Annual Audit Report

Remote Gambling and Software Technical Standards

Gatherwell

May 2024

Neterix Ltd
Viscount House
River Lane
Chester
CH4 8RH
Tel: +44 (0)333 335 0052
Email: info@neterix.com
Web: https://www.neterix.com

Disclaimer
This report and accompanying documents are provided "as is" with no warranties whatsoever. The audit report has been based on observations made during the visit and evidence provided. The owner remains solely responsible for the security of their product(s), services and sensitive information stored, including any liability arising from legal infringement or product warranty.

Executive Summary

This report documents the findings of an independent audit conducted by Neterix for Gatherwell Ltd based on the ISO 27001 controls required by the Gambling Commission's security requirements. The report details the auditor's findings along with any nonconformity reports and recommendations.

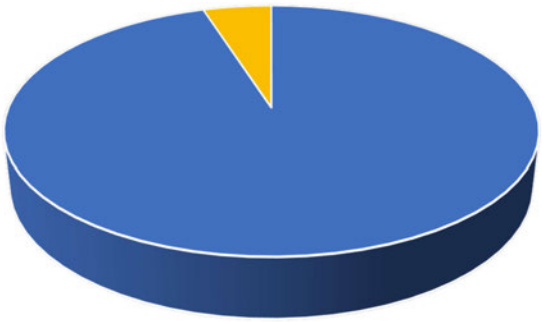
This compliance assessment evaluated the relevant sections from Annex A of the ISO/IEC 27001:2013 standard. These controls are stated in section 4 of the "Remote gambling and software technical standards" document published June 2017.

Gatherwell has successfully demonstrated their compliance with the requirements of this audit. Staff interviewed were able to clearly explain the policies and procedures followed. The team provided all evidence requested promptly. The combining of policies into a single document will make the topics more accessible to staff and the policy easier to maintain.

The issues raised in the previous audit have all been resolved with suitable remediations implemented. This assessment has not found any non-conformities and the observations raised are intended to further improve procedures already in place. They do not represent any security weaknesses with the systems or risk to data.

Having assessed Gatherwell's systems against the 61 relevant requirements from Annex A of ISO 27001:2013 the results are:

58 Compliant
3 Observations
0 Minor nonconformities
0 Major nonconformities
0 Non-applicable



Introduction

Established in 2003, Neterix has provided quality IT solutions to SMEs, large corporations and public bodies. Primarily working in the areas of networking and IT security, Neterix has a qualified and experienced team who ensure the highest level of service.

The lead auditor for the assessment is Dr Les Pritchard, a Charted IT Professional and IRCA qualified lead auditor for ISO/IEC 27001. He holds a PhD in Distributed Systems & Security and has conducted security and ISO 27001 audits for organisations with networks of up to 20,000 users. Les has been conducting remote gambling audits since 2010. He has also worked with the North Wales Police Hi-Tech Crime Unit on various digital forensics cases including network investigations and the reconstruction and extraction of evidence from large databases.

Neterix has determined that the above auditor has no direct commercial relationships or personal interests associated with Gatherwell Ltd.

Audit Overview

Contacts

The audit was conducted by Les Pritchard. As Gatherwell work as a fully remote business with no central office currently in place, the audit was conducted remotely via a video call. The audit process involved interviewing staff, reviewing evidence and observing operations and systems. Where appropriate, screensharing was used to demonstrate systems and sufficient evidence was collected to confirm the processes followed.

Primary contacts during the audit process were:

Name	Job Title
[redacted]	Senior Manager, Development
[redacted]	Full Stack Developer

Dates

The audit was conducted on the 15th May 2024.

Applicable Standards

The audit has been assessed for conformance with the following Gambling Commission technical standards:

Remote gambling and software technical standards, June 2017:
Sections 4: Security Standards:
Relevant sections of annex A to the ISO/IEC 27001:2013

Definitions

The assessment uses the following definitions when categorising each area evaluated.

Compliant – Policy and evidence viewed is fully compliant with ISO 27001 guidelines.

Observation – Policy is in place but is either not fully compliant with the ISO 27001 guidelines or the supporting evidence (or lack of) indicates potential concerns. This status does not signify a fail, but acts as a guide on how the process may be improved or allows time for evidence to be gathered by the next assessment.

Minor Nonconformity – A control has not been addressed or is not compliant with ISO 27001 guidelines. A course of action to remedy this must be agreed with appropriate time line.

Major Nonconformity – A fundamental failing has been identified by the auditor that affects several controls and means that the overall Information Security Management policies cannot be adhered to. Until resolved, this shortcoming will normally mean the organisation is NOT compliant with ISO 27001.

Background

Gatherwell was formed in 2013 with the aim of helping charities raise money through a simple ELM service. The company currently provides lotteries for a wide range of brands including councils and national charities, supporting thousands of causes.

Along with the individual lotteries, schools can join the 'Your School Lottery' service, which provides a no-risk method of running a lottery for their supporters. In addition to the guaranteed weekly prizes for supporters at each school, members are also entered into a separate draw across all schools with a prize of £25,000. The other lotteries are run as independent draws and the prize structure is defined by the charity.

Gatherwell operates as a virtual business with a meeting space available in Manchester. Staff operate remotely from home offices and access company resources through secure connections. Whilst the team is geographically separated, they communicate daily through video chat and instant messaging. There are no office servers, and all files and email are hosted through online services.

The database and web interface for staff and clients have been developed in-house. Both are hosted on Rackspace cloud servers. The website code does not include an RNG for generating results. Gatherwell use a combination of the Random.org service and the results of the Australian Lotto Superdraws as their source for generating results.

Critical Systems

Online servers

The websites, database and online management interfaces are hosted on servers at Rackspace. The web and staging servers do not hold any critical game or player information. A VoIP server used by internal staff is hosted at AWS.

Company data

As there is no central office network, Gatherwell use Google Workspace to host all company files and email. No player information is stored on the Google drive and data is subject to continual versioning and backups by Google. Some staff are provided with Office 365 licenses based on their role.

Payment Processing

Card payment processing is provided through third-party services. Gatherwell do not store or handle any card payment information. Card data is only stored in

tokenised form for future billing. Direct debit information is processed through a separate third-party service.

Server Information

IP Address	Role	OS	Location
[redacted]	Web server	Windows Server 2019 / IIS	Rackspace UK
	Production services	Windows Server 2019	Rackspace UK
	Database server	Windows Server 2019/ SQL Server	Rackspace UK
	Staging server	Windows Server 2019	Rackspace UK
	Integration server	Windows Server 2019	Rackspace UK
	VoIP server	Debian / 3CX	AWS EU-West

Primary Documents Reviewed

Document Name	SHA1 Sum
Policies	
A7 - Information Security Breach Reporting Procedure.pdf (May 2024)	AAC606CFFDAF5EA38DE114CBD1A4DADCB7AEA0E1
A7X - Information Security Breach Report Template.pdf	F94A0E40E8CA918C19EFD40362BA540E1D6C67FE
B2 - Supplier Relationships.pdf (May 2024)	BDED4AA2D7AAB65BE5C2B46AF6A83D2F2E37562C
Gatherwell Information Security Policy.pdf (October 2023)	948166B9A2858B33F7A82F4630D20F82AE03FC27
ISMS-Cryptographypolicy-Jumbo Interactive.pdf (April 2021)	862AA01DC9BC0D37E85888FB896FE189CB95EC9A
Additional Evidence	
1Password - Password Generator.png	FBD241EA89A9CE93387727FAB1E8E6BA20946746
1Password - Password Policy.png	975238025E1F718A652B5710BB40B6552E62B160
Backup Testing Log.pdf	225F0CAEF919EF54E71AFB465D42A4B0F435F085
BitLocker.png	B9BA671B7AE2F874511003F9C9BF398F86607127
Breach log and reports.png	BA41F46088F27F31871F7819802FC0A772D69E33
Database Backup Configuration.png	290A224E4CDC1398FE2F625110776DEB42439A39
Database Backup Transaction Log.png	6E2D00F26C1B973230D5EB17C0CA04681CB42DF9
Database Server User Accounts.png	1B520D82C83071DF7B2747C2A4E5C5183A44F012
Developer Training Log.pdf	BF3E0F28F88FD1304E1C44C183B527DE8411696B
Duo MFA for RDP.png	56376B1ADB7D1A376F9E4161D42889A249988673
GitHub pull requests.png	51305445C6F32B703F93C6C591CF73D4B982A57C
Google MFA Configuration.png	4B2191DA3EF39402EAF4CB4C602B4110F02B4C1C
Google Password Configuration.png	ED640F0F772D15AB632D22F7DDCA30FD9CFDB10B
Google User Security Report.png	ECEDF34225266A35C0C1C1D9301FC62BA9EF4CE0
[redacted]_ Leavers Form.xlsx	DD54D1ECECEAE06989ADED4E35716133EB7F76C4
IT Inventory - Offsite.pdf	CCBD2E35B7FF405AD5DD2DD6655E6E4749245DA2
IT Inventory.pdf	BF93F1D845C7C8CC4D4B9A6AA14DD7BE1C92F54C
IT Security - Training Log.pdf	E1A62BFC0112E4F3BF0A8100A771AC7BF0F1355D
LotteryPlus - Uptime Monitoring.png	F06E30151F51E5C905A5C8D64BAC7CF97E6C4BD4
Office 365.png	22533887CFB324D9C888BD140C2D9669151D47AD
Pingdom Monitoring.png	C5D4AF95DAD73E3FA16333A91BAF197B35EFD9ED
Rackspace - PROD_WEB snapshots.png	29F36B144D85C9F96583CDF6D426C7026027FC2A
Rollbar Monitoring.png	47CF83E0F9AA08CD273F1C9632FA4FFE69BB11ED
Slack - Production Monitoring.png	B88493B23845679EBA1AFF303B1C112420770879
Snyk dashboard.png	A35EF7792DABC36AD52CC93281C0FDEAEB25EC86
TLS Certificate.png	990AEE263E0337F971FDE621285706FAA93C5DD5
User access register- FEB2024.pdf	87B5F100D15695F81BA5FF56813C01A9F5683A4C
Windows Power and Sleep Settings.png	923C87D337D120F5E58962AEDC91CDECA08EE7DE
Windows Security Settings.png	A8255C83AAE7E7493FB78FF48F6FA4018E5A5A97

Audit Process

This audit complies with the requirement to have an annual external audit of the information security policies and processes. The audit reviewed policies, observed processes and systems and interviewed members of staff to establish a clear overview of company operations.

The following table summarises the audit findings, with further discussion of the controls that are not fully compliant included after it. Apart from where stated, it should be assumed that the processes were observed by the auditor and where practical, evidence was collected.

Audit Findings

Reference	Requirement	Requirement	Observations	Compliant	Observation	Minor nonconformity	Major nonconformity
A.5.1.1	Policies for information security	A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.	Gatherwell have developed information security related policies to cover the requirements of this audit and other regulations. Since the previous audit the new Legal Counsel has conducted a full review of the policies and collated most of them into a single document. The new *Information Security Policy* is intended to improve accessibility for staff. Logs previously stored in the policies have been moved to separate documents. The new document has been approved by management and shared with all staff through the company Google Drive.	√			
A.5.1.2	Review of the information security policy	The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	It was confirmed that all policies were subject to a review as part of the document restructure. The content was assessed by relevant staff and it was confirmed that no changes, with the exception of language improvements, were required. The new *Information Security Policy* contains a version table on the front page that includes approval details and the date of next review (30/06/2024).	√			

Reference	Requirement	Requirement	Observations	Compliant	Observation	Minor nonconformity	Major nonconformity
A.6.2.1	Mobile device policy	A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.	The appropriate use of end user devices is covered in the 'Devices and IT' section of the *Information Security Policy*. This includes the requirement for all devices to be password protected and have full disk encryption enabled with BitLocker. Evidence of this control was provided in *BitLocker.png*. The policy also highlights the importance of ensuring data is copied to the company network (i.e. Google Drive) regularly for protection.	√			
A.6.2.2	Teleworking	A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.	As the company is distributed, employees mostly work from home. Some staff may choose to use the hot-desking office in Manchester. The 'Remote working, access to premises and information' section of the *Information Security Policy* requires staff maintain secure working areas in their homes. Guidance is provided in the awareness training and during an employee's induction. All services used by the company require individual user authentication via HTTPS connections. It was stated that there is no requirement for a separate VPN.	√			

Reference	Requirement	Requirement	Observations	Compliant	Observation	Minor nonconformity	Major nonconformity
A.7.2.2	Information Security Awareness, Education and Training	All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.	Staff must complete an induction process that includes security awareness training when joining the company. All employees must complete annual refresher training and pass a knowledge quiz to demonstrate their understanding. Courses are provided through the parent company's 'Jumbo University' platform. Additional IT security training is delivered in-house and a log of completion was provided in *IT Security - Training Log.pdf*.	√			
A.7.3.1	Termination or change of employment responsibilities	Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced.	Staff leaving the company must return all equipment by their last day in accordance with the 'Devices and IT' section of the *Information Security Policy*. Where practical this may be done in-person, but more commonly the company will arrange a pickup. This is sent to the Senior Manager of Development for decommissioning. All access must be disabled by the last day of contract and the leaver would be reminded of any confidentiality clauses within their contract. No other responsibilities should remain post-employment.	√			

Reference	Requirement	Requirement	Observations	Compliant	Observation	Minor nonconformity	Major nonconformity
A.8.2.3	Handling of assets	Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	This is covered in the 'Asset management' section of the *Information Security Policy*. The policy defines the owners of each asset category and procedure for allocating devices. End user equipment is tracked in the *IT Inventory.pdf* document. Server equipment hosted in datacentres are recorded in the *IT Inventory - Offsite.pdf*. Data is classified in accordance with the *Information Security Policy* into tiers and access controls are applied appropriately.	√			
A.8.3.1	Management of removable media	Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization	The use of removable media for storing sensitive data is prohibited, as stated in the *Information Security Policy*. Staff are required to used Google Drive to store and transfer files with colleagues.	√			
A.8.3.2	Disposal of media	Media shall be disposed of securely when no longer required, using formal procedures	Media must be returned to the Senior Manager, Development when no longer required. Devices are securely erased in-house or if required, physically destroyed to ensure removal of any sensitive data. This requirement was previously included in a policy but could not be found in the new *Information Security Policy*. The required procedure should be added into the new policy.		√		

Reference	Requirement	Requirement	Observations	Compliant	Observation	Minor nonconformity	Major nonconformity
A.9.1.1	Access control policy	An access control policy shall be established, documented and reviewed based on business and information security requirements	Gatherwell's approach to allocating and managing access is covered in multiple sections of the *Information Security Policy*. Access is granted based on role following the principle of least privilege. The approach taken complies with business and information security requirements.	√			
A.9.1.2	Access to network and network services	Users shall only be provided with access to the network and network services that they have been specifically authorized to use	Access rights are granted by role in Google Workspace and the Lottery Plus system. Access controls are applied to Google Drive shares, limiting access to only essential staff. Where possible, single sign-on is used to allocate access to third party services. User access is monitored within Google Workspace and was evidenced in *Google User Security Report.png*. Access to the server infrastructure is restricted to a small number of approved staff.	√			

Reference	Requirement	Requirement	Observations	Compliant	Observation	Minor nonconformity	Major nonconformity
A.9.2.1	User registration and de-registration	A formal user registration and de-registration process shall be implemented to enable assignment of access rights.	The user creation and removal procedures are tracked within checklists stored in Google Docs. An example of a comprehensive leavers checklist was evidenced in [redacted]_ *Leavers Form.xlsx*. The document records the steps taken (including dates) to remove access to all systems used by Gatherwell. It was stated that there is a starter checklist, but the process has not been documented to the same level of detail. Whilst the start date of an employee can be established using the *IT Security – Training Log* and technical logs, recording the steps in more detail within a starter checklist would be beneficial.		√		
A.9.2.2	User access provisioning	A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services	Role-based rights are applied to user accounts, limiting their access to only essential information. The Lottery Plus system, Office365, and Google Workspace all have user access constraints in place. Access granted to internal systems and external services is tracked by Gatherwell in the *User Access Register*.	√			

Reference	Requirement	Requirement	Observations	Compliant	Observation	Minor nonconformity	Major nonconformity
A.9.2.3	Management of privileged access rights	The allocation and use of privileged access rights shall be restricted and controlled	The production systems and cloud services are only accessible to a select group of authorised employees. An IP allowlist further restricts this access. Since it has proven difficult to remotely administrator staff computers with the present technology stack, staff members have been granted administrative access to their work laptops. The Senior Manager of Development monitors the health of the devices and guides users on appropriate use of the privileges access rights.	√			
A.9.2.4	Management of secret authentication information of users	The allocation of secret authentication information shall be controlled through a formal management process	Random temporary passwords are set on new user accounts. This is passed to the employee either in person or by phone and they must reset this on first login. This process is overseen by the Senior Manager of Development. Users are given a 1Password account in accordance with the *Information Security Policy* to store all company related credentials.	√			
A.9.2.5	Review of user access rights	Asset owners shall review users' access rights at regular intervals	User access rights reviews are conducted on a regular basis to ensure accuracy and compliance with company requirements. The last review was conducted in February 2024 and documented in *User access register - FEB2024.pdf*.	√			

Reference	Requirement	Requirement	Observations	Compliant	Observation	Minor nonconformity	Major nonconformity
A.9.2.6	Removal or adjustment of access rights	The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change	On the last day of a contract, user access is deactivated. Before permanently deleting the accounts, any required data is extracted. To ensure removal from all company systems and services, the leavers form is used. An example of this form was evidenced in [redacted]_ *Leavers Form.xlsx*.	√			
A.9.3.1	Use of secret authentication information	Users shall be required to follow the organization's practices in the use of secret authentication information	The 'Devices and IT' section of the *Information Security Policy* defines the requirements for using passwords. Additional guidance is provided throughout the policy document, including specific requirements for all three tiers of data and RoyalTS (remote desktop) access credentials. Minimum password requirements are enforced through Google Workspace and were evidenced in *Google Password Configuration.png*.	√			
A.9.4.1	Information access restriction	Access to information and application system functions shall be restricted in accordance with the access control policy	The *Information Security Policy* covers the requirements for controlling access to data. Information assets are classified into three tiers based on sensitivity. Each tier has clear guidance on storage locations and sharing permissions. Google Drive serves as the primary company storage, with appropriate access controls applied in line with the policy.	√			

Reference	Requirement	Requirement	Observations	Compliant	Observation	Minor nonconformity	Major nonconformity
A.9.4.2	Secure log-on procedure	Where required by the access control policy, access to systems and applications shall be controlled by a secure logon procedure	Gatherwell requires both unique user authentication and HTTPS connectivity for all cloud services. Accounts are configured to automatically lock after multiple failed login attempts to prevent brute force attacks. Company Google accounts require MFA as part of the login procedure. Evidence of this was provided in *Google MFA Configuration.png*. MFA is now also enforced for RDP connections to servers, as evidenced in *Duo MFA for RDP.png*.	√			
A.9.4.3	Password management system	Password management systems shall be interactive and shall ensure quality passwords	In accordance with the *Information Security Policy*, minimum password requirements are enforced for company Google and 1Password accounts, as evidenced in *Google Password Configuration.png* and *1Password - Password Policy.png*. Along with saving credentials, staff are asked to use 1Password to generate passwords. This was illustrated in *1Password - Password Generator.png*.	√			

Reference	Requirement	Requirement	Observations	Compliant	Observation	Minor nonconformity	Major nonconformity
A 9.4.4	Use of privileged utility programmes	The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.	Privileged access to production servers and cloud environments has been limited to two senior employees within the development team. Evidence of the restrictions for the production database was provided in *Database Server User Accounts.png*. Due to the distributed nature of staff, Gatherwell has provided users with privileged access to their local devices. This allows for remote support, and staff are informed they may only use this access when authorised by the Senior Manager of Development.	√			
A.10.1.1	Policy on use of cryptographic controls	A policy on the use of cryptographic controls for protection of information shall be developed and implemented	The *Information Security Policy* details how data must be protected with encryption and passwords. The policy covers protection of data at rest and in transit. Specific guidance is provided for each data tier. Computers have full disk encryption enabled using BitLocker. The *Cryptography Policy* defines the minimum requirements for encryption, certificates and TLS connections. Signed TLS certificates are managed by the Development Team. The requirements in place follow industry best practices.	√			

Reference	Requirement	Requirement	Observations	Compliant	Observation	Minor nonconformity	Major nonconformity
A.10.1.2	Key management	A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle	Certificates for the websites are managed by the Cloudflare WAF service. Let's Encrypt is used to generate certificates to protect the communication between Cloudflare and the servers. Encryption keys and SSH keys are securely stored using 1Password. Key management is covered in the *Information Security Policy*, including minimum key size and key salting.	√			
A.11.2.1	Equipment siting and protection	Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access	The *Information Security Policy* outlines the necessary measures to protect equipment and data. Although staff primarily work from home, they must still ensure devices are locked when not in use and avoid leaving equipment unattended in public places. This guidance is provided during staff awareness training. Servers are hosted by Rackspace, which ensures appropriate security and environmental controls.	√			
A.11.2.7	Secure disposal or re-use of equipment.	All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use	Equipment no longer in use must be returned to the Senior Manager of Development. Devices are wiped or have their OS reset to defaults before they may be reallocated. Equipment no longer required must have all media wiped before being disposed. No end user equipment had been disposed since the previous audit, but it was confirmed that some laptops are in storage awaiting reallocation.	√			

Reference	Requirement	Requirement	Observations	Compliant	Observation	Minor nonconformity	Major nonconformity
A.11.2.8	Unattended user equipment	Users shall ensure that unattended equipment has appropriate protection	The *Information Security Policy* states that computers and other devices must be locked when not in use. Equipment must not be left unattended in the office overnight or when working in other locations. Computers are configured to automatically lock after 5 minutes of inactivity for additional protection. This was evidenced in *Windows Power and Sleep Settings.png*. The policy also requires mobile phones have autolocking enabled, whether they are company issued or are personal devices used to access Gatherwell email / documents.	√			
A.12.1.4	Separation of development, testing and operational environments.	Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment	Environments used for development, testing, and production do not share systems or data. Access to every environment is restricted by role-based user constraints. Suitable access controls have been applied to the GitHub repositories.	√			

Reference	Requirement	Requirement	Observations	Compliant	Observation	Minor nonconformity	Major nonconformity
A.12.2.1	Controls against malware	Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness	The *Information Security Policy* requires all computers and phones have approved virus protection software installed. They must be running up to date definitions and provide real-time scanning. Computers have Microsoft Defender enabled on deployment. This was evidenced in *Windows Security Settings.png*. Staff are provided with malware awareness training as part of their induction and in the annual courses. The Senior Manager of Development is responsible for responding to potential infections and ensuring data and systems are recovered.	√			

Reference	Requirement	Requirement	Observations	Compliant	Observation	Minor nonconformity	Major nonconformity
A.12.3.1	Information backup	Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy	The *Information Security Policy* highlights the importance of protecting data. Staff are required to store all company documents in Google Drive / Google Docs for protection against device failure. Daily snapshots are taken of the production webserver. The database is subject to regular backups to secure storage in accordance with the 'Devices and IT' section of the policy. Production data is subject to daily backups *(Database Backup Configuration.png)* to secure storage and transaction log backups every 5 minutes *(Database Backup Transaction Log.png)*, providing more granular restoration points. Restore tests are conducted to validate these processes. The outcome is recorded in the *Backup Testing Log*.	√			
A.12.4.1	Event logging	Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed	The Rollbar *(Rollbar Monitoring.png)* and Pingdom *(Pingdom Monitoring.png)* services are used to monitor servers and webpages. A central page provides the status of all branded site *(LotteryPlus - Uptime Monitoring.png)*. The business's Slack account receives automated alerts for system or application issues *(Slack - Production Monitoring.png)*.	√			

Reference	Requirement	Requirement	Observations	Compliant	Observation	Minor nonconformity	Major nonconformity
A.12.4.2	Protection of log information	Logging facilities and log information shall be protected against tampering and unauthorized access	Access to logs requires individual user authentication and is restricted to a small number of essential staff. Logs are only accessible in read-only form to prevent modification.	√			
A.12.4.3	Administrator and operator logs	System administrator and system operator activities shall be logged and the logs protected and regularly reviewed	Server internal logging systems are used to record administrator activity. Approved users must use their individual administrative accounts to allow for tracking of all actions. The lottery application records all administrator actions in the internal database logs. These logs are reviewed on a regular basis.	√			
A.12.4.4	Clock synchronisation.	The clocks of all relevant information processing systems within an organization or security domain shall be synchronised to a single reference time source	Company computers are configured to synchronise with Microsoft NTP services. The production servers use trusted public NTP sources to ensure accuracy of their system clocks.	√			

Reference	Requirement	Requirement	Observations	Compliant	Observation	Minor nonconformity	Major nonconformity
A.13.1.1	Network controls	Networks shall be managed and controlled to protect information in systems and applications	Staff are required to authenticate to Google Workspace, GitHub, and other company services using individual user accounts. Access to each system is role-based and MFA is required for all core systems. This includes remote desktop connections to production servers. Lottery players must authenticate to the site before accessing any account information. Company data is stored in Google Drive, organised by type, with appropriate user access controls applied.	√			
A.13.1.2	Security of network services	Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house outsourced	Internal IT systems are managed in-house following company policies and procedures. Production servers are hosted by Rackspace and AWS, while email services are hosted through Google Workspace. All three providers offer suitable service level agreements and hold ISO 27001 certification.	√			
A.13.1.3	Segregation in networks	Groups of information services, users and information systems shall be segregated on networks	Staff mainly work from home on private networks. Gatherwell does not operate any servers or services on local networks. Production and testing environments are completely segregated, with no shared resources. Data is separated by type and user-level permissions are applied according to the *Information Security Policy*.	√			

Reference	Requirement	Requirement	Observations	Compliant	Observation	Minor nonconformity	Major nonconformity
A.14.1.2	Securing application services on public networks	Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.	Connections to the Gatherwell website and web applications are encrypted using HTTPS. HTTP requests without encryption are automatically upgraded. Gatherwell uses the Cloudflare WAF service to protect the applications against malicious requests. Only traffic from Cloudflare IP addresses is permitted on the servers. Cloudflare manages the public certificates for the sites. Let's Encrypt certificates are used to encrypt communication between Cloudflare and Gatherwell servers.	√			
A.14.1.3	Protecting application service transactions	Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay	Production servers are hosted on a private VLAN in the datacentre, with no direct external access. Web traffic is allowed only from Cloudflare's reverse proxy, which scans all requests for malicious content. Communication between the web and database servers occurs over the private VLAN, using transactions to prevent third-party manipulation or accidental corruption.	√			

Reference	Requirement	Requirement	Observations	Compliant	Observation	Minor nonconformity	Major nonconformity
A.14.2.1	Secure development policy	Rules for the development of software and systems shall be established and applied to developments within the organization.	Following the restructuring of the policies, this area is now covered in the "Development Security Procedure" section of the *Information Security Policy*. The document defines the development process that must be followed from pitch to deployment. The previous audit found that whilst developers were provided with induction training, there was no on-going training in place to maintain awareness. It was confirmed that regular training has been reintroduced and a record of this was provided in *Developer Training Log*.	√			
A.14.2.2	System change control procedures	Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures.	The *Information Security Policy* details the steps that must be followed for managing changes and new features. This includes pitching the idea, defining metrics, planning with a Product Manager and the full lifecycle. All changes must be approved before development may begin and receive final sign-off before they can be published. Changes involving PII require the completion of a DPIA. Changes are tracked in Jira and pull requests must be approved before merging the change. This process was evidenced in *GitHub pull requests.png*.	√			

Reference	Requirement	Requirement	Observations	Compliant	Observation	Minor nonconformity	Major nonconformity
A.14.2.3	Technical review of applications after operating platform changes	When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.	Updates to servers must be fully evaluated on the test servers to ensure functionality before any production systems. The 'Operating platform changes' section of the *Information Security Policy* covers the steps that must be followed for all planned changes.	√			
A.14.2.4	Restrictions on changes to software packages	Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.	The 'Restrictions to changes on software' section of the *Information Security Policy* states that changes to the platform, third party software and operating systems are discouraged. Changes for new features, security, reliability or performance must be assessed to ensure they do not introduce any new risks.	√			
A.14.2.5	Secure system engineering principles	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts.	Developers are required to follow industry security best practices when building software. This includes having a good knowledge of the OWASP top 10 guidance. The 'Secure System Engineering Principles' section of the *Information Security Policy* lists the most common vulnerabilities and actions that should be taken to prevent them.	√			

Reference	Requirement	Requirement	Observations	Compliant	Observation	Minor nonconformity	Major nonconformity
A.14.2.6	Secure development environment	Organizations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.	Development is carried out on computers connected to private home networks. These systems must adhere to the requirements outlined in the 'Secure development environments' section of the *Information Security Policy*. The code undergoes testing in a secure test environment with limited access.	√			
A.14.2.7	Outsourced development	The organization shall supervise and monitor the activity of out-sourced system development.	Gatherwell do not outsource any development work. This is stated within the *Information Security Policy.*	√			
A.14.2.8	System security testing	Testing of security functionality shall be carried out during development.	Unit and functionality testing is performed on all code. Gatherwell uses the Snyk security static code analysis tool to scan for code weaknesses and vulnerable libraries. Evidence of this was provided in *Snyk dashboard.png*. The previous audit noted a problem that has arisen when performing PCI DSS scans of the branded payment pages. It was stated that following the audit the scanning provider offered a solution to this issue and it has now been resolved.	√			
A.14.2.9	System acceptance testing	Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.	Code updates must complete testing and QA before being approved for deployment to production. The testing process is recorded in Jira and a CI pipeline is used to manage the release and potential rollback of changes.	√			

Reference	Requirement	Requirement	Observations	Compliant	Observation	Minor nonconformity	Major nonconformity
A.14.3.1	Protection of test data	Test data shall be selected carefully, protected and controlled.	The 'Protection of test data' section of the *Development Security Policy* states that tier 1 data must not be used in the staging or development environments. Fake data is generated using a script for testing and these environments do not share any resources with production systems.	√			
A.15.1.1	Information security policy for supplier relationships	Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented.	New suppliers must be subject to a risk assessment and where PII is handled, a DPIA would be completed. The assessment is performed based on the criticality of the service and the data processed or stored. Evidence of the risk assessments and DPIAs have been provided in previous audits. It was stated that no new suppliers have been adopted since the last audit. The *Supplier Relationships Policy* describes the process for adding new suppliers and includes a list of all approved suppliers.	√			
A.15.1.2	Addressing security within supplier agreements	All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information	Agreements with suppliers include must security responsibilities. Suppliers are informed of the company's security requirements where applicable to ensure compliance.	√			

Reference	Requirement	Requirement	Observations	Compliant	Observation	Minor nonconformity	Major nonconformity
A.15.1.3	Information and communication technology supply chain	Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain	Gatherwell's primary IT providers Rackspace, AWS and Google hold ISO 27001 certification and provide suitable service level definitions within the terms and conditions. All other IT related providers address information security responsibilities within their agreements.	√			
A.15.2.1	Monitoring and review of supplier services	Organizations shall regularly monitor, review and audit supplier service delivery	Suppliers are reviewed annually in accordance with the *Supplier Relationships Policy*. The document records the last review date and the name of the reviewer for each supplier. It was confirmed all suppliers have been reviewed within the last year.	√			
A 15.2.2	Managing changes to supplier services	Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.	A senior manager must approve changes to supplier services after reviewing an updated risk assessment or, if necessary, a DPIA. Where necessary, an updated contract or terms of service may be agreed to reflect the changes.	√			
A.16.1.1	Responsibilities and procedures	Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.	The *Information Security Policy* states that the Data Protection Officer is responsible for "monitoring potential and actual security breaches". The *Information Security Breach Reporting Procedure* defines key roles for incident response and the procedures that must be followed for dealing with them.	√			

Reference	Requirement	Requirement	Observations	Compliant	Observation	Minor nonconformity	Major nonconformity
A.16.1.2	Reporting information security events	Information security events shall be reported through appropriate management channels as quickly as possible.	The *Information Security Policy* requires staff promptly report suspected incidents. The *Information Security Breach Reporting Procedure* provides more details on the reporting process. The *Information Security Breach Report Template* is used to capture all relevant information. Clients can report suspected incidents via their Gatherwell account manager.	√			
A.16.1.3	Reporting information security weaknesses	Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.	Potential security weaknesses must be reported through the same process as above. Vulnerabilities identified by the security testing are logged as Jira tickets for resolution.	√			
A.16.1.4	Assessment of and decision on information security events	Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.	The *Information Security Breach Reporting Procedure* outlines the steps to be followed when assessing reported incidents. It includes examples of incident types and evaluates the systems and data affected. The assessment and any decisions made are documented in the *Breach Log*. It was noted the log does not contain the date of each incident. Whilst this information could be found in the report documents, it would be beneficial to include them in this log for easy reference.		√		

Reference	Requirement	Requirement	Observations	Compliant	Observation	Minor nonconformity	Major nonconformity
A.16.1.5	Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures.	Incident response is managed by the SIRO in collaboration with the Privacy Specialists. The steps taken and communications with external parties are documented for reference. The *Information Security Breach Reporting Procedure* provides guidance on reporting incidents to the ICO if personal identifiable information (PII) is affected.	√			
A.16.1.7	Collection of evidence	The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.	As part of an investigation, relevant evidence and logs are collected in accordance with the *Information Security Breach Reporting Procedure*. The gathered data must be securely stored by the investigating team until it is no longer needed.	√			
A.18.2.1	Independent review of security policy	The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur.	Gatherwell confirmed their continued commitment to undertaking annual information security audits. The items raised in the previous audit have been resolved, with suitable remediations put in place. The company has continued to run PCI DSS security tests of their web sites.	√			

Evidence

Apart from where stated in the observations above, adequate evidence was provided to confirm the policies were being correctly followed.

Observations & Nonconformities

The following lists any controls that were found to not be fully compliant. Each instance includes an agreed course of corrective action and a date the action will be completed by.

Ref.	A.8.3.2	Control	Disposal of media	Status	Observation
Finding					
Devices must be securely erased in-house or if required, physically destroyed to ensure removal of any sensitive data. This requirement was previously included in a policy but could not be found in the new *Information Security Policy*.					
Corrective Action					
A secure disposal section should be added to the *Information Security Policy* that clearly states the requirements and provides an overview of the acceptable methods for securely erasing data.					
Management Response					
This observation was accepted, and it was confirmed this topic will be added to a policy.					
Action Date	August 2024				

Ref.	A.9.2.1	Control	User registration and de-registration	Status	Observation
Finding					
The *Leavers Form* tracks all actions taken to remove access to company data and systems. It was noted similar a log for starters is not used. Whilst the start date of an employee could be established using the *IT Security – Training Log* and technical logs, recording the steps taken in more detail within a starter checklist would be beneficial.					
Corrective Action					
Create a starter checklist that records all access granted with dates, hardware allocated and any other relevant induction processes that must be completed.					
Management Response					
It was agreed that having a documented starter checklist would be beneficial and the team confirmed one will be created.					
Action Date	August 2024				

Ref.	A.16.1.4	Control	Assessment of and decision on information security events	Status	Observation
Finding					
An incident assessment and any decisions made are documented in the *Breach Log*. It was noted the log does not contain the date of each incident.					
Corrective Action					
Whilst this information could be found in the report documents, it would be beneficial to include the date in this log for easy reference.					
Management Response					
Gatherwell accepted this observation and confirmed they will update the log to include the incident dates.					
Action Date	August 2024				

End of report