused. This method has the added benefit of minimising the risk of threats persisting in the environment.

### *System Monitoring*

Logging and monitoring applications are configured to monitor the security and availability of the Cloud Based Accounting system and alert security personnel for investigation and corrective action. The threat protection zone (TPZ) serves as a demilitarized zone (DMZ) to provide ingress and egress protection between the production environment and the Internet. Security monitoring tools and an IDS are configured to continuously monitor for suspicious activity indicative of malicious or unauthorised activity. Upon receiving alerts, security personnel investigate and respond as needed to mitigate the risk of a security incident. The security team runs reports on at least an annual basis to track resolution of technical vulnerabilities or misconfigurations. Internal vulnerability scans of Xero assets located behind the WAF are run twice daily. Additionally, on a quarterly basis, external vulnerability scans of the web application are performed to identify and analyse new vulnerabilities. Identified vulnerabilities are configured to notify operations and management personnel when service thresholds are exceeded and are triaged by product teams and monitored through resolution.

## *Incident Response*

Documented incident response and escalation procedures are in place to guide personnel in the monitoring, documenting, escalating, and resolving of problems affecting the Service. The customer portal is configured to allow customers to submit support requests and report potential incidents. A SIEM is used to manage event logs and the security response team is notified of critically significant events via an aggregate analytics system and notifications through messaging applications and e-mail. Security personnel take action on reported incidents in accordance with the incident management procedures. Incidents are assigned a severity which is defined with the incident response plan and escalation procedure. The incident response plan also defines roles and responsibilities for team members, noting their requirements in the incident management process. A centralized ticketing system is utilized to document, prioritize, escalate, and resolve problems affecting the service. Upon successful resolution of an incident, postmortem meetings are held, when applicable, to determine the root cause and identify lessons learned.

## *Data Backup, Business Continuity, and Disaster Recovery*

Backup policies and procedures are in place to guide personnel in the process of data backup and infrastructure recovery to meet Xero's availability objectives. An automated backup system is configured to perform full backups of production data at least daily to comply with documented data retention commitments and optimize recovery point objectives. Backups are encrypted at rest to secure data and protect sensitive information.

Every 180 days, backup copies are automatically migrated from Amazon S3 to Amazon Glacier, which is Amazon's archive storage service. Copies of these backups are made and stored for additional security measures, with cross-region backups migrated to Glacier after 14 days and same-region backups copied directly into Glacier. Backup copies of information, software and system images are tested on at least an annual basis in accordance with the established backup standard.

In some cases, an incident may rise to the level of a disaster. The incident response team escalates the incident to a disaster and triggers documented disaster recovery procedures. Production systems are implemented in a high availability architecture across multiple availability zones to help maintain availability during a disaster. Disaster recovery and incident response procedures are tested annually to ensure that the cloud service can be successfully and efficiently restored.

The Xero production service resides in the AWS US-East-1 region across three physically separate, isolated AWS data centers which are connected with low latency, high throughput, and highly redundant networking. Data is replicated across data centers located within AWS US-East-1 and US-West-2 regions. Xero has stores backups in Canada of new organisations with a Canadian location. These are backups of the primary database supporting Xero services, which stores base configuration and accounting data. These backups are in AWS CA-Central-1 region (Montreal)

Xero has a disaster recovery (DR) strategy in place which outlines Xero disaster recovery architecture, availability requirements for Xero services, Xero core infrastructure components, and the actions to be followed to support data center failover. The plan includes recovery time objectives (RTO), the recovery point objective (RPO), key teams, and recovery processes to be followed in the event of a data center failure. Methods for testing the plans may include walk-throughs or simulations.

A business impact analysis is performed on at least an annual basis that identifies RTOs and RPOs for each identified process and relates specific risks to their potential impact. Xero reviews and tests the business continuity plans on an annual basis that include regional and team-specific tests to help maintain a resilient service across all regions. Each individual team is responsible for maintaining its plans and training employees in roles and responsibilities as part of the business continuity plan (BCP) and DR testing.

## Data

The following table describes the information used and supported by the system.

Data Used and Supported by the System		
Data Description	Data Reporting	Classification
Customer data	Xero accounting system / customer portal	Confidential
Customer profile and billing information		
Customer support tickets and incident reports	Customer portal / ticketing system	

### *Data Encryption*

Documented policies and standards are in place that prohibit the transmission of sensitive information over the Internet or other public communications paths unless it is encrypted. Web servers utilize the TLS 1.2 and above encryption protocol to secure web communication sessions with customers. Confidential information is stored in Amazon S3 buckets and Amazon RDS instances are configured to encrypt data at rest with Advanced Encryption Standard (AES)-256 to prevent access by unauthorised parties. Xero relies on Software-as-a-Service (SaaS) providers' key management capabilities, including AWS Key Management Service (KMS), and obtains assurance over these processes as part of vendor reviews. Encryption keys that are managed by Xero are classified as confidential data and require strict encryption requirements in transit and at rest. Encryption key management procedures are defined and documented within the cryptography security policy and data controls standard.

### *Data Retention and Disposal*

Confidential information retention and disposal practices are communicated to customers via customer agreements, terms of use, and security documentation made available to customers via Xero's public-facing website. The current definitions of data classifications are documented in the data classifications standard. Customer data is classified as confidential and not disclosed to unauthorised parties. Xero retains customer data for a period of seven years following the termination of a customer agreement and removes customer data at the end of the seven-year retention period or upon customer request. Xero maintains procedures for customers to initiate these data deletion requests. The results of the disposal of customer confidential information are documented and tracked through resolution within the ticketing system.

### **Significant Changes During the Period**

The Xero Go application was retired on September 12, 2024. Customers were notified of the intended decommissioning on March 12, 2024, that included guidelines to export their or request deletion of information commensurate with regulatory requirements. Xero Go data not requested for deletion is retained for up to seven years in compliance with Xero's data retention policies.

### **Subservice Organizations**

The cloud hosting services provided by AWS were not included within the scope of this examination.

The following table presents the applicable Trust Services criteria that are intended to be met by controls at AWS, alone or in combination with controls at Xero, and the types of controls expected to be implemented at AWS to achieve Xero’s principal service commitments and system requirements based on the applicable trust services criteria.

Ref.	Control Activities Expected to be Implemented by the Subservice Organization	Applicable Trust Services Criteria
1.	AWS is responsible for implementing controls that ensure logical access to the underlying network, virtualization management, and storage devices is managed for its cloud hosting services where in-scope systems reside.	CC6.1 – CC6.3 CC6.5 – CC6.6
2.	AWS is responsible for implementing controls that ensure physical access to data center facilities, backup data, and other system components such as virtual systems and servers is restricted.	CC6.4 – CC6.5
3.	AWS is responsible for implementing controls to restrict and protect information during transmission, movement, and removal from the underlying storage devices for its cloud hosting services where in-scope systems reside.	CC6.7
4.	AWS is responsible for implementing controls that ensure the data center facilities are equipped with physical and environmental security safeguards.	A1.2

## CONTROL ENVIRONMENT

The control environment at Xero is the foundation for the other areas of internal control. It sets the tone of the organization and influences the control consciousness of its personnel. The components of the control environment factors include the integrity and ethical values; management’s commitment to competence; its organizational structure; the assignment of authority and responsibility; and the oversight and direction provided by the board of directors, audit committee, nomination committee, remuneration committee, and operations management.

### 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 Xero’s control environment, affecting the design, administration, and monitoring of control activities. Xero utilizes company-wide programmes and policies designed to promote integrity and ethical values among its personnel. Xero has published a code of conduct that details Xero’s standards and values and sets out expectations for behavior and conducting business at Xero. The code of conduct is available to all Xero directors, officers, employees, contractors, and consultants via the public-facing website and intranet. Employees receive code of conduct training on at least an annual basis to ensure that employees acknowledge the policies that comprise the code of conduct and the importance of the code of conduct to Xero’s business practices.

Employees are required to sign employment contracts that include non-disclosure agreements (NDAs) upon hire to acknowledge ethical and behavioral value, internal control responsibilities, and to agree not to disclose proprietary or confidential information. In addition, employees and contractors are required to acknowledge an acceptable use standard upon hire / onboarding prior to being granted access to Xero information assets. Background checks are conducted as a component of the hiring process for any employees or contractors in a position of trust to ensure that individuals align with Xero’s values of integrity and ethics. An online whistleblowing channel has been established for employees to anonymously report activities that may lead to or are unethical business practices. Concerns received are investigated, internally escalated, and reported on appropriately, including to the Chair of the Board, Chair of the People and Remuneration Committee (RemCo), Chair of the Audit and Risk Management Committee (ARMC), or the Board. Where required, the whistleblowing concern is also escalated to a regulator.

## **Board of Directors, Audit Committee, Nomination Committee, and Remuneration Committee Oversight**

Xero's commitments and control consciousness begins with the Board of Directors. The Board is responsible for overseeing and appraising Xero's strategies, policies, performance, function of internal control, and governance framework. The Board is composed of directors and non-executive directors independent from management who bring a mix of skills, knowledge, experience, diversity, and independence, together with a deep understanding of and competence to deal with current and emerging issues to guide the business. The Board meets with established committees at least annually to discuss and review business objectives such as company updates, company initiatives, risk management activities, and results from other committees: the ARMC, the RemCo, and the Nominations Committee (NomCo).

The ARMC, RemCo, and NomCo are comprised of at least three non-executive director members, a majority of whom are independent of management. The ARMC and NomCo meet with the Board quarterly while the RemCo meets with the Board on at least an annual basis to review areas including financial reporting, principles and policies, risk management, compliance, external audit functions, internal control processes, organizational structure and culture, remuneration, employee performance and development, and succession planning. The ARMC, NomCo, and RemCo establish and maintain charters that are reviewed at least every two years and are available via the public-facing website.

## **Organizational Structure and Assignment of Authority and Responsibility**

Xero's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Establishing a relevant organizational structure includes the consideration of key areas of authority, responsibility, and lines of reporting. Xero's organizational structure depends, in part, on its size and the nature of its activities. A security governance structure for information security is defined, and the defined roles and responsibilities are allocated to accountable leadership.

This factor includes how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. Conflicting duties and areas of responsibility are segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets. Xero has implemented organizational charts that communicate the defined key areas of authority, responsibility, and lines of reporting to personnel and are communicated to employees via the company intranet. In addition, documented job descriptions are in place to define the skills, responsibilities, and knowledge level required for particular jobs. Job descriptions are reviewed in response to major process, technology, perceived risk, or business changes and are approved by senior management and the PX (HR) team. Xero leadership demonstrates leadership and commitment to the effectiveness of the information security management system by ensuring information security policies and objectives are compatible with Xero's strategy, and that security objectives are achieved. To accomplish this, management integrates the information security management system into business processes, provides required resources, communicates the importance of conforming to requirements, supports management, and promotes continual improvement.

## **Commitment to Competence**

Competence is the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Xero's commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into requisite skills and knowledge. Security requirements and responsibilities are communicated to employees and contractors via mandatory security awareness training to support business and regulatory objectives. Upon hire, employees are required to complete security and privacy awareness training to ensure security best practices are communicated and adopted. Additionally, Xero employees and contractors are provided with security and privacy awareness training courses, which they will be reminded to complete on an annual basis. This training is the basis for a wider security education programme, where we deliver additional content throughout the year to raise awareness about security topics, and announce any changes to policies and procedures related to security. Skill-based training and development courses are available to employees via a learning management system (LMS) to maintain and advance the skill level of personnel.

## **Accountability**

Management establishes accountability by setting a strong tone at the top and holding those accountable for internal control responsibilities. Management communicates the internal control responsibilities and the criteria that employees will be measured against as well as incentives and other rewards. Roles and responsibilities are formally documented to define and communicate the associated responsibilities for particular roles.

---

## **RISK ASSESSMENT**

Xero has established a risk assessment framework to identify, analyse, mitigate, and manage risks relevant to the cloud-based accounting system. Various types of risks are considered, including but not limited to, fraud, personnel, technological, compliance, and vendor risks. Control activities serve as mechanisms for mitigating identified risks and help to ensure Xero achieves its commitments.

### **Objective Setting**

Xero recognizes the importance of the ongoing identification and management of risk in order to provide the board of directors and other committees with reasonable assurance that Xero's principal service commitments can be achieved. The risk assessment process includes the identification and analysis of risks that pose a threat to the organization's ability to provide in-scope services. The process starts with determining the organization's internal and external commitments as these commitments are key to understanding the risks and allow for the identification and analysis of those risks relative to the achievement of those commitments. Management has committed to customers carrying out certain objectives in relation to the services provided. These commitments are documented to ensure that the operations, reporting, and compliance objectives are aligned with the commitments and Xero's mission.

### **Risk Identification and Analysis**

Xero has implemented a security risk management framework to identify, assess, evaluate, and treat security risks, including the identification of vulnerabilities and control deficiencies in the IT environment. The identification of risks can be informed by defined organizational and operational objectives; metrics from monitoring tools; internal and external assessments; analysis of significant changes to the organization or service; and evolving developments in the threat landscape. The risk assessment process begins with establishing the context of the assessment and an asset inventory and threats and vulnerabilities to those assets. The asset management standard defines how assets are managed at Xero and requires an asset register to be maintained. Assets associated with Xero's information and information processing facilities are identified, documented in the asset register, and reviewed on at least an annual basis. The asset register also includes hardware, software, services, buildings, information and information processing facilities, and anything else that has value to Xero. Each entry includes the name of the asset owner who is responsible for asset management, the classification of data, and criticality of the asset to Xero.

Identified risks, vulnerabilities, and deficiencies are documented in a risk register for review by Xero's leadership team (XLT). The identified risks include internal and external risks related to strategic, operational, legal and compliance, financial and emerging risks. An analysis of the likelihood and impact of the risk occurring is performed and a quantifiable risk score is assigned to the identified risk. Risks which exceed the tolerance limits defined by the business have to be considered for protective measures and require the development of a risk treatment plan. The risk register is reviewed by the XLT on at least a semi-annual basis. Xero's risk management framework is managed by the Chief Financial Officer (CFO) function and overseen by the ARMC.

## **Risk Factors**

Management considers risks that can arise from both external and internal factors including the following:

### *External Factors*

- Technological developments
- Changing customer needs or expectations
- Competition that could alter marketing or service activities
- New legislation and regulation that could force changes in policies and strategies
- Natural catastrophes that could lead to changes in operations or information systems
- Economic changes that could have an impact on management decisions

### *Internal Factors*

- Significant changes in policies, processes, or personnel
- Types of fraud, fraud incentives and pressures for employees, fraud opportunities, and employee attitudes and rationalizations for fraud
- A disruption in information systems processing
- The quality of personnel hired, and methods of training utilized
- Changes in management responsibilities

## **Potential for Fraud**

Xero considers the pressures, opportunities, and motivation for fraud when assessing the risks to the company's objectives. The potential for fraud can occur in both financial and non-financial reporting. Other types of fraud include the misappropriation of assets and illegal acts such as violations of governmental laws.

Management realizes that the potential for fraud can occur when employees are motivated by certain pressures or incentivized to commit fraud. The absence of controls, or ineffective controls, provides an opportunity for fraud when combined with an incentive to commit fraud. Therefore, the annual risk assessment considers the potential for fraud.

## **Risk Mitigation**

Xero has defined and applies an information security risk mitigation process to select appropriate information security risk treatment options. Risk mitigation activities include the identification, selection, and development of control activities that reduce the assessed risks to predefined levels of acceptance, including risks arising from potential business disruptions; however, the relative costs versus benefits are also considered when determining the risk mitigation activities. Xero identifies, selects, and implements controls that contribute to risk treatment. These mitigation steps are documented within the risk register. The security risk team assists teams to identify risk treatment options and provides input as to the likely residual risk score once treatments are applied. A risk owner is assigned to each identified risk. Once the risk treatment plans and mitigation have been implemented to mitigate risk to a tolerable level, the risk owner provides approval and accepts the residual information security risks.

Risks that are assessed as presenting a significant risk to Xero, or which may require a substantial effort to remediate and/or have multiple owners, are escalated to the Security Governance Group (SGG). The SGG reaches a consensus assessment of the risk to Xero's business, agrees with the appropriate risk treatment strategy, and ensures it is communicated, prioritized, and resourced so that remediation occurs by the agreed target date.

During risk treatment, asset owners and management consider the following options:

- Accept: Decide to accept the risk and not to implement any control

- Transfer: Transfer the risk to other bodies (e.g., insurance)
- Mitigate/Control: Implement a control to mitigate the risk
- Avoid/Terminate: Forgo the system which has risk

Risk treatment plans are documented within a ticketing system and the risk register with a link to the risk acceptance document or treatment plan. The security risk team reviews accepted risks annually to ensure that the acceptance is still appropriate and within the business's risk appetite.

---

## TRUST SERVICES CRITERIA AND RELATED CONTROL ACTIVITIES

### Integration with Risk Assessment

Along with assessing risks, management has identified and put into effect actions needed to address those risks. In order to address risks, control activities have been placed into operation to help ensure that the actions are carried out properly and efficiently. Control activities serve as mechanisms for managing the achievement of the security, availability, and confidentiality categories.

### Selection and Development of Control Activities

The applicable trust services criteria and related control activities are included in Section 4 of this report to eliminate the redundancy that would result from listing the items in this section and repeating them in Section 4. Although the applicable trust services criteria and related control activities are included in Section 4, they are, nevertheless, an integral part of Xero's description of the system.

The description of the service auditor's tests of operating effectiveness and the results of those tests are also presented in Section 4, the Testing Matrices, adjacent to the service organization's description of controls. The description of the tests of operating effectiveness and the results of those tests are the responsibility of the service auditor and should be considered information provided by the service auditor.

### Trust Services Criteria Not Applicable to the In-Scope System

All criteria within the security, availability, and confidentiality categories are applicable to the Cloud Based Accounting system.

---

## INFORMATION AND COMMUNICATION SYSTEMS

Xero identifies, captures, and communicates pertinent information in a form and timeframe that enables personnel to carry out their responsibilities. Information systems produce reports containing operational, financial, and compliance-related information that make it possible to run and control the business. Xero deals not only with internally generated data, but also information about external events, activities, and conditions necessary to inform business decision-making and external reporting. Effective communication also occurs in a broader sense, flowing down, across, and up the organization. Personnel receive a clear message from top management that control responsibilities must be taken seriously. Personnel must understand their own role in the internal control system, as well as how individual activities relate to the work of others.

### *Internal Communications*

Xero has implemented various methods of internally communicating information, including objectives and responsibilities to support the functioning of internal control. Xero maintains communication with employees using corporate private social networks, internal knowledge bases, e-mail, and global employee meetings. The communication includes but is not limited to publication of Xero's policies and procedures, corporate events, new initiatives, strategies, market updates, awareness, and training (including security awareness). Xero has developed and implemented an information security management system (ISMS) for ensuring the confidentiality, integrity, and availability of its services and information assets. The ISMS operates within the context of Xero's activities, and is documented, maintained, and continually improved. Policies and procedures specific to Xero's operations, including those for managing security, availability, and confidentiality, are made available to Xero personnel on the company intranet as well as changes and updates. Xero employees and, where relevant, contractors receive appropriate awareness education and training in and regular updates on organizational policies and procedures, as relevant to their job function. The technical security knowledge base is reviewed on at least an annual basis by the technical security team and is made available for developers to use during development activities.

### *External Communications*

Xero has implemented various methods of communication with external parties to help provide assurance that customers understand their roles and responsibilities in the communication of significant events. Xero utilizes its website (via the terms of use), blog, e-mail, in-app notifications, and social media to communicate to external customers, vendors, and other parties. Through these communications, Xero communicates to a potential or current customer of Xero the functionality of the services provided, and the responsibilities of each party in relation to such services. In addition, information communicated to customers includes, but is not limited to, information on the boundaries that exist between Xero's provision of the services and a customer's use of the services.

Further, Xero's public-facing website describes security measures that Xero has in place, including network infrastructure and data security, privacy, and availability. Xero has implemented a security noticeboard on their website that is regularly updated with security information relevant to customers and other external parties. Customer commitments and responsibilities are communicated through Xero's terms of use and in agreements where applicable. The terms of use include basic conditions for Xero customers to adhere to relating to accessing and using Xero's computing systems or networks. An NDA is signed by third parties prior to confidential information being shared with them.

---

## **MONITORING**

Monitoring is a process that assesses the quality of internal control performance over time. It involves assessing the design and operation of controls and taking necessary corrective actions. This process is accomplished through ongoing activities, separate evaluation, or a combination of the two. Monitoring activities also include using information from communications from external parties such as user entity complaints and regulatory comments that may indicate problems or highlight areas in need of improvement. Management has implemented a self-assessment and compliance programme to ensure the controls are consistently applied as designed.

### *Ongoing Monitoring and Separate Evaluations*

Xero performs ongoing monitoring through both automated and manual activities. On a quarterly basis, external vulnerability scans of the web application are performed to identify and analyse new vulnerabilities. Identified vulnerabilities are configured to notify operations and management personnel when service thresholds are exceeded and are triaged by product teams and monitored through resolution.

A dedicated customer experience (CX) team is in place to service customer requests and monitor customer feedback on performance issues, which are communicated to the platform and product teams for resolution. Customers have the ability to file their own support tickets through Xero central support via the public-facing website.

In addition, Xero performs a review and evaluation of Xero's information security management system on at least an annual basis by conducting audits and reviews of security management activities (i.e., governance, risk and

assurance processes and activities), security documentation (e.g., policies, standards, and guidelines), and the controls implemented, through control effectiveness assessment, testing and audits. The security management system is also reviewed by the SGG on at least an annual basis to ensure compliance with standards.

#### *Subservice Organization Monitoring*

Xero maintains a vendor management programme that evaluates and monitors vendors, including AWS, to ensure compliance with Xero's requirements for third parties. Prior to onboarding new vendors, NDAs are established with third parties where sensitive information is included within the scope of the services to be provided to Xero. A vendor risk assessment is performed to determine a vendor's risk classification and evaluate associated vendor risks. Vendors classified as "critical" or "high risk" undergo additional due diligence assessments to ensure that vendors are capable of supporting Xero's service commitments. Xero conducts an annual review of active critical vendors to monitor for continued compliance with Xero's requirements.

#### **Evaluating and Communicating Deficiencies**

Deficiencies in Xero's internal control system can surface from numerous sources, including ongoing monitoring activities, separate evaluations of the internal control system and external auditing parties. Xero has developed processes for communicating identified deficiencies to the board of directors through updates on the security and compliance programme included in annual board meetings. Additionally, the ARMC meets quarterly to strategize remediation plans for any identified deficiencies. Mitigating strategies are developed for identified control gaps to promote continuous improvement of Xero's security programme. Alerts relevant to Xero are triaged and resolved in accordance with the vulnerability management policy. Security, availability, and confidentiality incidents, including customer related incidents, are tracked by security personnel via a ticketing system to document activities and the corresponding resolution.

---

## **COMPLEMENTARY CONTROLS AT USER ENTITIES**

Xero's controls are designed to provide reasonable assurance that the principal service commitments and system requirements can be achieved without the implementation of complementary controls at user entities. As a result, complementary user entity controls are not required, or significant, to achieve the principal service commitments and system requirements based on the applicable trust services criteria.

# SECTION 4

## TESTING MATRICES

## TESTS OF OPERATING EFFECTIVENESS AND RESULTS OF TESTS

### Scope of Testing

This report on the controls relates to the Cloud Based Accounting system provided by Xero. The scope of the testing was restricted to the Cloud Based Accounting system and its boundaries as defined in Section 3. Schellman conducted the examination testing over the period November 1, 2023, through October 31, 2024.

### Tests of Operating Effectiveness

The tests applied to test the operating effectiveness of controls are listed alongside each of the respective control activities within the Testing Matrices. Such tests were considered necessary to evaluate whether the controls were sufficient to provide reasonable, but not absolute, assurance that the applicable trust services criteria were achieved during the period. In selecting the tests of controls, Schellman considered various factors including, but not limited to, the following:

- the nature of the control and the frequency with which it operates;
- the control risk mitigated by the control;
- the effectiveness of entity-level controls, especially controls that monitor other controls;
- the degree to which the control relies on the effectiveness of other controls; and
- whether the control is manually performed or automated.

The types of tests performed with respect to the operational effectiveness of the control activities detailed in this section are briefly described below:

Test Approach	Description
Inquiry	Inquired of relevant personnel with the requisite knowledge and experience regarding the performance and application of the related control activity. This included in-person interviews, telephone calls, e-mails, web-based conferences, or a combination of the preceding.
Observation	Observed the relevant processes or procedures during fieldwork. This included, but was not limited to, witnessing the performance of controls or evidence of control performance with relevant personnel, systems, or locations relevant to the performance of control policies and procedures.
Inspection	Inspected the relevant audit records. This included, but was not limited to, documents, system configurations and settings, or the existence of sampling attributes, such as signatures, approvals, or logged events. In some cases, inspection testing involved tracing events forward to consequent system documentation or processes (e.g. resolution, detailed documentation, alarms, etc.) or vouching backwards for prerequisite events (e.g. approvals, authorizations, etc.).

### Sampling

Consistent with American Institute of Certified Public Accountants (AICPA) authoritative literature, Schellman utilizes professional judgment to consider the tolerable deviation rate, the expected deviation rate, the audit risk, the characteristics of the population, and other factors, in order to determine the number of items to be selected in a sample for a particular test. Schellman, in accordance with AICPA authoritative literature, selected samples in such a way that the samples were expected to be representative of the population. This included judgmental selection methods, where applicable, to ensure representative samples were obtained.

System-generated population listings were obtained whenever possible to ensure completeness prior to selecting samples. In some instances, full populations were tested in cases including but not limited to, the uniqueness of the event or low overall population size.

### Reliability of Information Provided by the Service Organization

Observation and inspection procedures were performed related to certain system-generated reports, listings, and queries to assess the accuracy and completeness (reliability) of the information used in the performance of our testing of the controls.

### Test Results

The results of each test applied are listed alongside each respective test applied within the Testing Matrices. Test results not deemed as control deviations are noted by the phrase “No exceptions noted.” in the test result column of the Testing Matrices. Any phrase other than the aforementioned constitutes either a test result that is the result of non-occurrence, a change in the application of the control activity, or a deficiency in the operating effectiveness of the control activity. Testing deviations identified within the Testing Matrices are not necessarily weaknesses in the total system of controls, as this determination can only be made after consideration of controls in place at user entities and subservice organizations, if applicable, and other factors. Control considerations that should be implemented by subservice organizations in order to complement the control activities and achieve the service commitments and system requirements are presented in the “Subservice Organizations” section within Section 3.

## SECURITY CATEGORY

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
<b>Control Environment</b>			
CC1.1 – COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
CC1.1.1	Terms of employment and Xero's ethical and behavioral values and expectations are communicated via employment contracts and the code of conduct.	Inspected the code of conduct and an example employment contract to determine that terms of employment and Xero's ethical and behavioral values and expectations were communicated via employment contracts and the code of conduct.	No exceptions noted.
CC1.1.2	Mandatory security awareness training includes security requirements and expectations of Xero employees in achieving internal control responsibilities to meet business and regulatory objectives.	Inspected the security and privacy awareness training material to determine that mandatory security awareness training included security requirements and expectations of Xero employees in achieving internal control responsibilities to meet business and regulatory objectives.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.1.3	Employees receive code of conduct training on at least an annual basis to ensure that employees acknowledge the policies that comprise the code of conduct and the importance of the code of conduct to Xero's business practices.	Inspected the code of conduct training material and results for a sample of current employees to determine that training was completed during the period for each employee sampled to help ensure that employees acknowledged the policies that comprised the code of conduct and the importance of the code of conduct to Xero's business practices.	No exceptions noted.
CC1.1.4	A communication channel is available for employees to submit whistleblower reports that are received by the Chair of the Board, the Chair of the ARMC, and the Chief Legal Officer.	Inspected the whistleblower policy to determine that a communication channel was available for employees to submit whistleblower reports that were received by the Chair of the Board, the Chair of the ARMC, and the Chief Legal Officer.	No exceptions noted.
CC1.1.5	Xero employees and contractors are provided with security and privacy awareness training courses, which they will be reminded to complete on an annual basis.	Inspected the security and privacy awareness education and training notifications to determine that Xero employees and contractors were provided with security and privacy awareness training courses, which they were reminded to complete on an annual basis.	No exceptions noted.
		Inspected the security and privacy awareness training results for a sample of employees hired during the period to determine that security and privacy awareness education and training was completed upon hire for each employee sampled.	No exceptions noted.
CC1.1.6	Employees and contractors agree to the IT acceptable use standard before they are granted access to Xero information assets.	Inspected the signed IT acceptable use Standard for a sample of employees hired during the period to determine that each employee and contractor sampled agreed to the IT acceptable use standard before they were granted access to Xero information assets.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.1.7	<p>Xero leadership demonstrates leadership and commitment to the effectiveness of the information security management system by:</p> <ol style="list-style-type: none"> <li>1) Ensuring its information security policy and objectives are compatible with Xero's strategy, and that security objectives are achieved</li> <li>2) Making sure the information security management system is integrated into Xero's business processes and the required resources are available</li> <li>3) Communicating the importance of conforming to requirements to ensure effective information security</li> <li>4) Supporting management to provide leadership and directing and supporting people to contribute to the effectiveness of the information security management system</li> <li>5) Promoting continual improvement</li> </ol>	<p>Inspected the IT security policy to determine that Xero leadership demonstrated leadership and commitment to the effectiveness of the information security management system by:</p> <ol style="list-style-type: none"> <li>1) Ensuring its information security policy and objectives are compatible with Xero's strategy, and that security objectives are achieved</li> <li>2) Making sure the information security management system is integrated into Xero's business processes and the required resources are available</li> <li>3) Communicating the importance of conforming to requirements to ensure effective information security</li> <li>4) Supporting management to provide leadership and directing and supporting people to contribute to the effectiveness of the information security management system</li> <li>5) Promoting continual improvement</li> </ol>	No exceptions noted.
CC1.2 – COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.			
CC1.2.1	The ARMC is comprised of at least three non-executive director members, a majority of who must be independent.	Inspected the ARMC board member listing to determine that the ARMC was comprised of at least three non-executive director members that were independent from management.	No exceptions noted.
CC1.2.2	The ARMC meets quarterly with the Board to review areas including financial reporting principles and policies, risk management, compliance, external audit functions, and internal control processes.	Inspected the ARMC committee meeting calendar invite and meeting agenda for a sample of quarters during the period to determine that the ARMC met with the Board for each quarter sampled and reviewed areas including financial reporting principles and policies, risk management, compliance, external audit functions, and internal control processes.	No exceptions noted.
CC1.2.3	The ARMC establishes and maintains a charter that is reviewed at least every two years and is available via the public-facing website.	Inspected the ARMC committee charter to determine that an established charter was maintained and reviewed at least every two years and was available via the public-facing website.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.2.4	The NomCo is comprised of at least three non-executive director members, a majority of who must be independent.	Inspected the NomCo board member listing to determine that the NomCo was comprised of at least three non-executive director members that were independent from management.	No exceptions noted.
CC1.2.5	The NomCo meets on at least an annual basis with the Board to review and make recommendations as to the size and composition of the Board and its committees, taking into account the appropriate mix of skills, knowledge, experience, diversity and independence.	Inspected the most recent NomCo meeting minutes to determine that the NomCo met with the Board during the period to review and make recommendations as to the size and composition of the Board and its committees, taking into account the appropriate mix of skills, knowledge, experience, diversity and independence.	No exceptions noted.
CC1.2.6	The Board, with assistance from the NomCo, reviews and evaluates its own performance, including against the requirements of the Board charter, on an annual basis.	Inspected the NomCo meeting minutes to determine that the Board and NomCo reviewed and evaluated performance during the period.	No exceptions noted.
CC1.2.7	The NomCo establishes and maintains a charter that is reviewed at least every two years and is available via the public-facing website.	Inspected the NomCo committee charter to determine that an established charter was maintained and reviewed at least every two years and was available via the public-facing website.	No exceptions noted.
CC1.2.8	RemCo is comprised of at least three non-executive director members, a majority of who must be independent.	Inspected the RemCo board member listing to determine that the RemCo was comprised of at least three non-executive director members that were independent from management.	No exceptions noted.
CC1.2.9	The RemCo charter is reviewed at least every two years and is available via the public-facing website.	Inspected the RemCo committee charter to determine that an established charter was maintained and reviewed at least every two years and was available via the public-facing website.	No exceptions noted.
CC1.2.10	To maintain independence, the Head of Assurance has a reporting line to the Chair of the Audit and Risk Management (ARM) Committee and meets on at least an annual basis with the Chair without management present.	Inspect the scheduled meetings the head of assurance has with the chair of the ARMC to determine that the head of assurance has a reporting line to the chair of the ARMC and meets at least on an annual basis without management present	No exceptions noted.
<b>CC1.3 – COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.</b>			
CC1.3.1	A security governance structure for information security is defined, and the defined roles and responsibilities are allocated to accountable leadership.	Inspected the security governance group charter to determine that information security was defined, and the defined roles and responsibilities were allocated to accountable leadership.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.3.2	Conflicting duties and areas of responsibility are segregated to reduce opportunities for unauthorised or unintentional modification or misuse of the organisation's assets.	Inspected the Xero organisational chart to determine that conflicting duties and areas of responsibility were segregated to reduce opportunities for unauthorised or unintentional modification or misuse of the organisation's assets.	No exceptions noted.
CC1.3.3	Job descriptions are in place which define roles and responsibilities, skills, knowledge levels and required competencies.	Inspected the job description for a sample of current employees to determine that documented job descriptions were in place for each employee sampled and defined roles and responsibilities, skills, knowledge levels and required competencies.	No exceptions noted.
CC1.3.4	Job descriptions are reviewed in response to major process, technology, perceived risk, or business changes and are approved by senior management and the PX (HR) team.	Inspected the review of a job description update to determine that job descriptions were reviewed in response to major process, technology, perceived risk, or business changes and were approved during the period by senior management and the PX (HR) team.	No exceptions noted.
CC1.4 – COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
CC1.4.1	A security governance structure for information security is defined, and the defined roles and responsibilities are allocated to accountable leadership.	Inspected the security governance group charter to determine that information security was defined, and the defined roles and responsibilities were allocated to accountable leadership.	No exceptions noted.
CC1.4.2	Background verification checks on candidates for employment or contract work are carried out in accordance with relevant laws and regulations, and are conducted in proportion to business requirements, the classification of the information to be accessed, and the perceived risks.	Inspected the completed background verification checks for a sample of employees and contractors hired during the period to determine that background verification checks were completed for each sampled employee or contractor in accordance with relevant laws and regulations and were in proportion to business requirements, the classification of the information to be accessed, and the perceived risks.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.4.3	Employees receive code of conduct training on at least an annual basis to ensure that employees acknowledge the policies that comprise the code of conduct and the importance of the code of conduct to Xero's business practices.	Inspected the code of conduct training material and results for a sample of current employees to determine that training was completed during the period for each employee sampled to help ensure that employees acknowledged the policies that comprised the code of conduct and the importance of the code of conduct to Xero's business practices.	No exceptions noted.
CC1.4.4	A communication channel is available for employees to submit whistleblower reports that are received by the Chair of the Board, the Chair of the ARMC, and the Chief Legal Officer.	Inspected the whistleblower policy to determine that a communication channel was available for employees to submit whistleblower reports that were received by the Chair of the Board, the Chair of the ARMC, and the Chief Legal Officer.	No exceptions noted.
CC1.4.5	Xero employees and contractors are provided with security and privacy awareness training courses, which they will be reminded to complete on an annual basis.	Inspected the security and privacy awareness education and training notifications to determine that Xero employees and contractors were provided with security and privacy awareness training courses, which they were reminded to complete on an annual basis.	No exceptions noted.
		Inspected the security and privacy awareness training results for a sample of employees hired during the period to determine that security and privacy awareness education and training was completed upon hire for each employee sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.4.6	<p>Xero leadership demonstrates leadership and commitment to the effectiveness of the information security management system by:</p> <ol style="list-style-type: none"> <li>1) Ensuring its information security policy and objectives are compatible with Xero's strategy, and that security objectives are achieved</li> <li>2) Making sure the information security management system is integrated into Xero's business processes and the required resources are available</li> <li>3) Communicating the importance of conforming to requirements to ensure effective information security</li> <li>4) Supporting management to provide leadership and directing and supporting people to contribute to the effectiveness of the information security management system</li> <li>5) Promoting continual improvement</li> </ol>	<p>Inspected the IT security policy to determine that Xero leadership demonstrated leadership and commitment to the effectiveness of the information security management system by:</p> <ol style="list-style-type: none"> <li>1) Ensuring its information security policy and objectives are compatible with Xero's strategy, and that security objectives are achieved</li> <li>2) Making sure the information security management system is integrated into Xero's business processes and the required resources are available</li> <li>3) Communicating the importance of conforming to requirements to ensure effective information security</li> <li>4) Supporting management to provide leadership and directing and supporting people to contribute to the effectiveness of the information security management system</li> <li>5) Promoting continual improvement</li> </ol>	No exceptions noted.
CC1.4.7	Job descriptions are in place which define roles and responsibilities, skills, knowledge levels and required competencies.	Inspected the job description for a sample of current employees to determine that documented job descriptions were in place for each employee sampled and defined roles and responsibilities, skills, knowledge levels and required competencies.	No exceptions noted.
CC1.4.8	Job descriptions are reviewed in response to major process, technology, perceived risk, or business changes and are approved by senior management and the PX (HR) team.	Inspected the review of a job description update to determine that job descriptions were reviewed in response to major process, technology, perceived risk, or business changes and were approved during the period by senior management and the PX (HR) team.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.5 – COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
CC1.5.1	The RemCo meets quarterly to oversee Xero's strategies and policies relating to organisational structure and culture, remuneration, employee performance and development, and succession planning.	Inspected the RemCo meeting calendar invite and meeting agenda for a sample of quarters during the period to determine that RemCo met for each quarter sampled to oversee Xero's strategies and policies relating to organisational structure and culture, remuneration, employee performance and development, and succession planning.	No exceptions noted.
CC1.5.2	A security governance structure for information security is defined, and the defined roles and responsibilities are allocated to accountable leadership.	Inspected the security governance group charter to determine that information security was defined, and the defined roles and responsibilities were allocated to accountable leadership.	No exceptions noted.
CC1.5.3	Terms of employment and Xero's ethical and behavioral values and expectations are communicated via employment contracts and the code of conduct.	Inspected the code of conduct and an example employment contract to determine that terms of employment and Xero's ethical and behavioral values and expectations were communicated via employment contracts and the code of conduct.	No exceptions noted.
CC1.5.4	Mandatory security awareness training includes security requirements and expectations of Xero employees in achieving internal control responsibilities to meet business and regulatory objectives.	Inspected the security and privacy awareness training material to determine that mandatory security awareness training included security requirements and expectations of Xero employees in achieving internal control responsibilities to meet business and regulatory objectives.	No exceptions noted.
CC1.5.5	A communication channel is available for employees to submit whistleblower reports that are received by the Chair of the Board, the Chair of the ARMC, and the Chief Legal Officer.	Inspected the whistleblower policy to determine that a communication channel was available for employees to submit whistleblower reports that were received by the Chair of the Board, the Chair of the ARMC, and the Chief Legal Officer.	No exceptions noted.
CC1.5.6	Xero requires employees as part of signing their employment contract, and contractors, to sign agreements that include non-disclosure provisions and asset protection responsibilities, upon hire.	Inspected the signed NDA for a sample of employees and contractors hired during the period to determine that Xero required employees to sign agreements that included non-disclosure provisions and asset protection responsibilities, upon hire, for each employee sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.5.7	NDA's are established with third parties during the procurement process where sensitive information is included within the scope of the services to be provided to Xero.	Inspected the NDA established with a sample of vendors onboarded during the period to determine that NDA's were established during the procurement process for each vendor sampled where sensitive information was included within the scope of the services to be provided to Xero.	No exceptions noted.
CC1.5.8	Xero leadership demonstrates leadership and commitment to the effectiveness of the information security management system by: <ol style="list-style-type: none"> <li>1) Ensuring its information security policy and objectives are compatible with Xero's strategy, and that security objectives are achieved</li> <li>2) Making sure the information security management system is integrated into Xero's business processes and the required resources are available</li> <li>3) Communicating the importance of conforming to requirements to ensure effective information security</li> <li>4) Supporting management to provide leadership and directing and supporting people to contribute to the effectiveness of the information security management system</li> <li>5) Promoting continual improvement</li> </ol>	Inspected the IT security policy to determine that Xero leadership demonstrated leadership and commitment to the effectiveness of the information security management system by: <ol style="list-style-type: none"> <li>1) Ensuring its information security policy and objectives are compatible with Xero's strategy, and that security objectives are achieved</li> <li>2) Making sure the information security management system is integrated into Xero's business processes and the required resources are available</li> <li>3) Communicating the importance of conforming to requirements to ensure effective information security</li> <li>4) Supporting management to provide leadership and directing and supporting people to contribute to the effectiveness of the information security management system</li> <li>5) Promoting continual improvement</li> </ol>	No exceptions noted.
<b>Communication and Information</b>			
CC2.1 – COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.			
CC2.1.1	Xero has defined and applies an information security risk assessment process. Xero has a risk management framework established to identify, report, and manage risks across key risk categories, including operational, strategic, legal, and financial.	Inspected the risk management framework to determine that Xero established an information security risk assessment process to identify, report, and manage risks across key risk categories, including operational, strategic, legal, and financial.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.1.2	Risk assessments are performed on in-scope Xero assets for the information security management system and take into account threats to and vulnerabilities of the asset. The results of the risk assessments are reviewed by management at least twice each year.	Inspected the Xero asset register, the most recent risk register, and the ARMC meeting invite and agenda for a sample of quarters during the period to determine that risk assessments were performed on in-scope Xero assets during the period and took into account threats to and vulnerabilities of the asset, and the results of the risk assessments were reviewed by management during each quarter sampled.	No exceptions noted.
CC2.1.3	The ARMC meets quarterly with the Board to review areas including financial reporting principles and policies, risk management, compliance, external audit functions, and internal control processes.	Inspected the ARMC committee meeting calendar invite and meeting agenda for a sample of quarters during the period to determine that the ARMC met with the Board for each quarter sampled and reviewed areas including financial reporting principles and policies, risk management, compliance, external audit functions, and internal control processes.	No exceptions noted.
CC2.1.4	Xero's legal counsel and leadership identify legislation applicable to Xero in order to meet legislative, statutory, regulatory, and contractual requirements for Xero's type of business, in relevant countries. Xero's approach to meet requirements is identified, documented, and kept up to date for each information system and the organisation.	Inspected the organisational chart to determine that Xero's legal counsel and leadership identified legislation applicable to Xero in order to meet legislative, statutory, regulatory, and contractual requirements in relevant countries, and Xero's approach to meet requirements was identified, documented, and kept up to date for each information system and the organisation.	No exceptions noted.
CC2.1.5	The high availability and disaster recovery strategy align with the company strategy and are reviewed at least annually.	Inspected the high availability and disaster recovery strategy to determine that the high availability and disaster recovery strategy aligned with the company strategy and were reviewed during the period.	No exceptions noted.
CC2.1.6	Xero has developed and implemented an ISMS for ensuring the confidentiality, integrity, and availability of its services and information assets. The ISMS operates within the context of Xero's activities, and is documented, maintained, and continually improved.	Inspected the ISMS framework to determine that Xero developed and implemented an ISMS for the confidentiality, integrity, and availability of its services and information assets that operated within the context of Xero's activities, and was documented, maintained, and continually improved.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.1.7	Xero evaluates the information security performance and the effectiveness of the ISMS on at least an annual basis.	Inspected the most recent internal audit and ISMS management review to determine that Xero evaluated the information security performance and the effectiveness of the ISMS during the period.	No exceptions noted.
CC2.1.8	Xero has an internal assurance function that provides independent and objective assurance and advice on Xero's organisational governance, risk management, and internal control processes.	Inspected the security assurance, performance, and compliance framework to determine that an internal assurance function that provided independent and objective assurance and advice on Xero's organisational governance, risk management, and internal control processes.	No exceptions noted.
<b>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.</b>			
CC2.2.1	Operating procedures for operational activities associated with information processing and communication facilities are documented and made available to users who need them. Xero security operations are covered in the operations security standard.	Inspected the operations security standard to determine that operating procedures for operational activities associated with information processing and communication facilities were documented and made available to users, and security operations were covered in the operations security standard.	No exceptions noted.
CC2.2.2	The responsibilities of Xero operational teams are defined in procedures and instructions, in Confluence, Jira, or other tools.	Inspected the operations security standard to determine that the responsibilities of Xero operational teams were defined in procedures and instructions, in Confluence, Jira, or other tools.	No exceptions noted.
CC2.2.3	Changes to Xero's organisation, business processes, information processing facilities and systems that affect information security are controlled, and change details are communicated to relevant persons.	Inspected the path to production standard and all-hands call meeting documentation to determine that changes to Xero's organisation, business processes, information processing facilities and systems that affected information security were controlled, and change details were communicated to relevant persons.	No exceptions noted.
CC2.2.4	Change management processes are in place to ensure that changes are recorded, evaluated authorised, planned, communicated, tested, and implemented successfully, before being deployed to production, in order to reduce the business impact of failed changes on Xero operation and its customers.	Inspected the change ticket for a sample of changes implemented during the period to determine that change management processes were in place to ensure that changes were recorded, evaluated authorised, planned, communicated, tested, and implemented successfully, before being deployed to production, in order to reduce the business impact of failed changes on Xero operation and its customers.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.2.5	An automated ticketing system is in place which allows internal and external system users to report security failures, incidents, and concerns. Incidents and security incidents are responded to and managed to resolution by the incident response manager and the security operations team, respectively.	Inspected the incident ticket for a sample of incidents during the period to determine that an automated ticketing system was in place which allowed internal and external system users to report security failures, incidents and concerns, and incidents, and security incidents were responded to and managed through to resolution.	No exceptions noted.
CC2.2.6	Xero has established information security objectives which are communicated to employees and reviewed on at least an annual basis.	Inspected the assurance, performance, and compliance framework to determine that information security objectives were communicated to employees and reviewed during the period.	No exceptions noted.
CC2.2.7	Xero has determined the need for internal and external communications regarding the ISMS that include: <ol style="list-style-type: none"> <li>1) Regular internal reporting on security risk exposure and compliance status, to Xero's security governance group, ARMC, and the Board</li> <li>2) External regulatory reporting to identified government and regulatory bodies, including mandatory notifications</li> <li>3) Ongoing updates to the Xero security noticeboard to inform external users how to remain secure against relevant threats and vulnerabilities</li> <li>4) Providing advice to external users/customers of the process and their responsibilities for reporting operational failures, incidents, problems, concerns, and complaints</li> </ol>	Inspected the most recent review of information security performance and ISMS effectiveness to determine that Xero has determined the need for internal and external communications regarding the ISMS that included: <ol style="list-style-type: none"> <li>1) Regular internal reporting on security risk exposure and compliance status, to Xero's security governance group, ARMC, and the Board</li> <li>2) External regulatory reporting to identified government and regulatory bodies, including mandatory notifications</li> <li>3) Ongoing updates to the Xero security noticeboard to inform external users how to remain secure against relevant threats and vulnerabilities</li> <li>4) Providing advice to external users/customers of the process and their responsibilities for reporting operational failures, incidents, problems, concerns, and complaints</li> </ol>	No exceptions noted.
CC2.3 – COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.			
CC2.3.1	Requirements for confidentiality or NDAs reflecting Xero's needs for the protection of information are identified, documented, and reviewed by the legal team.	Inspected the confidentiality and NDA template and most recent template review to determine that requirements for confidentiality or NDAs reflecting Xero's needs for the protection of information were identified, documented, and reviewed by the legal team.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.3.2	Xero requires employees as part of signing their employment contract, and contractors, to sign agreements that include non-disclosure provisions and asset protection responsibilities, upon hire.	Inspected the signed NDA for a sample of employees and contractors hired during the period to determine that Xero required employees to sign agreements that included non-disclosure provisions and asset protection responsibilities, upon hire, for each employee sampled.	No exceptions noted.
CC2.3.3	NDAs are established with third parties during the procurement process where sensitive information is included within the scope of the services to be provided to Xero.	Inspected the NDA established with a sample of vendors onboarded during the period to determine that NDAs were established during the procurement process for each vendor sampled where sensitive information was included within the scope of the services to be provided to Xero.	No exceptions noted.
CC2.3.4	The responsibilities of external users and customers are described on the Xero website.	Inspected the terms of use from the Xero website to determine that the responsibilities of external users and customers were described on the Xero website.	No exceptions noted.
CC2.3.5	Customers are able to file their own support tickets through Xero central support for operational failures, incidents, problems, concerns, and complaints.	Inspected the Xero central website to determine that customers were able to file their own support tickets through Xero central support for operational failures, incidents, problems, concerns, and complaints.	No exceptions noted.
CC2.3.6	An automated ticketing system is in place which allows internal and external system users to report security failures, incidents, and concerns. Incidents and security incidents are responded to and managed to resolution by the incident response manager and the security operations team, respectively.	Inspected the incident ticket for a sample of incidents during the period to determine that an automated ticketing system was in place which allowed internal and external system users to report security failures, incidents and concerns, and incidents, and security incidents were responded to and managed through to resolution.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.3.7	<p>Xero has determined the need for internal and external communications regarding the ISMS that include:</p> <ol style="list-style-type: none"> <li>1) Regular internal reporting on security risk exposure and compliance status, to Xero's security governance group, ARMC, and the Board</li> <li>2) External regulatory reporting to identified government and regulatory bodies, including mandatory notifications</li> <li>3) Ongoing updates to the Xero security noticeboard to inform external users how to remain secure against relevant threats and vulnerabilities</li> <li>4) Providing advice to external users/customers of the process and their responsibilities for reporting operational failures, incidents, problems, concerns, and complaints</li> </ol>	<p>Inspected the most recent review of information security performance and ISMS effectiveness to determine that Xero has determined the need for internal and external communications regarding the ISMS that included:</p> <ol style="list-style-type: none"> <li>1) Regular internal reporting on security risk exposure and compliance status, to Xero's security governance group, ARMC, and the Board</li> <li>2) External regulatory reporting to identified government and regulatory bodies, including mandatory notifications</li> <li>3) Ongoing updates to the Xero security noticeboard to inform external users how to remain secure against relevant threats and vulnerabilities</li> <li>4) Providing advice to external users/customers of the process and their responsibilities for reporting operational failures, incidents, problems, concerns, and complaints</li> </ol>	No exceptions noted.
<b>Risk Assessment</b>			
CC3.1 – COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.			
CC3.1.1	<p>Xero has defined and applies an information security risk assessment process. Xero has a risk management framework established to identify, report, and manage risks across key risk categories, including operational, strategic, legal, and financial.</p>	<p>Inspected the risk management framework to determine that Xero established an information security risk assessment process to identify, report, and manage risks across key risk categories, including operational, strategic, legal, and financial.</p>	No exceptions noted.
CC3.1.2	<p>Risk assessments are performed on in-scope Xero assets for the information security management system and take into account threats to and vulnerabilities of the asset. The results of the risk assessments are reviewed by management at least twice each year.</p>	<p>Inspected the Xero asset register, the most recent risk register, and the ARMC meeting invite and agenda for a sample of quarters during the period to determine that risk assessments were performed on in-scope Xero assets during the period and took into account threats to and vulnerabilities of the asset, and the results of the risk assessments were reviewed by management.</p>	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.1.3	The ARMC establishes and maintains a charter that is reviewed at least every two years and is available via the public-facing website.	Inspected the ARMC committee charter to determine that an established charter was maintained and reviewed at least every two years and was available via the public-facing website.	No exceptions noted.
CC3.1.4	Xero's legal counsel and leadership identify legislation applicable to Xero in order to meet legislative, statutory, regulatory, and contractual requirements for Xero's type of business, in relevant countries. Xero's approach to meet requirements is identified, documented, and kept up to date for each information system and the organisation.	Inspected the organisational chart to determine that Xero's legal counsel and leadership identified legislation applicable to Xero in order to meet legislative, statutory, regulatory, and contractual requirements in relevant countries, and Xero's approach to meet requirements was identified, documented, and kept up to date for each information system and the organisation.	No exceptions noted.
CC3.1.5	Appropriate procedures are implemented to ensure compliance with legislative, regulatory, and contractual requirements related to intellectual property rights and use of proprietary software products.	Inspected the employment agreement for a sample of employees hired during the period to determine that appropriate procedures were implemented, and that each employee sampled complied with legislative, regulatory, and contractual requirements related to intellectual property rights and use of proprietary software products.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.1.6	<p>Xero leadership demonstrates leadership and commitment to the effectiveness of the information security management system by:</p> <ol style="list-style-type: none"> <li>1) Ensuring its information security policy and objectives are compatible with Xero's strategy, and that security objectives are achieved</li> <li>2) Making sure the information security management system is integrated into Xero's business processes and the required resources are available</li> <li>3) Communicating the importance of conforming to requirements to ensure effective information security</li> <li>4) Supporting management to provide leadership and directing and supporting people to contribute to the effectiveness of the information security management system</li> <li>5) Promoting continual improvement</li> </ol>	<p>Inspected the IT security policy to determine that Xero leadership demonstrated leadership and commitment to the effectiveness of the information security management system by:</p> <ol style="list-style-type: none"> <li>1) Ensuring its information security policy and objectives are compatible with Xero's strategy, and that security objectives are achieved</li> <li>2) Making sure the information security management system is integrated into Xero's business processes and the required resources are available</li> <li>3) Communicating the importance of conforming to requirements to ensure effective information security</li> <li>4) Supporting management to provide leadership and directing and supporting people to contribute to the effectiveness of the information security management system</li> <li>5) Promoting continual improvement</li> </ol>	No exceptions noted.
CC3.1.7	<p>Risk assessments are performed on in-scope Xero assets for the information security management system and take into account threats to and vulnerabilities of the asset. The results of the risk assessments are reviewed by management at least twice each year.</p>	<p>Inspected the Xero asset register, the most recent risk register, and the ARMC meeting invite and agenda for a sample of quarters during the period to determine that risk assessments were performed on in-scope Xero assets during the period and took into account threats to and vulnerabilities of the asset, and the results of the risk assessments were reviewed by management.</p>	No exceptions noted.
CC3.1.8	<p>Xero evaluates the information security performance and the effectiveness of the ISMS on at least an annual basis.</p>	<p>Inspected the most recent internal audit and ISMS management review to determine that Xero evaluated the information security performance and the effectiveness of the ISMS during the period.</p>	No exceptions noted.
CC3.1.9	<p>Xero has an internal assurance function that provides independent and objective assurance and advice on Xero's organisational governance, risk management, and internal control processes.</p>	<p>Inspected the security assurance, performance, and compliance framework to determine that an internal assurance function that provided independent and objective assurance and advice on Xero's organisational governance, risk management, and internal control processes.</p>	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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.			
CC3.2.1	Xero has defined and applies an information security risk assessment process. Xero has a risk management framework established to identify, report, and manage risks across key risk categories, including operational, strategic, legal, and financial.	Inspected the risk management framework to determine that Xero established an information security risk assessment process to identify, report, and manage risks across key risk categories, including operational, strategic, legal, and financial.	No exceptions noted.
CC3.2.2	Risk assessments are performed on in-scope Xero assets for the information security management system and take into account threats to and vulnerabilities of the asset. The results of the risk assessments are reviewed by management at least twice each year.	Inspected the Xero asset register, the most recent risk register, and the ARMC meeting invite and agenda for a sample of quarters during the period to determine that risk assessments were performed on in-scope Xero assets during the period and took into account threats to and vulnerabilities of the asset, and the results of the risk assessments were reviewed by management.	No exceptions noted.
CC3.2.3	The ARMC establishes and maintains a charter that is reviewed at least every two years and is available via the public-facing website.	Inspected the ARMC committee charter to determine that an established charter was maintained and reviewed at least every two years and was available via the public-facing website.	No exceptions noted.
CC3.2.4	The asset management standard defines how assets are managed at Xero and requires an asset register to be maintained.	Inspected the asset management standard to determine that the asset management standard defined how assets were managed at Xero and required an asset register to be maintained.	No exceptions noted.
CC3.2.5	Assets associated with Xero's information and information processing facilities have been identified, documented in the Xero asset register, and are reviewed on at least an annual basis. The register also includes hardware, software, services, buildings, information and information processing facilities, and anything else that has value to Xero. Each entry in the Xero asset register includes the name of the asset owner who is responsible for asset management, the classification of data, and criticality of the asset to Xero.	Inspected Xero's asset register to determine that assets associated with Xero's information and information processing facilities were identified, documented, and were reviewed during the period and included hardware, software, services, buildings, information and information processing facilities with an assigned asset owner responsible for asset management, the classification of data, and criticality of the asset to Xero.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.2.6	<p>Xero leadership demonstrates leadership and commitment to the effectiveness of the information security management system by:</p> <ol style="list-style-type: none"> <li>1) Ensuring its information security policy and objectives are compatible with Xero's strategy, and that security objectives are achieved</li> <li>2) Making sure the information security management system is integrated into Xero's business processes and the required resources are available</li> <li>3) Communicating the importance of conforming to requirements to ensure effective information security</li> <li>4) Supporting management to provide leadership and directing and supporting people to contribute to the effectiveness of the information security management system</li> <li>5) Promoting continual improvement</li> </ol>	<p>Inspected the IT security policy to determine that Xero leadership demonstrated leadership and commitment to the effectiveness of the information security management system by:</p> <ol style="list-style-type: none"> <li>1) Ensuring its information security policy and objectives are compatible with Xero's strategy, and that security objectives are achieved</li> <li>2) Making sure the information security management system is integrated into Xero's business processes and the required resources are available</li> <li>3) Communicating the importance of conforming to requirements to ensure effective information security</li> <li>4) Supporting management to provide leadership and directing and supporting people to contribute to the effectiveness of the information security management system</li> <li>5) Promoting continual improvement</li> </ol>	No exceptions noted.
CC3.2.7	<p>Risk assessments are performed on in-scope Xero assets for the information security management system and take into account threats to and vulnerabilities of the asset. The results of the risk assessments are reviewed by management at least twice each year.</p>	<p>Inspected the Xero asset register, the most recent risk register, and the ARMC meeting invite and agenda for a sample of quarters during the period to determine that risk assessments were performed on in-scope Xero assets during the period and took into account threats to and vulnerabilities of the asset, and the results of the risk assessments were reviewed by management.</p>	No exceptions noted.
CC3.2.8	<p>Xero has an internal assurance function that provides independent and objective assurance and advice on Xero's organisational governance, risk management, and internal control processes.</p>	<p>Inspected the security assurance, performance, and compliance framework to determine that an internal assurance function that provided independent and objective assurance and advice on Xero's organisational governance, risk management, and internal control processes.</p>	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.3 – COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.			
CC3.3.1	Xero has defined and applies an information security risk assessment process. Xero has a risk management framework established to identify, report, and manage risks across key risk categories, including operational, strategic, legal, and financial.	Inspected the risk management framework to determine that Xero established an information security risk assessment process to identify, report, and manage risks across key risk categories, including operational, strategic, legal, and financial.	No exceptions noted.
CC3.3.2	Risk assessments are carried out on assets, taking into account their respective asset value with consideration of fraud risk. The annual risk assessments for critical assets are subjected to review in conjunction with the asset owner, and risks that surpass the predetermined tolerance level are regularly monitored by Xero's leadership team at least on a quarterly basis.	Inspected the Xero asset register, the most recent risk register, and the ARMC meeting invite and agenda for a sample of quarters during the period to determine that risk assessments were carried out on assets during the period and took into account their respective asset value with consideration of fraud risk, and critical assets were subjected to review in conjunction with the asset owner, and risks that surpassed the predetermined tolerance level were regularly monitored by Xero's leadership team for each quarter sampled.	No exceptions noted.
CC3.3.3	The ARMC reviews and approves the risk appetite parameters, risk dashboard, and treatments on a quarterly basis.	Inspected the ARMC meeting calendar invites and meeting agendas for a sample of quarters during the period to determine that the ARMC reviewed and approved the risk appetite parameters, risk dashboard, and treatments for each quarter sampled.	No exceptions noted.
CC3.4 – COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.			
CC3.4.1	Changes to Xero's organisation, business processes, information processing facilities and systems that affect information security are controlled, and change details are communicated to relevant persons.	Inspected the path to production standard and all-hands call meeting documentation to determine that changes to Xero's organisation, business processes, information processing facilities and systems that affected information security were controlled, and change details were communicated to relevant persons.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.4.2	Change management processes are in place to ensure that changes are recorded, evaluated authorised, planned, communicated, tested, and implemented successfully, before being deployed to production, in order to reduce the business impact of failed changes on Xero operation and its customers.	Inspected the change ticket for a sample of changes implemented during the period to determine that change management processes were in place to ensure that changes were recorded, evaluated authorised, planned, communicated, tested, and implemented successfully, before being deployed to production, in order to reduce the business impact of failed changes on Xero operation and its customers.	No exceptions noted.
CC3.4.3	A business continuity policy is defined to safeguard good service to Xero's customers, enhance the safety of staff, and protect the interests of other stakeholders.	Inspected the business continuity management policy to determine that a business continuity policy was defined to safeguard good service to our customers, enhance the safety of staff, and protect the interests of other stakeholders.	No exceptions noted.
CC3.4.4	The high availability and disaster recovery strategy align with the company strategy and are reviewed at least annually.	Inspected the high availability and disaster recovery strategy to determine that the high availability and disaster recovery strategy aligned with the company strategy and were reviewed during the period.	No exceptions noted.
CC3.4.5	Risk assessments are carried out on assets, taking into account their respective asset value with consideration of fraud risk. The annual risk assessments for critical assets are subjected to review in conjunction with the asset owner, and risks that surpass the predetermined tolerance level are regularly monitored by Xero's leadership team at least on a quarterly basis.	Inspected the Xero asset register, the most recent risk register, and the ARMC meeting invite and agenda for a sample of quarters during the period to determine that risk assessments were carried out on assets during the period and took into account their respective asset value with consideration of fraud risk, and critical assets were subjected to review in conjunction with the asset owner, and risks that surpassed the predetermined tolerance level were regularly monitored by Xero's leadership team for each quarter sampled.	No exceptions noted.
<b>Monitoring Activities</b>			
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.			
CC4.1.1	Information systems are reviewed on at least an annual basis for compliance with Xero's information security policies and standards.	Inspected the internal audit policy and the most recent internal audit to determine that information systems were reviewed during the period for compliance with Xero's information security policies and standards.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC4.1.2	Automated vulnerability scanning tools are used to perform daily scans to identify and analyse new vulnerabilities. Vulnerabilities identified are communicated to the product teams for review and remediation.	Inspected the daily automated vulnerability scan configurations and example remediation ticket resolved during the period to determine that automated vulnerability scanning tools performed daily network and agent vulnerability scans to identify and analyse new vulnerabilities and identified security vulnerabilities are triaged by the security team and monitored through resolution.	No exceptions noted.
CC4.1.3	A selected panel of independent third parties performs external web application penetration testing and reporting across products in production on at least an annual basis. The results of scans containing vulnerabilities are communicated to the product teams for review and remediation. The resolution state of each vulnerability is tracked once communicated with the product teams.	Inspected the most recent external web application vulnerability scanning report to determine that an independent third party performed external web application vulnerability scanning during the period, and that the results of scans containing vulnerabilities were communicated to the product teams for review and remediation, and that they resolution state of each vulnerability were tracked.	No exception noted.
CC4.1.4	Xero has developed and implemented an ISMS for ensuring the confidentiality, integrity, and availability of its services and information assets. The ISMS operates within the context of Xero's activities, and is documented, maintained, and continually improved.	Inspected the ISMS framework to determine that Xero developed and implemented an ISMS for the confidentiality, integrity, and availability of its services and information assets that operated within the context of Xero's activities, and was documented, maintained, and continually improved.	No exceptions noted.
CC4.1.5	Xero evaluates the information security performance and the effectiveness of the ISMS on at least an annual basis.	Inspected the most recent internal audit and ISMS management review to determine that Xero evaluated the information security performance and the effectiveness of the ISMS during the period.	No exceptions noted.
CC4.1.6	Xero has an internal assurance function that provides independent and objective assurance and advice on Xero's organisational governance, risk management, and internal control processes.	Inspected the security assurance, performance, and compliance framework to determine that an internal assurance function that provided independent and objective assurance and advice on Xero's organisational governance, risk management, and internal control processes.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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.			
CC4.2.1	Xero evaluates the information security performance and the effectiveness of the ISMS on at least an annual basis.	Inspected the most recent internal audit and ISMS management review to determine that Xero evaluated the information security performance and the effectiveness of the ISMS during the period.	No exceptions noted.
CC4.2.2	Xero has an internal assurance function that provides independent and objective assurance and advice on Xero's organisational governance, risk management, and internal control processes.	Inspected the security assurance, performance, and compliance framework to determine that an internal assurance function that provided independent and objective assurance and advice on Xero's organisational governance, risk management, and internal control processes.	No exceptions noted.
CC4.2.3	An automated ticketing system is in place which allows internal and external system users to report security failures, incidents, and concerns. Incidents and security incidents are responded to and managed to resolution by the incident response manager and the security operations team, respectively.	Inspected the incident ticket for a sample of incidents during the period to determine that an automated ticketing system was in place which allowed internal and external system users to report security failures, incidents and concerns, and incidents, and security incidents were responded to and managed through to resolution.	No exceptions noted.
<b>Control Activities</b>			
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.			
CC5.1.1	Conflicting duties and areas of responsibility are segregated to reduce opportunities for unauthorised or unintentional modification or misuse of the organisation's assets.	Inspected the Xero organisational chart to determine that conflicting duties and areas of responsibility were segregated to reduce opportunities for unauthorised or unintentional modification or misuse of the organisation's assets.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.1.2	<p>Xero has defined and applies an information security risk mitigation process to:</p> <ul style="list-style-type: none"> <li>a) Select appropriate information security risk treatment options</li> <li>b) Determine controls that are necessary to implement the information security risk treatment, based on Xero's Unified Controls Catalogue</li> <li>c) Document the chosen option and the selected controls in a security risk treatment plan</li> <li>d) Review and update Xero's Statement of Applicability that contains the necessary controls and justification for inclusions, whether they are implemented or not, and the justification for exclusions</li> <li>e) Obtain risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks</li> </ul>	<p>Inspected the risk management framework to determine that Xero defined and applied an information security risk mitigation process to:</p> <ul style="list-style-type: none"> <li>a) Select appropriate information security risk treatment options</li> <li>b) Determine controls that are necessary to implement the information security risk treatment, based on Xero's Unified Controls Catalogue</li> <li>c) Document the chosen option and the selected controls in a security risk treatment plan</li> <li>d) Review and update Xero's Statement of Applicability that contains the necessary controls and justification for inclusions, whether they are implemented or not, and the justification for exclusions</li> <li>e) Obtain risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks</li> </ul>	No exceptions noted.
CC5.1.3	<p>Xero has established information security objectives which are communicated to employees and reviewed on at least an annual basis.</p>	<p>Inspected the assurance, performance, and compliance framework to determine that information security objectives were communicated to employees and reviewed during the period.</p>	No exceptions noted.
CC5.1.4	<p>Xero has an internal assurance function that provides independent and objective assurance and advice on Xero's organisational governance, risk management, and internal control processes.</p>	<p>Inspected the security assurance, performance, and compliance framework to determine that an internal business assurance function was in place which provided independent and objective assurance and advice on Xero's organisational, governance, risk management and internal control processes and assisted the business in understanding and managing risk.</p>	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.2 – COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.			
CC5.2.1	<p>Xero has defined and applies an information security risk mitigation process to:</p> <ul style="list-style-type: none"> <li>a) Select appropriate information security risk treatment options</li> <li>b) Determine controls that are necessary to implement the information security risk treatment, based on Xero's Unified Controls Catalogue</li> <li>c) Document the chosen option and the selected controls in a security risk treatment plan</li> <li>d) Review and update Xero's Statement of Applicability that contains the necessary controls and justification for inclusions, whether they are implemented or not, and the justification for exclusions</li> <li>e) Obtain risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks</li> </ul>	<p>Inspected the risk management framework to determine that Xero defined and applied an information security risk mitigation process to:</p> <ul style="list-style-type: none"> <li>a) Select appropriate information security risk treatment options</li> <li>b) Determine controls that are necessary to implement the information security risk treatment, based on Xero's Unified Controls Catalogue</li> <li>c) Document the chosen option and the selected controls in a security risk treatment plan</li> <li>d) Review and update Xero's Statement of Applicability that contains the necessary controls and justification for inclusions, whether they are implemented or not, and the justification for exclusions</li> <li>e) Obtain risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks</li> </ul>	No exceptions noted.
CC5.2.2	<p>Xero has defined and documented standards for access control that outline processes for identifying and authenticating authorised users, restricting user access to authorised system components, and preventing and detecting unauthorised system access.</p>	<p>Inspected the access control standard to determine that Xero defined and documented standards for access control that outlined processes for identifying and authenticating authorised users, restricting user access to authorised system components, and preventing and detecting unauthorised system access.</p>	No exceptions noted.
CC5.2.3	<p>Requirements for new information systems or enhancements to existing information systems are defined for product teams in the path to production standard which include identification of security threats and compliance with the security architecture knowledge base that is kept up to date by the security architecture team and available to developers during development activities.</p>	<p>Inspected the path to production standard to determine that requirements for new information systems or enhancements to existing information systems were defined for product teams, which included identification of security threats and compliance with the security architecture knowledge base that was kept up to date by the security architecture team and was available to developers during development activities.</p>	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.2.4	The technical security knowledge base is reviewed on at least an annual basis by the technical security team and is made available for developers to use during development activities.	Inspected the technical security knowledge base via the corporate intranet site to determine that the technical security knowledge base was reviewed during the period by the technical security team and was made available for developers to use during development activities.	No exceptions noted.
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.			
CC5.3.1	<p>Xero leadership demonstrates leadership and commitment to the effectiveness of the information security management system by:</p> <ol style="list-style-type: none"> <li>1) Ensuring its information security policy and objectives are compatible with Xero's strategy, and that security objectives are achieved</li> <li>2) Making sure the information security management system is integrated into Xero's business processes and the required resources are available</li> <li>3) Communicating the importance of conforming to requirements to ensure effective information security</li> <li>4) Supporting management to provide leadership and directing and supporting people to contribute to the effectiveness of the information security management system</li> <li>5) Promoting continual improvement</li> </ol>	<p>Inspected the IT security policy to determine that Xero leadership demonstrated leadership and commitment to the effectiveness of the information security management system by:</p> <ol style="list-style-type: none"> <li>1) Ensuring its information security policy and objectives are compatible with Xero's strategy, and that security objectives are achieved</li> <li>2) Making sure the information security management system is integrated into Xero's business processes and the required resources are available</li> <li>3) Communicating the importance of conforming to requirements to ensure effective information security</li> <li>4) Supporting management to provide leadership and directing and supporting people to contribute to the effectiveness of the information security management system</li> <li>5) Promoting continual improvement</li> </ol>	No exceptions noted.
CC5.3.2	Xero has an internal assurance function that provides independent and objective assurance and advice on Xero's organisational governance, risk management, and internal control processes.	Inspected the security assurance, performance, and compliance framework to determine that an internal business assurance function was in place which provided independent and objective assurance and advice on Xero's organisational, governance, risk management and internal control processes and assisted the business in understanding and managing risk.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.3.3	Information security policies are reviewed at planned intervals, or if significant changes in the Xero environment occur, to ensure their continuing suitability, adequacy, and effectiveness.	Inspected the policies, standards, and guidelines review dashboard to determine that information security policies were reviewed during the period, or if significant changes in the Xero environment occurred, to ensure their continued suitability, adequacy, and effectiveness.	No exceptions noted.
CC5.3.4	A security governance structure for information security is defined, and the defined roles and responsibilities are allocated to accountable leadership.	Inspected the security governance group charter to determine that information security was defined, and the defined roles and responsibilities were allocated to accountable leadership.	No exceptions noted.
<b>Logical and Physical Access Controls</b>			
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.			
CC6.1.1	Production and non-production environments are segregated, with separate AWS accounts and VPCs for each environment.	Inspected the segmented production and non-production environment configurations and the VPC configurations to determine that production and non-production environments were segregated, with separate AWS accounts and VPCs for each environment.	No exceptions noted.
CC6.1.2	Xero maintains a wireless corporate network in corporate office locations which requires domain authentication and is tied to a user's LDAP credentials and a trusted certificate. Remote access to the internal network is also available over VPN and requires the user to connect using their LDAP credentials.	Inspected the VPN authentication configurations to determine that Xero maintained a wireless corporate network in corporate office locations which required domain authentication and was tied to a user's LDAP credentials and a trusted certificate and that remote access to the internal network was also available over VPN and required the user to connect using their LDAP credentials.	No exceptions noted.
CC6.1.3	The asset management standard defines how assets are managed at Xero and requires an asset register to be maintained.	Inspected the asset management standard to determine that the asset management standard defined how assets were managed at Xero and required an asset register to be maintained.	No exceptions noted.
CC6.1.4	Information assets are classified by asset owners according to their sensitivity as per the data classification standard which draws distinctions between Xero information and customer information.	Inspected the data classification standard to determine that information assets were classified by asset owners according to their sensitivity as per the data classification standard which draws distinctions between Xero information and customer information.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.1.5	Xero has defined and documented standards for access control that outline processes for identifying and authenticating authorised users, restricting user access to authorised system components, and preventing and detecting unauthorised system access.	Inspected the access control standard to determine that Xero defined and documented standards for access control that outlined processes for identifying and authenticating authorised users, restricting user access to authorised system components, and preventing and detecting unauthorised system access.	No exceptions noted.
CC6.1.6	The in-scope systems are configured to enforce predefined user accounts and minimum password requirements.	Inspected the company access control and password policies, authentication configurations for AWS, VPN, and Okta, and user listings for AWS, Okta, and Active Directory with the assistance of the security risk and compliance specialist to determine that the in-scope systems are configured to enforce predefined user accounts and minimum password requirements.	No exceptions noted.
CC6.1.7	Multiple security zones exist in production environments and are isolated by stateful inspection firewalls which include default denial settings.	Inspected the AWS security group configurations to determine that multiple security zones exist in production environments and are isolated by stateful inspection firewalls which include default denial settings.	No exceptions noted.
CC6.1.8	Access to the corporate network (including remote access) is authorised and authenticated and login attempts are logged.	Inspected the corporate VPN authentication configurations, Okta authentication configurations, and the SIEM logging configurations to determine that access to the corporate network (including remote access) was authorised and authenticated and login attempts were logged.	No exceptions noted.
CC6.1.9	Access to corporate systems and applications is controlled per the established access control standard and requires MFA and/or other secure authorization mechanisms.	Inspected the access control policy, VPN authentication configurations, and Okta authentication configurations to determine that access to corporate systems and applications was controlled per the established access control standard and required MFA and/or other secure authorisation mechanisms.	No exceptions noted.
CC6.1.10	Security groups are defined on in-scope systems to filter unauthorised inbound traffic from the Internet. Ingress and egress traffic is only permitted through explicitly approved network access control rules.	Inspected the AWS security group configurations to determine that security groups were defined on in-scope systems to filter unauthorised inbound traffic from the Internet and ingress and egress traffic was only permitted through explicitly approved network access control rules.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.1.11	Access to the production network is restricted to users on the corporate internal network (allow list users) and to Xero-owned devices.	Inspected the Okta production authentication configurations to determine that access to the production network was restricted to users on the corporate internal network (allow list users) and to Xero-owned devices.	No exceptions noted.
CC6.1.12	Users access the production network via access-controlled sessions to their workloads or instances which are authorised to the Xero corporate network. MFA is enforced for access to production including separate network username and password.	Inspected the VPN authentication configurations to determine that users accessed the production network via access-controlled sessions to their workloads or instances which were authorised to the Xero corporate network, and MFA was enforced for access to production including separate network username and password.	No exceptions noted.
CC6.1.13	An Identity management system is used to provision access to Xero; s production environment.	Inspected the Okta authentication configurations to determine that an identity management system was used to provision access to Xero's production environment.	No exceptions noted.
CC6.1.14	Privileged access is allocated to users on a need-to-use basis in line with their job responsibilities and is controlled as per the access control policy.	Inspected the access control policy, listing of AWS administrators, listing of active directory (AD) domain administrators, listing of Okta administrators with the assistance of the product manager, to determine that privileged access was allocated to users on a need-to-use basis in line with their job responsibilities and was controlled as per the access control policy.	No exceptions noted.
CC6.1.15	Permissions to individual accounts are restricted based on roles and job requirements.	Inspected the user access request for a sample of requests to the in-scope data systems and services during the period to determine that permissions to individual accounts was restricted based on roles and job requirements for each request sampled.	No exceptions noted.
CC6.1.16	Predefined security groups are in place for in-scope systems using role-based access privileges.	Inspected the listing of AWS user groups to determine that predefined security groups were in place for in-scope systems using role-based access privileges.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.1.17	The access rights of employees and external users to information and information processing facilities are removed based on automated notification on termination of their employment, contract, or agreement, or adjusted when changes to their role occur.	Inspected the HR termination evidence and user account listings for a sample of users terminated during the period to determine that access rights of employees and external users to information and information processing facilities was removed based on automated notification on termination of their employment, contract, or agreement, or adjusted when changes to their role occurred for each termination ticket sampled.	No exceptions noted.
CC6.1.18	Xero corporate systems and production environments enforce user passwords to adhere to established password standards for complexity, lockout, history, and expiry.	Inspected the password policy and the Okta password configurations to determine that Xero corporate systems and production environments enforce user passwords to adhere to established password standards for complexity, lockout, history, and expiry.	No exceptions noted.
CC6.1.19	Data storage mechanisms are configured to encrypt data at rest in accordance with the cryptography standard.	Inspected the cryptography standard and data at rest encryption configurations to determine that data storage mechanisms were configured to encrypt data at rest in accordance with the cryptography standard.	No exceptions noted.
AWS is responsible for implementing controls that ensure logical access to the underlying network, virtualization management, and storage devices is managed for its cloud hosting services where in-scope systems reside.			
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 when user access is no longer authorized.			
CC6.2.1	Users accounts are assigned unique user IDs which are identifiable to an individual user and are not reused once an individual has left Xero.	Inspected the listing of AWS administrators, listing of production AD domain administrators, listing of corporate AD domain administrators, listing of AWS management console users, and listing of Okta administrators to determine that users accounts were assigned unique user IDs which were identifiable to an individual user and were not reused once an individual has left Xero.	No exceptions noted.
CC6.2.2	Access to in-scope systems requires users to authenticate via an individual user account using multi-factor or two-step authentication.	Inspected the AWS management console, bastion host, VPN, and Okta authentication configurations to determine that access to in-scope systems required users to authenticate via an individual user account using multi-factor or two-step authentication.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.2.3	Permissions to individual accounts are restricted based on roles and job requirements.	Inspected the user access request for a sample of requests to the in-scope data systems and services during the period to determine that permissions to individual accounts was restricted based on roles and job requirements.	No exceptions noted.
CC6.2.4	The access rights of employees and external users to information and information processing facilities are removed based on automated notification on termination of their employment, contract, or agreement, or adjusted when changes to their role occur.	Inspected the HR termination evidence and user account listings for a sample of users terminated during the period to determine that access rights of employees and external users to information and information processing facilities was removed based on automated notification on termination of their employment, contract, or agreement, or adjusted when changes to their role occurred for each termination ticket sampled.	No exceptions noted.
CC6.2.5	Access to in-scope data, systems, and services is reviewed on a quarterly basis to confirm access is still appropriate.	Inspected the user access review for a sample of quarters during the period to determine that access to in-scope data, systems, and services was reviewed to confirm access was still appropriate for each quarter sampled.	The test of the control activity disclosed that the user access reviews were not completed for two of two quarters sampled.
	AWS is responsible for implementing controls that ensure logical access to the underlying network, virtualization management, and storage devices is managed for its cloud hosting services where in-scope systems reside.		
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, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.			
CC6.3.1	Permissions to individual accounts are restricted based on roles and job requirements.	Inspected the user access request for a sample of requests to the in-scope data systems and services during the period to determine that permissions to individual accounts was restricted based on roles and job requirements.	No exceptions noted.
CC6.3.2	The access rights of employees and external users to information and information processing facilities are removed based on automated notification on termination of their employment, contract, or agreement, or adjusted when changes to their role occur.	Inspected the HR termination evidence and user account listings for a sample of users terminated during the period to determine that access rights of employees and external users to information and information processing facilities was removed based on automated notification on termination of their employment, contract, or agreement, or adjusted when changes to their role occurred for each termination ticket sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.3.3	Access to in-scope data, systems, and services is reviewed on a quarterly basis to confirm access is still appropriate.	Inspected the user access review for a sample of quarters during the period to determine that access to in-scope data, systems, and services was reviewed to confirm access was still appropriate for each quarter sampled.	The test of the control activity disclosed that the user access reviews were not completed for two of two quarters sampled.
CC6.3.4	Privileged access is allocated to users on a need-to-use basis in line with their job responsibilities and is controlled as per the access control policy.	Inspected the access control policy, listing of AWS administrators, listing of AD domain administrators, listing of Okta administrators with the assistance of the product manager, to determine that privileged access was allocated to users on a need-to-use basis in line with their job responsibilities and was controlled as per the access control policy.	No exceptions noted.
CC6.3.5	Permissions to individual accounts are restricted based on roles and job requirements.	Inspected the user access request for a sample of requests to the in-scope data systems and services during the period to determine that permissions to individual accounts was restricted based on roles and job requirements.	No exceptions noted.
	AWS is responsible for implementing controls that ensure logical access to the underlying network, virtualization management, and storage devices is managed for its cloud hosting services where in-scope systems reside.		
CC6.4 – The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.			
AWS is responsible for implementing controls that ensure physical access to data center facilities, backup data, and other system components such as virtual systems and servers is restricted.			
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 longer required to meet the entity's objectives.			
AWS is responsible for implementing controls that ensure logical access to the underlying network, virtualization management, and storage devices is managed for its cloud hosting services where in-scope systems reside.			
AWS is responsible for implementing controls that ensure physical access to data center facilities, backup data, and other system components such as virtual systems and servers is restricted.			
CC6.6 – The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
CC6.6.1	The cryptography standard defines the security controls and operational practices applicable to customer data at rest, end user devices, backups, and web communication sessions. The standard also defines requirements for the annual generation, use, protection, audit, and rotation of cryptographic keys.	Inspected the cryptography standard to determine that it defined the security controls and operational practices applicable to customer data at rest, end user devices, backups, and web communication sessions and the requirements for the annual generation, use, protection, audit, and rotation of cryptographic keys.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.6.2	Operational responsibilities for network controls to protect information in networks, including separation, logging, and encryption are established in the operation security standard.	Inspected the operation security standard to determine that operational responsibilities for network controls to protect information in networks, including separation, logging, and encryption were established.	No exceptions noted.
CC6.6.3	Production and non-production environments are segregated, with separate AWS accounts and VPCs for each environment.	Inspected the segmented production and non-production environment configurations and the VPC configurations to determine that production and non-production environments were segregated, with separate AWS accounts and VPCs for each environment.	No exceptions noted.
CC6.6.4	Multiple security zones exist in production environments and are isolated by stateful inspection firewalls which include default denial settings.	Inspected the AWS security group configurations to determine that multiple security zones exist in production environments and are isolated by stateful inspection firewalls which include default denial settings.	No exceptions noted.
CC6.6.5	Access to the corporate network (including remote access) is authorised and authenticated and login attempts are logged.	Inspected the corporate VPN authentication configurations, Okta authentication configurations, and the SIEM logging configurations to determine that access to the corporate network (including remote access) was authorised and authenticated and login attempts were logged.	No exceptions noted.
CC6.6.6	Access to corporate systems and applications is controlled per the established access control standard and requires MFA and/or other secure authorization mechanisms.	Inspected the access control policy, VPN authentication configurations, and Okta authentication configurations to determine that access to corporate systems and applications was controlled per the established access control standard and required MFA and/or other secure authorisation mechanisms.	No exceptions noted.
CC6.6.7	Security groups are defined on in-scope systems to filter unauthorised inbound traffic from the Internet. Ingress and egress traffic is only permitted through explicitly approved network access control rules.	Inspected the AWS security group configurations to determine that security groups were defined on in-scope systems to filter unauthorised inbound traffic from the Internet and ingress and egress traffic was only permitted through explicitly approved network access control rules.	No exceptions noted.
	AWS is responsible for implementing controls that ensure logical access to the underlying network, virtualization management, and storage devices is managed for its cloud hosting services where in-scope systems reside.		

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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.			
CC6.7.1	The cryptography standard defines the security controls and operational practices applicable to customer data at rest, end user devices, backups, and web communication sessions. The standard also defines requirements for the annual generation, use, protection, audit, and rotation of cryptographic keys.	Inspected the cryptography standard to determine that it defined the security controls and operational practices applicable to customer data at rest, end user devices, backups, and web communication sessions and the requirements for the annual generation, use, protection, audit, and rotation of cryptographic keys.	No exceptions noted.
CC6.7.2	Operational responsibilities for network controls to protect information in networks, including separation, logging, and encryption are established in the operation security standard.	Inspected the operation security standard to determine that operational responsibilities for network controls to protect information in networks, including separation, logging, and encryption were established.	No exceptions noted.
CC6.7.3	Information involved in application services which passes over public networks is encrypted as per the established standards for data controls and for cryptography.	Inspected the cryptography security policy, the TLS encryption certificate, and SSL labs report to determine that information involved in application services which passes over public networks was encrypted as per the established standards for data controls and for cryptography.	No exceptions noted.
CC6.7.4	Transport encryption requirements are defined within the cryptography standard and comply with legal and regulatory requirements.	Inspected the cryptography security policy to determine that transport encryption requirements were defined within the cryptography standard and complied with legal and regulatory requirements.	No exceptions noted.
CC6.7.5	Employee workstations are protected with full disk encryption.	Inspected the workstation disk encryption configurations and registered client listings to determine that employee workstations were protected with full disk encryption.	No exceptions noted.
CC6.7.6	Data storage mechanisms are configured to encrypt data at rest in accordance with the cryptography standard.	Inspected the cryptography standard and data at rest encryption configurations to determine that data storage mechanisms were configured to encrypt data at rest in accordance with the cryptography standard.	No exceptions noted.
AWS is responsible for implementing controls to restrict and protect information during transmission, movement, and removal from the underlying storage devices for its cloud hosting services where in-scope systems reside.			

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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.			
CC6.8.1	Antivirus protection is enabled on end-user devices and virus definitions are updated automatically. Network traffic is inspected for malware, application, and server vulnerabilities, insider threats and unwanted application traffic.	Inspected the antivirus configurations and registered client listing to determine that antivirus protection was enabled on end-user devices and virus definitions were updated automatically and that network traffic was inspected for malware, application and server vulnerabilities, insider threats and unwanted application traffic.	No exceptions noted.
CC6.8.2	Security monitoring systems are in place to monitor and analyse the in-scope systems for possible or actual security breaches.	Inspected the logging and monitoring application configurations and example alerts generated during the period to determine that security monitoring systems were in place to monitor and analyse the in-scope systems for possible or actual security breaches.	No exceptions noted.
CC6.8.3	Systems in the production environment are hardened, based on CIS benchmarks.	Inspected the CIS benchmark guidelines to determine that systems in the production environment should be hardened, based on CIS benchmarks.	No exceptions noted.
CC6.8.4	The TPZ serves as a DMZ to provide ingress and egress protection between the production environment and the Internet.	Inspected the network diagram and security group configurations to determine that the TPZ served as a DMZ to provide ingress and egress protection between the production environment and the Internet.	No exceptions noted.
CC6.8.5	Security measures are in place to protect the corporate network from external threats.	Inspected the logging and monitoring application configurations, the TLS encryption certificate, and SSL labs reports to determine that security measures were in place to protect the corporate network from external threats.	No exceptions noted.
CC6.8.6	A web application firewall is in place in front of the TPZ for web application traffic. The firewall has policies and alerting in place to protect against malicious traffic.	Inspected the web application firewall policies to determine that a web application firewall was in place in front of the TPZ for web application traffic and that the firewall had policies and alerting in place to protect against malicious traffic.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
<b>System Operations</b>			
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.			
CC7.1.1	Operating procedures for operational activities associated with information processing and communication facilities are documented and made available to users who need them. Xero security operations are covered in the operations security standard.	Inspected the operations security standard to determine that operating procedures for operational activities associated with information processing and communication facilities were documented and made available to users, and security operations were covered in the operations security standard.	No exceptions noted.
CC7.1.2	Antivirus protection is enabled on end-user devices and virus definitions are updated automatically. Network traffic is inspected for malware, application, and server vulnerabilities, insider threats and unwanted application traffic.	Inspected the antivirus configurations and registered client listing to determine that antivirus protection was enabled on end-user devices and virus definitions were updated automatically and that network traffic was inspected for malware, application and server vulnerabilities, insider threats and unwanted application traffic.	No exceptions noted.
CC7.1.3	Security monitoring systems are in place to monitor and analyse the in-scope systems for possible or actual security breaches.	Inspected the logging and monitoring application configurations and example alerts generated during the period to determine that security monitoring systems were in place to monitor and analyse the in-scope systems for possible or actual security breaches.	No exceptions noted.
CC7.1.4	Systems in the production environment are hardened, based on CIS benchmarks.	Inspected the CIS benchmark guidelines to determine that systems in the production environment should be hardened, based on CIS benchmarks.	No exceptions noted.
CC7.1.5	The TPZ serves as a DMZ to provide ingress and egress protection between the production environment and the Internet.	Inspected the network diagram and security group configurations to determine that the TPZ served as a DMZ to provide ingress and egress protection between the production environment and the Internet.	No exceptions noted.
CC7.1.6	Security measures are in place to protect the corporate network from external threats.	Inspected the logging and monitoring application configurations, the TLS encryption certificate, and SSL labs reports to determine that security measures were in place to protect the corporate network from external threats.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.1.7	A web application firewall is in place in front of the TPZ for web application traffic. The firewall has policies and alerting in place to protect against malicious traffic.	Inspected the web application firewall policies to determine that a web application firewall was in place in front of the TPZ for web application traffic and that the firewall had policies and alerting in place to protect against malicious traffic.	No exceptions noted.
CC7.1.8	Event logs are sent to the cloud based SIEM tool and log management and analytics service that records user activities, exceptions, faults, and high-risk information security events and alerts are sent to the security response team and retained and reviewed on at least an annual basis.	Inspected the logging and monitoring application configurations, alerting configurations and example alert generated during the period, and the most recent security governance meeting documentation to determine that event logs were sent to the cloud-based log management and analytics service that recorded user activities, exceptions, faults, and high-risk information security events and alerts were sent to the security response team and retained and reviewed during the period.	No exceptions noted.
CC7.1.9	Information systems are reviewed on at least an annual basis for compliance with Xero's information security policies and standards.	Inspected the internal audit policy and the most recent internal audit to determine that information systems were reviewed during the period for compliance with Xero's information security policies and standards.	No exceptions noted.
CC7.1.10	Automated vulnerability scanning tools are used to perform daily scans to identify and analyse new vulnerabilities. Vulnerabilities identified are communicated to the product teams for review and remediation.	Inspected the daily automated vulnerability scan configurations and example remediation ticket resolved during the period to determine that automated vulnerability scanning tools performed daily network and agent vulnerability scans to identify and analyse new vulnerabilities and identified security vulnerabilities are triaged by the security team and monitored through resolution.	No exceptions noted.
CC7.1.11	A selected panel of independent third parties performs external web application penetration testing and reporting across products in production on at least an annual basis. The results of scans containing vulnerabilities are communicated to the product teams for review and remediation. The resolution state of each vulnerability is tracked once communicated with the product teams.	Inspected the most recent external web application vulnerability scanning report to determine that an independent third party performed external web application vulnerability scanning during the period, and that the results of scans containing vulnerabilities were communicated to the product teams for review and remediation, and that they resolution state of each vulnerability were tracked.	No exception noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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.			
CC7.2.1	Event logs are sent to the cloud based SIEM tool and log management and analytics service that records user activities, exceptions, faults, and high-risk information security events and alerts are sent to the security response team and retained and reviewed on at least an annual basis.	Inspected the logging and monitoring application configurations, alerting configurations and example alert generated during the period, and the most recent security governance meeting documentation to determine that event logs were sent to the cloud-based log management and analytics service that recorded user activities, exceptions, faults, and high-risk information security events and alerts were sent to the security response team and retained and reviewed during the period.	No exceptions noted.
CC7.2.2	Documented incident response procedures are in place to guide personnel that handle incidents and include the process for informing the entity about actual and potential events that impact system security and for submitting complaints as well as roles and responsibilities for teams involved. Procedures are communicated to employees and customers as required.	Inspected the security incident response plan and procedures to determine that documented procedures were in place to guide personnel in the handling of incidents and included the process for informing the entity about actual and potential events that impacted system security and for submitting complaints as well as roles and responsibilities for teams involved, and procedures were communicated to employees and customers.	No exceptions noted.
CC7.2.3	An automated ticketing system is in place which allows internal and external system users to report security failures, incidents, and concerns. Incidents and security incidents are responded to and managed to resolution by the incident response manager and the security operations team, respectively.	Inspected the incident ticket for a sample of incidents during the period to determine that an automated ticketing system was in place which allowed internal and external system users to report security failures, incidents and concerns, and incidents, and security incidents were responded to and managed through to resolution.	No exceptions noted.
CC7.2.4	Post-mortems are performed per the established security incident response plan to identify the root cause of security incidents and to identify and monitor incidents trends over time.	Inspected the post-mortem activities performed for a sample of incidents during the period to determine that post-mortems were performed for each incident sampled per the established security incident response plan to identify the root cause of security incidents and to identify and monitor incidents trends over time.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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.			
CC7.3.1	Documented incident response procedures are in place to guide personnel that handle incidents and include the process for informing the entity about actual and potential events that impact system security and for submitting complaints as well as roles and responsibilities for teams involved. Procedures are communicated to employees and customers as required.	Inspected the security incident response plan and procedures to determine that documented procedures were in place to guide personnel in the handling of incidents and included the process for informing the entity about actual and potential events that impacted system security and for submitting complaints as well as roles and responsibilities for teams involved, and procedures were communicated to employees and customers.	No exceptions noted.
CC7.3.2	An automated ticketing system is in place which allows internal and external system users to report security failures, incidents, and concerns. Incidents and security incidents are responded to and managed to resolution by the incident response manager and the security operations team, respectively.	Inspected the incident ticket for a sample of incidents during the period to determine that an automated ticketing system was in place which allowed internal and external system users to report security failures, incidents and concerns, and incidents, and security incidents were responded to and managed through to resolution.	No exceptions noted.
CC7.3.3	Post-mortems are performed per the established security incident response plan to identify the root cause of security incidents and to identify and monitor incidents trends over time.	Inspected the post-mortem activities performed for a sample of incidents during the period to determine that post-mortems were performed per the established security incident response plan to identify the root cause of security incidents and to identify and monitor incidents trends over time.	No exceptions noted.
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.			
CC7.4.1	Documented incident response procedures are in place to guide personnel that handle incidents and include the process for informing the entity about actual and potential events that impact system security and for submitting complaints as well as roles and responsibilities for teams involved. Procedures are communicated to employees and customers as required.	Inspected the security incident response plan and procedures to determine that documented procedures were in place to guide personnel in the handling of incidents and included the process for informing the entity about actual and potential events that impacted system security and for submitting complaints as well as roles and responsibilities for teams involved, and procedures were communicated to employees and customers.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.4.2	An automated ticketing system is in place which allows internal and external system users to report security failures, incidents, and concerns. Incidents and security incidents are responded to and managed to resolution by the incident response manager and the security operations team, respectively.	Inspected the incident ticket for a sample of incidents during the period to determine that an automated ticketing system was in place which allowed internal and external system users to report security failures, incidents and concerns, and incidents, and security incidents were responded to and managed through to resolution.	No exceptions noted.
CC7.4.3	Post-mortems are performed per the established security incident response plan to identify the root cause of security incidents and to identify and monitor incidents trends over time.	Inspected the post-mortem activities performed for a sample of incidents during the period to determine that post-mortems were performed per the established security incident response plan to identify the root cause of security incidents and to identify and monitor incidents trends over time.	No exceptions noted.
<b>CC7.5 – The entity identifies, develops, and implements activities to recover from identified security incidents.</b>			
CC7.5.1	Documented incident response procedures are in place to guide personnel that handle incidents and include the process for informing the entity about actual and potential events that impact system security and for submitting complaints as well as roles and responsibilities for teams involved. Procedures are communicated to employees and customers as required.	Inspected the security incident response plan and procedures to determine that documented procedures were in place to guide personnel in the handling of incidents and included the process for informing the entity about actual and potential events that impacted system security and for submitting complaints as well as roles and responsibilities for teams involved, and procedures were communicated to employees and customers.	No exceptions noted.
CC7.5.2	An automated ticketing system is in place which allows internal and external system users to report security failures, incidents, and concerns. Incidents and security incidents are responded to and managed to resolution by the incident response manager and the security operations team, respectively.	Inspected the incident ticket for a sample of incidents during the period to determine that an automated ticketing system was in place which allowed internal and external system users to report security failures, incidents and concerns, and incidents, and security incidents were responded to and managed through to resolution.	No exceptions noted.
CC7.5.3	Post-mortems are performed per the established security incident response plan to identify the root cause of security incidents and to identify and monitor incidents trends over time.	Inspected the post-mortem activities performed for a sample of incidents during the period to determine that post-mortems were performed per the established security incident response plan to identify the root cause of security incidents and to identify and monitor incidents trends over time.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
<b>Change Management</b>			
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.			
CC8.1.1	Changes to Xero's organisation, business processes, information processing facilities and systems that affect information security are controlled, and change details are communicated to relevant persons.	Inspected the path to production standard and all-hands call meeting documentation to determine that changes to Xero's organisation, business processes, information processing facilities and systems that affected information security were controlled, and change details were communicated to relevant persons.	No exceptions noted.
CC8.1.2	Change management processes are in place to ensure that changes are recorded, evaluated authorised, planned, communicated, tested, and implemented successfully, before being deployed to production, in order to reduce the business impact of failed changes on Xero operation and its customers.	Inspected the change ticket for a sample of changes implemented during the period to determine that change management processes were in place to ensure that changes were recorded, evaluated authorised, planned, communicated, tested, and implemented successfully, before being deployed to production, in order to reduce the business impact of failed changes on Xero operation and its customers.	No exceptions noted.
CC8.1.3	Separate development, test, and production environments are in place to reduce the risks of unauthorised access or changes to the production environment.	Inspected the separate development, test, and production environment configurations to determine that separated environments were in place to reduce the risks of unauthorised access or changes to the production environment.	No exceptions noted.
CC8.1.4	Production and non-production environments are segregated, with separate AWS accounts and VPCs for each environment.	Inspected the segmented production and non-production environment configurations and the VPC configurations to determine that production and non-production environments were segregated, with separate AWS accounts and VPCs for each environment.	No exceptions noted.
CC8.1.5	Requirements for new information systems or enhancements to existing information systems are defined for product teams in the path to production standard which include identification of security threats and compliance with the security architecture knowledge base that is kept up to date by the security architecture team and available to developers during development activities.	Inspected the path to production standard to determine that requirements for new information systems or enhancements to existing information systems were defined for product teams, which included identification of security threats and compliance with the security architecture knowledge base that was kept up to date by the security architecture team and was available to developers during development activities.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC8.1.6	Changes to systems within the development lifecycle are controlled through formal change control procedures.	Inspected the path to production standard to determine that changes to systems within the development lifecycle were controlled through formal change control procedures.	No exceptions noted.
CC8.1.7	Version control branch protections are enabled to restrict users from circumventing the change management process.	Inspected the version control branch protection configurations to determine that version control branch protections were enabled to restrict users from circumventing the change management process.	The test of the control activity disclosed that the version control branch protections were not configured to restrict users from circumventing the change management process.
CC8.1.8	The version control software is configured to monitor for actions performed by user accounts with administrative access, and alerts are configured to notify security personnel for investigation and remediation.	Inspected the monitoring and alerting configurations and an example alert to determine that version control software is configured to monitor for actions performed by user accounts with administrative access, and alerts are configured to notify security personnel for investigation and remediation.	No exceptions noted.
CC8.1.9	Access privileges to implement changes into the production environment are restricted to user accounts accessible by authorised personnel who do not have administrative access to the version control software.	Inspected the version control administrative user listing with the assistance of the principal engineer to determine that access privileges to implement changes into the production environment were restricted to user accounts accessible by authorised personnel who do not have administrative access to the version control software.	The test of the control activity disclosed that access privileges to implement changes into the production environment included personnel who had administrative access to the version control software.
CC8.1.10	A continuous integration application is used to control the approval, logging, and deployment of changes to the production environment and configured to send real-time notifications to the team responsible for the release when changes are implemented.	Inspected the continuous integration application configurations to determine that the continuous integration application tools were used to control the approval, logging, and deployment of changes to the production environment and sent real-time notifications to the team responsible for the release when changes were implemented.	No exceptions noted.
CC8.1.11	Documented procedures are in place to guide personnel in the rollback of unsuccessful changes.	Inspected the path to production standard to determine that documented procedures were in place to guide personnel in the rollback of unsuccessful changes.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC8.1.12	Logging of actions taken during development, including details about the change, timestamp, and user information, are recorded automatically via the continuous integration/continuous delivery systems.	Inspected the continuous integration application configurations to determine that logging of actions taken during development, including details about the change, timestamp, and user information, were recorded automatically via the continuous integration/continuous delivery systems.	No exceptions noted.
CC8.1.13	Production data resides only in the segregated production environment to ensure that confidential customer data is not used for testing purposes.	Inspected the data control standard and development tool configurations to determine that production data resided only in the segregated production environment to ensure that confidential customer data was not used for testing purposes.	No exceptions noted.
<b>Risk Mitigation</b>			
CC9.1 – The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
CC9.1.1	Risk assessments are carried out on assets, taking into account their respective asset value with consideration of fraud risk. The annual risk assessments for critical assets are subjected to review in conjunction with the asset owner, and risks that surpass the predetermined tolerance level are regularly monitored by Xero's leadership team at least on a quarterly basis.	Inspected the Xero asset register, the most recent risk register, and the ARMC meeting invite and agenda for a sample of quarters during the period to determine that risk assessments were carried out on assets during the period and took into account their respective asset value with consideration of fraud risk, and critical assets were subjected to review in conjunction with the asset owner, and risks that surpassed the predetermined tolerance level were regularly monitored by Xero's leadership team for each quarter sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC9.1.2	<p>Xero has defined and applies an information security risk mitigation process to:</p> <ul style="list-style-type: none"> <li>a) Select appropriate information security risk treatment options</li> <li>b) Determine controls that are necessary to implement the information security risk treatment, based on Xero's Unified Controls Catalogue</li> <li>c) Document the chosen option and the selected controls in a security risk treatment plan</li> <li>d) Review and update Xero's Statement of Applicability that contains the necessary controls and justification for inclusions, whether they are implemented or not, and the justification for exclusions</li> <li>e) Obtain risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks</li> </ul>	<p>Inspected the risk management framework to determine that Xero defined and applied an information security risk mitigation process to:</p> <ul style="list-style-type: none"> <li>a) Select appropriate information security risk treatment options</li> <li>b) Determine controls that are necessary to implement the information security risk treatment, based on Xero's Unified Controls Catalogue</li> <li>c) Document the chosen option and the selected controls in a security risk treatment plan</li> <li>d) Review and update Xero's Statement of Applicability that contains the necessary controls and justification for inclusions, whether they are implemented or not, and the justification for exclusions</li> <li>e) Obtain risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks</li> </ul>	No exceptions noted.
CC9.1.3	<p>The high availability and disaster recovery strategy align with the company strategy and are reviewed at least annually.</p>	<p>Inspected the high availability and disaster recovery strategy to determine that the high availability and disaster recovery strategy aligned with the company strategy and were reviewed during the period.</p>	No exceptions noted.
CC9.1.4	<p>Business continuity plans have been documented for Xero's business operations, financial performance, reputation, employees, and supply chains and are tested on at least an annual basis.</p>	<p>Inspected the Xero disaster recovery strategy and the most recently completed business continuity test to determine that business continuity plans were documented for Xero's business operations, financial performance, reputation, employees, and supply chains and were tested during the period.</p>	No exceptions noted.
CC9.1.5	<p>A business impact analysis is performed on at least an annual basis that identifies RTOs and RPOs for each identified process and relate specific risks to their potential impact.</p>	<p>Inspected the most recent business impact analysis to determine that a business impact analysis was performed during the period that identified RTOs and RPOs for each identified process and related specific risks to their potential impact.</p>	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC9.2 – The entity assesses and manages risks associated with vendors and business partners.			
CC9.2.1	Requirements for confidentiality or NDAs reflecting Xero's needs for the protection of information are identified, documented, and reviewed by the legal team.	Inspected the confidentiality and NDA template and most recent template review to determine that requirements for confidentiality or NDAs reflecting Xero's needs for the protection of information were identified, documented, and reviewed the by the legal team.	No exceptions noted.
CC9.2.2	Xero requires employees as part of signing their employment contract, and contractors, to sign agreements that include non-disclosure provisions and asset protection responsibilities, upon hire.	Inspected the signed NDA for a sample of employees and contractors hired during the period to determine that Xero required employees to sign agreements that included non-disclosure provisions and asset protection responsibilities, upon hire, for each employee sampled.	No exceptions noted.
CC9.2.3	NDAs are established with third parties during the procurement process where sensitive information is included within the scope of the services to be provided to Xero.	Inspected the NDA established with a sample of vendors onboarded during the period to determine that NDAs were established during the procurement process for each vendor sampled where sensitive information was included within the scope of the services to be provided to Xero.	No exceptions noted.
CC9.2.4	Third-party risk assessments are performed as part of the vendor onboarding and due diligence process to identify and assess information security risks associated with potential business partners.	Inspected the third-party risk assessment performed for a sample of vendors onboarded during the period to determine that a third-party risk assessment was performed for each vendor sampled as part of the onboarding and due diligence process to identify and assess information security risks associated with potential business partners.	No exceptions noted.
CC9.2.5	Third-party risk assessments of critical vendors are performed and reviewed on at least an annual basis to identify information security risks associated with the supply chain.	Inspected the third-party risk assessment performed for a sample of critical vendors to determine that a third-party risk assessment was performed for each critical vendor sampled and reviewed during the period to identify information security risks associated with the supply chain.	No exceptions noted.

## ADDITIONAL CRITERIA FOR AVAILABILITY

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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.			
A1.1.1	A logging and monitoring application is configured to monitor the availability of the production environment and alert the security team when certain events are detected.	Inspected the logging and monitoring application dashboard, configurations, and an example alert generated during the period to determine that a logging and monitoring application was utilized to monitor the availability of the production environment and alerted the security team when certain events were detected.	No exceptions noted.
A1.1.2	Product teams are responsible for monitoring resources for capacity planning and forecasting utilization of products on a monthly basis.	Inspected the product team capacity planning and forecasting meeting minutes for a sample of months during the period to determine that product teams were responsible for monitoring resources for capacity planning and forecasting utilization of products for each month sampled.	No exceptions noted.
A1.1.3	Xero is hosted on AWS, and the platform and individual products are configured to automatically scale to meet processing and storage requirements.	Inspected the AWS autoscaling configurations to determine that Xero was hosted on AWS, and the platform and individual products were configured to automatically scale to meet processing and storage requirements.	No exceptions noted.
A1.1.4	The Xero platform is implemented in a high-availability configuration which uses multiple, redundant availability zones in a single AWS region and is based on the good practice guidelines set by AWS for managed EC2 instances.	Inspected the AWS server and database configurations to determine that the Xero platform was implemented in a high-availability configuration which used multiple, redundant availability zones in a single AWS region and was based on the good practice guidelines set by AWS for managed EC2 instances.	No exceptions noted.
A1.1.5	Xero production infrastructure is configured to perform backups on at least a daily basis and backups are replicated across two separate AWS regions.	Inspected the production infrastructure backup and replication configurations to determine that Xero production infrastructure was configured to perform backups on at least daily basis and backups were replicated across two separate AWS regions.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.2 - The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.			
A1.2.1	Backup copies of information, software and system images are taken and tested on at least an annual basis in accordance with the established backup standard.	Inspected the most recent test of the BCP and DR plan test and most recent automated restore results to determine that backup copies of information, software and system images were taken and tested during the period in accordance with the established backup standard.	No exceptions noted.
A1.2.2	The Xero platform is implemented in a high-availability configuration which uses multiple, redundant availability zones in a single AWS region and is based on the good practice guidelines set by AWS for managed EC2 instances.	Inspected the AWS server and database configurations to determine that the Xero platform was implemented in a high-availability configuration which used multiple, redundant availability zones in a single AWS region and was based on the good practice guidelines set by AWS for managed EC2 instances.	No exceptions noted.
A1.2.3	Business continuity plans have been documented for Xero's business operations, financial performance, reputation, employees, and supply chains and are tested on at least an annual basis.	Inspected the Xero disaster recovery strategy and the most recently completed business continuity test to determine that business continuity plans were documented for Xero's business operations, financial performance, reputation, employees, and supply chains and were tested during the period.	No exceptions noted.
A1.2.4	A business impact analysis is performed on at least an annual basis that identifies RTOs and RPOs for each identified process and relate specific risks to their potential impact.	Inspected the most recent business impact analysis to determine that a business impact analysis was performed during the period that identified RTOs and RPOs for each identified process and related specific risks to their potential impact.	No exceptions noted.
AWS is responsible for implementing controls that ensure the data center facilities are equipped with physical and environmental security safeguards.			
A1.3 - The entity tests recovery plan procedures supporting system recovery to meet its objectives.			
A1.3.1	Business continuity plans have been documented for Xero's business operations, financial performance, reputation, employees, and supply chains and are tested on at least an annual basis.	Inspected the Xero disaster recovery strategy and the most recently completed business continuity test to determine that business continuity plans were documented for Xero's business operations, financial performance, reputation, employees, and supply chains and were tested during the period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.3.2	A high availability test of both the Xero application and database environments is performed at least annually.	Inspected the most recent high availability test results to determine that a high availability test of both the Xero application and database environments was performed during the period.	No exceptions noted.

## ADDITIONAL CRITERIA FOR CONFIDENTIALITY

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
C1.1 - The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.			
C1.1.1	Information assets are classified by asset owners according to their sensitivity as per the data classification standard which draws distinctions between Xero information and customer information.	Inspected the data classification and handling policy to determine that information assets were classified by asset owners according to their sensitivity as per the data classification standard which drew distinctions between Xero information and customer information.	No exceptions noted.
C1.1.2	Xero's legal counsel and leadership identify legislation applicable to Xero in order to meet legislative, statutory, regulatory, and contractual requirements for Xero's type of business, in relevant countries. Xero's approach to meet requirements is identified, documented, and kept up to date for each information system and the organisation.	Inspected the organisational chart to determine that Xero's legal counsel and leadership identified legislation applicable to Xero in order to meet legislative, statutory, regulatory, and contractual requirements in relevant countries, and Xero's approach to meet requirements was identified, documented, and kept up to date for each information system and the organisation.	No exceptions noted.
C1.1.3	Records are protected and retained in accordance with legislative, regulatory, contractual, and business requirements established in the data retention policy, document and records management standard, and data control standard.	Inspected the data retention policy, document records management standard, and data control standard to determine that records were protected and retained in accordance with established legislative, regulatory, contractual, and business requirements.	No exceptions noted.
C1.2 - The entity disposes of confidential information to meet the entity's objectives related to confidentiality.			
C1.2.1	Information assets are classified by asset owners according to their sensitivity as per the data classification standard which draws distinctions between Xero information and customer information.	Inspected the data classification and handling policy to determine that information assets were classified by asset owners according to their sensitivity as per the data classification standard which drew distinctions between Xero information and customer information.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
C1.2.2	Data retention and disposal policies and procedures are in place to help guide personnel in the disposal of customer data when the end of the retention period is reached.	Inspected the data retention and disposal policy to determine that data retention and disposal policies and procedures were in place to help guide personnel in the disposal of customer data when the end of the retention period was reached.	No exceptions noted.
C1.2.3	Customer data is deleted from production databases in accordance with retention and disposal requirements upon customer contract termination or receipt of deletion request from customers.	Inspected the data deletion ticketing documentation for a sample of customer data deletion requests during the period to determine that customer data was deleted from production databases once the end of the seven-year retention period was reached following customer contract termination or receipt of deletion request for each customer data deletion request sampled.	No exceptions noted.

# SECTION 5

## OTHER INFORMATION PROVIDED BY XERO

## MANAGEMENT’S RESPONSE TO QUALIFYING MATTERS

### Operating Effectiveness Qualifications

The accompanying description of the Cloud Based Accounting system in Section 3 states that version control branch protections are enabled to restrict users from circumventing the change management process and that access privileges to implement changes into the production environment are restricted to user accounts accessible by authorized personnel who do not have administrative access to the version control software. However, controls related to restricting change implementation to personnel who did not have administrative access to the version control software were not consistently performed during the period, and therefore were not operating effectively throughout the period November 1, 2023, to October 31, 2024. As a result, controls did not provide reasonable assurance that Xero's service commitments and system requirements were achieved based on trust services criterion CC8.1, which states, "The entity authorizes, designs, develops, or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives."

#### Management's Response:

Xero acknowledges the discrepancy identified regarding branch protection and access privileges in our cloud-based accounting system. The noted exception relates to the absence of restrictions on certain administrative privileges in version control software, which allowed some users to implement changes without fully adhering to our intended change management process.

This gap occurred due to previously accepted risk that administrative users would always be subject to peer review. However, upon review, we have found inconsistencies in the application of these controls across the organisation, particularly in instances where branch protection controls were not enabled by default and had to be manually enforced.

To address this, Xero will initiate a comprehensive set of actions to enhance branch protection and enforce peer review practice through centralised management of branch protection controls. While administrative access is operationally necessary, we can ensure compliance through effective organisation-level controls, along with alerting, audit logging, and incident response notifications in cases of breaches.

These corrective actions demonstrate Xero's commitment to meeting our service commitments and system requirements in alignment with SOC 2 principles. We believe these improvements will provide reasonable assurance that changes to our infrastructure, data, and software are properly controlled and authorized in compliance with trust services criterion CC8.1.

## MANAGEMENT’S RESPONSE TO TESTING EXCEPTIONS

### Security Category

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.2.5 CC6.3.3	Access to in-scope data, systems, and services is reviewed on a quarterly basis to confirm access is still appropriate.	Inspected the user access review for a sample of quarters during the period to determine that access to in-scope data, systems, and services was reviewed to confirm access was still appropriate for each quarter sampled.	The test of the control activity disclosed that the user access reviews were not completed for two of two quarters sampled.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
<b>Management's Response:</b>	<p>Xero carries out a Quarterly Access Review (QAR) of all employees with access to key systems and platforms. At the start of the QAR, each employee who is required to carry out the review is contacted, and given a link to the review in Xero's Platform Access Management System (PACMAN). At regular cadence throughout the course of the QAR, those yet to complete the review receive further correspondence reminding them of the need to complete it.</p> <p>When the QAR is over, Xero's Security Identity Team provides the Security Risk and Compliance Team with the results of the QAR. Security Risk and Compliance then activate the defined escalation process, in which those who failed to complete the QAR, or their manager, are contacted. Metrics are also provided to the Leadership Team.</p> <p>Often, upon being advised of their failure to complete the QAR, reviewers will attempt to do it. However, PACMAN doesn't allow this beyond the set deadline. We are investigating how to address this.</p> <p>Anyone expecting to be away for an extended period delegates their managerial responsibilities through our HR system. This should include the QAR. Xero has identified that there is an issue whereby this delegation is not being captured by PACMAN, meaning a QAR may be sent to a manager who has already delegated that task. This is something we are also looking to address.</p> <p>We are also planning to include the reviewer <u>and</u> their manager in the QAR correspondence and reminders. This will give managers visibility of the QAR, making the manager aware it is underway, which may also help in addressing the delegation issue by allowing the manager to advise the Security team if a delegation is in place.</p>		
CC8.1.7	Version control branch protections are enabled to restrict users from circumventing the change management process.	Inspected the version control branch protection configurations to determine that version control branch protections were enabled to restrict users from circumventing the change management process.	The test of the control activity disclosed that the version control branch protections were not configured to restrict users from circumventing the change management process.
<b>Management's Response:</b>	<p>Xero has identified that branch protection, which enforces peer review in our code repository, is not enabled by default and must be manually activated by each repository owner. To mitigate risks associated with this, Xero has implemented monitoring that alerts the team to any instances where these protections are bypassed.</p> <p>A comprehensive set of requirements will soon be introduced to further reduce this risk by defining essential controls for branch protection and peer review. In addition, a more rigorous peer review process will be established to reinforce compliance and ensure that changes are thoroughly reviewed before deployment.</p>		
CC8.1.9	Access privileges to implement changes into the production environment are restricted to user accounts accessible by authorized personnel who do not have administrative access to the version control software.	Inspected the version control administrative user listing with the assistance of the principal engineer to determine that access privileges to implement changes into the production environment were restricted to user accounts accessible by authorized personnel who do not have administrative access to the version control software.	The test of the control activity disclosed that access privileges to implement changes into the production environment included personnel who had administrative access to the version control software.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
<b>Management's Response:</b>	<p>Xero has identified that this exception related to access privileges arose from a previously accepted risk, allowing certain admins to implement changes in the production environment. This decision was made based on the assumption that all changes would be subject to a peer review (as specified in control CC 8.1.7), though we have since observed that while some sampled changes were peer-reviewed, the process is not consistently enforced across the organisation.</p> <p>Multiple cases, such as branch protections being disabled without adequate follow-up, have highlighted gaps in peer review adherence.</p> <p>To address this, Xero will initiate a comprehensive set of actions to enhance branch protection and enforce peer review practice through centralised management of branch protection controls. While administrative access is operationally necessary, we can ensure compliance through effective organisation-level controls, along with alerting, audit logging, and incident response notifications in cases of breaches.</p>		