WOODS VALLDATA

Information Security Management

Information Security Management

© The Woods Group Limited (trading as Woods Valldata).

All rights reserved. This document may contain confidential and proprietary information which may be subject to intellectual property rights (including, but not limited to, trademarks) of The Woods Group Limited.

The Woods Group and Woods Valldata are a trademark or registered trademark.

Acknowledgement of trademarks

Other product names, company names, marks, logos and symbols referenced herein may be the trademarks or registered trademarks of their registered owners.

Document Details Document Details

Document Detail	
Title	Information Security Management
Type	Guide/Aide Memoire
Effective Date	05/11/2024
Revision Period	Annual

Owner

Name	Function
Paula Robinson	Head of Compliance

Change History

Version	Date	Revision Description
1.0	4 January 2017	Initial version, reviewed and approved by Managing Director.
1.1	16 January 2017	Updated branding.
1.2	12 June 2017	Updated Incident Reporting section to include IT system monitoring and reporting.
1.3	22 June 2017	Expanded Data Protection section to reflect Woods Valldata internal policy
1.4	24 January 2018	Updated to include reference to GDPR, expanded data protection section.
2.0	03 September 2018	Updated to aligned Woods and Valldata Policies. Rebranded

Version	Date	Revision Description
2.1	1 May 2019	Updated to reflect changes to Ops Forum. Removed reference to Lead Supervisory Authority and added reference to UK and EEA.
3.0	29 June 2020	Reviewed, added reference to ISO 27001 certification. Updated scope to reflect information on ISO 27001 certificate, updated Ops Forum members. Expanded Change Control section and added information relating to back-ups.
3.1	13 July 2021	Reviewed, changed GDPR Fact Sheet to Data Protection Fact Sheet. Updated Ops Forum membership.
4.0	06 July 2022	Reviewed, updated Ops Forum membership. Added details of 2FA on non-console access, section on logging and monitoring, agile methodology and reference to the CIG. Minor amends to job tiles and terms.
5.0	17 August 2023	Reviewed, update Ops Forum membership. Amended Back-up section, System and Network Access Control section. Updated frequency of vulnerability scans to monthly. Minor terminology and grammar amends.
6.0	05 November 2024	Reviewed, updated ISO 27001 version, removed reference to Ops Forum and CIG. Updated awareness section and added Appendix A which covers the due-diligence questions WV is regularly asked, with responses.

1.0 Contents

2.0 Information Security Management

Introduction

To support information security management Woods Valldata has implemented an information security management system (ISMS) which is certified to the International Standard for Information Security Management (ISO/IEC 27001:2022).

The purpose of information security management is to protect information and associated information processing facilities, to minimise business interruption or damage by preventing and reducing the impact of security incidents. This is achieved through protecting the:

- Confidentiality of information
- Integrity of information
- Availability of information and resources.

Purpose

This document outlines Woods Valldata's approach to information security management, which aims to ensure there are sufficient controls in place to protect the company's information and associated information processing facilities from a wide range of threats, and to ensure compliance to its legal, regulatory and contractual requirements e.g.:

- The Gambling Commission Remote Gambling and Software Technical Standards (GC RTS)
- The Payment Card Industry Data Security Standard (PCI DSS)
- Data Protection Act 2018 (DPA)
- General Data Protection Regulation (EU) 2016/679 (GDPR)
- UK-GDPR.

This document provides an overview of the information contained within Woods Valldata information security policies and processes. Woods Valldata does not provide copies of its internal policies or processes due to confidentiality reasons, however it is more than happy to share the policies in person if required.

It should be noted that Woods Valldata is audited by independent external bodies for Gambling Commission Remote Gambling and Software Technical Standards (GC RTS), Payment Card Industry Data Security Standard (PCI DSS) and ISO 27001 International Standard for Information Security Management (ISO 27001) purposes, which includes reviewing and assessing Woods Valldata information security measures and documentation.

Scope

The scope of the Woods Valldata ISMS relates to the provision of outsourced activities to Charities, including Litho and digital printing, response handling, mailing and fulfilment, raffle and lottery management, document management which includes response handling payment services.

This scope includes the management of outsourced services provided to Woods Valldata by third parties (e.g. contractors and outsourced service providers) that have a significant / material impact on the delivery of Woods Valldata services to its Charity partners.

Activities which fall within the ISMS scope include all those which involve holding, obtaining, recording, using, sharing or managing employees, company, Charity partner and supporter information or data.

Reference Material

This document is supported by a number of internal policies, processes, procedures and documented information, some of which are detailed below:

- IMS Framework
- Information Security Policy
- Data Protection Policy
- Data Protection Compliance Fact Sheet
- Access Control Policy
- Visitor and Building Contractor Access Control Policy
- Starters, Movers and Leavers Procedure
- Information Classification, Handling and Protection Policy
- Information Retention Policy
- Acceptable Use Policy
- Mobile Device and Remote Working Policy
- Incident Reporting, Escalation and Management Process
- Change Management Process
- IT Security Policy
- Information Assurance Schedule
- Role Based Profile Matrix

Information Security Policy

Woods Valldata has implemented an Information Security Policy which outlines its intention with regards to information security. This Policy is supported by a number of topic specific policies, processes and procedures. Woods Valldata Information Security Policy is approved by the CEO and policies, processes and procedures are communicated to all, where applicable, as part of the induction process and at least on annual basis. All Woods Valldata information security policies, processes and procedures are available to staff via Woods Valldata SharePoint site.

It is the policy of Woods Valldata to ensure that:

- Information will be protected against unauthorised access, use or disclosure
- Confidentiality of information will be assured
- Integrity of information will be maintained
- Contractual, regulatory and legislative requirements will be met, including the management and maintenance of GC RTS and PCI DSS Level 1, as well as certification to ISO 27001
- Information security requirements will be aligned with Woods Valldata organisational strategies and objectives
- All relevant information related to legal, regulatory and contractual requirements is communicated to the business
- An ongoing and robust risk management programme is managed and maintained
- The effectiveness and efficiency of the information security measures shall be reviewed via independent internal audits, performance monitoring and management reviews

- Third parties engaged in the support of Woods Valldata will be controlled through suitable contracts, service level agreements and definitions of requirements, service delivery monitoring, review and audits
- The information security responsibilities of third parties will be defined and agreed in accordance with Woods Valldata Third Party Management Policy
- Business continuity plans will be produced, maintained and exercised to ensure that in the event of a disruption, Woods Valldata can continue to deliver an acceptable level of service of its critical activities to its interested parties
- Information security training will be provided to all users during the induction process and on an on-going basis to ensure they are educated on their information security responsibilities
- All breaches of information security, actual or suspected, will be reported and investigated in line with the Incident Reporting, Escalation and Management Process
- Information security controls will be commensurate with the risks faced by Woods Valldata
- Information security supports Woods Valldata business goals and objectives
- Woods Valldata information security responsibilities are defined and communicated.

All policies and processes are reviewed at least annually, or after significant change, to ensure they remain suitable and effective.

Information Security Risk Management

Woods Valldata follows a balanced information risk strategy based on formal methods for risk assessment, risk management and risk acceptance in line with best practice i.e. ISO 31000:2018 Risk Management – Principles and Guidelines.

Woods Valldata seeks to undertake a risk assessment as a means of determining and confirming that its information security measures reduce the impact or likelihood of an information security incident and enables continual improvement. Its information security risk management approach applies to all information and associated information processing facilities.

Information Security Organisation

Woods Valldata Senior Management Team

The Senior Management Team provides leadership and direction in evaluating information security risks, setting the risk appetite, risk policy and strategy. It is also responsible for the implementation, monitoring and effectiveness of the ISMS and conducting management reviews to ensure that information security remains appropriate, effective and aligned to the strategic direction of Woods Valldata.

Monthly and quarterly meetings are held to collectively conduct a full management review.

Head of Compliance

The Head of Compliance is responsible for the implementation and on-going management of the ISMS. This includes implementing and/or monitoring agreed standards, procedures and guidelines to ensure compliance to Woods Valldata policies and procedures.

The Head of Compliance is the Data Protection Officer, holds a Personal Management Licence (PML) issued by the Gambling Commission and holds the key positions as defined by the Gambling Commission for Compliance Governance and Money Laundering Reporting Officer for Woods Valldata. The Head of Compliance reports to a member of the Board

Information Security Responsibilities

All staff, whether permanent or temporary, are responsible for the protection of Woods Valldata information and assets, enabling the confidentiality, integrity and availability of these assets to be maintained. Information security roles and responsibilities are documented within the Roles, Responsibilities and Authorities matrix (RACI), and individuals are informed and trained on their roles and responsibilities.

Independent Review of Information Security

As Woods Valldata processes payment card data, it is required to be compliant with the Payment Card Industry Data Security Standard (PCI DSS). Woods Valldata is assessed every 12 months by a Qualified Security Assessor (QSA) organisation which performs an assessment of its compliance against the Standard.

Woods Valldata is licensed and regulated by the Gambling Commission (GC) and is therefore required to comply with the GC's Remote Gambling and Software Technical Standards (RTS), which includes a set of security requirements. These requirements are based on a subset of controls contained in the Annex A of ISO 27001:2022, the International Standard for Information Security Management. In order to satisfy the GC's annual independent ISMS audit requirement, Woods Valldata engages a qualified third party to conduct its independent information security audit in accordance with the requirements of the GC Security Audit Advice.

Woods Valldata is also certified to ISO 27001:2022 and is externally audited by a UKAS accredited certification body annually.

The Compliance Team also conduct internal audits of the Company's working practices and information security measures, as documented within the Information Assurance Schedule. Results are reported and reviewed by the process / control owner and the Senior Management Team.

The Head of Compliance provides a quarterly compliance management pack to the Senior Management Team which details the following:

- A summary of the 'red' risks and their treatment actions
- A count of outstanding actions on the improvement log
- Audits completed since the last quarter and their actions (internal and external)
- Outstanding actions from previous audits (internal and external)
- Status of Compliance Training by Team (induction and annual)
- No of documents past their review date by team

This pack is used to ensure the Senior Management Team have visibility of the compliance status of each area of the business.

3.0 UK Data Protection Laws

Woods Valldata Data Protection Policy covers its requirements for the processing of personal and sensitive/special categories personal data (personal data), as defined by the Data Protection Act 2018, UK-GDPR and General Data Protection Regulations (EU) 2016/679 (GDPR) for which Woods Valldata is the 'data controller'. Woods Valldata information security measures include ensuring personal data is processed in-line with the principles of the laws:

- Personal data shall be processed fairly, lawfully and in a transparent manner
- Personal data shall only be obtained for specified, explicit and legitimate purposes

- Personal data shall be adequate, relevant and limited to the purpose(s) for which it is processed
- Personal data shall be accurate, and where necessary up to date
- Personal data shall not be kept for longer than is necessary
- Personal data shall be processed in accordance with the rights of the data subjects
- Personal data shall be protected from unauthorised and unlawful processing and against accidental loss or destruction or damage by appropriate technical and organisational controls
- Personal data shall not be transferred to a country or territory outside the UK or EEA
- It shall be responsible for, and be able to demonstrate, compliance with the principles of applicable data protections laws.

The policy also covers situations where Woods Valldata acts as a 'data processor'. The 'data controller' is responsible for detailing its requirements for processing personal data, together with other information, to enable Woods Valldata to process personal data on its behalf, this includes enabling the controller to comply with the rights of a data subject. The data controller's requirements must not, under any circumstances, conflict with the principles of the data protection laws or other legal and regulatory requirements Woods Valldata or the data controller are subject to.

Fair, Lawful and Transparent Processing

Where Woods Valldata is acting as the Data Controller it will ensure:

- All forms used to collect personal data clearly state the purpose for which the information is being collected.
- All data subjects are provided with a privacy notice before personal information is collected and recorded
- It does not use personal data for any purposes other than those advised to data subjects directly
- It will only process personal data:
    - Where it is necessary for compliance with the law, the performance of a contract, with a view to establishing a contract, or
    - Where it is in the organisation's legitimate business interests to do so.
    - Where this is not possible, or in the case of sensitive/special categories of personal data (see below), consent of the individual shall be sought to enable the personal data to be processed.
- Obtains explicit consent of the individual concerned for all processing of sensitive / special categories of personal data; unless:
    - It is information relating to racial/ethnic origin, religion or disability that is being collected purely for monitoring equality of opportunity or treatment
    - It relates to the employment of Woods Valldata staff
- All data processors it engages formally agree that personal data will not be used for any purpose other than the agreed purpose and the contract in place includes any controls Woods Valldata is subject to, where applicable
- Personal data is not disclosed to third parties unless:
    - Required to by law
    - There is a contract and associated agreement in place to ensure that any processing by the third party will be within the law

  - It is necessary in order to fulfil a legitimate purpose that has been advised to the data subject.

Where Woods Valldata is acting as a Data Processor it will ensure:

- It does not process personal data for any purposes other than those advised by the Data Controller in writing
- The rights to the personal data provided by the Data Controller are reserved to the Data Controller.
- It does not make any use of personal data or allow any use of the personal data except for the purpose of the services provided to the Data Controller.
- It will not subcontract or engage a third party in the processing of personal data without written authorisation from the Data Controller
- It will not transfer personal data outside of the UK, EEA without written authorisation from the Data Controller
- Provide the Data Controller a 'Supporter Personal Data Information Asset Register' which includes:
  - A description of the categories of data subjects and of the categories of personal data
  - The purposes of the processing
  - How long the personal data will be retained for
  - The types of third party who are involved in the processing of supporter personal data

Subject Rights

Woods Valldata has measures in place to ensure it can comply with the rights of the data subject in a timely manner, whether that is the right to rectification of personal data, right to restrict or object to processing or the right of access to their personal data. All subject access requests received from supporters will be passed to the Charity partner for response, Woods Valldata will assist the Charity partner in responding to all subject right requests as applicable.

Technical and Organisational Measures

The following sections and Appendix A of this document provides details of the technical and organisational measures in place to protect information and information processing facilities owned and entrusted to Woods Valldata.

Data Protection Officer

The Woods Valldata Data Protection Officer is the Head of Compliance.

4.0 Information Security Measures

The following sections cover the key information security control areas which Woods Valldata has implemented to ensure compliance with its legal, regulatory and contractual requirements. Please also refer to Appendix A for the responses to questions asked in information security, data protection and cyber security due-diligence questionnaires.

Human Resources Security

Pre-Employment Screening

A HR Security Policy is in place which defines Woods Valldata requirements for 'on-boarding', screening, induction, awareness and movers and 'off-boarding'. The HR Security Policy is supported by a number of processes and procedures, a summary of which can be found below.

Woods Valldata has adopted a pre-employment screening programme for all new staff whether permanent or temporary. Human Resources (permanent staff) and line managers (agency and contractor staff) are responsible for ensuring this screening process is followed. The following checks are undertaken on all staff as part of the onboarding process:

- Identify Check
- Right to Work
- Proof of Residence
- Proof of Activity
- Criminal Record Check / Disclosure and Barring Service (DBS)

Certain roles may from time to time require further screening to be undertaken, this will be identified by a member of the Senior Management Team and could include:

- Proof of Qualifications
- Credit Check

Starters, Movers and Leavers

Woods Valldata has implemented a Starters, Movers and Leavers Procedure which ensures all staff, whether permanent, temporary or via agency are on-boarded, changed or terminated in a consistent manner and that the relevant training is undertaken and access permissions provided or revoked.

Information Security Awareness and Training

Information security awareness and training commences upon joining and continues at appropriate intervals to ensure that each individual is aware of their information security roles and responsibilities. This awareness programme comprises in-house developed and off-the shelf e-learning, quizzes, face to face training, poster campaigns and newsletter articles.

The awareness and training covers topics such as:

- Data Protection
- GC RTS
- PCI DSS
- ISO 27001
- Cyber security topics, including phishing simulation campaigns
- Charity partner information security requirements
- Woods Valldata working practices

As part of the induction and annual awareness training all staff are required to sign a declaration (whether physically or electronically) to indicate they have been provided training, they are aware of their obligations and agree to abide by Woods Valldata policies and processes.

Third Party Supplier Management

Third parties are managed as part of Woods Valldata third party governance process. Woods Valldata will conduct due-diligence checks and risk assessments on any third party that has access or potential access to information owned by or entrusted to Woods Valldata, or any third party involved in the supply chain of its key products and services to ensure their information security and business continuity controls meet the requirements of Woods Valldata and its Charity partners.

Third parties will be subject to formal contracts and agreements, which will include measures to ensure services provided by third parties are monitored and reviewed at regular intervals, as appropriate.

Physical Security

Woods Valldata has implemented physical security measures to ensure the appropriate security of all information assets and processing facilities, including where information is held by third parties. Access by staff and third parties will be controlled in line with Woods Valldata Access Control Policy and Role Based Profile Matrix.

Physical Access Control

Woods Valldata operates an access card system at its offices; each card is programmed based on an individual’s job role or function. Access levels are documented within the Role Based Profile Matrix which is approved by Woods Valldata Management.

CCTV is in operation within the external perimeter of the building, and specific internal areas e.g. internal ingress areas, Inbound Operations and Outbound Operations.

Visitors, Contractors and Agency Staff (Guests)

All Guests are required to report to Reception where they will be booked in prior to being collected from Reception. Visitors will be provided with a visitor badge and will be escorted whilst on site.

Contractors and agency staff will be provided with an access card which has limited unescorted access to the site as per the Role Based Profile Matrix.

All Guests are required to sign a confidentiality agreement, including site rules, upon arrival. Returning Guests who have not been on site within a 3-month period will be required to re-sign the agreement.

Inbound Operations and Raffle Room (Secure Area)

A secure area has been identified within the Woods Valldata premises where further physical security restrictions apply. No bags, outdoor clothing or mobile phones are permitted in this area.

All guests to those areas including members of staff who do not regularly work in that area must be authorised by the manager/supervisor of the secure area before entry and will be closely supervised whilst in the secure area. A record of entry and exit to the secure area is maintained.

Audio Visual Recording

Photography and any other form of audio-visual recording within Woods Valldata premises are strictly prohibited, unless approved by the CEO, CFO or Head of Compliance.

Information Protection

Woods Valldata has implemented an Information Classification, Handling and Protection Policy which defines the levels of classification used within Woods Valldata, how information can be handled from conception to destruction.

Information Classification

There are four levels of information classification within Woods Valldata, i.e. Confidential Restricted, Confidential, Internal Use Only and Unrestricted.

It is accepted that information generated by external parties may have different levels of classification or descriptions, if there is any uncertainty on how externally classified information maps to Woods Valldata classification, then a classification of 'Confidential' or higher will always be adopted.

Supporter personal data, including cardholder data is classified as 'Confidential – Restricted' no matter what form it takes or whether sensitive /special categories of personal data is included.

Information Handling

Measures have been implemented to protect data whether in use, transit or at rest. All information will be created, amended, stored, distributed and destroyed in line with the Woods Valldata Information Classification, Handling and Protection Policy.

Information will be protected in a manner commensurate with its sensitivity, regardless of where it resides, what form it takes, what technology is used to handle it, or what purpose(s) it serves.

The Information Classification, Handling and Protection Policy includes the systems in which supporter personal data is permitted to reside and in the case of network resources the folder structure to use.

Woods Valldata will only send via email the supporter URN, surname and transactional reference internally or to a Charity partner, if additional personal data is required to be shared then the Woods Valldata, or the Charity partner's SFTP will be used. It is not possible to restrict what a supporter sends in via email, however access to these emails is limited to the Supporter Services team within Woods Valldata.

Data held within Microsoft Azure, SFTP, backups and within the Cardholder Data Environment (CDE) is encrypted at rest. Data held on the SFTP is also password protected, but this is dependent on individual Charity partner requirements so does not apply to all data.

Information Retention

To prevent the premature destruction or prolonged holding of information that needs to be retained for a specified period to satisfy legal, regulatory and contractual requirements, an Information Retention Policy, and accompanying schedule has been implemented. Retention periods relating to personal data processed on-behalf of Charity partners has been supplied in a separate Information Asset Register (IAR).

When information reaches its maximum retention period, whether held in paper or electronic format, it will be deleted or disposed of in line with the Information Classification Handling and Protection Policy.

Information Disposal and Destruction

All information will be disposed of in line with the Information Classification Handling and Protection Policy when no longer required. All paper media, irrespective of its classification, is sent off site for secure destruction using an approved third party.

All data and software are securely deleted from all removable media prior to be sent off site for secure disposal and destruction via an authorised third party disposals agent, where it will be disposed of in accordance with the WEEE (Waste Electrical and Electronic Equipment) Directive.

The agent will provide Woods Valldata with a certificate to confirm that the media has been destroyed, a destruction certificate is kept for 3 years.

IT Security

Technical and organisational controls have been implemented within Woods Valldata to ensure digital information, and associated information processing facilities, are protected in line with legal, regulatory and contractual requirements.

Acceptable Use / Mobile Device and Remote Working

An Acceptable Use Policy has been implemented which defines Woods Valldata rules on topics such as:

- Email and Internet Use
- Clear Desk, Working Area and Clear Screen
- Equipment, Data and Information Protection
- Passwords
- Social Networking
- Malicious Code Protection
- Intellectual Property Rights, including copyright protected material.

A Mobile Device and Remote Working Policy has been implemented to ensure information and equipment is protected when working outside of Woods Valldata premises and in-line with other policies and requirements. All mobile devices are encrypted, and remote working is restricted to authorised members of staff and requires multi-factor authentication.

Only company provided mobile phones are authorised to access the company email system; mobile phones are encrypted and can be remotely wiped if lost or stolen. USB devices are blocked as standard; where USB devices are authorised by the Head of Compliance or CTO only encrypted USB devices are permitted.

System and Network Access Control

Access to the Woods Valldata network and data is controlled through a number of user identification and authentication methods. All users are assigned a unique user ID with least privilege access granted, as per the Woods Valldata Role Based Profile Matrix. Privileged users have a separate account for administrator access from their user account. Access to systems and services is reviewed by the information / system owner.

Multi-factor authentication is required for remote network access originating from outside the Woods Valldata network. Multi-factor authentication is also required internally for non-console administrative access.

Other access controls measures include network segmentation using physical and virtual networks to restrict access between systems, services, and environment and databases, IP filtering to restrict access to public facing systems and various database and user access controls to segregate different Charity partners’ data.

Wireless Networks

Wireless networks are configured on the Woods Valldata internal network only; access is restricted to authorised company devices through MAC address filtering. Monthly scans and inspections are undertaken to ensure only authorised wireless access points are installed.

A guest wireless network is provided but there is no connection to the internal networks from this network.

Penetration Testing

External penetration testing is performed at least annually and after any significant infrastructure or application upgrades or modification. Internal penetration testing is conducted at least annually, or six monthly if part of the card holder data environment (CDE). Penetration tests are conducted by a PCI DSS approved scanning vendor (ASV).

All critical, high or exploitable issues detected on any device within the Woods Valldata infrastructure will be remedied within 30 days, in line with PCI DSS requirements, and a re-test will be conducted. A risk-based approach will be taken to address all other findings.

Vulnerability Management

Woods Valldata has adopted a layered approach to reduce vulnerabilities within its IT infrastructure. System hardening has been implemented by ensuring each server has only one primary function. This requirement prevents functions that require different security levels from co-existing on the same server, and only the necessary services, protocols, daemons, etc., as required for the function of the system, are enabled.

All software and firmware in use never exceed the ‘end of life’ dates of that particular product.

A patch management regime is also in place, which includes reviewing security alerts every 24 hours and taking the necessary actions based on the criticality of the alert.

Formal vulnerability scanning is conducted across all systems and networks both inside the network and against Woods Valldata network perimeter. The scanning is performed monthly and after any significant change in the network.

Malicious Code Protection

All systems provided by Woods Valldata have approved malicious code protection software installed which is kept up to date. On systems where the risk of infection is insignificant, or malicious code products are not available, frequent reviews are undertaken to identify any suspicious activity or performance degradation.

Backups

Woods Valldata data hosted in Chippenham is backed up on premises before syncing to Microsoft Azure. Data hosted in Microsoft Azure is backed up within Azure. All back-up data is encrypted, and backups are held for 12 months.

The frequency and type of back-up is dependent on the rate of change to the data and/or system and can range from every 10 minutes (transactional logs) to every 24 hours.

Logging and Monitoring

All system logs are monitored in real time and alerts are raised in the event of unauthorised access, whether successful or attempted. Logs are 'shipped' to a central server and kept for 12 months. File integrity monitoring is also in place to alert if log files, and other critical files are changed; logs cannot be changed on the central server.

Change Management

A formal Change Management process is followed within Woods Valldata to ensure changes are made in line with regulatory, contractual and internal requirements.

The Process covers system development, system acquisition, infrastructure (physical and IT), business and process change as well as requests received from Charity partners relating to changing or adding to their service offering.

System Acquisition, Development and Maintenance

The proposed acquisition of new system would initially follow the Third-Party Process, which includes undertaking a risk assessment on the provider, their service and the impact to the data and operations of the business. The CFO or Finance Manager and Head of Compliance will approve all new third parties prior to engaging after assessing the results of the risk assessment.

Woods Valldata follow the Agile development methodology. Security is considered at the design phase of all new systems; the Head of Compliance is a member of the ICT Change Board to ensure that all security and compliance requirements have been considered for all changes and new deployments.

Changed to existing systems and software, whether third party or in-house developed are reviewed and approved by the ICT Change Board. ICT changes require a formal risk assessment to be conducted prior to approval, as well as testing and acceptance criteria to be developed, and regression and roll-back processes to be available before the change can be implemented.

Acceptance criteria for the transfer of ICT changes from the development to operational environments is established by the ICT Change Board which meets weekly.

Process and Building Changes

All process or building changes that could affect Woods Valldata GC, GC RTS, PCI DSS or ISO compliance, whether ISO 27001, ISO 9001 or ISO 14001, are reviewed and approved by the Senior Management Team or Head of Compliance prior to implementation.

Charity partner Service Offering Changes

When a Charity partner wishes to add to or amend their existing service offering the Commercial Team will raise this request via the 'Authority to Offer' change process to ensure Charity partner service offerings are aligned with Woods Valldata's operational and compliance measures as well as business strategy.

5.0 Incident Management

An Incident Reporting, Escalation and Management Process has been established which details how information security breaches, events, incidents, non-conformities and weaknesses are reported, effectively responded to and managed.

The process applies to

- A break down in integrity of Woods Valldata security infrastructure leading to the disclosure or potential disclosure of confidential or higher information
- A compromise of the availability of IT systems or infrastructure
- Any event that could lead to or is negatively impacting the confidentiality, integrity and/or availability of Woods Valldata information and associated information processing facilities, including information entrusted to Woods Valldata by its Charity partners
- Issues affecting the quality of service to Charity partners

- A deviation from Woods Valldata policies, processes or standards.

Incidents are categorised as low, medium (managed), high (serious) and critical (major), based on the severity of impact to Woods Valldata, its staff, its Charity partners and the services provided to those Charity partners. Escalation mechanisms have been implemented to ensure any response and recovery is appropriate and prompt.

This Process includes identifying and implementing actions to eliminate the cause of any non-conformance, prevent recurrence and prevent its occurrence elsewhere. Actions taken are appropriate to the nonconformity and area of the business affected.

Incidents are analysed by the Senior Management Team to identify trends, review the effectiveness of the controls in place, whether human, technical or procedural, and to identify areas of improvement.

IT System Monitoring, Reporting and Escalation

24/7 system monitoring is in place across the Woods Valldata IT platform ensuring that incidents that could affect the IT infrastructure are responded to and dealt with in a timely manner. System monitoring includes, but is not limited to system availability, capacity, and performance (disk space, CPU etc), hardware status (individual components of the hyper converged infrastructure), service status, loss of power or connectivity, intrusion or malicious code detection and file integrity monitoring, and applies to both Charity partner facing services such as website, Charity partner portals, DAT reporting and SFTP as well as internal services.

The system monitoring tools will alert IT ‘on-call’ personnel via email and/or text, depending on the severity of the incident. IT personnel will triage the incident to confirm its severity and attempt to fix the issue, where feasible and appropriate.

Any incident deemed critical will be escalated internally as per the Incident Reporting, Escalation and Management Process, which includes ensuring Charity partners are informed as soon as practically possible but no later than 24 hours of the incident being known.

Incident Management Team

Woods Valldata has established an Incident Management Team (IMT) which will provide direction and support in the event of a critical incident. This centralised approach ensures that recovery requirements for affected departments are satisfied while minimising confusion and duplication of effort.

The IMT is responsible for:

- Managing internal and external communications
- Directing response and recovery activities
- Monitoring the recovery progress
- Providing or reallocating recovery resources.

In the event of a major incident, the IMT will be convened and the situation assessed.

The IMT is responsible for managing the incident, providing information to staff, Charity partners, invoking business continuity and making tactical decisions to assist in the recovery effort.

An Incident Management and Business Continuity Plan has been developed to assist the IMT with this process.

Business Continuity

Business continuity measures and plans have been established to reduce the likelihood and/or impact (to Woods Valldata and its Charity partners) of a critical incident occurring. These measures include ensuring resilience and redundancy is built into the IT infrastructure to remove any single points of failure.

Exercising and Testing

Business continuity plans are reviewed annually or within 45 days of any major operational or system changes that will have a material effect on the contingency strategy. Plans will be exercised at least once a year or within 45 days of any major change.

An exercise report is completed prior to any exercise taking place. The report details the aims and objectives of the exercise, resources required, and any risks associated with conducting the exercise. A post-exercise review takes place to identify any issues or improvement opportunities identified as part of the exercise.

6.0 Performance Evaluation

Verification Checks and Audit

The Head of Compliance, in consultation with the Senior Management Team is responsible for establishing an annual assurance programme to ensure continued compliance to legal, regulatory, company and Charity partner requirements. This programme consists of verification checks and formal audits. All business processes are subject to internal audits; the frequency of audits will be risk based and will take into consideration the criticality of the process, the type of information processed and details of previous incidents.

The priorities for these checks and audits are based upon legal and regulatory requirements, risk assessment results, along with the results from incident management and previous audits.

Formal audits are both procedural and technical to verify control implementation and maturity as well as to validate technical configurations and vulnerabilities. Audit reports are produced, and any findings are reviewed by the process owner and Senior Management Team. The results from monthly IT Compliance reviews, conducted by the Head of Compliance, are reviewed, and signed off by the CFO and CTO.

External / third party audits are also managed and co-ordinated as part of the assurance programme.

7.0 Continual Improvement

Corrective and improvement controls are applied to documents, processes, controls and practices. Corrective actions are taken to eliminate the cause of any nonconformity, prevent recurrence and prevent its occurrence elsewhere. The corrective action taken needs to be appropriate to the nonconformity and area of the business affected. Records are maintained of all corrective actions and improvements. Opportunities for continual improvement, including corrective actions, are discussed, and prioritised by the Senior Management Team.

8.0 Appendix A

The following table provides Woods Valldata's response to the questions it frequently receives in Information Security, Data Protection and Cyber Security due-diligence questionnaires from Charity Partners. Supporting certificates, registrations and documents can be downloaded from the Woods Valldata website, within the My Account area.

Ref	Question	Woods Valldata's Response
Certification Status		
1.	Is your organisation certified to ISO 27001:2022?	Yes, via a UKAS accredited certificate body. Certificate number: 232975
2.	Is your organisation registered with the ICO?	Yes, registration number Z9778401.
3.	Is your organisation certified to Cyber Essentials or Cyber Essentials Plus?	No, WV however is subject to several external audits covering most, if not all the requirements in CE/CEP.
4.	What other certifications, accreditations or compliance certificates does your organisation hold?	Woods Valldata (WV) is: • Compliant PCI DSS Service Provider • Compliant to Gambling Commission Remote Technical Standards • BACs Approved Bureau • SafeSupplier verified • ISO 9001:2015 certified • ISO 14001:2015 certified
Organisational Security		
5.	Who is responsible for Information security and data protection generally within your organisation?	The Head of Compliance (HoC) is responsible for Compliance across the business and is the company's Data Protection Officer. The HoC is supported by various members of the Senior Management Team in relation to specific elements such as the CTO for IT and cyber security and the Head of HR for people security.
6.	What experience does the person(s) in Q5 possess?	The HoC has been working in an information security, business continuity and data protection role for over 20 years. This includes being a qualified information security, business continuity and data protection consultant and trainer, CSA Star Auditor and previously a qualified PCI DSS QSA.

Ref	Question	Woods Valldata's Response
7.	Does the person(s) in Q5 report to a member of the Board?	Yes, the HoC reports to the CFO.
8.	What processes are in place to identify and ensure compliance with all the applicable and legal regulatory requirements relating to this service, in all jurisdictions where you operate from?	WV has implemented a compliance management system to identify all legal, regulatory and contractually requirements and to ensure that the appropriate control measures are in place to meet those requirements.
9.	How are Information security, data protection, cyber security risks assessed and how frequently is this done?	A review of WV's risk register is completed quarterly or after significant change. In addition, risk assessments are completed as part of change management, incident, management, third party management, privacy impact assessments and vulnerability assessments so it's a continuous process to ensure all risks are understand and mitigation is implemented, where possible.
10.	What screening is completed on staff, and are all staff screened?	All staff undergo DBS checks, as well as the required proof of identity and right to work checks no matter their role. In addition, qualification and financial checks will also be done for specific roles.
11.	Does your organisation have policies in place for information security and data privacy, and how often are these reviewed?	WV has several policies and procedures that cover information security and data privacy, such as: • Information Security Policy • Data Protection Policy • Information Classification, Handling & Protection Policy • Mobile Device and Remote Working Policy • Information Retention Policy & Schedule • IT Security Policy • HR Security Policy • Third Party Management Policy • Incident Reporting, Escalation & Management Procedure • Change Management Procedure • Subject Access Request and Right to be Forgotten Process • Privacy Impact Assessment Guide

Ref	Question	Woods Valldata's Response
		All policies, processes and procedures are reviewed at least annually or after significant change.
12.	How does your organisation go about checking that your security policies and standards are being applied?	An internal audit programme is in place, as well as spot checks and monthly and quarterly reviews. The frequency of internal audits, spot checks and reviews are risk based. In addition, WV is subject to annual external audits for ISO 27001, PCI DSS, GC RTS, BACs, SafeSupplier, ISO 9001, ISO 14001 as well audits conducted by our Charity Partner's and their audit bodies such as Crowe and BDO.
Awareness and Training		
13.	How does your organisation make staff aware of information security, data protection and cyber security risks, policies and compliance requirements?	Awareness and training commence upon joining and continues at appropriate intervals (no longer than 12 months) to ensure that individuals are aware of their compliance roles and responsibilities. This awareness programme comprises of in-house developed e-learning specific to the data, systems and processes within WV, cyber e-learning and phishing simulations, quizzes, face to face training, poster campaigns and newsletter articles.
14.	How does your organisation ensure third parties and contractors are made aware of information security, data protection and cyber security risks, policies and compliance requirements?	All training and awareness requirements are identified as part of the WV Third Party Management process. In some instances, this could result in the individual being deemed 'staff' and they would therefore undergo the same training and awareness as detailed in Q13.
15.	Does your organisation require staff to formally acknowledge their information security and data protection responsibilities?	Yes, as part of each annual awareness training module staff are required to acknowledge they have been provided training and to agree to comply with the company's policies and processes, as they apply to their role. A record of this acknowledgment is maintained for a minimum of 3 years.
Data Protection		
16.	Does your organisation legally need to appoint a Data Protection Officer (DPO)?	No, however the Head of Compliance is the company's DPO and reports directly to a member of the Board.

Ref	Question	Woods Valldata's Response
17.	Does your organisation process personal data, where it is acting as a data processor, outside of the UK?	Yes, WV has an office in Romania however no data is sent to Romania; the team there access all personal data directly on UK servers and systems via VPN access using MFA. There is other processing in the EEA, but this is service specific; the details of all sub processors and locations personal data is processed is included in the Statement of Works for the service being provided.
18.	Does your organisation transfer personal data, where it is acting as a data processor, outside of the EEA?	No, all personal data is processed in the UK or EEA.
19.	Does your organisation have processes in place for identifying and managing transfers outside of the EEA?	In the event a transfer outside of the UK and EEA was needed a Privacy Impact Assessment would be conducted; this would form part of WV's change management and third-party management processes. No transfer outside of the EEA would take place, where WV is acting as a data processor on behalf of its charity partners, without prior approval.
20.	Does your organisation have a process in place for conducting privacy impact assessments?	Yes, a Privacy Impacy Assessment (PIA) screening process is integrated into our Change Management and Third-Party processes to ensure that any new processing or change to how or where personal data is processed is assessed and approved. The PIA screening form is reviewed and signed off by the Head of Compliance prior to the change being approved or third party engaged to ensure all required data protection measures are implemented as default. This would include, where applicable, written authorisation from Charity partners.
21.	Please provide a list of all third-party suppliers that may be involved in the provision of your organisation's service(s) and what their role is, including any that may be supplying IT services to your organisation.	The names and locations of the third parties used is documented within the Statement of Works for the contracted services as they are service and client dependant. In summary third-party suppliers are used for the following activities: • Cloud hosted applications e.g. email (internal and email thanking) and ticketing • Cloud backup • Data cleansing and validation, e.g. PAF, MPS, TPS, bank checker

Ref	Question	Woods Valldata's Response
		- Payment providers, e.g. payment cards and BACs - Payment couriers, e.g. cheque collections to clearing house - Secure paper and electronic media destruction - Secure storage of physical archiving.
22.	Please explain what due diligence your organisation undertakes on third-party suppliers?	WV has an extensive Third-Party Management process in place, which ensures the appropriate due diligence is undertaken based on the service being provided and the types of data they need to access and why. These methods would be agreed as part of contract and reviewed as part of the third-party management process to ensure the information was being shared / accessed in a secure manner and in line with legal, regulatory or contractual requirements WV is subject to.
23.	Does your organisation maintain documentation in-line with Article 30 of GDPR and UK GDPR?	Yes, an Information Asset Register (IAR) is available to clients that details the purposes for which the data is being processed, the types of data being processed, where the data is sourced from and the retention period that applies. The client version of the IAR is a subset of the internal version which details systems and user groups that apply to that processing.
24.	Does your organisation have a process in place for executing Data Subject Rights Requests?	Yes, please refer to the Data Protection Compliance Fact Sheet for further information about each of the data subject rights.
25.	How does your organisation protect personal data in transit?	All data is encrypted in transit using TLS 1.2 or higher. All encryption methods are compliant with PCI DSS.
26.	Is all personal data encrypted?	Data held within Microsoft Azure, SFTP, backups and within the Cardholder Data Environment (CDE) is encrypted at rest. Data held on the SFTP is also password protected, but this is dependent on individual Charity partner requirements so does not apply to all data.

Ref	Question	Woods Valldata's Response
27.	What controls have been put in place to prevent unauthorised viewing, copying or emailing of personal data?	Depending on the task being undertaken some machines are blocked from functions such as email access, internet access, cut and paste, notepad etc. Personal data is not permitted to be sent via email and alerts are in place to flag any potential breaches of this rule. Only the permitted number of digits of a PAN is visible once a payment card has been entered. Hashing is used so an individual's bank account number is not shown in full on outgoing supporter correspondence. Periodic checks are also undertaken to verify that personal data is only being saved to 'approved' systems and locations.
28.	Does your organisation have a formal retention and destruction program to ensure information is securely destroyed when no longer needed?	Information retention periods are set based on the purposes for which it is being processed. Where possible automated retention scripts are used to delete any data past its retention period. Locations where automated retention scripts are enabled are sampled during the monthly IT Compliance reviews to validate data is being removed in line with their retention period. Where deletion is a manual task, Information Asset Owners (IAO) are responsible for scheduling this in at least annually, these locations are sampled at least annually to ensure IAOs are completing this activity. For physical response devices and records in the core database(s) are subject to client retention periods and no data is deleted or destroyed without written instruction from the client. All paper resources are sent off-site for secure destruction.
29.	Does the supplier restrict the use of the live data or information for non-production purposes or testing?	Yes, however there are specific instances where a client may require us to use live data as part of UAT or proofing to enable the end-to-end solution to be fully verified. This is kept to a minimum and agreed in advance.

Ref	Question	Woods Valldata's Response
Access Control – Physical and Logical		
30.	Explain how access is granted and revoked in terms of physical and logical access?	WV has a Starters, Leavers and User Changes process in place using automated workflow and ticketing systems to ensure all access whether physical or electronic is approved, granted/revoked in line with the Role Based Profile matrix.
31.	How does your organisation restrict access to electronic data on a business needs to know basis?	Access to data, no matter the system, is based on least privileged access which is documented within the Role Based Profile matrix.
32.	Does your organisation assign each user a unique ID?	Yes, generic or shared IDs are only permitted in exceptional circumstances and would not be granted as part of the normal starters or user changes process. In those exception circumstances the Head of Compliance would need to approve, but only once a risk assessment has been undertaken to identify any additional controls that are required. Any exceptions are recorded on the risk register.
33.	How does your organisation ensure separation of duties between business as usual and privileged access accounts?	System Admins have a separate account to their normal day to day account. The Role Based Profile matrix identifies which roles are permitted to have a System Admin account.
34.	How does your organisation ensure separation of duties between developer/test accounts and production accounts?	Developers have a separate account to their normal day to day account. The Role Based Profile matrix identifies which roles are permitted to have a developer account. Developer accounts only have access to development systems.
35.	How does your organisation restrict physical access to your site, building, offices, data centre?	Access is restricted to authorised personnel using an access card system. Physical access cards and lanyards are provided with photo ID to all employees. All other staff members will have different coloured lanyards and access cards to differentiate between visitors, agency staff and contractors. Physical access is approved, granted and revoked in line with the Role Based Profile matrix based on job role and via the Starters, Leavers and User Changes process.

Ref	Question	Woods Valldata's Response
36.	Explain the formal program for the review of access to systems supporting client information?	The Role Based Profile matrix is reviewed at regular intervals with Information Asset Owners to ensure documented access is up to date. This is also reviewed against access that has been provisioned. In addition, as part of the monthly IT Compliance reviews the Head of Compliance verifies that all starters, leaver and user change requests have been actioned as per the Role Based Profile matrix.
37.	Does your organisation have a formal password policy that ensures strong passwords are defined and maintained?	Yes, Woods Valldata's password policy requires a minimum of 12 characters, complex passwords, password change history restrictions and forced password changes at intervals that align, at the bare minimum, with PCI DSS, restrictions.
38.	Does your organisation require strong authentication such as multi factor authentication (MFA) when accessing systems supporting the client or the client's information from an untrusted location?	Yes, MFA is enforced for: • remote network access originating from outside the Woods Valldata network. • internally for non-console administrative access. Clients can enable MFA when accessing the WV SFTP site, this is an end-user configurable option and not set at system level to enable users to use their preferred method of MFA. Other portals such as Contact Manager and DAT are restricted to the client's IP address; work is underway however to enable MFA on these portals so that IP restrictions to be lifted. MFA is also in the process of being implemented and rolled out to the following systems: • Lottery client portal for both internal and external users. • internal systems processing cardholder data.
Vulnerability Management		
39.	How does your organisation maintain secure systems and applications, and identify new threats and exploitation techniques?	WV adopts a layered approach to this which consists of posture checking, vulnerability management, patch management, SIEM, system hardening, network segmentation and change control. The processes and systems associated with these technical control measures are verified as part of the various external audits, tests and scans WV is subject to as well as part of the monthly IT Compliance reviews conducted by the HoC.

Ref	Question	Woods Valldata's Response
40.	How often does your organisation scan and test systems for security vulnerabilities?	Monthly internal and external vulnerability scans are performed, as well as continuous posture checking of software and activity. Penetration tests are conducted at least annually on all internal and external networks. In addition, six monthly segmentation testing is conducted on internal and external networks in scope of the WV's PCI cardholder data environment.
41.	What timescales does your organisation operate to implement mitigations to vulnerabilities?	This is dependent on a variety of factors such as severity, whether it is exploitable, whether there is a mitigation available etc. but it would always be in-line with PCI DSS requirements at the very least whether it is in-scope of PCI DSS or not. The HoC verifies as part of the monthly IT Compliance reviews that vulnerabilities are being addressed in line with the WV policy.
42.	How often does your organisation apply updates or patches?	A patch management tool is used to either automatically push the update out once approved or identify machines that need for it to be applied manually. Any software that cannot be managed via the patch management tool such as firmware on network infrastructure is checked at least monthly to identify any available updates. When a patch is released by a vendor it is assessed based on the target device, severity, testing required etc. therefore some patches may take longer than others to be applied but all patches would be applied in-line with PCI DSS requirements at the very least whether it is in-scope of PCI DSS or not. The HoC verifies as part of the monthly IT Compliance reviews that patches are being applied in line with the WV policy.

Ref	Question	Woods Valldata's Response
43.	How often does your organisation maintain and update anti-virus software?	WV utilises a cloud-based solution for malicious code protection which pushes updates out multiple times a day. Weekly reports are generated to identify any machines that have not connected to the solution within the last 7 days, as well as any machines not running the software. All systems in use within WV has malicious code protection software installed. As part of the monthly IT Compliance review the HoC verifies that machines flagged on the weekly reports and alerts are being addressed accordingly.
44.	Please provide details of the network and server architecture which forms part of the service delivery platform/infrastructure and where this will be located?	We do not provide this level of information; this is deemed confidential restricted due to the possibility it can be used by cyber criminals to target malicious activity against Woods Valldata's infrastructure. Our network and server infrastructure are assessed by external auditors as part of our PCI DSS, ISO 27001 and GC RTS external audits to ensure applications and software are still supported, that patches are being applied, including firmware, and that vulnerabilities are being addressed etc.
45.	Can you confirm that penetration testing is performed by a CREST and/ or CHECK registered penetration tester?	Yes, Woods Valldata uses URM Consulting Limited.
Acquisition, Development and Change Management		
46.	Please provide details the organisations' approach to IT service delivery, software development including the use of specific methodologies. For example: Prince2; ITIL (list others).	Woods Valldata aligns its processes with the following methodologies: • Agile • ITIL • SCRUM • Prince2 • Plan Do Check Act
47.	How does your organisation manage changes to systems that may impact clients?	A formal Change Management process is followed within Woods Valldata to ensure changes are made in line with regulatory, contractual and internal requirements.

Ref	Question	Woods Valldata's Response
		The Process covers system development, system acquisition, infrastructure (physical and IT), business and process change as well as requests received from Charity partners relating to changing or adding to their service offering. This Change Management process is externally verified as part of WV's PCI DSS, GC RTS and ISO 27001 audits.
48.	Please provide details of the applications/software architecture which forms part of the service delivery platform/infrastructure.,	In the main applications used in the provision of services to clients is hosted and developed in house. Any OTS application or cloud services used either internally and/or in the delivery of the services to clients would undergo the necessary scans, testing and due-diligence to ensure they remain in-support, patches are applied, and the necessary scans and technical testing is conducted. All applications and cloud services used by WV are in-scope of WV's ISO 27001 and GC RTS external audits, and where necessary PCI DSS assessment, all of which verify that they being developed securely and using supported methodologies and frameworks. Where a cloud service processes personal data then this would be specified within the Statement of Works for that service.
49.	Is development carried out with secure coding standards techniques? Please specify which resources you consult for secure coding techniques.	Yes, this is a mandatory control of PCI DSS and ISO 27001. OWASP is one of the resources utilised.
50.	What configuration management processes are in place to ensure the integrity of the solution through development, testing and deployment?	As part of any development process the requirements, including confidentiality, integrity and availability (CIA) elements of information are defined. All development changes are code reviewed by another developer and then tested by another team before being tested as part of UAT. Additional post deployment testing or verification or monitoring would be implemented post deployment. This is as per the formal development and test policy and processes which are validated as part of our PCI DSS, ISO 27001 and GC RTS audits.
51.	How does your organisation maintain a formal program to document an owner of all technology systems and	Information Asset Owners (IAO) are assigned to all systems or data; this is recorded within the Role Based Profile matrix to ensure access to

Ref	Question	Woods Valldata's Response
	assets for the purposes of maintaining accountability over management of a client's information?	those systems or Data is approved by the IAO, and where necessary the Head of Compliance. The Head of Compliance has oversight of all access requests, is on the ICT change Board and responsible for approving all third-party access. Also, only a member of the Compliance Team has permissions to update the Role Based Profile matrix.
52.	How does your organisation maintain a formal program to regularly test the design, implementation and operation of technology controls? How often is this updated?	A monthly IT compliance review is conducted by the Head of Compliance to verify technical controls are working as required. In addition, security requirements are defined and agreed as part of the design, acquisition, and development process, which are also verified as part of the change control approval process. Configuration standards would form part of the security requirements, these are based on industry standards and these standards are reviewed at least annually to ensure they reflect industry best practice. In addition, vulnerability assessments are carried out after an upgrade or deployment, and where necessary a Pen Test is also conducted to verify no new vulnerabilities have been introduced and segmentation controls remain in place.
Incident Management and Business Continuity		
53.	What monitoring is in place to identify and prioritise indications of potential malicious activity?	Realtime monitoring and alerting tools are in place across all firewalls and systems analysing activity, events, file integrity monitoring etc. Realtime alerts would be generated to notify the support personnel.
54.	Does your organisation maintain a formal program for capturing, monitoring and alerting on logs from technology systems?	Yes, logs are harvested, monitored and alerted on in real-time. All logs are kept for 12 months in line with PCI DSS requirements. Alerts would be escalated in line with company's Incident Reporting, Escalation and Management Process.
55.	What incident management processes are in place within your organisation for reporting and responding to security incidents or service issues?	WV Incident Reporting, Escalation and Management Process in place to ensure all events and incidents, whether security, availability or integrity related are reported and escalated based on severity.
56.	What processes are in place within your organisation to deal with a major incident?	All incidents, no matter the severity would be reported and escalated as per the Incident Reporting, Escalation and Management Process.

Ref	Question	Woods Valldata’s Response
		Where appropriate the Incident Management Team would be invoked to oversee and manage a major incident.
57.	Please provide details of your organisation’s business continuity management process and plans.	Please refer to the Woods Valldata Business Continuity Management document on the resilience, redundancy and recovery measures in place as well as details of the Incident Management Team.
58.	How often is the business continuity plan tested?	The Incident Management and Business Continuity Plan is tested at least annually or after significant change. This is verified as part of Woods Valldata’s PCI DSS, GC RTS and ISO 27001 annual audits.
59.	Does the organisation maintain a formal program for the backup and restoration of information?	Yes, the frequency and type of back-up is dependent on the rate of change to the data and/or system and can range from every 10 minutes (transactional logs) to every 24 hours. Data stored on site at our Chippenham office is backed up to a device on-site before synchronising to a cloud back-up. Data stored in the cloud is backed up to the cloud. A schedule of restores is in place to validate not only full system restores but data restores.
60.	Has your organisation had to report a data breach or security incident in the last 12 months to a regulatory body, and if yes, specify whether any personal data was lost in the breach?	No.
61.	Has the ICO or any regulatory body issued either a notice to improve or a statutory fine to your organisation?	No.
62.	Has your organisation experienced any personal data breaches in the past 12 months that were not reportable to the ICO or any regulatory body? If so, how many and what caused them, and how many data subjects were affected?	Due to the manual nature of some of the tasks, e.g. hand enclosing, there have been instances of double enclosures or mis matched enclosures. Checks are in place to prevent these from happening, but human error cannot be eradicated completely. The types of personal data involved in the breaches fall into one of the following: • Name and address only • Name, address, sort code and partial bank account number.

Ref	Question	Woods Valldata’s Response
		• Name, sort code and full bank account number. There have been no breaches of cardholder data, sensitive / special category personal data.