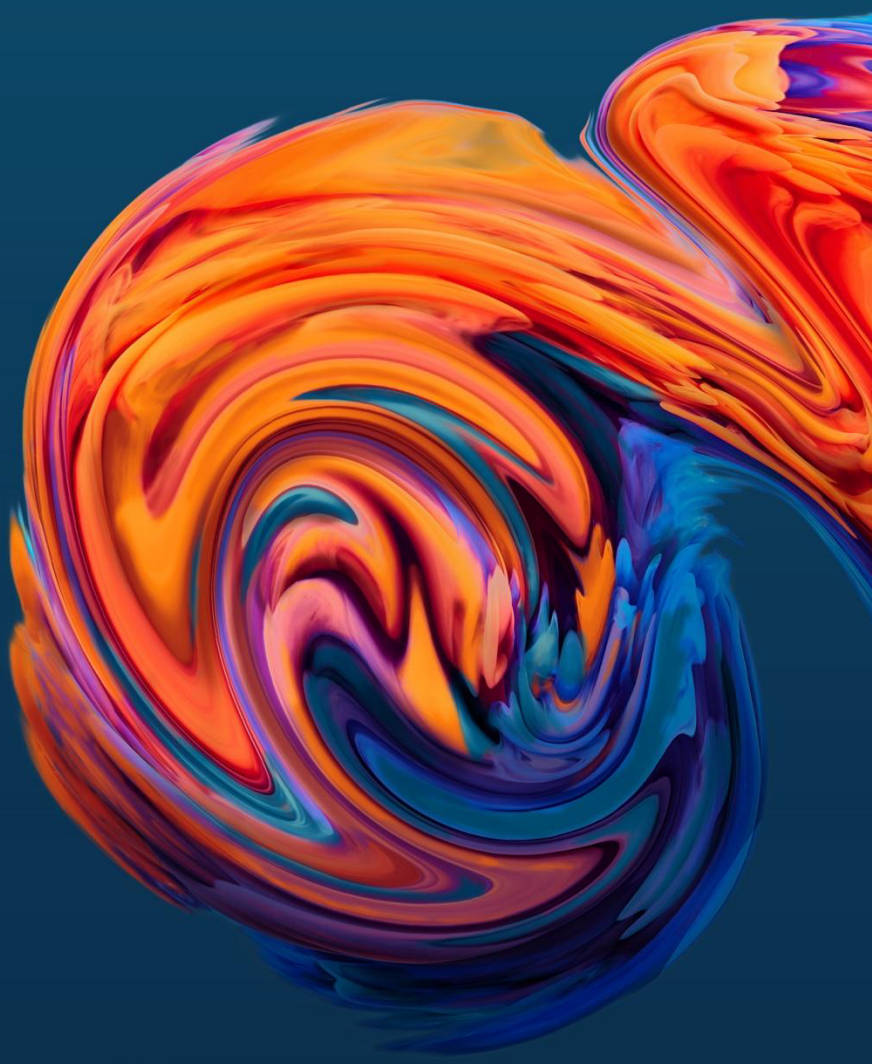
URM Getting the Balance Right



Gambling Commission Remote Gambling and Software Technical Standards (RTS) Internal Audit

Prepared for:

Woods Valldata

1.0 Preface

1.1 Prepared By

Name	Function
[redacted]	Senior Consultant

1.2 Reviewed and Authorised By

Name	Function
Martin Jones	Director

1.3 Client Distribution

Name	Function
Paula Robinson	Head of Compliance

1.4 Contact Details

Address	Telephone
Blake House Manor Park Manor Farm Road Reading Berkshire RG2 0JH	0118 206 5410

1.5 Change History

Version	Date	Revision Description
0.1	07 November 2025	Initial Draft
1.0	11 November 2025	Final Draft

Contents

1.0 Preface 2

1.1 Prepared By 2
1.2 Reviewed and Authorised By 2
1.3 Client Distribution 2
1.4 Contact Details 2
1.5 Change History 2

2.0 Overview 4

2.1 Woods Valldata 4
2.2 Technical Scope 4
2.3 Other Regulatory Requirements 5
2.4 Scope of Audit and Methodology Employed 5
2.5 About URM 5
2.6 Auditor Credentials 5
2.7 References 6

3.0 Key Audit Findings 6

4.0 Audit Scope 6

4.1 Audit Details 6
4.2 Objectives 7
4.3 Auditees Interviewed 7
4.4 Documents/Evidence Reviewed 9
4.5 Key Applications and Systems 11
4.6 Sampling 13
4.7 Acknowledgements 13

5.0 Details of Nonconformities and Opportunities for Improvement 13

5.1 Nonconformities and Observations from Previous Audits 13
5.2 Nonconformities and Observations from This Audit 13

Appendix A – Remote Gambling and Software Technical Standards – URM Review 14

2.0 Overview

2.1 Woods Valldata

Woods Group Limited, trading as Woods Valldata (WV), provides specialist funding services to the charity sector. It employs approximately 150 employees at its headquarters at Lansdowne House, Bumpers Way, Bumpers Farm, Chippenham, Wiltshire, SN14 6NG and approximately 40 employees in Romania. WV delivers a range of services including managing raffles and lotteries, fund management, mailing services, direct debit processing, and lottery website hosting.

WV is licensed and regulated by the Gambling Commission (GC) under 2 licences as detailed below:

- Woods Group Limited (Trading as Woods Valldata)
  - Remote Operating Licence : 003586-R-310429-015
  - Non-remote Operating Licence: 003586-N-103664-016.

WV is required to comply with the GC Remote Gambling and Software Technical Standards (RTS) which were updated in November 2024. Chapter 4 of the RTS specifies a set of security requirements based on a subset of the controls in Annex A of ISO/IEC 27001:2022 (ISO 27001), the International Standard for Information Security Management. ISO 27001 is supported by ISO/IEC 27002:2022 (ISO 27002), which provides implementation guidance on the controls contained in Annex A of ISO 27001.

The GC requires that the RTS controls of licence holders are independently audited on an annual basis. To fulfil this, WV engaged URM Consulting Services Ltd (URM) to conduct an audit which took place on 4 and 5 November 2025. In line with the requirements of the GC Security Audit Advice, this report presents the audit findings, based on interviews with WV staff and management, as well as an examination of relevant policies, procedures, and supporting documentation.

2.2 Technical Scope

WV delivers its specialist funding services to the charity sector, including its raffle and lottery services, through a range of in-house developed applications, Windows services, and website APIs. Applications are hosted on either on-site Windows server infrastructure or cloud-based Azure infrastructure and are predominantly Microsoft .NET based. Although a number of versions of .NET are utilised, all are still fully supported by Microsoft and WV has ongoing plans to transition its code to the latest version. The Windows server estate is based on [redacted] and the databases utilise [redacted]. Azure Platform as a Service (PaaS) is used to host supporter-facing functionality such as websites, email and databases which make up approximately 10% of the WV code base. WV utilises a software random number generator (RNG) for conducting raffle and lottery draws on all platforms utilised by the organisation. The RNG is based on Microsoft's RNGCryptoServiceProvider Class and is implemented in VB.Net. It was tested and approved by Gambling Associates; a GC approved testing company listed on its website.

During the audit, the processes for the secure development and maintenance of all code and on-site infrastructure were reviewed as were the infrastructure support processes. A list of key systems reviewed can be found in Section 4.5.

2.3 Other Regulatory Requirements

As WV handles credit card information to take payments from client supporters, it is required to comply with the Payment Card Industry Data Security Standard (PCI DSS). WV is assessed annually by a PCI qualified security assessor (QSA) and a report on compliance (RoC) and attestation of compliance (AoC) are produced. WV is also a Tier A Bacs Approved Bureau (Bureau Number B20999).

WV is certified to the following standards:

- **ISO/IEC 27001:2022** – Information security, cybersecurity and privacy protection — Information security management systems — Requirements
- **ISO 9001:2015** – Quality management systems — Requirements
- **ISO 14001:2015** – Environmental management systems — Requirements with guidance for use.

2.4 Scope of Audit and Methodology Employed

On Tuesday 4 November and Wednesday 5 November 2025, URM conducted a formal audit of WV's compliance with Chapter 4 of the GC's RTS. The audit was conducted by [redacted], Senior Consultant at URM, in line with the requirements of the GC Security Audit Advice as updated in November 2024.

The audit was conducted onsite at Lansdowne House and was based on interviews with key staff, a site tour and an inspection of documentation and evidential records. The audit covered all services provided from the Lansdowne House location.

A list of interviewees can be found in Section 4.3 of this report and a list of documentation and records reviewed can be found in Section 4.4.

2.5 About URM

URM Consulting Services Limited (URM) is dedicated to providing high quality, cost-effective and tailored consultancy, auditing, and training services in the areas of information and cyber security, data protection, business continuity, and risk management. Specific areas of expertise include assisting organisations certify to standards such as ISO 27001 (450+), ISO 22301, Cyber Essentials, and PCI DSS (URM is a PCI QSAC) and comply with standards and frameworks such as SOC 2 and NIST CSF 2. URM also has a hugely experienced Data Protection Team, which has a 20-year track record in assisting organisations to comply with legislation, most notably the Data Protection Act and, more latterly, the GDPR.

One of URM's distinctive competencies is its ability to deliver both governance, risk, and compliance (GRC) services, along with a comprehensive range of cybersecurity consulting and penetration testing services. Through its services and risk management software (Abriska), URM's mission is to assist organisations in achieving the levels of information security (IS), data protection and business continuity which are commensurate with their business objectives and culture.

.

2.6 Auditor Credentials

[redacted] (Senior Consultant) has more than 17 years' experience in information security and has worked in information technology for over 30 years. For the last 9 years, [redacted] has been focused on the provision of consultancy and auditing services to a wide range of private and public sector organisations. [redacted] holds the Certified Information Security Manager (CISM) and Certified Information Systems Auditor (CISA) qualifications. He is also a PCI QSA.

2.7 References

The following references are made in this report:

- Gambling Commission Remote Gambling and Software Technical Standards – November 2024 (RTS)
- GC Security Audit Advice – September 2024
- ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems — Requirements (ISO 27001)
- ISO/IEC 27002:2022 Information Security, Cybersecurity and Privacy Protection – Information Security Controls (ISO 27002).

3.0 Key Audit Findings

No significant nonconformities were identified during the audit and, therefore, URM confirms that WV is compliant with all requirements of the GC RTS. During the audit, the information security processes and controls implemented by WV were observed to be well designed and documented. There was also clear evidence that these processes and controls were operating effectively and that there was a comprehensive oversight framework implemented by the Compliance Team to help assure this. WV was observed to be operating a well-established information security management system (ISMS) which also contributed to the organisation's information security maturity. WV's supplier management and role-based access management processes, information security awareness programme and physical security management were noted to be areas of particular strength. During the audit, all interviewees were observed to have a good understanding of both the importance of information security to the organisation and their specific information security responsibilities. WV's commitment to continual improvement over the last 12 months was evidenced during the audit by the rollout of multi-factor authentication (MFA) to a wider range of systems and the deployment of content security policies and integrity checking for PCI DSS in-scope websites.

Appendix A of this report contains a table detailing the evidence reviewed and conformance status of each of the security requirements from Chapter 4 of the RTS.

4.0 Audit Scope

4.1 Audit Details

Process / Area / Department	Report Reference	Date
All activities to support the gaming services undertaken at: Woods Group Limited (trading as Woods Valldata) Lansdowne House Bumpers Way Bumpers Farm Chippenham Wiltshire SN14 6NG.	2025-01	07 November 2025

Auditor	Referenced Standards
[redacted] (URM)	Gambling Commission Remote Gambling and Software Technical Standards (November 2024) ISO/IEC 27001:2022 ISO/IEC 27002:2022

4.2 Objectives

Objectives
The objectives of the audit were to: • Assess compliance against the Gambling Commission RTS (November 2024) • Assess compliance against WV's own information security policies and procedures • Identify opportunities for improvement.

4.3 Auditees Interviewed

Auditee	Role	Area Covered
Paula Robinson	Head of Compliance	5.1 (Policies for information security) 5.10 (Acceptable use of information and other associated assets) 5.15 (Access control) 5.16 (Identity management) 5.17 (Authentication information)

Auditee	Role	Area Covered
		5.18 (Access rights) 5.19 (Information security in supplier relationships) 5.20 (Addressing information security within supplier relationships) 5.21 (Managing information security in the ICT supply chain) 5.22 (Monitoring, review and change management of supplier services) 5.23 (Information security for use of cloud services) 5.24 (Information security incident management planning and preparation 5.25 (Assessment and decision on information security events) 5.26 (Response to information security incidents) 5.28 (Collection of evidence) 5.35 (Independent review of information security) 6.3 (Information security awareness, education, and training) 6.8 (Information security event reporting)
[redacted]	Compliance Officer	5.19 (Information security in supplier relationships) 5.20 (Addressing information security within supplier relationships) 5.21 (Managing information security in the ICT supply chain) 5.22 (Monitoring, review and change management of supplier services) 5.23 (Information security for use of cloud services) 5.35 (Independent review of information security) 6.3 (Information security awareness, education, and training) 6.8 (Information security event reporting) 7.8 (Equipment siting and protection)
[redacted]	Technical Architect	8.25 (Secure development life cycle) 8.26 (Application security requirements) 8.27 (Secure system architecture and engineering principles) 8.29 (Security testing in development and acceptance) 8.30 (Outsourced development) 8.31 (Separation of development, test, and production environments) 8.32 (Change management)

Auditee	Role	Area Covered
		8.33 (Test Information)
[redacted]	Infrastructure Support Engineer	7.10 (Storage media) 7.14 (Secure disposal of re-used of equipment) 8.1 (user endpoint devices) 8.2 (Privileged access rights) 8.3 (Information access restriction) 8.5 (Secure authentication) 8.7 (Protection against malware) 8.13 (Information backup) 8.15 (Logging) 8.17 (Clock synchronisation) 8.18 (Use of privileged utility programs) 8.20 (Networks security) 8.21 (Security of network services) 8.22 (Segregation of networks) 8.24 (Use of cryptography)
[redacted]	People and Culture Coordinator	6.5 (Responsibilities after termination or change of employment) 6.7 (Remote working)
[redacted]	Head of People and Culture	6.5 (Responsibilities after termination or change of employment) 6.7 (Remote working)
[redacted]	Assistant Facilities Manager	5.18 (Access rights) 7.8 (Equipment siting and protection)

4.4 Documents/Evidence Reviewed

Document	Version and Date
Information Security Policy	Version 2.5, dated 24/04/2025
Information Classification Handling and Protection Policy	Version 3.6, dated 03/10/2025
Mobile Device and Remote Working Policy	Version 2.6, 20/10/2025
Site Rules and Confidentiality Agreement	Version 6.0, dated 01/09/2025
Visitors Log 2025	N/A

Document	Version and Date
Physical and Environmental Security Policy	Version 2.5, dated 24/04/2025
Information Security Awareness Training Presentation	N/A
Information Security 2025/26 Test	N/A
Non-IT Access Staff Annual Compliance Briefing	Version 1.2, dated 26/10/2025
Terms and Conditions of Employment Template	Dated October 2025
Resignation Acknowledgement Letter Template	Dated October 2024
Access Control Policy	Version 2.7, dated 20/10/2025
Starters, Movers, and Leavers Procedure	Version 5.0, dated 03/11/2025
Role-Based Profile Matrix	N/A
Acceptable Use Policy	Version 2.7, dated 20/10/2025
IT Security Policy	Version 3.0, dated 27/03/2025
Software SSL and Domain Inventory	N/A
Asset Register	N/A
IT Infrastructure Daily Check Sheet	Dated 05/11/2025
[redacted] Backup Report	Dated 05/11/2025
Systems Without [redacted] Report	Dated 04/11/2025
Network Diagram	Dated October 2024
Development and Testing Policy	Version 3.2, dated 29/04/2025
Development and Testing Process	Version 3.3, dated 25/04/2024
Coding Standards and Code Review Guidelines	Version 2.2, dated 29/04/2025
Release Approval Checklist	N/A
Third Party Management Policy	Version 4.1, dated 24/04/2025
Third Party Management Process	Version 3.1, dated 24/04/2025

Document	Version and Date
Approved Supplier List	Version 4.0, dated 31/10/2024
Third Party Checklist	N/A
[redacted] Privacy Impact Assessment Screen Form	Dated January 2020
Third Party Compliance Review Sept 2025	Dated 30/09/2025
Arrow Business Communications Service Review	Dated 18/06/2025
Creditcall Service Review	Dated 06/05/2025
Standard Purchase Order	N/A
Incident Reporting Escalation and Management Procedure	Version 4.2, dated 28/03/2025
Woods Valldata Issues Log	N/A
Incident Management and Business Continuity Plan	Version 4.1, dated 20/10/2025
[redacted] Incident Report	February 2025

4.5 Key Applications and Systems

The table below details the key applications that support the delivery of WV's information security processes and controls.

System	Applicable Controls
SharePoint	5.1, 5.16, 5.20, 6.5, 8.3
Microsoft Forms	5.16
Active Directory	8.3, 8.17
[redacted] Endpoint Protection	7.10, 8.5, 8.7
Zendesk	5.16, 5.17, 5.18, 5.24, 5.25, 5.26, 7.10, 7.14, 8.15, 8.21
[redacted]	6.3
[redacted]	8.24

System	Applicable Controls
[redacted]	8.5
[redacted]	8.1, 8.7, 8.15
[redacted]	8.1
[redacted]	8.13
Azure Front Door	8.20
[redacted]	8.20
[redacted]	8.21
[redacted]	8.20
[redacted]	8.21
Microsoft Azure DevOps	8.32
Microsoft Azure GitHub	8.31, 8.32
[redacted]	8.24

Internally developed systems that are core to the delivery of WV's gambling products are listed in the table below:

System	Purpose
Admin System	Supporter Appeals, Raffle and Lottery Portal, Database and RNG
Classic and Response	Supporter Appeals and Raffle Database
Contact Manager	Appeals and Raffle Portal for Classic and Response system
Azure Lotteries and Websites	New Lottery Websites, Portal and Database, RNG and Supporter Portal.
Client Branded Raffle Websites	Raffle website per client, enabling on-line ticket sales that feed into corresponding database

System	Purpose
Client Branded Lottery Websites	Lottery websites per client, enabling lottery sign-ups via direct debit that feed into the Admin System.
Raffle RNG	RNG system for running raffle draws from Classic and Response.
Smartview	Supporter Appeals, Raffle and Lottery Portal, Database and RNG

4.6 Sampling

The audit used a sampling approach to determine levels of conformance with policy and the requirements of the GC RTS. It also represents a snapshot in time. Therefore, nonconformities may exist that have not been identified.

4.7 Acknowledgements

URM would like to thank WV and those listed in Section 4.3 above for their hospitality, openness, and cooperation during the audit.

5.0 Details of Nonconformities and Opportunities for Improvement

5.1 Nonconformities and Observations from Previous Audits

No findings were raised during the GC RTS audit conducted in November 2024.

5.2 Nonconformities and Observations from This Audit

No nonconformities were identified during this audit.

Appendix A – Remote Gambling and Software Technical Standards – URM Review

This Section details WV's compliance status with the security controls specified within the GC RTS. The table below provides a summary statement of the requirements, WV's compliance status, a short narrative describing the evidence seen to support the requirement, and the supporting documents observed. These comments are based on information provided by WV's staff and a review of relevant records and documentation.

Control Ref	Control Name	Control Description	Status	Evidence of Compliance	Related Documents/ Records
5	**Organisational Controls**				
5.1	Policies for information security	Information security policy and topic-specific policies should be defined, approved by management, published, communicated to, and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.	Compliant	WV has an established set of information security policies which includes an Information Security Policy that details the organisation's high-level information security principles and a number of more detailed, topic-specific policies. All information security policies reviewed during the audit were observed to have a standard document structure that was consistently applied and included a policy purpose, policy scope, responsibilities and a full document history with version numbers. All information security policies are required to be reviewed at least annually and following any significant business change. During the audit, no policies were identified as being overdue for review and the document history and version control sections of each policy were observed to provide details of the completed periodic reviews and any associated document updates. As evidence of this, the latest versions of the following documents were reviewed: • Information Security Policy (version 2.5, dated 24/04/2025) was observed to have been reviewed and updated to reference the	Information Security Policy IT Security Policy Information Classification Handling and Protection Policy

Control Ref	Control Name	Control Description	Status	Evidence of Compliance	Related Documents/ Records
				• organisation's compliance to the SafeSupplier verification service and to reflect organisational structure changes • IT Security Policy (version 3.0, dated 27/03/2025) was observed to have been updated to include additional requirements for PCI DSS version 4.0 and for system and application account management and to reflect updates in the technology estate • Information Classification Handling and Protection Policy (version 3.6, dated 03/10/2025) was observed to have been updated to reflect organisation structure changes. The information security policies were observed to be available to all employees who have IT access. The Information Security Policy was reviewed, and it was observed to include details of information security responsibilities and a set of information security policy statements specifying WV's high-level information security objectives and the organisation's requirements for • Risk management • Third party management • Business continuity • Information security training • The management of information security breaches • Internal and external auditing. The Policy also specifies how information security is governed and monitored across the organisation and how any deviations to information security policies should be authorised and managed.	

Control Ref	Control Name	Control Description	Status	Evidence of Compliance	Related Documents/ Records
5.10	Acceptable use of information and other associated assets	Rules for the acceptable use and procedures for handling information and other associated assets should be identified, documented, and implemented.	Compliant	Rules for the acceptable use and handling of information and other assets were observed to be documented in the Acceptable Use Policy (version 2.7, dated 20/10/2025). This Policy details how all employees should: • Protect corporate equipment, data, and information • Securely use resources including email and the internet on corporate devices and networks • Follow clear desk and working area guidelines • Protect corporate and third party intellectual property rights • Protect assets against malicious code • Manage their passwords securely • Report incidents. The Policy outlines the required controls for physical security, operations within secure areas and the communications room, as well as procedures for managing visitors, contractors, and agency staff. All employees are expected to comply with these requirements.. It was observed that the Policy's most recent update included an expansion of the requirements related to the use of MFA across the organisation. The Mobile Device and Remote Working Policy (version 2.6, dated 20/10/2025) was reviewed and observed to specify the security measures that employees must follow to safeguard corporate mobile devices while travelling and working remotely. It also specifies the actions employees should take if their allocated corporate mobile device is lost or stolen.	Acceptable Use Policy Mobile Device and Remote Working Policy

Control Ref	Control Name	Control Description	Status	Evidence of Compliance	Related Documents/ Records
5.15	Access control	Rules to control physical and logical access to information and other associated assets should be established and implemented based on business and information security requirements.	Compliant	The Access Control Policy (version 2.7, dated 20/10/2025) was reviewed and observed to include details of how access to WV physical sites, networks and infrastructure must be managed. The Policy states that: • Access to information assets and information processing facilities will be protected by appropriate physical and logical authentication and authorisation controls • Access provisioning is role-based and provided on a 'need to know' basis in relation to the fulfilment of the individual's job role or function • All information and information processing facilities must be owned by a named individual • No access will be provided to employees via generic or shared accounts • WV premises will be protected in compliance with the Physical and Environmental Security Policy. It was observed that the latest version of the Policy was updated to reflect organisational changes and the expanded use of MFA across the organisation.	Access Control Policy
5.16	Identity management	The full life cycle of identities should be managed.	Compliant	The Starters, Movers and Leavers Procedure (version 5.0, dated 03/11/2025) was reviewed and observed to contain details of the responsibilities of line managers, the HR Team, the IT Infrastructure Team, and the Reception Team in the management of employee identities. SharePoint workflows are utilised to manage the procedures for employees joining and leaving the organisation and for employee role changes. All actions related to these procedures are captured in Zendesk tickets and the procedures are used for all permanent, temporary and agency employees.	Starters, Movers and Leavers Procedure Role-Based Profile Matrix Example Zendesk tickets

Control Ref	Control Name	Control Description	Status	Evidence of Compliance	Related Documents/ Records
				There is a SharePoint page that provides access to these workflows for all employees. This page was reviewed and the New Starter Request workflow was observed to require an online form to be completed to initiate the joiner process. This form is typically completed by the new employee's line manager. The Form was observed to require the following information to be populated: • New employee name • Job title • Department • Position type • Whether the role requires IT access and an email account • Whether a corporate mobile phone is required. The form can also be used to detail any access the new employee requires in addition to the standard role-based access detailed in the Role-Based Profile Matrix. This additional access will be reviewed by The Compliance Manager and the new employee's line manager may be required to provide an appropriate justification before it is provisioned. Any access provisioned in addition to the standard role-based access is documented as an exception within the Role-Based Profile Matrix. Once the New Starter Request Form has been completed, the SharePoint workflow sends it to the People and Culture Team to review and approve. Then if IT access is required, the workflow creates a Zendesk ticket for the Infrastructure Team to process and an email is sent to the Facilities Team so that it can create a physical access card for the new employee on their first day. An example email to the Facilities Team for an agency worker starting on 28/10/2025 was reviewed.	

Control Ref	Control Name	Control Description	Status	Evidence of Compliance	Related Documents/ Records
				2 example Zendesk tickets for starters were reviewed: • Ticket 460003 – This ticket related to a Campaign Manager who started on 08/09/2025. The ticket was created on 08/08/2025 and was observed to document all completed actions to allocate a device to the employee and provision their access which included a specific request from the line manager for Contact Manager and DAT access • Ticket 469940– This ticket related to a Supporter Services Executive who started on 28/10/2025. This was a fixed-term agency role. The ticket was created on 24/10/2025 and was observed to document all completed actions to allocate a device to the employee and provision their access. Both permanent and fixed-term roles are managed in the same way but often fixed-term roles have to be processed in a shorter timer-period than permanent roles (as evidenced in the 2 examples above). Example tickets for 2 leavers were also reviewed: • Ticket created on 11/08/2025 for a Business Analyst who left on 29/10/2025. All actions were completed by 04/11/2025 • Ticket created on 22/09/2025 for a Senior Account Manager who left on 31/10/2025. All actions were completed by 04/11/2025. Both tickets documented the steps taken to remove all system access for each leaver and it was observed that the Compliance Manager is actively reviewing leaver tickets to verify that a complete audit trail exists for all removed access, including any exceptions listed in the Role-Based Profile Matrix.	

Control Ref	Control Name	Control Description	Status	Evidence of Compliance	Related Documents/ Records
				The SharePoint User Changes Form was reviewed and observed to require the employee's details and any changes to these to be populated along with details of whether IT access changes or physical access changes are required. Only the People and Culture Team and line managers are able to request these changes and many of these requests relate to changes in the employees reporting to a specific line manager or changes to an employee's job title so only require Active Directory (AD) updates. Employees who require extended leave (such as maternity leave) will have their access deactivated at the start of their leave and then reactivated when they return. During the audit, a machine operator who leaves for extended periods and then returns to work was discussed. In this case, the Receptionist disables their access card on their last day and then re-enables it when they return to work. An example ticket for an employee access change was reviewed: • Ticket 470618 – This ticket was created on 30/10/2025 and related to provisioning access to the HR-Managers-Only SharePoint site to an Account Director. This ticket was required as the employee had been previously promoted to this role and this additional access had been missed from the initial role change Zendesk ticket even though it was documented as a role requirement in the Role-Based Profile Matrix.	
5.17	Authentication information	Allocation and management of authentication information should be	Compliant	The Acceptable Use Policy was reviewed and observed to include a 'Passwords' section which details how employees should securely manage their WV authentication information.	Acceptable Use Policy

Control Ref	Control Name	Control Description	Status	Evidence of Compliance	Related Documents/ Records
		controlled by a management process, including advising personnel on the appropriate handling of authentication information.		Employees who need their password reset are required to raise a Zendesk ticket for it to be reset by the Infrastructure Team. This Team receives notifications of any accounts that are locked due to multiple failed login attempts and will message the relevant employee to determine whether there is an issue and to confirm that their account is still secure.	
5.18	Access rights	Access rights to information and other associated assets should be provisioned, reviewed, modified, and removed in accordance with the organisation's topic-specific policy on and rules for access control.	Compliant	Access rights are managed on a 'need-to-know' basis in relation to the fulfilment of the individual's job role or function. The Role-Based Profile Matrix specifies the access to be provisioned for each role within WV. The aim of this spreadsheet is to ensure that there is consistency in the provisioning of access rights and that details of all provisioned logical and physical access is recorded in a single document. The Matrix spreadsheet was reviewed and observed to contain a number of tabs including: • **Default Access Levels** – This documents the default WV core system access levels each WV team or employee group (for example, the Supporter Services Team, the Compliance Team, and emergency key holders) should be provisioned with. These access levels were reviewed and observed to include multiple sub-groups for some teams to provide a greater level of granularity in access rights • **Exceptions** – This tab documents all exceptions to the default access levels. These exceptions relate to specific employee access that it is not appropriate to manage at a departmental basis. The tab was	Role-Based Profile Matrix

Control Ref	Control Name	Control Description	Status	Evidence of Compliance	Related Documents/ Records
				reviewed, and sample exceptions noted included information about employees who had access: o The Gallagher access control system o The CCTV system in Lansdowne House o The lottery portal and lottery analytics systems. A specific exception discussed during the audit was the remote network access provisioned to 2 external contractors. This access is only provisioned when needed and is disabled at all other times • **Service Accounts** – This is a new tab which details all the accounts that have been created to enable specific systems to operate across the IT estate • **WV Network Security** – This tab documents all network shares, their owners and who requires access (this is predominantly managed via AD groups) • **WV Security Groups** – This documents all AD function and security groups and their members. There are also tabs in the Matrix that document the green, red and blue network shares and how these are mapped and the employees who have building keys and building alarm fobs. The Head of Compliance is the only employee who can update the Matrix, and these updates are fully documented including the source of the update and the associated Zendesk ticket. This ensures that a full audit trail of all changes to access control requirements is maintained. The Facilities Team (which also manages the Lansdowne House reception desk) is responsible for managing site and secure area access which involves	

Control Ref	Control Name	Control Description	Status	Evidence of Compliance	Related Documents/ Records
				the management of physical access cards, building keys and building alarm codes. The Team implements physical access restrictions through the configuration of employees' physical access cards so that they only have access to secure areas where their role requires it.	
5.19	Information security in supplier relationships	Processes and procedures should be defined and implemented to manage the information security risks associated with the use of supplier's products or services.	Compliant	The Third-Party Management Policy (version 4.1, dated 24/04/2025) was reviewed and observed to detail the due diligence and ongoing management requirements when engaging and using suppliers. The Policy details the supplier management responsibilities of relationship owners, the Compliance Team, the Finance Team, information owners, managers, and employees. It also specifies a set of high-level principles for the management of suppliers and the requirements for • Supplier contract and formal agreement management • Due diligence processes for onboarding new suppliers • Risk assessments of suppliers • The ongoing monitoring and review of supplier services • Managing changes to supplier agreements and services. The Third Party Management Process (version 3.1, dated 24/04/2025) was reviewed and observed to contain flowcharts for supplier assessment, engagement, change and termination. Suppliers are documented in the Approved Suppliers List (version 4.0, dated 31/10/2024) which was reviewed and observed to include the following information about each supplier: • Company name • Relationship owner • Supplier type	Third Party Management Policy Third Party Management Process Approved Suppliers List Third Party Checklist [redacted] Privacy Impact Assessment Screen Form

Control Ref	Control Name	Control Description	Status	Evidence of Compliance	Related Documents/ Records
				• Supplier area • Contract type • Whether they are a key supplier. The list also includes details of the information access the supplier requires and the certifications (such as PCI DSS, ISO 27001, ISO 9001, ISO 14001, and Cyber Essentials) that the supplier has and when these expire. The Compliance Team conducts a quarterly review of the Approved Suppliers List to confirm that it is comprehensive and up to date. This review also ensures that any listed suppliers that are not going to be utilised in the future are formally retired. The Head of People and Culture is responsible for approving suppliers of HR services such as employment agencies. For other service types, if engaging a new supplier is necessary, the requestor is required to complete the Third-Party Checklist. This Checklist was reviewed and observed to include a series of preliminary questions regarding the supplier and the proposed service, addressing considerations such as whether: • It will be a critical service • System access will be required • Access to site will be required • The service involves processing, storing, or transmitting information. Based on the responses to these initial questions, further, more detailed questions are then required to be responded to and if applicable, the relationship owner is required to collect supporting evidence for the responses.	

Control Ref	Control Name	Control Description	Status	Evidence of Compliance	Related Documents/ Records
				The completed Third Party Checklist and associated supporting evidence is reviewed by the Compliance Team which will also conduct other applicable checks such as reviewing the prospective supplier's: • Anti-slavery policy • Sustainability policy • Artificial intelligence policy • Terms and conditions • Website • Relevant certifications. If a prospective supplier will have access to personal information, a privacy impact assessment will also be conducted. An example Privacy Impact Assessment Screen Form for Bishop Fleming which provides payroll services was reviewed. This Form was completed in January 2020 and was observed to include questions on: • The type of personal information to be processed • Who will access the personal information • How long the personal information will be stored. The relationship owner is responsible for completing this Form, which is then reviewed by the Head of Compliance who will also add details of any resultant risks or required actions. For [redacted], this included determining how personal information would be removed from the previous supplier. If the Compliance Team approves the prospective supplier, its details are then passed onto the Finance Team to conduct financial due diligence checks. If these are passed, the prospective supplier is added to the Approved Suppliers List, and the Finance Team inform the relationship owner of this.	

Control Ref	Control Name	Control Description	Status	Evidence of Compliance	Related Documents/ Records
				If the Compliance Team is unable to approve a prospective supplier (for example, because it does not have the expected information security certifications) it will be escalated to the Chief Executive Officer (CEO) to make a decision based on the level of business risk.	
5.20	Addressing information security within supplier agreements	Relevant information security requirements should be established and agreed with each supplier based on the type of supplier relationship.	Compliant	WV does not have its own standard supplier contract, so typically uses the supplier's contract templates. When onboarding a supplier, the relationship owner and the Compliance Team will both review the supplier's contract and provide the supplier with feedback on any issues. Contracts are stored in a restricted access SharePoint directory with a folder allocated for each supplier. Other relevant supplier information such as supplier certification evidence, supplier review evidence, supplier policies, and insurance certificates are also stored in this directory. Confidentiality or non-disclosure agreements (NDAs) will typically form part of the contract with the supplier. However, if there is a significant engagement with a supplier prior to a contract being signed, WV may require the supplier to sign a stand-alone NDA. For suppliers that are engaged on a work order basis, WV has a Standard Purchase Order. This was reviewed and observed to include a set of standard terms and conditions which includes clauses on confidentiality, intellectual property rights, data protection, service termination, and indemnity. The Finance Team will block any invoice associated with a supplier that is not on the Approved Supplier List which ensures that the supplier onboarding	Standard Purchase Order

Control Ref	Control Name	Control Description	Status	Evidence of Compliance	Related Documents/ Records
				processes always have to be followed even if the plan is to pay the supplier via a company credit or debit card.	
5.21	Managing information security in the ICT supply chain	Processes and procedures should be defined and implemented to manage the information security risks associated with the ICT products and services supply chain.	Compliant	Suppliers delivering information and communication technology services are subject to WV's standard due diligence checks during the Supplier Onboarding Process. If a supplier is going to utilise sub-contractors, this has to be formally approved by WV. The Compliance Team will review the full supply chain to determine whether the sub-contracting presents any data processing or information security risks that need to be resolved or managed.	
5.22	Monitoring, review and change management of supplier services	The organisation should regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery	Compliant	For critical suppliers, relationship owners are required to conduct regular service reviews. An example review for Arrow Business Communications (dated 18/06/2025) was reviewed and it was observed that there was a documented agenda and a set of meeting notes. The agenda was based on a standard format which included: • Review of actions • Supplier performance • Contract exits clauses and notice period • Incidents/issues/risks • Licences and certifications • Requests for change • Feedback from interested parties • Capacity plan forecasts • Financial/commercial performance	Arrow Business Communications Service Review Creditcall Service Review Third Party Compliance Review Sept 2025

Control Ref	Control Name	Control Description	Status	Evidence of Compliance	Related Documents/ Records
				• Sustainability/Climate change performance • Service improvement plan • AOB. The supplier provides telephony services to WV and it was observed in the meeting notes that all applicable topics from the standard agenda had been addressed during the review. The latest service review for Creditcall (dated 06/05/2025) which provides payment processing services to WV was also reviewed and observed to have included a discussion on supplier performance, capacity, and the supplier's service improvement plan. On a quarterly basis, the Compliance Officer conducts a supplier review to ensure that the relationship owners have been conducting appropriate supplier service reviews and that all the required evidence of supplier certifications is up to date. The Third Party Compliance Review for September 2025 (dated 30/09/2025) was examined and found to outline key details, including whether any new suppliers had been onboarded during the last quarter, overdue service reviews for critical suppliers, and outdated supplier certification evidence, e.g., expired ISO and waste carrier certifications. Evidence of the emails sent to relationship owners to resolve all the outstanding issues were also reviewed. During the quarterly Operations Review meetings, a review of supplier issues is conducted. As an example of this, these meetings are currently monitoring	

Control Ref	Control Name	Control Description	Status	Evidence of Compliance	Related Documents/ Records
				the ongoing issues with Royal Mail performance and the potential impact changes in their service levels may present to WV. Approved suppliers that have not been engaged for over 18 months are required to undergo the due diligence process again. This is also the case if the services provided by a supplier change or the supplier undergoes a significant organisational change such as being acquired by a larger company. It is the relationship owner's responsibility to inform the Compliance Team of these types of change in supplier relationships so that they can be appropriately managed.	
5.23	Information security for use of cloud services	Processes for acquisition, use, management and exit from cloud services should be established in accordance with the organisation's information security requirements.	Compliant	Cloud service suppliers are managed using the standard WV supplier management processes. When onboarding new suppliers, potential exit strategies (which are particularly important for cloud service suppliers) are reviewed and there is a supplier offboarding process flow to ensure that WV and client data is appropriately transferred or wiped.	
5.24	Information security incident management planning and preparation	The organisation should plan and prepare for managing information security incidents by defining, establishing, and communicating	Compliant	The Incident Reporting Escalation and Management Process (version 4.2, dated 28/03/2025) was reviewed and observed to detail the information security incident management procedure which is defined as covering all issues, weaknesses and nonconformities relating to WV information and information processing facilities	Incident Reporting Escalation and Management Process

Control Ref	Control Name	Control Description	Status	Evidence of Compliance	Related Documents/ Records
		information security incident management processes, roles, and responsibilities.		The Process is owned by the Head of Compliance and applies to all employees working for WV. Zendesk is used to document and track the progress of all incidents and tickets. All employees and clients have access to the Zendesk system so both internal and external tickets can be created. The Process documents key incident management responsibilities including: • **Incident Management Team** – This team is invoked for significant incidents that require a formal level of management. One of the Team's responsibilities is to determine whether the business continuity or disaster recovery processes need to be initiated • **Head of Compliance** – Responsible for overseeing the management of major incidents (unless the IMT is invoked), breaches of personal data and breaches of the GC Licence Conditions and Code of Practice (GC LCCP). The Head of Compliance is also responsible for overseeing the production of incident reports when these are requested either internally or by clients • **Assignee/Incident Manager** – Responsible for overseeing the management of a specific incident including assessing its impact. If an incident is categorised as a problem the assignee/incident manager is also responsible for adding details to the Issues Log in SharePoint. The assignee/incident manager role can be fulfilled by any employee who is senior enough to be able to effectively manage the issue. The Process also includes an incident severity matrix which has descriptions, examples and escalation and ownership requirements for the following categories of incident: • Incident • Managed incident	

Control Ref	Control Name	Control Description	Status	Evidence of Compliance	Related Documents/ Records
				• Major incident • Serious incident.	
5.25	Assessment and decision on information security events	The organisation should assess information security events and decide if they are to be categorized as information security incidents.	Compliant	Incident managers are responsible for assessing an incident and determining any required responses. Depending on the results of this assessment, the incident will be managed as either: • An incident which is a low impact issue or a near miss that can typically be managed and resolved utilising BAU processes and therefore does not need to be escalated beyond the assignee or team directly involved • A problem which is either: o An incident impacting the confidentiality, integrity or availability of data which may have a potential impact on client services, compliance, or service quality o A significant near miss which is an event which if it had not been detected could have caused a major impact. Managed incidents, major incidents, and serious incidents are all treated as problems as they will all require some level of senior management involvement. Problems are all documented in the Woods Valldata Issues Log which was reviewed and observed to contain the following information for each recorded problem: • Date • Owner • Issue type • Zendesk ticket number • Summary • Consequence	Woods Valldata Issues Log

Control Ref	Control Name	Control Description	Status	Evidence of Compliance	Related Documents/ Records
				• Outcome • Source (for example, client, third party etc.) • Corrective action type (for example, employee training, system enhancement etc.) • Data closed • Compliance Impact. The Issues Log is used to ensure that the Management Team has appropriate visibility of all problems and it is reviewed in management meetings to: • Determine whether there are trends or common factors associated with the problems being raised • Ensure that appropriate action have been taken to reduce the likelihood of a re-occurrence of the incident. An incident that has an information security impact can be identified in the Issues Log as it will have the 'Compliance Impact' field populated to specify that it impacts data protection, PCI DSS, or service availability etc.	
5.26	Response to information security incidents	Information security incidents should be responded to in accordance with the documented procedures.	Compliant	Incident managers are responsible for ensuring that all relevant information is obtained about the incident and that responses to help resolve the incident are completed in a timely manner. Some example incident tickets in Zendesk were reviewed to evidence how they were responded to: • Ticket 468602 related to a raffle data breach and was therefore classified as a problem and added to the Issues Log. The ticket detailed the investigation that was conducted and the steps taken to resolve the incident. This problem was reviewed at the monthly	Woods Valldata Issues Log Example Zendesk tickets [redacted] Incident Report

Control Ref	Control Name	Control Description	Status	Evidence of Compliance	Related Documents/ Records
				Operations Forum to ensure that it received appropriate management focus • Ticket 470806 – Created on 03/11/20205. This incident related to a fulfilment run failing with an error code. Although there are established processes for resolving this type of issue, it was raised as an incident as it had to be fully investigated. The ticket was observed to detail the investigation that had been conducted and that that it was raised at 9:45 and had been fully resolved by 14:20. The issue impacted internal teams but had no impact on clients or supporters. Incidents may also be raised for issues not caused by WV, but which are impacting it. An example discussed during the audit related to a client that was using a third party mailing service provider that had multiple issues which resulted in a large number of supporter calls to WV. WV also had to ensure that the issues did not impact the integrity of any of the draws which it was running. For serious incidents, WV may decide that there is business value in producing an internal incident report to provide a detailed analysis of the incident and its associated responses. There may also be situations when clients request this type of report as well. The Head of Compliance will usually be responsible for producing this report which will be based on the Client Facing Incident Report Template. An example incident report produced in February 2025 was reviewed. This related to incident 441110 which was a [redacted] issue where some supporters were not added to the draw. The report was observed to contain: • An incident summary	Incident Management and Business Continuity Plan

Control Ref	Control Name	Control Description	Status	Evidence of Compliance	Related Documents/ Records
				• The incident details • The investigation findings • Actions taken to address the nonconformity • Corrective actions • Details of who was notified. The quarterly key performance indicators (KPIs) delivered to the Senior Management Team include the number of problems and incidents raised for each department. Most departments have established thresholds for problem and incident volumes. When these thresholds are exceeded, an investigation must be conducted to identify whether the root cause stems from a process deficiency or a training gap, and to determine the appropriate resolution. The Incident Management and Business Continuity Plan (version 4.1, dated 20/10/2025) was reviewed and observed to include an action sheet for each department detailing how it should respond to a major incident. A recent example of when the Incident Management Team was required to invoke the Incident Management and Business Continuity Plan was on 05/03/2025. This was in response to a direct debit claim file missing its submission date for 3 clients. The associated incident ticket (ticket number 442759) was observed to include full details of what was discussed in each Plan meeting and the actions and decisions taken as well as details of how each client was managed.	

Control Ref	Control Name	Control Description	Status	Evidence of Compliance	Related Documents/ Records
5.28	Collection of evidence	The organisation should establish and implement procedures for the identification, collection, acquisition, and preservation of evidence related to information security events.	Compliant	To ensure the secure collection and subsequent management of evidence that may be required for legal or regulatory investigations, the Incident Management and Business Continuity Plan includes a Secure Evidence Process, and a Secure Evidence Form template for documenting the steps to be followed when physical or electronic evidence needs to be secured. The Process details: • How evidence must be securely collected and preserved • How the chain of custody must be managed and documented • How investigations of evidence must be conducted • That any analysis of evidence must utilise a copy and not the original evidence. The Process specifies that the individual securing the evidence must complete the Secure Evidence Form and anyone handling the evidence must sign for its receipt and document on the form when they received the evidence and from whom. The Process also specifies that third party forensic specialists need to be engaged if it is determined that there are not suitable in-house skills to securely manage and analyse the evidence. During the audit, the Head of Compliance confirmed that there has never been a requirement for WV to utilise the Secure Evidence Process.	Incident Management and Business Continuity Plan
5.35	Independent review of	The organisation's approach to managing information security	Compliant	WV is subject to an annual external PCI DSS audit in May and an annual external ISO 27001 audit in June. In the May 2025 PCI DSS audit, WV was	

Control Ref	Control Name	Control Description	Status	Evidence of Compliance	Related Documents/ Records
	information security	and its implementation including people, processes and technologies should be reviewed independently at planned intervals, or when significant changes occur.		required to be compliant to all applicable controls from the new PCI DSS version 4.0 for the first time. In February 2025, WV underwent an audit conducted by an organisation serving multiple WV clients. This audit was primarily finance-based but it did require some IT control evidence and evidence of the organisation's PCI DSS attestation. The Compliance Team has an internal audit schedule which covers ISO 27001 clauses and controls. The Compliance Team also performs monthly IT Compliance Reviews to verify that key IT processes and controls, such as daily system checks, vulnerability scanning, and the operation of the Web Application Firewall (WAF),are functioning effectively, and that IT teams are appropriately responding to security alerts. The Compliance Manager has an Information Assurance Schedule which includes details of what PCI DSS control evidence needs to be captured each month. During the audit, the types of issues these reviews identify were discussed and it was stated that they typically relate to gaps in record keeping. The Compliance Officer reviews the Approved Supplier List on a quarterly basis to ensure that all supplier management processes are operating effectively.	
6	**People Controls**				

Control Ref	Control Name	Control Description	Status	Evidence of Compliance	Related Documents/ Records
6.3	Information security awareness, education, and training	Personnel of the organisation and relevant interested parties should receive appropriate information security awareness, education and training and regular updates of the organisation's information security policy, topic-specific policies, and procedures, as relevant for their job function.	Compliant	All employees who have IT access are required to complete annual information security awareness training which is updated each year based on information security changes and issues that have occurred within WV and the wider environment. The training occurs in October and this year's training course was reviewed and observed to include information on: • Information and information processing facilities • Confidentiality, integrity, and availability • Policies and processes • Physical security • Secure areas • Managing visitors, contractors, and agency employees • Information classification • Document management and control • Clear working spacers • Keeping information secure • Password security • MFA • Email, internet and system use • Phishing and malicious code • Social networks • Mobile device and remote working • Incident management. Once the relevant employees have completed the course, they are required to undertake a test of understanding which is updated each year and has a required pass mark of 80%. The Information Security 2025/26 test was reviewed and observed to contain a range of multiple choice questions and a	Information Security Awareness Training Presentation Information Security 2025/26 Test Non-IT Access Staff Annual Compliance Briefing

Control Ref	Control Name	Control Description	Status	Evidence of Compliance	Related Documents/ Records
				requirement for employees to formally acknowledge that they have been given information security awareness training. The Compliance Team receives all test results and employees are required to retake the test until they achieve the pass mark. If the Compliance Team identifies that there may be an issue with an employee's understanding of a particular area, it is discussed with the employee's line manager and any required remediation actions identified. Employees without IT access are given an annual compliance briefing. The Non-IT Access Staff Annual Compliance Briefing document (version 1.2, dated 26/10/2025) was reviewed to evidence this. These employees are required to sign a formal acknowledgment that they have received this briefing. Starters in the organisation are required to complete an 'Introduction to Compliance' course as well as complete either the security awareness training or read the compliance briefing as part of their employee induction. Depending on role, some employees are required to complete additional annual training. For example, employees who handle personal data are required to complete data protection training. Additionally, applicable employees must undertake training related to the Gambling Act and PCI DSS requirements. Each of these courses has an associated test of understanding which has a required 80% pass mark. This training is distributed across the year (for example, PCI DSS training occurs in April and Gambling Act training occurs in July or August). The [redacted] platform is used to carry out monthly phishing simulations, including one exercise for all employees and a targeted exercise for a specific subset of staff. As an example of this, in May 2025, there was a generic	

Control Ref	Control Name	Control Description	Status	Evidence of Compliance	Related Documents/ Records
				exercise that went to all employees and a Barclays Bank-based exercise that went to the Finance Team and the Senior Leadership Team. The [redacted] phishing dashboards were reviewed and found to provide a detailed breakdown for each exercise, including the number of employees who opened the phishing email, clicked on the embedded link, and entered sensitive information such as usernames and passwords. If an employee clicks on the phishing link they are taken to a screen which explains that it is a phishing simulation and how they should have identified this. If an employee clicks on an exercise link more than once during a campaign, they are required to retake their information security awareness training. During Cyber Security Awareness Month (October 2025), the Compliance Team ensured that employees were aware of this initiative and also published WV specific information on the month's 4 core recommended actions: • Software updates – The best practice that WV employees should be following • Passwords and MFA - The best practice that WV employees should be following and information on how WV has been rolling out a wider implementation of MFA over the last 3 to 4 months • Phishing - How employees should be recognising and reporting phishing attempts. WV utilises the [redacted] Human Vulnerability Assessment Tool to determine the organisation's current information security awareness maturity compared to other organisations and to help identify any areas of awareness weakness that it needs to improve.	

Control Ref	Control Name	Control Description	Status	Evidence of Compliance	Related Documents/ Records
				During the site tour, it was noted that there were a variety of information security awareness posters displayed throughout the site.	
6.5	Responsibilities after termination or change of employment	Information security responsibilities and duties that remain valid after termination or change of employment should be defined, enforced, and communicated to relevant personnel and other interested parties.	Compliant	All new permanent and fixed term employees are required to formally sign and date a WV contract before they start their employment. The People and Culture Team retains scanned copies of these contracts (which are also signed by the Head of People and Culture) in a secure, restricted access SharePoint directory. The Terms and Conditions of Employment Template (dated October 2025) was reviewed and observed to contain highlighted sections that are included or excluded based on the employment type of the new hire (e.g., permanent, fixed-term). The Template was observed to include clauses that related to confidentiality, data protection, place of work, disciplinary policy and procedure, grievance policy and procedure, conflicts of interest, secondary employment and intellectual property. Specific details observed for these clauses included: • The data protection clause relates to the organisation's use of employee data and specified that this is kept for 6 years after employment is terminated • The intellectual property clause primarily relates to the organisation's ownership of intellectual property created by the employee during their employment • The confidentiality clause states that its requirements remain in place for 12 months after employment terminates. The Terms and Conditions of Employment Template also has an appendix containing a set of restrictive covenants including that employees cannot work for a set of restricted businesses for 6 months after they leave WV.	Terms and Conditions of Employment Template Resignation Acknowledgement Letter Template

Control Ref	Control Name	Control Description	Status	Evidence of Compliance	Related Documents/ Records
				During the audit, the Head of People and Culture detailed how the Terms and Conditions of Employment are currently being formally reviewed by the organisation in preparation for them being updated. When an employee leaves WV, the People and Culture Team provides them with a formal resignation acknowledgement letter. The Resignation Acknowledgement Letter Template (dated October 2024) was reviewed and observed to contain a reminder that the employee is bound by all relevant contractual clauses during and after employment. Leaving employees are also reminded of their post-termination contractual responsibilities during their exit interview with the People and Culture Team.	
6.7	Remote working	Security measures should be implemented when personnel are working remotely to protect information accessed, processed, or stored outside the organisation's premises.	Compliant	Although it is not formally documented in employee contracts, WV operates a hybrid working policy whereby all employees who have a laptop and have a role that allows for effective remote working can work from home. However, the organisation requires all employees to be at the office a minimum of 3 days per week unless an approved alternative arrangement has been formally agreed. Employees are also expected to obtain approval from their line manager if they need to work from a remote location other than their home address. Employees are not provided with any WV-issued remote working equipment other than their role-requirement laptop and mobile phone. All employees who work remotely are required to complete a Display Screen Equipment (DSE) assessment for their home environment.	Mobile Device and Remote Working Policy

Control Ref	Control Name	Control Description	Status	Evidence of Compliance	Related Documents/ Records
				The Mobile Device and Remote Working Policy specifies the security measures that employees are required to follow when working outside of the office including working securely in public places and ensuring corporate assets such as laptops are secured when travelling and working remotely. It also requires employees to minimise the amount of confidential information in paper format or on removable media that they transport to and from the office. All remote access to the WV network is secured with MFA.	
6.8	Information security event reporting	The organisation should provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.	Compliant	The Acceptable Use Policy was reviewed and observed to state that all employees must report any security issues or weaknesses that they identify at the earliest opportunity to either their line manager or another available manager. Employees can also email the Zendesk system which then creates an associated incident ticket.	Acceptable Use Policy
7	**Physical Controls**				
7.8	Equipment siting and protection	Equipment should be sited securely and protected.	Compliant	WV maintains a Computer Room located on the first floor of Lansdowne House. Access to this room is secured by a WV access card operated lock and only the IT Infrastructure Team, the Facilities Team and the designated emergency key holders have authorised access.	Site Rules and Confidentiality Agreement Visitors Log 2025

Control Ref	Control Name	Control Description	Status	Evidence of Compliance	Related Documents/ Records
				The Computer Room was visited during the audit, and it was observed that there were 7 cabinets containing server infrastructure, network devices and the door access and UPS systems. All cabinets were locked and all cabinets, infrastructure and the associated cabling were observed to be appropriately labelled. Cabinets and cabling were observed to be easily accessible, and all cabling appeared to be in good condition and was well organised with overhead cable trays being utilised to feed cables to the cabinets. The Computer Room has an air conditioning system consisting of 3 units. Power supplies to the IT equipment and the air-conditioning units are protected by a UPS system which is automatically tested on a weekly basis. Any issues with this system cause an alert to be raised for the Infrastructure Team to investigate. For additional power supply protection, there is an on-site diesel generator that can provide protection in the event of a full power outage. The generator is regularly tested to ensure it is operating effectively. It was observed that the Computer Room is used as a secure storage location for spare IT equipment and hard drives awaiting secure disposal. This equipment was all tidily stored on shelving and did not hinder access to any of the IT cabinets.	Physical and Environmental Security Policy (version 2.5, dated 24/04/2025)

Control Ref	Control Name	Control Description	Status	Evidence of Compliance	Related Documents/ Records
				There is a locked network cabinet in the Mailroom which contains network switches and a dedicated UPS. The key to this cabinet is stored in the Computer Room and the mailroom is a secure area with restricted access. As part of its daily checks, the IT Infrastructure Team inspects both the Computer Room and the network cabinet to ensure they are operating effectively and have no issues. The physical security of Lansdowne House was reviewed during a site tour. All secure areas such as the post room, banking room and supporter services room were observed to be protected by doors with electronic ID card-operated locks and were monitored by CCTV cameras. Only employees with a role-based justification have access to these secure areas. Visitors are required to be chaperoned by an employee at all times and have to sign in and out when visiting the secure areas of the building. The main building entrance has a manned reception desk and there is a formal visitor management process which includes ensuring that all visitors are issued with a visitor lanyard that must be worn at all times and sign a Site Rules and Confidentiality Agreement (version 6.0, dated 01/09/2025) confirming that they understand all relevant onsite behaviour, safety, and security requirements. The Visitors Log 2025 spreadsheet managed by the Facilities Team was reviewed and observed to contain details on all visitors including when they arrived and left the site, their host, and their reason for visiting the site. Employees are required to notify the Facilities Team in advance of any visitors.	

Control Ref	Control Name	Control Description	Status	Evidence of Compliance	Related Documents/ Records
				To confirm adherence to this requirement, the Compliance Manager's notification regarding the auditor's two-day visit was reviewed It was observed that the Reception Desk had a console showing output from all the site's CCTV cameras. The Physical and Environmental Security Policy (version 2.5, dated 24/04/2025) was reviewed and observed to detail WV requirements for managing physical and environmental security. During the audit, the management of Lansdowne House was observed to be compliant to all of these requirements.	
7.10	Storage Media	Storage media should be managed through their life cycle of acquisition, use, transportation, and disposal in accordance with the organisation's classification scheme and handling requirements.	Compliant	WV uses a [redacted] End Point Protection system ([redacted]) Policy to prevent the use of removable media on WV end user devices. There are a small number of permanent role-based exceptions to this Policy which are linked to specific devices in [redacted]. The Asset Register was reviewed and it was observed that each asset that was enabled to use removable media was marked as such. The Infrastructure Team is also able to provide temporary rights to use removable media if an employee has an appropriate justification. Reasons for using removable media were discussed during the audit and it was stated that accessing data provided by clients was one of the most frequent. WV does not manage a stock of corporate removable media devices. The [redacted] system provides reports which detail all use of removable media and a Zendesk alert is raised for end-users who make repeated	Asset Register

Control Ref	Control Name	Control Description	Status	Evidence of Compliance	Related Documents/ Records
				unsuccessful attempts to use removable media. The Infrastructure Team will investigate these alerts to understand why these attempts are being made. See Control A.7.14 for details on how storage media is securely destroyed.	
7.14	Secure disposal or re-use of equipment	Items of equipment containing storage media should be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	Compliant	Laptops returned by employees are wiped as soon as possible and securely stored in a locked IT cupboard for either reallocation or destruction. In some circumstances (for example when a senior employee leaves) there is a requirement to delay wiping the device as it may contain retrievable information or retain access to specific systems. In these cases, the device is securely stored until the Infrastructure Team receives confirmation that it can be wiped. If the Infrastructure Team determines that a returned laptop cannot be reallocated, it is marked for disposal, and the hard drive is removed and securely stored in the Computer Room. These hard drives are stored until there is enough equipment to warrant engaging a third party to securely dispose of it. At the time of the audit, no secure disposal of hard drives had taken place for the past year. However, a Zendesk ticket had been raised to initiate disposal, as a sufficient number of hard drives had been marked for destruction to warrant the process. Laptops marked for disposal (minus their hard drive) are collected by a specialist third party for recycling.	
8	**Technical Controls**				

Control Ref	Control Name	Control Description	Status	Evidence of Compliance	Related Documents/ Records
8.1	User endpoint devices	Information stored on, processed by or accessible via user endpoint devices should be protected.	Compliant	The Infrastructure Team is responsible for managing the WV endpoint device estate. The Team maintains an Asset Register of all user endpoint devices which was reviewed and observed to contains details of each device's: • Asset ID (all devices have an asset tag) • Model • Status • Allocated team • Allocated employee. The laptop allocated to [redacted] was inspected and the asset record in the Asset Register reviewed to confirm that they matched. Also the record for a Dell Optiplex 3050 PC due for decommissioning was reviewed against the actual asset to confirm that it was accurate. The WV user endpoint device estate contains a range of Windows devices of different ages which has meant that over the last 12 months there has been a requirement to replace a number of Windows 10 devices with Windows 11 models. Also, some employees have a role requirement for higher specification machines such as the Development Team which requires laptops with more powerful processors than other employees. The estate also contains a small number of Macbooks. All devices have the same basic build and the Infrastructure Team stores a set of standard builds in a secure SharePoint directory. All PCs and laptops (including Macbooks) have a [redacted] agent installed which allows the Infrastructure Team to manage Windows updates, software updates, and machine patching centrally. The [redacted] dashboard was reviewed to evidence the information on user	IT Security Policy. Asset Register

Control Ref	Control Name	Control Description	Status	Evidence of Compliance	Related Documents/ Records
				endpoint device operating system versions and patching status available to the Infrastructure Team. It was noted that the dashboard included details on which devices currently require restarting to enable a patch to be deployed. If required, the Team is able to force a device restart centrally to ensure all patches are fully deployed. As employees do not have local admin rights on their endpoint devices, the Infrastructure Team can utilise [redacted] to remotely log in to complete tasks that require administrator rights. The Infrastructure Team utilises [redacted] which has laptop information that is updated in real time and can be used to identify if any new devices have joined the WV network. The [redacted] console was reviewed to evidence this. The Infrastructure Team stores spare laptops in a locked cabinet near to its allocated desk area. The key to this cabinet is stored in a lockable drawer. During the audit, this cabinet was inspected and observed to contain a small number of laptops ready for reallocation. When an employee joins WV, the HR Team or the starter's line manager will specify in the SharePoint New Starter Request Form whether the new employee requires IT access, a laptop, and a mobile phone. Once this request has been approved by the HR Team, if IT access is required a Zendesk ticket is automatically created and allocated to the Infrastructure Team. On the new employee's first day, the Infrastructure Team provides them with their required devices and assists them in logging in for the first time and setting up MFA.	

Control Ref	Control Name	Control Description	Status	Evidence of Compliance	Related Documents/ Records
				When an employee leaves the organisation, they hand their allocated laptop and mobile phone to their line manager or the HR Team who return it to the Infrastructure Team. The Infrastructure Team then updates the devices' status in the Asset Register and locks the devices in its cabinet. Typically, devices are wiped and rebuilt immediately upon an employee's departure. However, depending on the leaver's role, the laptop may need to be securely stored for a period of time to allow the line manager to retrieve any necessary information before the device is wiped. During this time, the laptop is marked in the Asset Register as formerly belonging to the leaver. Once it has been wiped it is then marked as being ready for reallocation or if it has reached end of life and needs to be securely disposed of. The Infrastructure Team maintains a separate register of corporate mobile phones which includes details of the model, phone number, and the employee it is allocated to. The IT Security Policy was reviewed and observed to include an 'IT Asset Management' section that details requirements for managing IT asset inventories and IT asset secure disposal. The Infrastructure Team's processes were all evidenced to be compliant with these requirements.	
8.2	Privileged access rights	The allocation and use of privileged access rights should be restricted and managed.	Compliant	The Role-Based Profile Matrix outlines the privileged access requirements associated with each role. Any additional privileged access granted to specific employees beyond their role-based entitlements is recorded as an exception. Privileged access rights are managed via the standard joiners, movers, and leavers processes.	Role-Based Profile Matrix

Control Ref	Control Name	Control Description	Status	Evidence of Compliance	Related Documents/ Records
				There are a small number of employees who require administration access to systems. This was evidenced in the Role-Based Profile Matrix where it is documented that only the Technical Architect, the IT Tech Ops Team and the IT Infrastructure Team have administration rights to network and IT systems. The Matrix also shows that the Compliance Manager has administration access to SharePoint. Developers have administration access to their own development environment. Employees with administration access to the network have separate administration and standard accounts, the former only being used for activities that specifically require privileged access and the latter for all other activities. This was confirmed by an Infrastructure Support Engineer who has both types of account. Only the 2 members of the Infrastructure Team have domain administration privileges. There is no business requirement to temporarily allocate privileged access rights to employees.	
8.3	Information access restriction	Access to information and other associated assets should be restricted in accordance with the established topic-specific policy on access control.	Compliant	Each role's standard information access requirements are documented in the Role-Based Profile Matrix. Access to shared SharePoint directories is documented in the Role-Based Profile Matrix 'WV Network Security' tab which lists each shared directory and its associated owners and members. Access to these directories is managed via the use of AD security groups.	Role-Based Profile Matrix

Control Ref	Control Name	Control Description	Status	Evidence of Compliance	Related Documents/ Records
				Wherever possible and applicable, systems are configured to include accounts with varied levels of privileges (for example, standard and admin) to facilitate appropriate information access restrictions in line with WV policies.	
8.5	Secure authentication	Secure authentication technologies and procedures should be implemented based on information access restrictions and the topic-specific policy on access control.	Compliant	The Acceptable Use Policy was reviewed and observed to include a 'Passwords' section which details how employees should securely manage their WV authentication information. It also specifies the minimum complexity requirements for all passwords and that: • Passwords must expire after 90 days • A password must not be the same as any of the previous 24 passwords used • Accounts will lock after 5 failed access attempts. The Acceptable Use Policy was also observed to include an 'MFA' section which specifies the following requirements: • Remote access to WV systems must use MFA as an additional authentication mechanism • MFA is mandatory when accessing systems within the Cardholder Data Environment (CDE), whether directly or via a remote desktop from within the network. Additionally, remote access to the CDE via VPN is explicitly prohibited. • Where supported MFA must be enforced across all cloud services. These requirements are in line with the changes to MFA implementation that WV has been deploying over the last 12 months.	Acceptable Use Policy

Control Ref	Control Name	Control Description	Status	Evidence of Compliance	Related Documents/ Records
				Discussions with the Infrastructure Support Engineer confirmed that remote access to the WV network requires MFA and that employees have to be a member of a specific AD group. A [redacted] VPN is utilised for all remote access connectivity. [redacted] is utilised to provide MFA for access to secure systems and infrastructure such as the CDE. The Duo portal was reviewed to evidence this. During the audit, the Infrastructure Support Engineer demonstrated that MFA is required when accessing the [redacted] portal.	
8.7	Protection against malware	Protection against malware should be implemented and supported by appropriate user awareness.	Compliant	A [redacted] agent is installed on all user endpoint devices including Macbooks and all Windows servers. It is a cloud-based service which continually scans all devices and any installed removable media for malware. The system is configured to automatically update its system software and virus definition files and these updates are provisioned via the internet so user endpoint devices do not need to be connected to a WV VPN to receive them. End users have minimum visibility of the system on their devices (it runs silently in the background with no user interface or icons and is not present on the device's taskbar) and they cannot disable the system or re-configure it. The [redacted] system is used to provide a monthly report of any devices that do not have [redacted] installed. The latest Systems Without [redacted] Report (dated 04/11/2025) was reviewed and observed to contain no entries.	Systems Without [redacted] Report

Control Ref	Control Name	Control Description	Status	Evidence of Compliance	Related Documents/ Records
				The Infrastructure Support Engineer was observed logging into the [redacted] console, which requires MFA. Dashboards displaying details of all devices with [redacted] installed were reviewed as part of the assessment. The most recent alert raised by the system was also reviewed. This alert was dated 24/10/2025 and was a false positive as it related to work that the Infrastructure Support Engineer was conducting. During the audit, the Infrastructure Support Engineer confirmed that the organisation has few issues with malware and there have been no recent alerts that have required the Team to proactively respond to a virus infection.	
8.13	Information backup	Backup copies of information, software and systems should be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.	Compliant	[redacted] is utilised to manage all WV backups. There are 2 onsite [redacted] servers which store backup files for a specified time period before they are transferred to Azure cloud storage. [redacted] backup schedules have been implemented based on infrastructure type and business requirements. For example, core production servers are backed up daily and jump boxes and test servers are backed up weekly. [redacted] produces a daily backup report detailing the status of all backup schedules. This report is delivered to the IT mailbox and is also saved in SharePoint. An example [redacted] Backup report for 05/11/2025 was reviewed to evidence this. Each backup job also produces an email notification detailing its status and examples of these emails in the IT mailbox were observed. If a specific backup job fails, the system attempts to re-run it a specified number of times (which is configurable in the [redacted] system). If none of these re-runs are successful the Infrastructure Team can either re-run the job	IT Security Policy Infrastructure Daily Check Sheet [redacted] Backup Report

Control Ref	Control Name	Control Description	Status	Evidence of Compliance	Related Documents/ Records
				manually immediately or if required, investigate and resolve the root cause of the issue before attempting a re-run. [redacted] is utilised to validate each backup on a regular basis. The system does this by using each backup to initiate a virtual machine (VM) and boot it to a Windows login screen where all required processes are then checked to be active. The IT Infrastructure Team has a set of daily checks that it conducts. The IT Infrastructure Daily Check Sheet for 05/11/2025 was reviewed and observed to have tasks to check the daily [redacted] backup, cloud backup and [redacted] reports for any failures. For any backup failures, the Check Sheet has a comment on the nature of the failure and any actions taken. The Infrastructure Support Engineer confirmed that systems and data do not need to be restored from backup very frequently and that one of the reasons for this is that the file servers have functionality that enables deleted files to be directly restored for a period of 7 days after their deletion. The IT Security Policy was reviewed and observed to specify a set of backup requirements including: • Ensuring integrity and availability of information assets in alignment with documented business needs • Utilising both cloud-based and on-site backups to safeguard data • Regular testing of backup recovery procedures to validate effectiveness • Implementing backup mechanisms that support timely system and data recovery in accordance with business requirements	

Control Ref	Control Name	Control Description	Status	Evidence of Compliance	Related Documents/ Records
				All backup processes examined during the audit were confirmed to be fully compliant with these policy provisions.	
8.15	Logging	Logs that record activities, exceptions, faults, and other relevant events should be produced, stored, protected, and analysed.	Compliant	The [redacted] is utilised for log collection and analysis. Logs are collected from all servers, network devices and user endpoint devices on a continual, real time basis and these logs are stored for 12 months. The Log Analyzer alert dashboard was reviewed and a sample of recent alerts were all observed to included details of the event type, date, time, source, and outcome. Alerts related to the PCI DSS in-scope infrastructure have associated Zendesk tickets automatically raised. An example ticket (number 470990) related to a file integrity monitoring alert was reviewed to evidence this. The Infrastructure Team conducts a daily review of [redacted] alerts to identify any that require investigation or mitigating actions. Access to the logs stored in [redacted] is limited to employees with a role-based justification.	Example Zendesk tickets
8.17	Clock synchronization	The clocks of information processing systems used by the organisation should be	Compliant	Network Time Protocol (NTP) is used to obtain a standard time from an internet-based time source, and this is synchronised with the WV network domain controllers which are then used to synchronise the time on all network infrastructure and user endpoint devices.	

Control Ref	Control Name	Control Description	Status	Evidence of Compliance	Related Documents/ Records
		synchronized to approved time sources.		AD is utilised to manage clock synchronisation across the network and only the Infrastructure Team has access to the AD Group Policies to be able to re-configure this.	
8.18	Use of privileged utility programs	The use of utility programs that can be capable of overriding system and application controls should be restricted and tightly controlled.	Compliant	Within WV, there is no use of privileged utility programs by employees without administrator privileges which means that these users are not able to override access controls to gain enhanced access rights. In addition to this, end users do not have local admin rights on their corporate devices so are not able to install unapproved applications or programs themselves.	
8.20	Networks security	Networks and network devices should be secured, managed, and controlled to protect information in systems and applications.	Compliant	The WV Network Diagram document (dated October 2024) was reviewed and observed to be owned by the CTO and to include details of the WV network's physical topology, logical topology, the CDE in-scope network and the CDE out of scope network. The physical topology diagram was reviewed and observed to contain details of the network's firewalls and switches and how these are connected. The logical topology diagram was reviewed and observed to contain details of the VLAN structure which consists of: • PCI in-scope CDE • PCI in-scope non-CDE • Out of scope • Development and test systems • PCI in-scope management.	Network Diagram

Control Ref	Control Name	Control Description	Status	Evidence of Compliance	Related Documents/ Records
				The Compliance Manager maintains a cardholder dataflow diagram. The WV network is composed of two segments: the green network, which serves as the strategic core infrastructure, and the blue network, which contains only legacy domain controllers. These legacy components are maintained to ensure that the external communications they facilitate continue to function reliably.. The plan is to eventually decommission these remaining blue domain controllers. The network is secured by a pair of [redacted] firewalls which are fully synchronised and act as a redundant pair. The firewalls are under change control and the rulesets are fairly static. Only the Infrastructure Team is able to update the firewall rules each of which is required to have a documented justification. In line with PCI DSS requirements, there is a 6-monthly firewall rule review to ensure that all rules are still valid and that they are correctly configured. The network includes a DMZ positioned between the firewalls and the switches. WV is transitioning to using Azure Front Door as the external interface for users, as this provides additional website security and helps to simplify internal network management. WV websites are protected by a [redacted] WAF.	
8.21	Security of network services	Security mechanisms, service levels and service requirements of network services	Compliant	In line with PCI DSS requirements, monthly internal and external vulnerability scans are conducted. Nessus is utilised for the internal scans and [redacted] for the external scans. Any critical or high vulnerabilities identified in the PCI DSS in-scope network are patched within 30 days. All	Example Zendesk tickets

Control Ref	Control Name	Control Description	Status	Evidence of Compliance	Related Documents/ Records
		should be identified, implemented, and monitored.		other identified vulnerabilities are also targeted to be patched within 30 days but these are prioritised on a risk basis so may be outstanding for longer periods. All activity related to vulnerability mitigation and patching is managed via Zendesk tickets with a ticket being produced for each completed scan. Example Zendesk tickets for the scans completed in September 2025 were reviewed to evidence this. These tickets remain open until all critical and high vulnerabilities associated with the scan have been resolved. The Nessus console was reviewed and observed to group vulnerabilities by VLAN.	
8.22	Segregation of networks	Groups of information services, users and information systems should be segregated in the organisation's networks.	Compliant	The logical topology diagram details how the network is segregated into VLANs, structured according to business and security needs (see Control 8.20). Regular segmentation penetration testing is conducted to ensure that the VLANs are all appropriately secured. The CDE is securely isolated from the rest of the internal network, in compliance with PCI DSS requirements.	Network Diagram
8.24	Use of cryptography	Rules for the effective use of cryptography, including cryptographic key management, should	Compliant	The Development and Testing Policy (version3.2, dated 29/04/2025) and the IT Security Policy both have sections detailing how cryptography is applied across the WV network and application estate. As part of the standard configuration for all WV laptops, BitLocker is utilised for hard drive encryption.	Development and Testing Policy IT Security Policy

Control Ref	Control Name	Control Description	Status	Evidence of Compliance	Related Documents/ Records
		be defined, and implemented.		All remote connections to the WV network must be established through the [redacted] VPN, which is configured using standard IPsec encryption protocols. All servers in the CDE are encrypted in line with PCI DSS requirements. WV encourages clients to utilise its dedicated portal for the import and export of client system data as it has strong levels of security and encryption implemented. If clients choose alternative methods, WV ensures that the solution employed meets their specified compliance requirements. The Infrastructure Team is responsible for the management of all SSL certificates for client-facing websites. The Software SSL and Domain Inventory document was reviewed and observed to include a list of all WV domains and SSL certificates. Listed information for each certificate was observed to include: • Domain name • Domain expiry date • The third-party SSL certificate authority. • Hosting provider • SSL certificate expiry date. The inventory is reviewed monthly by the Infrastructure Team to identify any SSL certificates due for renewal. Discussions during the audit, highlighted that the transition to Azure Front Door will mean that fewer SSL certificates will need to be managed internally by the Infrastructure Team.	Software SSL and Domain Inventory

Control Ref	Control Name	Control Description	Status	Evidence of Compliance	Related Documents/ Records
8.25	Secure development life cycle	Rules for the secure development of software and systems should be established and applied.	Compliant	The Development and Testing Policy was reviewed and observed to detail the principles that should be followed when developing and testing software for WV internal or WV client use to ensure that risks related to insecure programming are minimised. The Policy details a set of requirements related to: • Architecture and design • Documentation • Secure coding • Peer review • Testing. It was noted that the Policy has been updated in the last 12 months to mandate that: • All new applications that require a clients to sign in must be protected behind Azure B2C and all cloud-hosted applications must utilise MFA • Content security policies (CSP) and integrity checking must be utilised to securely lockdown JavaScript and the iframes used in PCI DSS in-scope websites • External websites must be routed via Azure Front Door to ensure that they are protected by a WAF and CSP • All websites that are in scope of PCI must have daily tampering checks implemented. These new requirements were discussed with the Technical Architect who detailed how they had been implemented into the WV estate and embedded in the development lifecycle.	Development and Testing Policy Development and Testing Process Coding Standards and Code Review Guidelines

Control Ref	Control Name	Control Description	Status	Evidence of Compliance	Related Documents/ Records
				The Development and Testing Process (version 3.3, dated 25/04/2024) was reviewed and observed to include a development and testing process flow detailing the process responsibilities of: • Requestor • IT Logistics Manager • Development • IT Architect/Senior Developer • Affected/interested parties. The Coding Standards and Code Review Guidelines (version 2.2, dated 29/04/2025) were reviewed and observed to detail how: • Code should be formatted and labelled • Comments should be utilised • The logging framework should be applied • The .NET standards should be implemented. The code review guidelines in the document detail how the OWASP top 10 security risks should be mitigated. The Technical Architect confirmed that the development lifecycle is utilised for all internally and client raised changes, production bugs, and infrastructure changes.	
8.26	Application security requirements	Information security requirements should be identified, specified, and approved when	Compliant	All proposed changes (apart from service requests, see Control 8.32) are assessed at a number of stages during the development lifecycle. Once a change has been formally documented as a Request For Change (RFC) and has been entered as a Product Backlog Item (PBI), the Development Team	

Control Ref	Control Name	Control Description	Status	Evidence of Compliance	Related Documents/ Records
		developing or acquiring applications.		utilises the information in the RFC to conduct an estimation of effort for the change. This estimation is based on a checklist of 'True/False' questions designed to assess whether the proposed change will: • Impact multiple clients • Impact PCI DSS compliance • Impact GDPR compliance • Affect existing games • Involve an externally-sourced data feed • Impact Gambling Commission reporting • Potentially impact application security • Potentially impact data security. The RFC and the estimation output are then reviewed in the weekly ICT Meeting to determine whether there are additional requirements (including security requirements) that need to be included in the change. The ICT Meeting is attended by the Chief Technology Officer, Technical Architect, change owners and the Head of Compliance (who is able to provide compliance and security specific input). Changes are also assessed to ensure that they meet all WV information security policy requirements such as those relating to access management, encryption and network security. When projects are implemented to deliver new applications or significant new functionality, senior management including the Head of Compliance will be involved in defining business and security requirements.	

Control Ref	Control Name	Control Description	Status	Evidence of Compliance	Related Documents/ Records
				Once deployed to production, applications are subjected to periodic internal and external vulnerability scanning and penetration testing to ensure that all WV and client security requirements are being met on an ongoing basis.	
8.27	Secure system architecture and engineering principles	Principles for engineering secure systems should be established, documented, maintained, and applied to any information system development activities.	Compliant	The Development and Testing Policy includes a set of detailed secure system engineering principles covering areas such as: • JavaScript • Iframes • Azure Front Door hosting • Authentication • Session management • Authorisation • Input data validation • Data encoding • Client security • Error handling/logging • System hardening • Cryptography. During the development lifecycle checkpoints and in the ICT Meetings, there are multiple reviews to ensure that these principles are being followed.	
8.29	Security testing in development and acceptance	Security testing processes should be defined and implemented in the development life cycle.	Compliant	The ICT Meeting is responsible for reviewing whether proposed changes will have a security impact and ensuring that significant changes have undergone all required security testing. The peer reviewing of code is required to ensure that all new code is secure and is compliant to WV coding standards.	

Control Ref	Control Name	Control Description	Status	Evidence of Compliance	Related Documents/ Records
				Dependant on the type of change being tested, the Test Team will ensure that testing against relevant OWASP requirements is completed and that vulnerability scans are conducted on the new code. The Compliance Manager will ensure that all compliance requirements have been considered and that the business analysts and development team have fully considered all aspects of the end-to-end business processes. All newly developed code is scanned to detect any dependent components that may contain vulnerabilities requiring remediation..	
8.30	Outsourced development	The organisation should direct, monitor and review the activities related to outsourced system development.	Compliant	Currently, WV does not outsource any development to third parties. If contractors were to be employed for specialist development work, they would be provided with access to the WV development environment and use the same processes and tools as WV employees. This would mean that they would be subject to the same information security policies, processes, and controls as the internal Development Team.	
8.31	Separation of development, test, and production environments	Development, testing and production environments should be separated and secured.	Compliant	Production and non-production systems are segmented into separate VLANs, which was evidenced through discussion with the Infrastructure Team and viewing the WV network diagram. Developers conduct all coding activities on their local laptop environments and source code resides in Microsoft Azure Git repositories which only the Development Team has access to.	Network Diagram

Control Ref	Control Name	Control Description	Status	Evidence of Compliance	Related Documents/ Records
				The deployment of code to production environments is controlled with a number of checkpoints to ensure that all code is appropriately reviewed, tested, and approved before deployment.	
8.32	Change management	Changes to information processing facilities and information systems should be subject to change management procedures.	Compliant	WV follows an Agile approach for system development with changes being grouped into fortnightly sprints. Microsoft Azure DevOps (DevOps) is utilised for requirement management and change control within the development lifecycle. This system has been configured with a set of company-wide policies to govern the change process. These policies include: • Requiring all changes to be linked to a PBI • Mandating peer review for all changes • Prohibiting employees from approving their own changes for release. Code deployment is, currently, a mix of manual and automated Continuous Integration and Continuous Delivery/Deployment (CI/CD) processes Most changes are requested by clients who are able to raise these via their account manager or directly in Zendesk. If the change involves a service request, such as a client requesting a data extract or an update to database records, it is typically added directly to the product backlog. However, if the change relates to functionality, an account manager or business analyst (depending on the complexity) is assigned as the change owner and is responsible for documenting it as a formal Request for Change (RFC). An example RFC (number 38603) was reviewed and observed to relate to a change in sortation of items. Information documented on this RFC was observed to include:	Example Request For Change Release Approval Checklist

Control Ref	Control Name	Control Description	Status	Evidence of Compliance	Related Documents/ Records
				• Requestor • RFC title • Change summary • Reason for change • Systems impacted by the change • Business areas impacted by the change • Whether a Data Protection Impact Assessment (DPIA) is required • Acceptance criteria for the change. This RFC also had a file attached showing the required file structure for the change. Once the RFC is complete, a PBI is created in DevOps and the Development Team completes an estimation of the change's impact (see Control 8.26). This estimation and the RFC are reviewed in the weekly ICT Meeting to determine whether the change has all required details, is cost effective and is in line with business strategy. If the change is not approved, the RFC or estimation may be revisited or more detail on the required change obtained from the client. If the meeting approves the change and it has been requested by a client, the change owner is responsible for producing a change quote that is delivered to the client. If the client rejects the quote, the request is deleted from the product backlog. Approved RFCs are reviewed in the fortnightly prioritisation meeting that is managed by the Scrum Master and attended by the business analysts and change owners. This meeting is responsible for scheduling the change into a fortnightly sprint. There are separate BAU (RFC) and project workstreams but their PBIs follow the same process. Most RFCs are managed as a PBI	

Control Ref	Control Name	Control Description	Status	Evidence of Compliance	Related Documents/ Records
				containing a single task but if required they can be broken into multiple tasks. RFCs are usually allocated to a single sprint whereas projects may be allocated across multiple sprints. Once the change has been allocated to a sprint, its associated RFC is updated with the relevant sprint number and the change is allocated to a specific developer. The DevOps system is used to manage the code lifecycle. During the audit, the Technical Architect walked through the system, showing the stages each PBI progresses through. Each change has its own branch from the master in the GitHub code repository and when a developer creates a code branch they are required to associate it with the relevant PBI number so that there is an appropriate level of traceability. Code development is conducted on the allocated developer's local laptop environment and once this has been completed and the developer has unit tested the change appropriately, it is marked for peer review. There is a Coding Standards Checklist to help ensure that peer reviews are conducted consistently and they are managed in DevOps which enables a full audit trail of all peer review feedback to be maintained. During the audit, example peer reviews in DevOps were reviewed and observed to contain a side-by-side comparison of the old and new code and a set of feedback associated with specific areas of highlighted code. This feedback can either be suggestions for code improvements or a specific request to change the code. Once all feedback has been appropriately responded to, the code is approved for testing.	

Control Ref	Control Name	Control Description	Status	Evidence of Compliance	Related Documents/ Records
				WV uses Azure pipelines to automate the build of the releases that are deployed to the test environment for the Test Team to conduct functional, end-to-end and regression testing. WV is aiming to utilise test scripts to automate as much testing as possible but currently there is still a mix of manual and automated testing. If defects are identified, these are raised as tasks against the PBI. When the Test Team has completed its testing, has attached the test evidence to the PBI, and approved the change, it is moved to user acceptance testing. This testing is typically conducted internally by the change owner who is then responsible for formally signing off the change. Depending on the type of change, the change owner may also require the requesting client to review and approved the change as well. Once this is completed, the Scrum Master is responsible for determining if the change needs to go back to the ICT Meeting to be approved for release. If this is the case, the ICT Meeting will typically review the test evidence before making a decision. There is a Release Approval Checklist which is utilised to ensure that all stages of the development lifecycle have been appropriately completed. This Checklist was reviewed for a specific release and observed to contains checks that: • The implementation plan has been approved • Functionality testing has been completed • End user testing has been completed • Security testing has been completed • Backout testing has been completed.	

Control Ref	Control Name	Control Description	Status	Evidence of Compliance	Related Documents/ Records
				Some of these checks are not mandatory for all releases, but all releases require an implementation plan and a regression plan. The DevOps system was reviewed and it was observed that a release goes through 'Approval for Release', 'Approved for Release Date' and 'Awaiting Release' stages. WV systems have different release schedules based on business and client requirements. The ICT Meeting will formally close a change once there is evidence that it is operating correctly and has not caused any issues. This may be some time after its initial release. The change owner is responsible for ensuring that all associated system and operational documentation has been appropriately updated. The emergency change process follows the standard change process but some steps are expediated such as ICT approval being obtained by email rather than via a scheduled meeting.	
8.33	Test information	Test information should be appropriately selected, protected, and managed.	Compliant	The Development and Testing Policy prohibits the use of personnel data for testing purposes unless prior approval is obtained from either the data-owning client or the Head of Compliance. It also states that live credit card primary account numbers (PANs) must never be utilised in non-production environments. The Test Team typically creates new fictional test data for each stage of testing that it completes.	Development and Testing Policy

Control Ref	Control Name	Control Description	Status	Evidence of Compliance	Related Documents/ Records
				The test, staging and production environments are all segregated to ensure that the data in each environment is fully protected and cannot be transferred between environments.	