## ISO 27001 - Statement of Applicability

Legend (for Selected Controls and Reasons for controls selection)

Version 3.1 - 21 June 2024

**BR: business requirements/adopted best practices, this includes legal and regulatory obligations**

**RA: results of risk assessment or risk treatment**

**Implemented: control is in place and in use**

**Not implemented: control is not in place and/or in use**

**Not applicable: control is not required to be in place or in**

| *ISO 27001/2:2022 Reference* | *Control Title (Name) ISO 27001/2:2022* | *BR* | *RA* | *Control wording* | *Policies and Procedures (Documentation)* | |
|---|---|---|---|---|---|---|
| A5.1 | Policies for information security | Y | Y | A set of policies and standards for information security are defined, approved by management, published, and available to employees.<br><br>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. This is managed using an ISMS document register and review schedule. | ISMS Framework<br><br>Policies and Standards on Helpcentre<br><br>Document and Records Management Standard<br><br>ISMS Document Register and Review Schedule | |
| A5.2 | InfoSec roles and responsibilities | Y | Y | A security governance structure for information security is defined, and the defined roles and responsibilities are allocated to accountable leadership. | ISMS Framerwork<br><br>Risk Management Framework<br><br>Assurance, Performance, and Compliance Framework<br><br>SGG Charter | |
| A5.3 | Segregation of duties | Y | Y | Conflicting duties and areas of responsibility are segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization’s assets. | Access Control Standard<br><br>Assurance, Performance and Compliance Framework | |
| A5.4 | Management responsibilities | Y | Y | Team leads and managers require all employees and contractors to secure information in accordance with the organization's established policies and procedures.<br><br>Employees receive training on a regular basis to ensure that employees and contractors conform to the terms and conditions of employment, which includes Xero's IT Security Policy, IT Acceptable Use standard, and appropriate methods of work and continue to have the appropriate skills and qualifications.<br><br>The Chair of the Board, the Chair of RemCo, and the Chief Legal Officer/Whistleblowing Officer receive whistleblower reports when submitted via the whistleblower@xero.com email. The next steps are determined by the Chief Legal Officer/Whistleblowing Officer and supporting team. | IT Security Policy<br><br>IT Acceptable Use<br><br>Whistleblower Policy | |

| | | | | | | |
|---|---|---|---|---|---|---|
| A5.5 | Contact with authorities | Y | N | Contact details for relevant authorities are maintained as part of the incident response documents. When the Xero Legal team is notified of a breach or incident requiring notification, the Xero Legal team notifies regulators of any breaches as legally required. | Regulatory Incident Notification Obligations<br><br>Security Incident Response Plan<br><br>Privacy Incident Management Framework<br><br>Privacy Incident Notifications Playbook | |
| A5.6 | Contact with special interest groups | Y | N | Management maintains contacts with special interest groups or other specialist security forums and professional associations will be maintained. | Interested parties<br><br>Competencies and Contact with special interest groups | |
| A5.7 | Threat intelligence | Y | Y | Xero uses a variety of internal and external tools and resources to provide timely and relevant threat intelligence to the business. These resources help to identify the threats, techniques and procedures that Xero needs to understand in order to protect our information systems and assets and reduce the impact of such threats.<br><br>Xero communicates relevant threat intelligence to the business, and significant events may result in escalation to security incidents. Threats are also considered in Xero's Threat Modelling process, the outputs of which can result in risks being raised for appropriate risk management.<br><br>Additionally, outputs from threat intelligence help inform Xero's preventive and detective security controls and inform decision making for prioritization of patching, control tasks, incident management and vulnerability management. | SEC-Crowdstrike Threat Intel - Recon Notifications runbook<br><br>SEC-Data Classification and Sharing Guide<br><br>SEC-CTI Glossary<br><br>SEC Threat Intelligence Reports<br><br>SEC-Cyber Threat Intelligence<br><br>SEC Threat Actor Types and Motivations | |
| A5.8 | Information Security in Project Management | Y | N | Information security is addressed and reviewed in project management, regardless of the type of the project.<br><br>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 Technical Security Knowledge Base that is kept up to date by the Technical Security team and available to developers during development activities.<br><br>The Technical Security Knowledge Base is reviewed on at least an annual basis by the Technical Security team and made available for developers to use during development activities. | IT Security Policy<br><br>Template - Project Management Task Checklist<br><br>Project Kick-off Checklist- TEMPLATE<br><br>Security Assurance, Performance, and Compliance Framework<br><br>Path to Production Standard<br><br>Security Architecture Knowledge Base | |
| A5.9 | Inventory of information and other associated assets | Y | Y | The asset management standard defines how assets are inventoried and managed at Xero and requires an asset registry to be maintained.<br><br>Assets associated with Xero's information and information processing facilities have been identified, documented in the Xero Asset Registry, and kept up to date.<br><br>The Registry is based on a decentralised set of Registers & Catalogues (the inventory) that also includes hardware, software, services, buildings, information and information processing facilities, and anything else agreed as meeting the Xero Asset definition for Xero. | Asset Management Security Standard | |

| | | | | | | |
|---|---|---|---|---|---|---|
| A5.10 | Acceptable use of information and associated assets | Y | Y | Employees and contractors agree to the IT Acceptable Use Standard before they are given access to Xero information assets.<br><br>The Data Controls standard includes requirements that must be followed for the handling, processing, storing and transferring of information based on the classification of the asset. | IT Security Policy<br><br>IT Acceptable Use Standard<br><br>Data Controls Standard | |
| A5.11 | Return of assets | Y | N | Employees and contractors are required to return Xero owned assets and information upon termination of their employment, contract or agreement. | Human Resources Security<br><br>Asset Management Security standard | |
| A5.12 | Classification of information | Y | Y | 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. | Data Classifications Standard<br><br>Asset Management Security standard | |
| A5.13 | Labelling of information | Y | N | Asset owners label information assets following the the Data Controls standard for each classification identified in the Data Classifications standard. This includes the labelling of electronic and physical information assets. | Data Controls Standard<br><br>Document and Records Management Standard<br><br>AWS Tagging Standards | |
| A5.14 | Information transfer | Y | Y | The Data Controls standard defines requirements to protect information during electronic transfer including encryption, confidentiality agreements, approval, and review by the Security Team.<br><br>Agreements have been established with external parties to address the responsibilities for information transfer controls such as access and encryption.<br><br>Information involved in electronic messaging is protected per the established Data Controls standard and appropriate legal requirements.<br><br>Other:<br>Paas Networks<br>Social media policy | Data Controls Standard<br><br>Security Standard for IT Suppliers and Cloud Services | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| A5.15 | Access control | Y | Y | Xero has defined and documented standards for access control that outline processes for identifying and authenticating authorized users, restricting user access to authorized system components, and preventing and detecting unauthorized system access.<br><br>The in-scope systems are configured to enforce predefined user accounts, minimum password requirements and AWS access keys are rotated.<br><br>Multiple security zones exist in all production environments and are isolated by stateful inspection firewalls which include default denial settings.<br><br>Users are only provided with access to the network and network services that they have been specifically authorized to use.<br><br>Appropriate security groups are defined on in-scope systems to filter unauthorized inbound traffic from the internet. Ingress and egress traffic is only permitted through explicitly approved network access control rules.<br><br>Access to the production network is restricted to users on the corporate internal network (whitelisted users) and to Xero-owned devices.<br><br>User accounts are separate from the corporate network and require MFA.<br><br>Access to the corporate network (including remote access) is authorized, authenticated, and login attempts are logged. | IT Security Policy<br><br>Access Control Standard<br><br>Operations Security Standard | | Y |
| A5.16 | Identity management | Y | Y | Users accounts are assigned unique user IDs which are identifiable to an individual user and are not reused once an individual has left Xero.<br><br>Access to in-scope systems requires users to authenticate via a valid individual user account using multi-factor or two-step authentication. | Access Control Standard | | |
| A5.17 | Authentication information | Y | Y | Management of secret authentication information of users<br>The allocation of secret authentication information is controlled per the Access Control standard and supporting processes.<br><br>Secret Information includes:<br>Passwords<br>Encryption Keys<br>Hardware tokens<br>API Access keys<br>Vendor Supplied and Default Accounts<br><br>Standards are established for secrets and authentication information provision and handling (including certificates, keys and passwords).<br><br>See: Access control Standard and Data Controls Standard<br><br>Xero corporate systems and production environments enforce user passwords to adhere to established password standards for complexity, lockout, history and expiry. | Access Control Standard<br><br>Litmos Dashboard | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| A5.18 | Access rights | Y | Y | An Identity management system is used to provision access to Xero production environment.<br><br>All requests for new access or modification of access to data, systems and services follow an approval process.<br><br>Access to to data, systems and services in-scope is reviewed on a quarterly basis to confirm access is still appropriate.<br><br>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. | Access Control Standard<br><br>Quarterly Access Review Docs | | Y |
| A5.19 | Information security in supplier relationships | Y | Y | The Security Standard for IT Suppliers and Cloud Services defines Xeros requirements to identify and manage security risks before access is granted to Xero IT systems or sensitive information. | Data Controls Standard<br><br>Security Standard for IT Suppliers and Cloud Services | | |
| A5.20 | Addressing security within supplier agreements | Y | Y | Information security requirements are established in agreements with each vendor that accesses, processes and or stores Xero information.<br><br>The Security/Legal teams review controls within third-party attestation reports to ensure they meet organizational Security, Availability and Confidentiality requirements. Issues are tracked to resolution. | Security Standard for IT Suppliers and Cloud Services | | |
| A5.21 | Managing information security in the ICT supply chain | Y | Y | 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.<br><br>Critical third-party risk assessments are performed and reviewed on at least an annual basis to identify information security risks associated with the supply chain. | Security Standard for IT Suppliers and Cloud Services | | |
| A5.22 | Monitoring, review and change management of supplier services | Y | Y | The Security Standard for IT Suppliers and Cloud Services is established and requires relationships and services from third party suppliers to be managed and monitored.<br><br>Risk assessments and service agreements are refreshed per the Security Standard for IT suppliers upon changes are made to the services procured. | Security Standard for IT Suppliers and Cloud Services<br><br>Supplier & Software Security Risk Management Guideline | | |
| A5.23 | Information Security for the Use of Cloud Services | Y | Y | Xero follows a structured onboarding process for cloud service providers. During this process, security requirements are thoroughly addressed in contractual agreements, assurance reports are diligently reviewed and ongoing monitoring of security assurance activities occurs throughout the use of their services. Additionally, Xero has established policies for managing cloud services, which have been effectively communicated to relevant stakeholders. | Security Standard for IT Suppliers and Cloud Services<br><br>OneTrust Supplier Risk Management<br><br>Supplier & Software Security Risk Management Guideline | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| A5.24 | Information security incident management planning and preparation | Y | Y | 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.<br><br>Procedures are communicated to employees and customers as required and appropriate. | Security Incident Response Plan<br><br>Security Operations process overview and incident handling guidelines<br><br>Security Incident Management - Runbooks | |
| A5.25 | Assessment of and decision on information security events | Y | Y | The Security Operations team assesses, classifies, and prioritizes information security events as per the established Security Incident Response Plan that defines the processes for incident response, including containment, escalation, documentation, analysis, resolution, notification, and root-cause analysis. | Security Incident Response Plan<br><br>Security Operations process overview and incident handling guidelines<br><br>Incident Response Process | |
| A5.26 | Response to information security incidents | Y | Y | The incident response procedures are supported by an Incident Response Plan and predefined runbooks which define the processes for incident response, including containment, escalation, documentation, analysis, resolution, notification, and root cause analysis. | Security Incident Response Plan<br><br>Security Operations process overview and incident handling guidelines<br><br>Incident Response Process | |
| A5.27 | Learning from information security incidents | Y | Y | 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. | Security Incident Response Plan | |
| A5.28 | Collection of evidence | Y | N | Forensic analysis processes are established to identify, collect, acquire and preserve evidence in a safe and defensible manner and are performed by trained or authorised individuals. | Security Incident Response Plan<br><br>Forensics processes<br><br>Internal IT incident Response | |
| A5.29 | Information security during disruption | Y | Y | Information security requirements are determined and embedded within the established business continuity and disaster recovery plans.<br><br>Information Security Continuity processes have been established to define how Xero will maintain information security during a crisis or adverse event.<br><br>Verify, review, and evaluate information security continuity processes have been established to regularly test that information security continuity controls are valid and effective during a crisis or adverse event.<br><br>Parent Control-<br>Business continuity and disaster recovery plans have been documented and tested regularly. | Business Continuity Planning & Disaster Recovery Planning<br><br>High Availability and Recovery Controls | |

| | | | | | | |
|---|---|---|---|---|---|---|
| A5.30 | ICT readiness for business continuity | Y | Y | Xero's BCM is designed to reduce the impact of business disruption for Xero in a cost beneficial manner, and prepare the company to respond effectively to business disruptive events which will contribute to protecting Xero employees, the Xero brand and reputation as well as giving our customers confidence in the resilience of our business.<br><br>The high availability and disaster recovery strategy align with the company strategy and are reviewed at least annually.<br><br>High availability and recovery controls are defined in the highly available scaling strategy for the AWS environment used by all Xero product groups.<br><br>Business continuity plans have been documented for Xero's business operations, financial performance, reputation, employees and supply chains. Business impact assessment activities relate specific risks to their potential impact. RPOs and RTOS are identified where appropriate.<br><br>The business continuity plans and high availability controls are tested and reviewed at least annually and updated where required.<br><br>Methods for testing the plans may include walkthroughs or simulations. However the regular automated failover of services due to failure or planned maintenance activities is sufficient proof of successful uninterrupted failover.<br><br>Exercising and testing of business continuity plans is a key activity in preparing the company and its staff for unplanned events. | Business Continuity Policy<br><br>Xero Disaster Recovery Strategy<br><br>Business Continuity Planning & Disaster Recovery Planning<br><br>High Availability and Recovery Controls" | |
| A5.31 | Identification of applicable legislation and contractual requirements | Y | Y | Xero's legal team, Government Experience Team, Compliance teams, and leadership take steps to identify legislation applicable to Xero. This is done in order to facilitate compliance with legislative, statutory, regulatory, and contractual requirements for our type of business in all relevant countries. Xero's approach to meeting these requirements is identified, documented, and kept up to date for both the Xero product and the organization.<br><br>Agreements are reviewed by the security and legal teams to ensure cryptographic controls are in compliance with applicable regulations.<br><br>Legislation and Regulations: Including but not limited to privacy. | Assurance, Performance and Compliance Framework<br><br>Product Risk and Regulatory Compliance<br><br>Cryptography Security Standard<br><br>IT Security Policy | |
| A5.32 | Intellectual property rights | Y | N | Appropriate procedures are implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products. | Using Open Source Copyright material at Xero<br><br>Using Open Source Libraries at Xero<br><br>IT Acceptable use standard | |
| A5.33 | Protection of records | Y | N | Records are protected and retained in accordance with the legislatory, regulatory, contractual and business requirements established in the Data Retention Policy, Document and Records Management Standard, and Data Control standard. | Document and Records Management Standard<br><br>Security Event Logging Standard<br><br>Data Retention Policy | |

| | | | | | | |
|---|---|---|---|---|---|---|
| A5.34 | Privacy and protection of personally identifiable information | Y | N | The Responsible Data Use Policy has been established to meet relevant legislation and regulation and is communicated to all employees and contractors involved in the processing of personally identifiable information.<br><br>The privacy obligations of Xero are expressed in Xero's privacy notice and terms of use, both of which are available on the Xero public-facing website for all customers. | Responsible Data Use Policy<br><br>Privacy Notice<br><br>Terms of Use | |
| A5.35 | Independent review of information security | Y | Y | Xero's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes, and procedures for information security) is reviewed independently at planned intervals or when significant changes occur.<br><br>Internally, this is done by the Internal Audit function, which is independent of the teams responsible for the development and implementation of technical and non-technical controls. Xero's Security teams perform regular reviews of implemented technical controls. These reviews include security technical assessments, regular scanning of deployed systems, code reviews, and more.<br><br>Xero has a penetration testing framework in place whereby throughout the year different parts of our platform and applications are tested by external penetration testing providers.<br><br>On an annual basis, Xero is audited by external audit service providers: ISO 27001, SOC 2, and Financial audits are performed every 12 months.<br><br>All results of these independent reviews are recorded and reported to Xero Leadership, Audit & Risk Management Committee, and any remediation is documented and monitored through to completion.<br><br>Twice per year Xero Leadership, through the Security Governance Group, performs a Management Review for Xero's Information Security Management System. All results of any independent security reviews are input to this Management Review. | Security Assurance, Performance, and Compliance Framework | |
| A5.36 | Compliance with policies, rules and standards for information security | Y | Y | Managers regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies and standards.<br><br>Information systems are reviewed on at least an annual basis for compliance with Xero's information security policies and standards.<br><br>The Security team performs external web application vulnerability scanning and reporting across all products in production on at least an annual basis.<br><br>The results of scans containing high severity vulnerabilities are communicated to the product teams for review and remediation.<br><br>Xero has a penetration testing framework in place whereby throughout the year different parts of our platform and applications are tested by external penetration testing providers. | Assurance, Performance, and Compliance Framework<br><br>Security Vulnerability Management Standard<br><br>Operations Security Standard<br><br>Security and Application Penetration testing guidelines | |
| A5.37 | Documented operating procedures | Y | Y | Operating procedures for operational activities associated with information processing and communication facilities are documented within the Operation Security Standard and made available to all users who need them.<br><br>The responsibilities of Xero operational teams are defined in the team's own procedures and instructions, in Confluence, Jira, or other tools. | Operations Security Standard | |

| | | | | | | |
|---|---|---|---|---|---|---|
| A6.1 | Screening | Y | Y | Background verification checks on all 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.<br><br>Screening activities are carried out when we hire new staff, for any staff or contractors who will be in a position of trust, and before we give external people access to Xero information and systems. | Human Resources Security | |
| A6.2 | Terms and conditions of employment | Y | Y | Xero's security requirements are integrated in the terms of employment and agreements that employees sign when they sign their contract. These include security policies and standards, data privacy requirements, and disciplinary processes. New hires receive code-of-conduct materials, and US staff receive a handbook as required by law.<br><br>Mandatory training is completed on at least an annual basis that covers the policies which support the Code of Conduct including the Privacy, Security, Securities Trading Policy, and Responsible Data Use. | Human Resources Security<br><br>Code of Conduct<br><br>Responsible Data Use | |
| A6.3 | Information security awareness, education and training | Y | Y | Xero employees and contractors are provided with security and privacy awareness training courses, which they will be reminded to complete on an annual basis (unless they have an approved exception).<br><br>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. | Human Resources Security<br><br>Litmos Dashboard | |
| A6.4 | Disciplinary process | Y | Y | Xero has a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.<br><br>If any Xero staff or contractors don't meet their security responsibilities or misuse Xero IT systems, we will investigate and may take disciplinary action. Possible action includes removing access to Xero services, dismissal from Xero for employees or termination of contracts with contractors, and seeking damages or prosecution. | Human Resource Security | |
| A6.5 | Responsibilities after termination or change of employment | Y | N | Termination or change of employment responsibilities<br>Information security responsibilities and duties that remain valid after termination or change of employment should be defined, communicated to the employee or contractor and enforced. | Human Resource Security<br><br>Access Control Standard | |
| A6.6 | Confidentiality or non-disclosure agreements | Y | Y | Requirements for confidentiality or non-disclosure agreements reflecting Xero's needs for the protection of information are identified, documented, and reviewed by the legal team.<br><br>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.<br><br>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.<br><br>Employees are required to acknowledge the IT Acceptable Use and IT Security Standards, which describe the responsibilities and expected behaviour with regard to information and information system usage, upon hire and in order to return or destroy assets upon termination. | Human Resources Security Standard<br><br>Data Controls Standard<br><br>IT Acceptable Use<br><br>NDA template | |

| | | | | | | |
|---|---|---|---|---|---|---|
| A6.7 | Remote working | Y | Y | Security measures are implemented to protect information accessed, processed, or stored at teleworking sites per the Flexible Working, Access Control, and Data Controls standards. | Flexible Working Policy<br><br>Access Control Standard<br><br>Data Controls Standard<br><br>Customer Privacy and Security Considerations | |
| A6.8 | Information security event reporting | Y | Y | The responsibilities of external users and customers are described on the Xero website.<br><br>Customers are able to file their own support tickets through Xero Central support for operational failures, incidents, problems, concerns, and complaints.<br><br>An automated ticketing system is in place which allows internal and external system users to report security failures, incidents, and concerns.<br><br>Incidents and security incidents are responded to and managed through to resolution by the Incident Response Manager and the Security Operations team, respectively.<br><br>Employee and contractors report potential security weaknesses identified through an automated ticketing system. The Security Operations team review and escalate them as per documented incident management procedures.<br><br>Customers and other external users raise support tickets identifying potential security weaknesses identified through an automated ticketing system. The Customer Support Team review and escalate them as per documented incident management procedures. | Reporting security incident on HelpCentre<br><br>IT Acceptable Use Standard<br><br>Raising a nonconformity to the Security Team<br><br>Security Vulnerability Management Standard | |
| A7.1 | Physical security perimeters | Y | Y | Physical access controls and monitoring mechanisms (such as access card readers and CCTV) have been implemented to restrict access to physical non-production systems (Xero offices and workspaces). | Building Security Standard | |
| A7.2 | Physical entry | Y | Y | Personnel entering Xero offices are required to use their assigned access and physical identification cards or sign in at the front desk which is centrally logged.<br><br>Xero has no Information Processing Facilities (IPF) hosted on site. The assets we have on site handle information however are not considered as our processing facilities. This control is therefore not applicable for our ISMS. | Building Security Standard | |
| A7.3 | Securing offices, rooms and facilities | Y | N | Xero buildings and workspaces are designed to prevent sensitive documents and user computing sessions from being visible to unauthorised person(s).<br><br>Xero has developed processes that standardise the way the Workplace Experience teams across the world perform their tasks in securing Xero buildings. | Building Security Standard | |

| | | | | | | |
|---|---|---|---|---|---|---|
| A7.4 | Physical security monitoring | Y | Y | Xero has implemented cloud-based access control and CCTV systems to monitor its sites. Access to data within these these systems is restricted to a limited number of the WX team who are responsible for management of these systems.<br><br>Any request for access to the data from someone outside of the WX team follows a request process via Zendesk. Upon receiving such a request WX contact the relevant teams within Xero (e.g. Legal) for approval before any information is shared.<br><br>Any proposed use of a co-working environment not solely occupied by Xero takes into account Xero's access control and physical security monitoring requirements. | Building Security Standard | |
| A7.5 | Protecting against physical and environmental threats | Y | Y | Controls have been designed and implemented to protect and detect fire, flood, earthquake, explosion, civil unrest and other forms of natural or man made-disaster. | IT Security Policy<br><br>Building Security Standard | |
| A7.6 | Working in secure areas | N | Y | Secure areas are restricted to authorized persons. | IT Security Policy | |
| A7.7 | Clear desk and clear screen | Y | Y | A clear desk and clear screen policy is established in the IT Acceptable Use standard which is provided to employees and contractors as part of onboarding. | IT Acceptable Use Standard<br><br>Building Security Standard | |
| A7.8 | Equipment siting and protection | Y | Y | Controls have been implemented to protect Internal IT equipment within Xero Offices from environmental threats, hazards, and unauthorised access. | IT Security Policy<br><br>Building Security Standard | |
| A7.9 | Security of assets off-premises | Y | Y | Use of information storage and processing equipment off-site is authorised by Internal IT per the established Asset Management Security Standard and Flexible-Working standard. | Asset Management Security standard<br><br>IT Acceptable Use Standard<br><br>Flexible Working Policy | |

| | | | | | | |
|---|---|---|---|---|---|---|
| A7.10 | Storage media | Y | N | Procedures are implemented for the management of removable media in accordance with:<br>1) the Data Controls standards, where removable media is included in "hard copy" (which is defined as information in hard copy / transportable form (printouts, USB, etc);<br>2) the IT Acceptable Use standard, which includes expectations in relation to removable media containing sensitive information; and<br>3) the Operations Security Standard in relation to backup media.<br><br>Procedures are established for the destruction of physical and electronic media based on the sensitivity of the information to support the Data Controls standards. Xero has agreements in place with third parties for secure collection and disposal for each office.<br><br>Xero sanitise any hardware or media that is being disposed of in line with the highest classification of data that has been stored on it, as specified in the Data Controls standard.<br><br>For the information processing facilities equipment, Xero rely on AWS processes for the secure sanitisation and destruction of drives.<br><br>Procedures are established to protect physical information (electronic and paper based) during transit to support the established Data Controls standard.<br><br>Internal IT authorizes the removal of equipment prior to being removed off-site. | Data Controls Standard<br><br>IT Acceptable Use Standard<br><br>Operations Security Standard<br><br>Asset Management Security Standard | |
| A7.11 | Supporting utilities | Y | Y | Supporting utilities (electricity, telecommunications and air conditioning) are implemented and monitored to meet business needs, equipment manufacturer's specification and local legal requirements. | IT Security Policy<br><br>Building Security Standard | |
| A7.12 | Cabling security | Y | Y | Network cabling at Xero offices is located within the secure perimeter and protected from interception. Access to the Internal IT room is approved by the Internal IT team. | IT Security Policy<br><br>Building Security Standard | |
| A7.13 | Equipment maintenance | Y | Y | The environmental controls which protect equipment in comms rooms are maintained to ensure availability of Xero services. | IT Security Policy<br><br>Building Security Standard | |
| A7.14 | Secure disposal or re-use of equipment | Y | Y | Procedures have been established for the secure disposal and reuse of equipment. Secure deletion techniques are applied to ensure information is non-retrievable | Asset Management Security Standard | |
| A8.1 | User endpoint devices | Y | Y | Access to the production network is restricted to users on the corporate internal network (whitelisted users) and to Xero-owned devices.<br><br>User access to applications and information is restricted when mobile devices are in use. Remote erasure is enabled for mobile devices.<br><br>Unattended equipment is protected in line with the access control and password standards which are provided in awareness training and part of onboarding employees and contractors. | IT Acceptable Use<br><br>Data Controls Standard | |

| | | | | | | |
|---|---|---|---|---|---|---|
| A8.2 | Privileged access rights | Y | Y | 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.<br><br>Permissions to individual accounts are restricted based on roles and job requirements.<br><br>Predefined security groups are in place for in-scope systems using role-based access privileges. | Access Control Standard | |
| A8.3 | Information access restriction | Y | Y | Access to data and functions within Xero systems is restricted through defined roles and access rights (e.g. read, write and delete). Access to bulk export data from applications is restricted to specific user roles and /or other application controls. | Access Control Standard | |
| A8.4 | Access to source code | Y | N | Access to Xero source code is restricted following the rule of least privilege based on job function. | Data Classifications Standard<br><br>Data Controls Standard | |
| A8.5 | Secure authentication | Y | Y | Access to the corporate network is authorized and authenticated and all login attempts are logged.<br><br>Access to corporate systems and applications is controlled per the established access control standard and requires MFA and/or other secure authorisation mechanisms.<br><br>Users access the production network via access-controlled sessions to their workloads or instances which are authorized to the Xero corporate network. MFA is enforced for access to production including separate network username and password. | Access Control Standard | |
| A8.6 | Capacity management | Y | Y | Product teams are responsible for monitoring resources for capacity planning and forecasting utilization of products.<br><br>Xero is hosted on AWS, and the platform and individual products can automatically scale to meet processing and storage requirements. | Operations Security Standard | |

| | | | | | | |
|---|---|---|---|---|---|---|
| A8.7 | Protection against malware | Y | Y | Detection, prevention and recovery controls to protect against malware have been implemented. These are combined with appropriate user awareness measures.<br><br>Antivirus protection is enabled on all end-user devices (laptops and desktops) and virus definitions are updated automatically. Network traffic is inspected for malware, application and server vulnerabilities, insider threats and unwanted application traffic.<br><br>Security monitoring systems are in place to monitor and analyse the in-scope systems for possible or actual security breaches.<br><br>Systems in the production environment are hardened, based on CIS benchmarks.<br><br>The threat protection zone (TPZ) serves as a demilitarized zone (DMZ) to provide ingress and egress protection between the Production environment and the Internet.<br><br>Security measures are in place to protect the corporate network from external threats.<br><br>A web application firewall is in place in front of the threat protection zone (TPZ) for all web application traffic. The firewall has policies and alerting in place to protect against malicious traffic. | Operations Security Standard | |
| A8.8 | Management of technical vulnerabilities | Y | Y | Security vulnerabilities and patches are risk assessed, tested and applied to assets according to the established Vulnerabilities Management framework.<br><br>The Security team reports and notifies engineering teams of technical vulnerabilities or misconfigurations on at least a monthly basis for remediation.<br><br>An automated patch management system is used to ensure patches are up-to-date and installed according to predetermined timeframes.<br><br>Information systems are reviewed on at least an annual basis for compliance with Xero's information security policies and standards.<br><br>The Security team performs external web application vulnerability scanning and reporting across all products in production on at least an annual basis.<br><br>The results of scans containing high severity vulnerabilities are communicated to the product teams for review and remediation.<br><br>Xero has a penetration testing framework in place whereby throughout the year different parts of our platform and applications are tested by external penetration testing providers. | Assurance, Performance, and Compliance Framework<br><br>Security Vulnerability Management Standard<br><br>Operations Security Standard<br><br>Security and Application Penetration testing guidelines | |

| | | | | | | |
|---|---|---|---|---|---|---|
| A8.9 | Configuration management | Y | Y | Platform<br>Software, hardware, services and networks are configured based on Xero's business needs and threat modelling. Threat modelling is performed by asset owners on a regular basis.<br><br>Asset owners are responsible for the lifecycle of standardised templates, configuration practices, and policy for detecting misconfiguration of configurations.<br><br>Configuration is automatically evaluated against policy on a regular cadence for any misconfiguration. Policy violations are reported to asset owners, who are responsible for remediating all non-compliant configuration changes. Additionally, Xero's Security Operations team receives notifications and triages high priority policy violations.<br><br>Privileged access is limited and unnecessary functions disabled. Configuration changes follow Xero's release or change management procedure and be fully approved and documented. Change control processes are also followed for changes to configuration policy.<br><br>Corporate Environment<br>Xero has an established OS image and default networking template, as well as Global Session, Authentication, Device Assurance, Password & Authenticator Policies baselines.<br><br>All changes to configurations are made through the IT change process. Each change is logged by the requesting team as a Zendesk change ticket to Internal IT. | Operations Security Standard<br><br>Path to Production | |
| A8.10 | Information deletion | Y | Y | Xero's Data Retention Policy stipulates the required retention periods for our data to make sure retention of data is consistent with our values, meets our legal obligations, and our business needs.<br><br>For data requiring deletion, Xero has a defined process managed by US DRE who alert the relevant product teams of the need for data to be deleted. US DRE receive notification when this has been carried out.<br><br>Xero employs a variety of data deletion mechanisms, including hard delete, soft delete and obfuscation. The type of mechanism used is dependent on the product, type of data and the use of the data. | Data Retention Policy | |
| A8.11 | Data masking | Y | Y | The Xero Data Classification Standard contains direction on how to determine the sensitivity of the data, and the associated Data Controls Standard provides guidance on how each classification level is to be protected by means of security and privacy controls and the need for specific classifications of data to be obfuscated or masked in such a way that it cannot be linked back to its original source.<br><br>Xero's Cryptographic Security Standard includes encryption protocols to be used for data at rest and stipulates hashing requirements for data requiring obfuscation. | Data Classification Standard<br><br>Data Controls Standard<br><br>Cryptographic Security Standard | |
| A8.12 | Data leakage prevention | Y | Y | Xero has classified its data in accordance with established data classification standards, and it is automatically labeled on Google Drive. The system can automatically recognize sensitive datasets, issuing warnings to users before sharing such information. Moreover, a monitoring system is active to identify externally shared sensitive files. In addition to these measures, steps such as restricting mass storage devices on employee laptops, blocking the ability to auto-forward emails to unapproved domains, automatic remediation of any open link sharing that contains certain data sets have been taken to prevent the unauthorized copying or sharing of sensitive documents. | Data Classification Standard<br><br>Data Control Standard | |

| | | | | | | |
|---|---|---|---|---|---|---|
| A8.13 | Information backup | Y | Y | 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. | Operations Security Standard | |
| A8.14 | Redundancy of information processing facilities | Y | Y | The Xero platform is implemented in a high-availability configuration which uses multiple, redundant availability zones (AZs) in a single AWS region and is based on the good practice guidelines set by AWS for managed EC2 instances.<br><br>Xero production databases and backups are replicated across two separate AWS regions (US-East-l and US-West-2) which allows for the loss of an availability zone with no impact on overall availability. | Xero - High Availability and Recovery Controls<br><br>Xero Disaster Recovery Strategy | |
| A8.15 | Logging | Y | Y | Event logs are sent to the cloud-based log management and analytics service that record user activities, exceptions, faults, and information security events that are retained and reviewed on at least an annual basis.<br><br>Included in the logs are user account activities including actions performed in the command line interface, and the cloud management console.<br><br>Logging of actions taken during development, including details about the change, timestamp and user information, are recorded automatically.<br><br>Logging facilities and log information are protected against tampering and unauthorized access in line with the Security Event Logging Standard.<br><br>Administrator and operator logs:<br>System administrator and system operator activities are logged and the logs protected and regularly reviewed. | Security Event Logging Standard<br><br>Managing Security Operations Alerts Process | |

| | | | | | | |
|---|---|---|---|---|---|---|
| A8.16 | Monitoring activities | Y | Y | Xero has implemented log and application management services to collect and monitor the security and availability of the Cloud-Based Accounting System. Logs or events from our products, cloud environments and critical security services are sent to those services to enable Xero teams to monitor the applications and environments. Product teams are responsible for monitoring their CPU and memory utilisation.<br><br>Select log sources, like cloud audit, system logs, IDP and EDR logs are sent in full to the SIEM which are then used by Security to monitor for suspicious activity. Some log sources, like product application logs, are not sent in full to the SIEM. Instead, we monitor those logs via queries for specific security events and forward the results of those queries to the SIEM. The Security Operations and Defence pods implement and tune the rules provided by the SIEM as well as custom ones.<br><br>We also employ MDR services for our Akamai ingress, Crowdstrike EDR and Check Point services to help provide 24x7 monitoring of those respective services. The vendors providing the MDR service will notify Xero when events need our attention.<br><br>Xero also incorporates threat intelligence data into our SIEM solution, enabling them to be alerted to activity from known IOCs moving forward. Furthermore, we employ retrospective scanning of IOCs in select log sources that would contain those IOCs.<br><br>In case of alerts, from MDR or the SIEM, security personnel promptly investigate and respond, taking corrective actions, including initiation of an incident if necessary. | Security Event Logging Standard | |
| A8.17 | Clock synchronization | Y | Y | Clocks are synchronised to a single reference time source.<br><br>Clocks are synchronised a time source in their respective environment, in line with the Security Event Logging Standard. | Security Event Logging Standard | |
| A8.18 | Use of privileged utility programs | Y | N | The use of privileged utility programs that are capable of overriding system and application controls are risk assessed, and controls are put in place to reduce the risk or restrict use as agreed with the accountable owner of the system.<br><br>e.g Windows programs that require UAC or UNIX software with setuid or similar privileges (that includes su and sudo themselves which are setuid). | Access Control Standard<br><br>Operations Security Standard | |

| | | | | | | |
|---|---|---|---|---|---|---|
| A8.19 | Installation of software on operational systems | Y | Y | Installation of software on operational systems<br>Approval of software on operational systems is maintained.<br><br>Xero uses continuous integration software to manage, track and provide control over versions of source code for release.<br><br>Controls have been implemented to prevent or detect and act upon the introduction of unauthorized or malicious software.<br><br>Systems in the production environment are hardened based on CIS benchmarks.<br><br>Restrictions on software installation<br>Rules governing the installation of software by users are established and implemented.<br><br>Xero has defined and documented guidelines for Access Control that outlines processes for identification and authentication of authorized users, restriction of user access to authorized system components and prevention and detection of unauthorized system access.<br><br>Security monitoring systems are in place to monitor and analyze the in-scope systems for possible or actual security breaches. | IT Acceptable Use Standard | |
| A8.20 | Networks security | Y | Y | Operational responsibilities for network controls to protect information in networks, including segregation, logging, and encryption are established in the Operation Security Standard. | Operations Security Standard | |
| A8.21 | Security of network services | Y | Y | Service Agreements with network services providers include requirements from Xero to provide secure services. | Operations Security Standard | |
| A8.22 | Segregation of networks | Y | Y | Production and non-production environments are segregated, with separate AWS accounts and virtual private clouds (VPCs) for each environment.<br><br>Xero maintains a wireless corporate network in all 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. | Operations Security Standard | |
| A8.23 | Web filtering | Y | Y | Xero has implemented web filtering to reduce its exposure to malicious content. Xero uses third party tools to block access to malicious websites on the corporate network. Additional web filtering controls are in place for those employees outside of the corporate network accessing Xero systems via the VPN. The vendor enforces clear policies, and regularly updates the list of blocked sites and urls. Further controls are provided via Xero's office productivity provider when using its browser products.<br><br>Xero's Acceptable Use Standard specifically defines those websites that are considered unsuitable for browsing.<br><br>Periodic audits ensure ongoing effectiveness, enhancing resilience against evolving cyber threats. | IT Acceptable Use Standard | |

| | | | | | | |
|---|---|---|---|---|---|---|
| A8.24 | Use of cryptography | Y | Y | The Cryptography Standard defines the security controls and operational practices applicable to customer data at rest, end user devices, backups and web communication sessions.<br><br>The standard also defines requirements for the annual generation, use, protection, audit, and rotation of cryptographic keys.<br><br>The Cryptography Standard defines requirements for the annual generation, use, protection, audit, and rotation of cryptographic keys.<br><br>Cryptography processes are defined and operated by the Security Engineering team to control encryption keys and to encrypt (and decrypt) data.<br><br>These processes include requirements to protect and restrict access to encryption keys during generation, storage, use, and destruction. | IT Security Policy<br><br>Cryptography Security Standard | |
| A8.25 | Secure development life cycle | Y | Y | The Technical Security team directly engages with product teams to provide security guidance throughout the development life cycle, and liaises with the product team and other security teams to solve specific technical security problems. | IT Security Policy<br><br>Path to Production<br><br>Security Architecture Knowledge Base | |
| A8.26 | Application security requirements | Y | Y | Information involved in application services which passes over public networks is encrypted as per the established standards for data controls and for cryptography.<br><br>The cryptography standard defines the security controls and operational practices applicable to customer data at rest, end-user devices, backups and web communication sessions.<br><br>Information involved in applications service transactions are protected from unauthorized access or loss of integrity as per the data controls standard.<br><br>Transport encryption requirements are defined within the cryptography standard and comply with legal and regulatory requirements.<br><br>Information involved in applications service transactions are protected from unauthorized access or loss of integrity per the established Data Controls standard. Transport encryption requirements are defined within the Cryptography Standard and comply with legal and regulatory requirements. | Operations Security Standard<br><br>Data Controls Standard | |
| A8.27 | Secure system architecture and engineering principles | Y | Y | Secure system engineering principles and procedures are documented, maintained and applied to all in-house information system engineering activities.<br><br>Supplier security engineering principles of relevant outsourced information systems are reviewed during third party security risk assessments and applied per contractual agreements. | IT Security Policy | |

| | | | | | | |
|---|---|---|---|---|---|---|
| A8.28 | Secure coding | Y | Y | 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. Logging of actions taken during development, including details about the change, timestamp, and user information, is recorded automatically within the CI/CD systems.<br><br>Access privileges to develop code and 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. The ability to make changes to source code during development from the version control software is restricted to authorized personnel.<br><br>Xero utilises tools to carry out continuous inspection of code quality, which perform automatic reviews with static analysis of code to detect bugs and security vulnerabilities. Xero also consumes reports on duplicated code, coding standards, unit tests, code coverage, code complexity, comments, bugs, and security vulnerabilities. | Path to Production | |
| A8.29 | Security testing in development and acceptance | Y | Y | Production code changes are required to pass Quality Assurance testing prior to release into production. Testing activities and results are recorded in the build management and continuous integration tool.<br><br>System acceptance testing:<br>Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions. | IT Security Policy<br><br>Operations Security<br><br>Path to Production | |
| A8.30 | Outsourced development | Y | N | Contracts have been established with individuals and Consultants to perform development activities which are inline with formally documented contract templates. All contractors are onboarded in the same way as other Xero employees. | IT Security Policy<br><br>Security Standards for IT Suppliers and Cloud Services | |

| | | | | | | |
|---|---|---|---|---|---|---|
| A8.31 | Separation of development, test and production environments | Y | Y | Segregated development, test, and production environments are in place to reduce the risks of unauthorized access or changes to the production environment.<br><br>Access to these environments is logically restricted to only development teams which require it.<br><br>Production and non-production environments are segregated, with separate AWS accounts and virtual private clouds (VPCs) for each environment.<br><br>Xero has established policies and procedures to appropriately protect secure environments for system development and integration efforts that cover the entire system development lifecycle.<br><br>Application development and testing occurs in development, test and UAT environments. A continuous integration/continuous delivery (CI/CD) pipeline is created to move packages to the livestage and production environments.<br><br>Segregated development (stage), test and production environments are in place to reduce the risks of unauthorized access or changes to the production environment. Access to these environments is logically restricted to only development teams which require it. | IT Security Policy<br><br>Operations Security Standard<br><br>Path To Production | |

| | | | | | | |
|---|---|---|---|---|---|---|
| A8.32 | Change management | Y | Y | Changes to Xero's organisation, business processes, information processing facilities and systems that affect information security are controlled, and change details are communicated to all relevant persons.<br><br>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.<br><br>Changes to systems within the development lifecycle are controlled through formal change control procedures. The defined change management and release management procedures describe the change and release processes and how each type of release (including emergency or hot fixes and roll backs) occur and the required approval controls.<br><br>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.<br><br>Documented procedures are in place to guide personnel in the rollback of unsuccessful changes.<br><br>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.<br><br>Technical review of applications after operating platform changes. Changes to operating systems, applications, databases are reviewed and tested to ensure there is no adverse impact on organizational operations or security. Business continuity/ High avail plans are updated where appropriate.<br><br>Restrictions on changes to software packages:<br>Modifications to software/packages from vendors are controlled per the secure development lifecycle. This is to ensure built in security controls are not compromised and to maintain vendor support where possible. | Operations Security Standard<br><br>Path to Production Standard<br><br>Change Management<br><br>IT Security Policy<br><br>Change Management Process by Phase | |
| A8.33 | Test information | Y | N | Production data resides only in the segregated production environment to ensure that confidential customer data is not used for testing purposes. | Data Controls Standard | |
| A8.34 | Protection of information systems during audit testing | Y | Y | Information systems audit controls.<br>Audit requirements and activities involving verification of operational systems are planned and agreed to minimise disruptions. | Operations Security Standard<br><br>ISMS Internal Audit Procedure<br><br>Security Event Logging Standard | |