Audit Type:	Remote Stage Two Audit
Organisation:	Mentoring West Midlands Community Interest Company
Address:	Suite 6, Graphic House , 15-18 New Rd , Willenhall , West Midlands , WV13 2BG
Standard(s):	BS EN ISO/IEC 27001:2017
Client Representative(s):	Mr Chris Dyer
Total number of employees:	19
Site(s) audited:	As Above
Date of Audit:	06 February 2023 (2) days
Lead Auditor:	Angus McBain
Full Audit Team:	Angus McBain, Muzaffar Mirza

This report is confidential and distribution is limited to the audit team, client representative and the British Assessment Bureau (BAB) office.

Section A: Audit Objectives

Stage 2 Audit

- to confirm that the management system conforms with all of the requirements of BS EN ISO/IEC 27001:2017;
- to confirm the Scope statement; represents the organisation's certified activities on the Certificate of Registration;
- to confirm that the organisation has effectively implemented BS EN ISO/IEC 27001:2017;
- to confirm that the Management System is capable of achieving the organisation’s policies and objectives;
- to review links between the internal audits, management reviews and continuous improvement

Section B: Scope(s) of certification

Provision of professional mentoring services aimed at high risk offenders and other challenging and vulnerable groups across the UK.

Section C: Current audit findings and conclusions

The BAB Audit Team conducted a process-based audit, focussing on significant aspects, risks and objectives as required by BS EN ISO/IEC 27001:2017.

The audit methods used were interviews, observation of activities and review of documentation and records.

The structure of the audit was in accordance with the audit plan and audit planning process.

Number of nonconformities identified	0	Major	0	Minor
Number of opportunities for improvement identified	3			

Based on the results of this audit and the system's demonstrated state of development and maturity, management system certification is recommended. This recommendation will be independently verified by the British Assessment Bureau Head Office.

Section D: Audit Findings

Clause : Opening Meeting and Close out of previous findings

The opening meeting was attended by Chris Dyer (MD) Tracy Jennings (Business Administrator) and Angus McBain and Muzaffar Mirza (BAB). There were no Health and Safety issues raised that would affect the audit.
This audit is being completed remotely. All evidence has either been seen electronically or via video link and interviews have been carried out with top management and employees via digital platforms where possible. Where this could not be completed electronically, findings have been raised to be reviewed at the next audit. Based on the complexity of the business the full audit has been completed remotely in the allotted timeframe

Clause 4: Context of the Organisation

Mentoring West Midlands Community Interest Company are a Private limited Company, Community Interest Company (CIC) incorporated on 10 December 2012.
They specialise in providing mentoring and support across the West Midlands. Their work involves direct engagement with men and women, who commit serious crimes, or work with family members who are affected by these circumstances. Within this they engage with long term unemployed, and those out of education, with a particular focus on people coming from complex and challenging backgrounds. Currently, assisting people back into work, vocational training and education makes up approximately fifty per cent of their work. They are passionate about focusing on the importance of strong and positive role models and direct a lot of our energies towards supporting people, young and old, to make better informed decisions about their behaviour and in turn understanding how their actions and thinking affects others.

Mentoring West Midlands Community Interest Company (MWM) have become increasingly aware of the value and importance of information they hold and therefore the need to deliver a high level of security to Information and Communications Technology (ICT) systems and paper records stores. The organisation have reviewed and analysed key aspects of itself and its stakeholders to determine the strategic direction of the company. Through this Management Strategic Planning process they have made the decision to look to maintain ISO 27001 certification. The adoption of a formal standard such as ISO 27001 is designed to support a consistent, effective and secure management system that meets their legal obligations and demonstrates their commitment to good Information Security practices.

The scope of the management system has been established as ‘Provision of professional mentoring services aimed at high risk offenders and other challenging and vulnerable groups across the UK’ and it is reflected in their Mentoring Guidance Document, v36.

Interested parties have been documented in the ISMS and these include:
• Customers- Genus service users, ETE service users: Delivery of high-quality support/mentoring, delivery of accredited courses. Efficient and professional service and readily available staff. Adhere to all regulations i.e. HSE, HR, GDPR and NCFE.
• External providers: Continuation of services, new areas of work, prompt payments per Terms and Conditions. Good long-term relationships.
• Staff: Continuation of job, wages paid on time, professional development, promotion opportunities within MWM, good communication
• Owner/MD: No fines/Offences

Internal and external factors have been documented and examples include:
• Internal: Faulty Electrical Equipment
• External: Unauthorised access to building

The Management System is well structured and reflects the operational processes through documented procedures included in the company’s ISMS, with clearly identified inputs and outputs throughout.

Clause 5: Leadership

Leadership is clear at MWM, which was demonstrated at the opening meeting with Chris Dyer (MD) and Tracy Jennings (Business Administrator) both of whom attended the audit. Chris and Tracy are committed to continually improving the management of the Information Security Management System, and the Information Security policy.
The employees are communicated with as part of the induction process, security procedures and security awareness training along with meetings where the organisation’s operations as well as the data security management will be covered. Updates are usually via email. Documents are held on their secure system (Advice Pro). A communication relating to the management system was seen, dated 26-01-2023.

They demonstrate their commitment to continual improvement with regular performance reviews, internal audits, management reviews and customer liaison.

The Information Security Policy and associated policies in place and are regularly reviewed and maintained by Top Management as per the documented information procedure. The Information Security Policy is dated 01-2023 and signed by the MD.
Some examples of related ISMS policies and evidence of the above include:
• Access Control Policy 01-2023
The above policies are readily available to all staff via their secure system (Advice Pro) and are also covered at Induction. Please refer to clause 7 of this report for further information on this process.
A communication was seen dated 24-01-2023 relating to the ISMS.

Relevant SOA Controls evidenced: A5.1.1, A5.1.2

An organisational chart was evidenced; this was seen to be at and job
descriptions are in place. It was observed that roles and responsibilities applicable to ISMS were clearly defined. This was evidenced against the below samples:
• Business Administrator: TJ
• MD: CD
• ISO: CD

Relevant SOA Controls evidenced: A6.1.1, A6.1.2

Clause 6: Planning

They have a Risk Register that fully covers the CIA considerations. Risks include:
• Risk: Unauthorised access to building. Risk is 8 (CIA)
• Controls: Intercom access to main building and different key coded access to office areas, specific members of staff only have full sets of keys and fob/code for alarm system. Remaining staff permanently located at the hub have main front door key only, which can only be used once alarm has been deactivated and other locks opened. CCTV in place 24 hours a day, which MD can access remotely as and when required. In place is a clear desk policy, door locks, locked filing cabinets. Access to all other staff and visitors via intercom at main external front door, then allowed access to specific areas within building depending on purpose of visit. Whole building is alarmed. Agreement in place with Securitas for out of hours response in the event of security alarm activation.
• Risk: Unauthorised Access to laptops. Risk is 9 (CIA)
• Controls: Password controlled. Data back-up - one with all files saved onto Microsoft OneDrive, other with De facto as back up
• Risk: Malware attack. Risk is 24 (CIA)
• Controls: Firewalls, Anti-virus software
Their risks are monitored and reviewed and discussed at management reviews.

The organisation has determined their risk methodology for evaluation of information security asset groups. The application of CIA in terms of their asset groups have been noted, with examples being:
• A.8.1.1 Inventory of Assets: All employees sign a asset form when assets are issued and countersign
• A.8.1.3: Acceptable use of assets: All policies and procedures for acceptable use is documented in the Mentoring Guidance Document and as part of the full induction, and is communicated regularly to existing staff, via staff meetings. Asset form details responsibility for 'owner' whilst in charge of the equipment issued.
• A.8.2.3: Handling of assets: Outlined in the Mentoring Guidance Document, v36
• A.8.3.1: Management of removable media: Removable media is strictly controlled, and all assets are signed out and in and witnessed by a third party. The asset list is kept electronically and manually, which is kept locked away, with only senior management access. All laptops are password controlled and no personal information is allowed to be stored on them. Staff have individual MWM mobile phones which require a pin number to access. Staff have their own individual work area on Advice Pro to store documents. Staff have been issued with combination lock secure cases to transfer files.
• A.11.2.5: Removal of assets: Staff who are homebased are issued with a MWM laptop, printer, scanner, combination lockable case, shredder etc via an asset form, required to sign for it and allowed to remove them. They are signed out. No data is stored locally on the laptops and all laptops are password protected. Staff are requested to save documents into their individual area on Advice Pro. GDPR followed and adhered to (see GDPR folder and individual HR files)"
Further considerations include:
• Risk: Unauthorised Access to laptops. Risk is 9 (CIA)

• Controls: Password controlled. Data back-up - one with all files saved onto Microsoft OneDrive, other with De facto as back up

The Risk Treatment Plan has been defined within the ISMS. The definition includes reference to the required headings within Annex A of the ISO 27001:2013 Standard.
The Statement of Applicability, version 8, dated 01-2023 was noted to have identified controls to mitigate risks following identification, analysis and evaluation and was evidenced.
Some controls are not documented within this section as they are covered elsewhere in the report.
The following was observed:
• A 6.1.3 Contact with authorities.
• Objective: Appropriate contacts with relevant authorities shall be maintained.
• Reason for Selection: BR/BP
• Auditor Note / evidence: Due to the nature of our organisation we are required to update authorities on a regular basis. Either Face-to-Face, via email or via CJSM. All SLA's adhered to.
• A 6.1.4 Contact with special interest groups.
• Objective: Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintain
• Reason for Selection: BR/BP
• Auditor Note / evidence: This can be a requirement of an SLA , the MD to authorise and act as main point of contact.
• A 6.1.5 Information security in project management.
• Objective: Information security shall be addressed in project management, regardless of the type of the project
• Reason: BR
• Auditor Note / evidence: Due to the highly sensitive nature of our work we have the same level of controls regardless of the project.
• A 6.2.1 Mobile device policy.
• Objective: A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.
• Reason for Selection: BR
• Auditor Note/evidence: Outlined in the Mentoring Guidance Document section 5
• Mobile phone contract with O2 with admin dashboard. Increased vigilance on accessing records for mobile phones
• A 6.2.2 Teleworking.
• Objective: A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking.
• Reason for Selection: BR/BP
• Auditor Note/evidence: If staff are required to write a document about a service user/case on their own IT system then this must be uploaded as an attachment immediately. The original document on their IT system must then be destroyed immediately so only the secure, online version remains.
• A8.3.1 Management of removable media.
• Objective: Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.
• Reason for implementation: BR/BP
• Auditor Note/evidence: Removable media is strictly controlled, and all assets are signed out and in and witnessed by a third party. The asset list is kept electronically and manually, which is kept locked away, with only senior management access. All laptops are password controlled and no personal information is allowed to be stored on them. Staff have individual MWM mobile phones which require a pin number to access. Staff have their own individual work area on Advice Pro to store documents. Staff have been issued with combination lock secure cases to transfer files."
• A8.3.2 Disposal of media. Objective: Media shall be disposed of securely when no longer required, using formal procedures.
• Reason for implementation: BR/BP
• Auditor Note/evidence: Laptops are handed back in when an employee leaves or are no longer needed. They are checked before being reissued or stored in a lockable filing cabinet in the office or if become obsolete are wiped clean and disposed off via an professional contractor. A certificate is then issued.
• A8.3.3 Physical media transfer.
• Objective: Media containing information shall be protected against unauthorized access, misuse or corruption during transportation.
• Reason for implementation: BR/BP
• Auditor Note/evidence: All media to be uploaded electronically onto Advice Pro and then destroyed. Staff outside of the Head Office have secured lockable cases to use for the transfer of documents if and when required.

• A9.2.6 Removal or adjustment of access rights.
• Objective: The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.
• Reason for implementation: BR/BP
• Auditor Note/evidence: Access to Advice Pro and emails are removed on termination of employment. External party users are strictly monitored and restricted.
• A9.3.1 Use of secret authentication.
• Objective: Users shall be required to follow the organization's practices in the use of secret authentication information
• Reason for implementation: BR/BP
• Auditor Note/evidence: User Agreement Policies in place and are outlined with each log in to Advice Pro.
• A9.4.1 Information access restriction.
• Objective: Access to information and application system functions shall be restricted in accordance with the access control policy.
• Reason for implementation: BR/BP
• Auditor Note/evidence: Advice Pro is restricted to active project involvement only. CJSM email system used for all relevant information sharing.
• A9.4.2 Secure log-on procedures.
• Objective: Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure,
• Reason for implementation: BR/BP
• Auditor Note/evidence: Advice Pro is restricted to active project involvement only.
• CJSM email system used for all relevant information sharing.
• A9.4.3 Password management system.
• Objective: Password management systems shall be interactive and shall ensure quality passwords,
• Reason for implementation: BR/BP
• Auditor Note/evidence: Advice Pro is restricted to active project involvement only. CJSM email system used for all relevant information sharing.
• A9.4.4 Use of privileged utility programs.
• Objective: The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.
• Reason for implementation: BR/BP
• Auditor Note/evidence: Only MD/ ISM have overriding access. All page views can be monitored.
• A9.4.5 Access control to program source code.
• Objective: Access to program source code shall be restricted.
• Reason for implementation: BR/BP
• Auditor Note/evidence: No source code is kept on premises, but if ever the occasion arises where it is, it would fall under the remit of the Information Security Officer, and as such, access would be restricted.
• A10.1.1 Policy on the use of cryptographic controls.
• Objective: A policy on the use of cryptographic controls for protection of information shall be developed and implemented.
• Reason for implementation: BR/BP
• Auditor Note/evidence: Passwords are set for access to any data kept on any server. Service User personal data is only sent via Secure mail (CJSM). Passwords sent to the intended recipient only. 256-bit encryption for Advice Pro. 256-bit encryption for CJSM, email and 1 and 1 email
• A10.1.2 Key management.
• Objective: A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.
• Reason for implementation: BR/BP
• Auditor Note/evidence: Sign in agreement every time a user signs in to Advice Pro.
• A11.1.1 Physical security perimeter.
• Objective: Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.
• Reason for implementation: BR/BP
• Auditor Note/evidence: Key controlled access set for authorised members of staff with a full set of keys for the building. MD, Operations Manager and Business Administrator have keys. All visitors and staff access the building via intercom at the main front door. Access to MD and admin offices is restricted and kept locked unless there is more than one member of staff. If a person is working alone then the door is kept locked. MWM office is triple locked and access controlled via intercom with CCTV in place. A signing in/out form in head office as soon as you enter is to be completed by all staff and visitors.
• A11.1.2 Physical entry controls.

• Objective: Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.
• Reason for implementation: BR/BP
• Auditor Note/evidence: Key controlled access set for authorised members of staff with a full set of keys for the building. MD, Operations Manager and Business Administrator have keys. All visitors and staff access the building via intercom at the main front door. Access to MD and admin offices is restricted and kept locked unless there is more than one member of staff. If a person is working alone then the door is kept locked. MWM office is triple locked and access controlled via intercom with CCTV in place. A signing in/out form in head office as soon as you enter is to be completed by all staff and visitors.
• A11.1.3 Securing offices, rooms and facilities.
• Objective: Physical security for offices, rooms and facilities shall be designed and applied.
• Reason for implementation: BR/BP
• Auditor Note/evidence: Key controlled access set for authorised members of staff with a full set of keys for the building. MD, Operations Manager and Business Administrator have keys. All visitors and staff access the building via intercom at the main front door. Access to MD and admin offices is restricted and kept locked unless there is more than one member of staff. If a person is working alone then the door is kept locked. MWM office is triple locked and access controlled via intercom with CCTV in place. A signing in/out form in head office as soon as you enter is to be completed by all staff and visitors.
• A11.1.4 Protecting against external and environmental threats.
• Objective: Physical protection against natural disasters, malicious attack or accidents shall be designed and applied.
• Reason for implementation: BR/BP
• Auditor Note/evidence: Advice Pro's on-line access means that in the event of natural or malicious attack, business continuity would not be affected on a day-to-day basis. With a double penetration test being conducted it is more secure against malicious attacks. If a flood was to arise at head office, precautions will be put in place.
• A11.1.5: Working in secure areas
• Objective: Procedures for working in secure areas shall be designed and applied
• Reason: BR/BP
• Auditor Note/evidence: Clear desk policy for all employees. When a desk is left unattended any sensitive information must be closed off. Only the MD. Operations Manager and Business Administrator have keys to unlock the building.
• A11.1.6 Delivery and loading areas.
• Objective: Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.
• Reason for implementation: BR/BP
• Auditor Note/evidence: When orders are placed, instructions are given to use the intercom at the front door on arrival, then deliveries are brought upstairs to the office and signed for during business hours.
• A11.2.1 Equipment siting and protection.
• Objective: Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.
• Reason for implementation: BR/BP.
• Auditor Note/evidence: All MWM computers are password protected. All information is uploaded to Advice Pro and then wiped off laptops; All central files created by the Business Administrator are stored on the password protected One Drive, which is only accessible by the Director (ISM), Business Administrator and the Administrative Officer. Hard copy files are discouraged but when unavoidable e.g. due to partner requirements some items are stored away in locked filing cabinet, but this is only for short periods e.g. NCFE documents, workbooks. Sampling of files on laptops takes place randomly.
• A11.2.2. Supporting utilities.
• Objective: Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.
• Reason for implementation: BR/BP
• Auditor Note/evidence: Software back up and Advice Pro policy. Staff issued with surge protected extension leads to use at all times with MWM equipment issued.
• A11.2.3. Cabling security.
• Objective: Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage.
• Reason for implementation: BR/BP
• Auditor Note/evidence: All cabling is done with CAT6 cabling which contains and uses all 4 copper wires.
• A11.2.4. Equipment maintenance.
• Objective: Equipment shall be correctly maintained to ensure its continued availability and integrity.
• Reason for implementation: BR/BP
• Auditor Note/evidence: All equipment PAT tested
• A11.2.5. Removal of assets.
• Objective: Equipment, information or software shall not be taken off-site without prior authorization.

• Reason for implementation: BR/BP
• Auditor Note/evidence: Staff who are homebased are issued with a MWM laptop, printer, scanner, combination lockable case, shredder etc via an asset form, required to sign for it and allowed to remove them. They are signed out. No data is stored locally on the laptops and all laptops are password protected. Staff are requested to save documents into their individual area on Advice Pro. GDPR followed and adhered to (see GDPR folder and individual HR files)
• A11.2.6. Security of equipment and assets off-premises.
• Objective: Security shall be applied to off-site assets taking into account the different risks of working outside the organization's premises.
• Reason for implementation: BR/BP
• Auditor Note/evidence: Staff who are homebased are issued with a MWM laptop, printer, scanner, combination lockable case, shredder etc via an asset form, required to sign for it and allowed to remove them. They are signed out. No data is stored locally on the laptops and all laptops are password protected. Staff are requested to save documents into their individual area on Advice Pro. GDPR followed and adhered to (see GDPR folder and individual HR files)
• A11.2.7. Secure disposal or reuse of equipment.
• Objective: All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.
• Reason for implementation: BR/BP
• Auditor Note/evidence: Data Protection Act, GDPR, WEEE regulations
• A11.2.8. Unattended user equipment.
• Objective: Users shall ensure that unattended equipment has appropriate protection.
• Reason for implementation: BR/BP
• Auditor Note/evidence: Only access the system when alone or with another member of MWM contracted staff. If away from computer, always log out to ensure no-one else can view or access information.
• A11.2.9. Clear desk and clear screen policy.
• Objective: A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.
• Reason for implementation: BR/BP
• Auditor Note/evidence: This is set out in the Mentoring Guidance Document and Homeworking Policy and a "sterile corridor" of case management is a fundamental basis of our work and ethos.
• A12.1.1 Documented operating procedures.
• Objective: Operating procedures shall be documented and made available to all users who need them.
• Current Control: Mentoring Guidance Document
• Reason for implementation: BR
• Overview of implementation: Mentoring Guidance Document and sign in for CJSM, Advice Pro and VIA Learning Centre
• Auditor Note: Mentoring Guidance Document, v36 and sign in for CJSM, Advice Pro and VIA Learning Centre
• A12.1.2. Change management.
• Objective: Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.
• Reason for implementation: BR
• Auditor Note/evidence: Changes to the organisation, business processes, information processing facilities and systems that affect information security are put through the ISM and Director, these are reported back to the Advisory Group as and when required. Documentation is version controlled and noted in each index. See GDPR folder/MWM Policy and Guidance folder for examples of version control.
• A12.1.3. Capacity management
• Objective: The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.
• Reason for implementation: BR
• Auditor Note/evidence: Internal monitoring is used. Advice Pro has an unlimited capacity so there will not be an issue storing data.
• A12.1.4. Separation of development, testing and operational environments.
• Objective: Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.
• Reason: BR
• Auditor Note/evidence: Advice Pro Access means that all new areas are access controlled.
• A12.2.1. Controls against malware.
• Objective: Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.
• Reason: BR

• Auditor Note/evidence: User Agreement and windows Defender. We only use Chrome to ensure that we have a secure connection. Passwords are never saved on a device. No personal information is stored on a work device.
• A12.3.1. Information backup.
• Objective: Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.
• Reason for implementation: BR
• Auditor Note/evidence: Only Secure online versions of documentation to be kept.
• Advice Pro is backed up nightly with physical building and network infrastructure compliant with ISO27001.
• A12.4.1. Event logging.
• Objective: Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.
• Reason for implementation: BR/BP
• Auditor Note/evidence: Only Secure online versions of documentation to be kept. Advice Pro is backed up nightly with physical building and network infrastructure compliant with ISO27001.
• A12.4.2. Protection of log information.
• Objective: Logging facilities and log information shall be protected against tampering and unauthorized access.
• Reason for implementation: BR/BP
• Auditor Note/evidence: Advice Pro Log in sent by secure email and changed on first use
• A12.4.3. Administrator and operator logs.
• Objective: System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.
• Reason for implementation: BR/BP
• Auditor Note/evidence: Advice Pro page views and edits can be monitored.
• A12.4.4. Clock synchronisation.
• Objective: The clocks of all relevant information processing systems within an organization or security domain shall be synchronised to a single reference time source.
• Reason for implementation: BR/BP
• Auditor Note/evidence: Advice Pro will control this
• A12.5.1. Installation of software on operational systems.
• Objective: Procedures shall be implemented to control the installation of software on operational systems.
• Reason for implementation: BR/BP
• Auditor Note/evidence: Software only to be installed by MD or ISM with MD agreement.
• A13.1.1. Network controls.
• Objective: Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimise disruptions to business processes.
• Reason for implementation: BR/BP
• Auditor Note/evidence: Not on a network
• A13.1.2. Security of network services.
• Objective: Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.
• Reason for implementation: BR/BP
• Auditor Note/evidence: Not on a network
• A13.1.3. Segregation in networks.
• Objective: Groups of information services, users and information systems shall be segregated on networks.
• Reason for implementation: BR/BP
• Auditor Note/evidence: Not on a network
• A13.2.1. Information transfer policies and procedures.
• Objective: Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.
• Reason for implementation: BR/BP
• Auditor Note/evidence: If the need arises for service user information to be transferred manually, staff have been issued with combination locking transfer cases. Otherwise, any service user information including passwords are transmitted to the recipient only through secure email, Advice Pro or CJSM. Migration of information will be managed securely through CJSM
• A13.2.2. Agreements on information transfer.
• Objective: Agreements shall address the secure transfer of business information between the organization and external parties.
• Reason for implementation: BR/BP
• Auditor Note/evidence: If the need arises for service user information to be transferred manually, staff have been issued with combination locking transfer cases. Otherwise, any service user information including passwords are transmitted to the

recipient only through secure email, Advice Pro or CJSM.
• A13.2.3. Electronic messaging.
• Objective: Information involved in electronic messaging shall be appropriately protected.
• Reason for implementation: BR/BP
• Auditor Note/evidence: E-mail disclaimers are used. Sensitive Information is sent via CJSM secure email.
• A13.2.4. Confidentiality or nondisclosure agreements.
• Objective: Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, regularly reviewed and documented.
• Reason for implementation: BR/BP
• Auditor Note/evidence: Legal requirement and fundamental nature of our organisation to keep information protected. GDPR legislation - retention of data, privacy notices
• A14.1.1. Information security requirements analysis and specification.
• Objective: The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.
• Reason for implementation: BR/BP
• Auditor Note/evidence: Legal requirements, CJSM, Advice Pro including certification, closure and deletion of files, staff individual areas, use of task functionality within Advice Pro, 1and1 secure email, GDPR
• A14.1.2. Information security requirements analysis and specification.
• Objective: Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.
• Reason for implementation: BR/BP
• Auditor Note/evidence: No application services are passed over public networks
• A14.1.3. Protecting application services transactions.
• Objective: Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.
• Reason for implementation: BR/BP
• Auditor Note/evidence: No application services transactions are used.
• A14.2.1. Secure development policy.
• Objective: Rules for the development of software and systems shall be established and applied to developments within the organization.
• Reason for implementation: BR/BP
• Auditor Note/evidence: No software development is used within MWM
• A14.2.2. System change control procedures.
• Objective: Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures.
• Reason for implementation: BR/BP
• Auditor Note/evidence: No software development is used within MWM
• A14.2.3. Technical review of applications after operating platform changes.
• Objective: When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.
• Reason for implementation: BR/BP
• Auditor Note/evidence: Any changes to be agreed and approved by management meetings and must follow Caldicott Principles, GDPR
• A14.2.4. Restrictions on changes to software packages.
• Objective: Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.
• Reason for implementation: BR/BP
• Auditor Note/evidence: Requires MD approval
• A14.2.5. Secure system engineering principles.
• Objective Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts.
• Current Control: Not Used
• Reason for implementation: BR/BP
• Overview of implementation: Not Used
• Auditor Note: Not Used
• A14.2.6. Secure development environment.
• Objective: Organizations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.

• Reason for implementation: BR/BP
• Auditor Note/evidence: No software development is used within MWM
• A14.2.7. Outsourced development.
• Objective: The organization shall supervise and monitor the activity of outsourced system development.
• Reason for implementation: BR/BP
• Auditor Note/evidence: No software development is used within MWM
• A14.2.8. System security testing.
• Objective: Testing of security functionality shall be carried out during development.
• Reason for implementation: BR/BP
• Auditor Note/evidence: No software development is used within MWM
• A14.2.9. System security testing.
• Objective: Testing of security functionality shall be carried out during development.
• Reason for implementation: BR/BP
• Auditor Note/evidence: No software development is used within MWM
• A14.3.1. Protection of test data.
• Objective: Test data shall be selected carefully, protected and controlled.
• Reason for implementation: BR/BP
• Auditor Note/evidence: No test data is used
• A15.1.1. Information security policy for supplier relationships.
• Objective: Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented.
• Current Control: Advice Pro SLA/Data Policy
• Reason for implementation: BR/BP
• Overview of implementation: Supplier relationships are such that contracts and formal SLA's are in place.
• Auditor Note: Advice Pro SLA/Data Policy
• A15.1.2. Addressing security within supplier agreements.
• Objective: All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information
• Reason for implementation: BR/BP
• Auditor Note/evidence: Advice Pro SLA/Data Policy
• A15.1.3. Information and communication technology supply chain.
• Objective: Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.
• Reason for implementation: BR/BP
• Auditor Note/evidence: Advice Pro SLA/Data Policy
• A15.2.1. Monitoring and review of supplier services.
• Objective: Organizations shall regularly monitor, review and audit supplier service delivery.
• Reason for implementation: BR/BP
• Auditor Note/evidence: All Suppliers to be approved by the MD in advance of working on behalf of MWM, no background information is shared on service users.
• A15.2.2. Managing changes to supplier services.
• Objective: Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.
• Reason for implementation: BR/BP
• Auditor Note/evidence: Whenever failures in SLA's or service failures leading to near SLA breaches happen as a direct result of the suppliers failings a review of supplier practices and suitability is carried out, and alternative suppliers are sought.
• A16.1.1. Responsibilities and procedures. Objective: Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.
• Reason for implementation: BR/BP
• Auditor Note/evidence: All issues to be reported to MD/ISM in first Instance
• A16.1.2. Reporting information security events.
• Objective: Information security events shall be reported through appropriate management channels as quickly as possible.
• Reason for implementation: BR/BP
• Auditor Note/evidence: All issues to be reported to MD/ISM in first Instance. Advice Pro keeps an auditable footprint of all changes.
• A16.1.3. Reporting information security weaknesses.
• Objective: Employees and contractors using the organization's information systems and services shall be required to note and

report any observed or suspected information security weaknesses in systems or services.
• Reason for implementation: BR/BP
• Auditor Note/evidence: All issues to be reported to MD/ISM in first Instance. Advice Pro keeps a footprint of all changes / page views , edits and Log In attempts etc. User agreement signed each time someone logs into Advice Pro. Access can be immediately halted remotely.
• A16.1.4. Assessment of and decision on information security events.
• Objective: Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.
• Reason for implementation: BR/BP
• Auditor Note/evidence: Dependant on the severity of breach / security incident, access to Advice Pro is centrally controlled so changes to or the removal of access to the system is ultimately managed by the MD/ISM.
• A16.1.5. Response to information security incidents.
• Objective: Information security incidents shall be responded to in accordance with the documented procedures.
• Current Control: Mentoring Guidance Document
• Reason for implementation: BR/BP
• Overview of implementation: Outlined in the Mentoring Guidance Document i.e potential disciplinary action taken against individual. Due to the nature of the information we deal with all staff adhere to Caldicott Principles, GDPR.
• Auditor Note: Mentoring Guidance Document, v36
• A16.1.6. Learning from information security incidents.
• Objective: Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.
• Reason for implementation: BR/BP
• Auditor Note/evidence: Incidents are discussed in Management Meetings and fed back to Team meetings if action is needed.
• A16.1.7. Collection of evidence.
• Objective: The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.
• Reason for implementation: BR/BP
• Auditor Note/evidence: Logs and events are stored in Advice Pro. Email threads are saved and stored in HR files if deemed relevant

.

The SoA was observed to be on version 8, dated 01-2023

ISMS objectives have been identified and documented within the Mentoring Guidance Document, version 36.
They include:
• Target: To achieve ISO27001 and retain the necessary internal systems and processes to manage the maintenance of the standard and create an environment of continuous improvement both operational and in terms of policy and procedure
• Measure: Certification with a UKAS-accredited Certification Body
• Target: Zero ICO reportable incidents
• Measure: Management review, supported via ISSG meetings and annual audit process supported by staff training and staff supervision where required
• Target: All InfoSec risks accepted and / or have effective risk treatment plans in place
• Measure: Risk register, managed through ISSG meetings and annual audit process
• Target: We endeavour to ensure all commissioner/service user related data is handled securely and confidentially
• Measure: Data breaches, management reviews and systems integrity and oversight through ISSG and annual audits
These objectives are monitored and reviewed and discussed at management reviews by the MD.

Clause 7: Support

OFI	OFI	(7 - 27001) The company would benefit from delivering an ISMS focused awareness training with its workforce. This was raised as an Opportunity for improvement.
OFI	OFI	(7 - 27001) The company would benefit from raising Data Protection compliant CCTV signage on the perimeter of their building. This was raised as an Opportunity for improvement.

Due to the company's small size, the HR Structure is led and managed by Chris Dyer, Director, and Tracy Jennings, Business Support Administrator. Jade Taylor, Finance Support/Administrator, also supports the HR and operation functions.

The company organisational chart was evidenced in MWM Via Learning Centre Organisation Chart V29 - January 2023, version 29, dated 01/2023, to support the interview with Chris Dyer, Director and Tracy Jennings, Business Support

Administrator. All electronic records and Job Descriptions are stored in the company's protected drive on Office 365 and Google Drive with user rights. At the time of this audit, a sample of two job descriptions was available and furnished below:

Administrator, based at Willenhall HQ – evidenced in HR interview.
Specialist Mentor – evidenced in HR interview.

Job descriptions were found to be specific to the role the company desires to hire. The job descriptions also include features of ISO 27001:2017 responsibilities. Chris Dyer, Director, informed that the company only advertise their jobs via indeed.com. The use of a recruitment agency is little to none as all the candidates apply via indeed.com. The company do not use sub-contractors, and all approved suppliers undergo contractual arrangements.

All employees and contractors are responsible for complying with policies and procedures, including reporting any events or security incidents.

Clause applicable C7.

The virtual tour was completed via the Microsoft Teams Platform, assisted by Tracy Jennings, Business Support Administrator. Suite 6, Graphic House, 15-18 New Rd, Willenhall, West Midlands, WV13 2BG, is based in West Midlands and attached to a private carpark used by company employees. Mentoring West Midlands Community Interest Company is a rented office based on the 2nd floor of this building. The building is a multi-tenanted block housing nine other different entities. Fixed cameras operated by the estate surround the external perimeter of the building, but the property lacks Data protection approved CCTV signage. The property does not have a loading bay area, and all incoming and outgoing deliveries are taken from the entrance door of the building. The entrance of the building is protected with a locked door with an intercom facility. Only four employees have a key to the entrance door. There is no access to this office Out of Hours. The communal areas were covered with fire extinguisher coverage, and a sample was seen, Foam – 6 litres and CO2 – 2KG litres serviced by Saddlers Fire Services in December 2022.

The office setting is equipped with ergonomic furniture. The office has good coverage of portable fire fighting equipment and fixed fire detection devices. The office is also equipped with a Swann Security intruder alarm system. The company do not have Servers onsite; hence there is no fire suppression system. The fire alarm for the building is tested weekly and every Weekend. It was noted that the company’s Health and Safety Poster had contact details of Health and Safety Representatives Chris Dyer, Director and Tracy Jennings, Business Support Administrator. Chris Dyer, Director, is chasing the landlord to conduct the fire drill.

The office has one Fellow cross shred shredder for confidential waste. The company do not generate a large amount of confidential waste. Hence it is collected once a month by the waste carrier. All the cables arrive in the electrical risers and, from here, get distributed into the office via raised flooring or false ceiling. All windows in the offices are equipped with provision blinds for confidentiality preventing external parties from viewing anything on screens inside the building.

The relevant SOA Controls evidenced: A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6.

Due to the company's size, the HR function is managed by Chris Dyer, Director and Tracy Jennings, Business Support Administrator. Chris Dyer explained that the company needs to undergo a large amount of due diligence as subject to audits from various organisations and commissionaires due to the nature of the work involved. The competence of the organisation branches out into two essential elements one is the qualification and other experience. All employees must have at least Level 3 qualification and three years of operational experience. This is the minimum criteria for an interview as the role requires particular skills for the job. The recruitment process effectively is a step-by-step process in terms of recruitment, very detailed and of the same level as any regulatory body example Local Authority when it comes to screening and vetting.

The recruitment process was explained by Chris Dyer, Director, and it is furnished below:

Advertisement is mainly done through uk.indeed.com, and it is tracked via the uk.indeed.com dashboard.
All the CVs received from the aspiring candidates are sieved by Chris Dyer, Director.
The sieved CVs are then passed on to Tracy Jennings, Business Support Administrator.
Tracy Jennings, Business Support Administrator, sent documentation to the candidates, including the Job Description, Job Applicants' Privacy Notice, Expense form, Criminal Record Self Disclosure Form and Conflict of Interest Form in September 2020. These forms must be completed and sent before arriving for a face-to-face employment interview.
A documentation checklist is sent to the employee via email, ideally, what documentation the candidate needs to bring, an

example: Passport, Driving License, Proof of address, highest qualification of the candidate etc., at the interview.
Before the candidate came for an interview, the company would have checked the candidate's background.
The interview is a standardised scoring system (on a Richter scale of 1 to 5) with set questions across all roles. These two or three sets of questionnaires are retained per the company's data retention policy.
An entire audit trail is available from the questionnaire so that the interview process is fair.
Once the candidate has passed the interview, the candidate's Right To Work checks is carried out at the interview stage.
After the interview stage, the company would check two sequential employment references, Enhanced DBS, address checks and other Identification checks to ensure they meet the criteria of their customers.
Once the candidate's pre-employment screening is completed, the candidate's Terms and Conditions are sent out to the candidate's email after completing satisfactory checks per their checklist. This information is kept as an audit trail as any refusal needs to retain with reasons why the company denies employment. This is done as the organisation is subject to audits from different regulatory and federal bodies. Example: Her Majesty Prison and Probation, and the organisation needs to provide this data to them to satisfy their conformance.

The employee onboarding process for all employees encompasses three weeks of detailed Induction, which is sent to these new starters before commencing Induction. The company would create a company email address on secure email so that all communication is sent to the employees via this email. This three-week Induction also includes Induction with Chris Dyer, Director, shadowing different personnel in the operations and following different departments to understand the role better. The probation period lasts for 13 weeks, and there is Supervision planned for new starters every two weeks. Supervision is used to track employees' performance and any support the new starter would need in the first 13 weeks of their employment with the organisation. This is part of the employee onboarding process. After the probation period, the employee's line manager would carry out monthly Supervision to keep track of employees' performance and support. The organisation also believes in promoting staff from within and relies less on external recruitment. This was also confirmed during the employee interview, as he was promoted twice in the last two years.

The company's HR assigns online training to employees via the HL Online training platform. The records are stored on HL Online Training and in the training matrix on office 365.

A sample of the following HR documents was evidenced:

Retention of Data Checklist V3 January 2023, version 3, dated 01/2023
Access to Fair Assessment Policy, dated 23/06/2022
14.09.20 Mentoring Guidance Document v36, version 36, dated 14/06/2020 (act as company handbook)
Lone Working and Staff Safety cited under section 10 of the 14.09.20 Mentoring Guidance Document v36, version 36, dated 14/06/2020
Staff Training and Assessment Policy, cited under section 14 of the 14.09.20 Mentoring Guidance Document v36, version 36, dated 14/06/2020
Whistleblowing Policy, cited under section 17 of the 14.09.20 Mentoring Guidance Document v36, version 36, dated 14/06/2020
Information Management (internal and external) and creating a 'Sterile Corridor', Principles of the Data Protection Act 2018 (GDPR) and MWM Policy, cited under section 18 14.09.20 Mentoring Guidance Document v36, version 36, dated 14/06/2020
Disciplinary Procedure, cited under Section 24 of the 14.09.20 Mentoring Guidance Document v36, version 36, dated 14/06/2020.

The company adopted the Caldicott Principles, covered through the Guidance Document and at the Induction. These include:-

Principle 1: Justify the purpose for using confidential information
Every proposed use or transfer of personally identifiable information within or from an organisation should be clearly defined and scrutinised. An appropriate guardian should regularly review its continuing uses.

Principle 2: Don't use personal confidential data unless necessary
Identifiable information should only be used if it's essential for the specified purposes. The need for this information should be considered at each stage of the process.

Principle 3: Use the minimum necessary personal confidential data
Where personally identifiable information is essential, each item should be considered and justified. This is so the minimum amount of data is shared, and the likelihood of identifiability is minimal.

Principle 4: Access to personal confidential data should be on a strictly need-to-know basis
Only those who need Access to personal confidential data should have Access to it. They should also only have Access to the data items that they need.

Principle 5: Everyone with Access to personal confidential data should be aware of their responsibilities
Action should be taken to ensure those handling personally identifiable information are aware of their responsibilities and obligation to respect patient and client confidentiality.

Principle 6: Understand and comply with the law
Every use of personally identifiable data must be lawful. Organisations that handle confidential data must have someone responsible for ensuring that the organisation complies with legal requirements.

Principle 7: The duty to share information can be as essential as the duty to protect patient confidentiality
Health and social care professionals should be confident to share information in the best interests of their patients and within the framework set out by these principles. They should also be supported by the policies of their employers, regulators, and professional bodies.

All employment contracts are issued via email after the successful completion of pre-employment and enhanced DBS checks. Contracts of employment have the following clauses for Details Of Parties, Nature of work, Timetable, Termination, Salary and other payment, Staff training, expenses, sickness and absenteeism, holidays, Access to documents, COPYRIGHT and Confidentiality and Conflicts Of Interest, contacts, Principles, Tax And National Insurance and Bank Details, Professional Practices, Publicity, Alternations, Force Majeure, Governing Law / Jurisdiction. A sample of the contract of employment was evidenced:

Employee 1: HC
Contract of employment signed by employee: 06/02/2023
Induction completed: Planned to take place next week

Employee 2: SK
Contract of employment signed by employee: 01/02/2023
Induction completed: Undergoing Induction at the moment

HR record cited during the audit for Screening / Vetting checks:

Employee 1:
Enhance Criminal Disclosure completed: 17/09/2022
ID Check: 17/02/2022
Right to Work checks: 27/09/2022
2 x References checked: 30/08/2022

Employee appraisals completed (evidence cited during the audit):

Employee 1 – Date Supervision completed 17/01/2023
Employee 2 – Date Appraisal completed 01/12/2022

All leavers are processed as per the company handbook. The company had only one leaver in 2022 until now. A sample of leavers was evidenced and furnished below. The line manager processed this, and IT equipment was returned and handed over to the IT department. The exit interview was completed as part of the leaver process.

Employee Name: redacted
Date: 20/01/2023
Asset form completed: 20/01/2023
Email terminated: 20/01/2023
Laptop returned: Yes
Access cards returned: Yes

The relevant SOA Controls evidenced: A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1, A.8.1.4, A.9.2.6.

Training records are held in Office 365 and Google Cloud environments. A sample of training evidence was seen during the audit:

Chris Dyer, Director, informed that ISMS awareness spread all over the induction and includes GDPR training, but the company still needs specific ISMS awareness training. This is evidenced in the company's induction and meetings. An opportunity for improvement was raised for the company to develop a specific ISMS awareness training module.

Employee 1: AL
Induction: T
(In House) Health and Safety: T
(In House) First Aid Information: T
(In House) Active Pro (Case Management):N/A
(In House) Child and Vulnerable Adult Safeguarding: T
(Online) Prevent (R) : T
(Online) GDPR (R) : T
(Online) Safeguarding of Vulnerable Adults (R): T
(Online) Drugs and Alcohol Awareness (R): T
(Online) Mental Health Awareness (R): T
(Online) Equality, Diversity and Human rights (R): T
(Online) Working with Sex Offenders (R): T
(Online) LGBTQ+ (R): T
(Online) Fire Safety: N/A
(Online) COSHH: N/A
(Online) First Aid: N/A
BPF Training: T
Education and Training Award Level 3: T
CATS: N
Trauma Informed Practice Training: T

Employee 2: LH
Induction: T
(In House) Health and Safety: T
(In House) First Aid Information: T
(In House) Active Pro (Case Management):N/A
(In House) Child and Vulnerable Adult Safeguarding: T
(Online) Prevent (R) : T
(Online) GDPR (R) : T
(Online) Safeguarding of Vulnerable Adults (R): T
(Online) Drugs and Alcohol Awareness (R): T
(Online) Mental Health Awareness (R): T
(Online) Equality, Diversity and Human rights (R): T
(Online) Working with Sex Offenders (R): T
(Online) LGBTQ+ (R): T
(Online) Fire Safety: N/A
(Online) COSHH: N/A
(Online) First Aid: N/A
BPF Training: T
Education and Training Award Level 3: T
CATS: T
Trauma Informed Practice Training: T

T = trained,
N = not trained
N/A = not applicable

All employees are communicated via weekly meetings at 09:00, to alert them of any risks and threats. All changes are communicated via their line managers, Teams, Zooms calls and emails.

HL Online Training provided a sample of ISMS training.

Name: AW
Username: AW
Course Title: Data Protection completed 16/12/2022
Course Title: Drugs and Alcohol awareness completed 16/12/2022
Course Title: Equality, Diversity and Human Rights – General Awareness completed 16/12/2022
Course Title: Mental Health Awareness completed 16/12/2022
Course Title: Safeguarding of vulnerable adults completed 16/12/2022

The two non-managers employees were interviewed. The details are furnished below:

JE – Specialist ETE Mentor, started with the organisation on 23rd April 2021 as Specialist Mentor on a six-month contract.
He reports directly to DD, the Team leader.
Length of service: JE has been with the company for almost two years in April 2023.
Induction: He went through 3 detailed weekly plans of induction, which included shadowing various operations to understand his role. JE also had an induction with Chris Dyer, Director. His ISMS training was spread all over the three weeks but haven't seen a specific one.
Training - refresher training was given to JE annually, including all training completed on HL Online Training. He also confirmed that he goes through the monthly Supervision (company's appraisals) process with his line manager – DD, and Team Leader. His subsequent Supervision is planned for March 2023. These are part of one email chain with an audit trail.
ISMS awareness – JE demonstrated a basic understanding of confidentiality and information integrity and knew that information is critical to business and has to be confidential and not freely available.
ISMS communication – JE confirmed that most of the confirmation is done face-to-face via weekly meetings and emails.
Data breach – JE will communicate directly with his line manager and Chris Dyer, Director, upon discovering a data breach.

TJ – Business Support Administrator, started with the organisation on 12th September 2022 as Business Support Administrator.
She reports directly to Chris Dyer, Director.
Length of service: TJ has been with the organisation for the last five months.
Induction: When TJ joined, she went through 3 weeks of induction with Chris Dyer, Director and shadowed various functions in the office to understand her role. She understands elements of ISMS training over her induction.
Training - She also confirmed she completed HL Online Training and her 13 weeks probation, which encompasses biweekly Supervision. But now she has her Supervision every month with her line manager – Chris Dyer, Director.
ISMS awareness – TJ demonstrated an excellent basic of the ISMS concept.
ISMS communication – TJ confirmed that most of the confirmation is done face-to-face and via email.
Data breach – On discovering a physical break-in, TJ will communicate directly with her line manager, contact Metropolitan Police, and inform all relevant parties without putting herself in danger.

The company will look into delivering comprehensive ISMS training soon.

Summary:
Overall, both employees interviewed had a basic understanding of ISMS Awareness and knew where to look for documentation. They were evident in their commitment to the ISMS and had admirable details describing their job roles and responsibilities.

The relevant SOA Controls evidenced: A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1, A.8.1.4, A.9.2.6.

All organisations' asset is maintained via an excel sheet stored on Google Drive and Office 365. Jade Taylor, Finance Support/Administrator and Tracy Jennings, Business Support Administrator, take care of the register to keep it updated. The organisation's comprehensive asset list was evidenced. At the time of the audit, the company had 144 IT equipment registered on the Hardware Assets inventory dated 06/02/2023. The document is below the asset categories:

Date placed on inventory: 14/04/2016
Owner: Chris Dyer
Asset Type: LAPTOP
Make: HP
Model: 640

Serial No: 5CG5261Y86
Location: Disposed of 27.02.2020
Security Classification: ICT
Checked on 03/02/2023: Up to date

Date placed on inventory: 31/05/2016
Owner: Chris Dyer
Asset Type: LAPTOP
Make: HP
Model: ProWorkbook
Serial No: 6576GH667P78
Location: Head Office - Admin 3
Security Classification: ICT
Checked on 03/02/2023: reassigned

Date placed on inventory: 29/09/2022
Owner: Chris Dyer
Asset Type: Laptop
Make: DELL
Model: N/A
Serial No: 6095011
Location: Daniel Scates
Security Classification: ICT
Checked on 03/02/2023: Up to date

The relevant SOA Controls evidenced: A.8.1.1, A.8.1.2, A.8.1.3, A.8.2.3.

The organisation stores and manages all the documentation, including all versions and dates tracked in master documentation, Version Control Spreadsheet 2023, version 8, dated 02/2023. At the time of the audit, the sample documents were found to be dated, versioned and controlled by the document's owner. The distribution of these documents is controlled on the company's Google Drive and Office 365, with user access rights and document protection found in a place with RBAC. The document owner is responsible for updating the document and keeping the register up to date. A sample was evidenced, and it is furnished below:

GDPR Data Register - Building Positive Futures L1, V2 September 2018
GPDR Data Register - Conflict Management L1, V2 September 2018
GDPR Data Register - Life Skills and Preparation L1, V1 November 2018
GDPR Data Register - Coventry DV, V1 May 2018
GDPR Data Register - Coventry SAC, V1 May 2018
GDPR Data Register - HMPPS ETE, V2 September 2018
GDPR Data Register - Talent Match, V1 May 2018
GDPR Data Register - Young Person/Family Referrals, V1 May 2018
GDPR - Employee Privacy Notice, V2 - January 2023
GDPR - Job Applicant Privacy Notice, V4 - January 2023
GDPR - Previous Employee Details, V1 May 2018
GDPR - Principal Statement, V4- January 2023
GDPR - Recruitment Pack, V4- January 2023
GDPR - Retention of Data Checklist, V3 - January 2023
GDPR - Subject Access Request Form, V1 May 2018
Health and Safety Policy Overview V13 - January 2023
Health and Safety - COSHH sheets, V4 - January 2023
Health and Safety Risk Assessments, V10 - January 2023
Homeworking Policy, V5 - January 2023
Homeworking Risk Assessment, V2 - February 2023
HR Recruitment Checklist, V9 - January 2023
HR File Record Sheet, V14 - January 2023
Information Security Steering Group Meetings
Inventory, Updated as a when

ISMS Policy, V13 - January 2023
Job Descriptions, Various
Learner Induction Checklist, V9 - September 2022
MWM Guidance Document, Sep-20
NCFE Complaints Policy and Procedure, Sep-23
NCFE End of Course Next Steps, Sep-23
NCFE End of Course Training Evaluation Form, Sep-23
NCFE First Aid Policy, Sep-23
NCFE Malpractice Policy, Sep-23

All the documents are stored on the secure administration-level access of the network as per their network IT Policy. These documents are shared with employees on RBAC shared drive with read-only access. All the HR-related documents are stored in the HR Google and Office 365 One drive, and various access levels are assigned depending on the role and responsibilities.

A sample of a Supplier contract – Advice Pro was evidenced and included ten detailed clauses relevant to Confidentiality Information, Obligation of receipt, Ownership of Confidential information, Terms, Governing Law etc. The advice pro has ISO27001 certification.

Advice Pro's Security and Data Privacy was evidence, dated January 2023.

The company does not use any more suppliers besides Advice Pro and Amazon Business.

All the records are protected from loss, destruction, falsification, unauthorised release, or access in accordance with legislative, regulatory, contractual, and business requirements. The retention period for all types of the record is defined as under EB Register of Data - HR. The sample of data retention is furnished below:

Emails: Immediate Effect on Leaving the company
HR Records: Retention Period - 1 month from the date of leaving
Timesheets and Annual leaves: Retention Period - 2 years from the date of leaving
HR Records for sickness/P45 etc.: Retention Period - 3 years from the date of leaving
Employee pay records: Retention Period - 6 years from the date of leaving.
The relevant SOA Controls evidenced: A.12.3.1, A.12.4.2, A.13.2.1, A.18.1.3.

Clause 8: Operation

OFI OFI (8 - 27001) The company would benefit from hosting Business Continuity Plan desktop exercise with its workforce. This was raised as an Opportunity for improvement.

The company operations are based on Microsoft 365 Cloud and Google Drive environment. The data from syncs in real-time with up daily to Office 365. If the business loses the office/production facility, the company will access their data from the cloud and arrange work from home. At the time of the audit, it was ascertained that 90% of employees work from remote locations as the systems are competent for remote working. During the pandemic, the whole company was working remotely from home. The company's Business Continuity Plan, dated 02/2023, details different scenarios for Business Recovery Arrangements. Chris Dyer, Director, provides leadership and (recovery) in the aftermath following the onset of a disruptive / disaster incident.

The organisation's data is backed up daily via Office 365, Chris Dyer, Director, informed that all the emails and documents are backed up on Office 365, and the company can restore the data even in the event of hardware failure or theft of equipment from the Cloud environment.

The policies are discussed annually in Management Review Meetings or whenever significant changes occur, scope including limitations and exclusions, authorities and delegations required, criteria for type and scale of incidents to be addressed and references to standards, guidelines, and regulations.

As the company has been operating remotely for over three years now, they haven't documented the table top exercise yet, but moving forward, Chris Dyer, Director, informed that he would document the table top exercise in the next annual staff training.

The company does not perform annual penetration tests as they are moving to a new system – Advice Pro, on 10th February 2023, which will be penetration tested, and reports will be available for evidence.

The relevant SOA Controls evidenced: A.12.3.1, A.17.1.1, A.17.1.2, A.17.1.3, A.17.2.1, A.18.2.3.

The company's ISMS documented procedures includes a series of Standard Operating Procedures and all the ISMS policies. The list of mandatory documents seen and verified is furnished below:

Scope of the Policy, cited in ISMS Policy, Version 13, dated January 2023
Training Matrix, Version 33, January 2023
Mentoring Guidance Document, Version 36, 14.09.20 (Acts as Access Control Policy)
Business Continuity and Business Plan, dated February 23
Statement of Applicability, Version 8, January 2023
Mentoring West Mids CIC Risk Assessment ISO27001 June 2020, version 10, dated June 2020
Risk Treatment Plan, cited in ISMS Policy, Version 13, dated January 2023
Risk Assessment Methodology, cited in ISMS Policy, Version 13, dated January 2023
GDPR - Retention of Data Checklist. Version 3, January 2023
ISMS Policy, Version 13, dated January 2023
Organisational Chart, Version 29, February 2023
Version Control Master List, Version 8, February 2023

The ISMS Policy, Version 13, dated January 2023, under section 8, refers to the Risks Assessment Methodology process which connects to the risk treatment detailed in their Statement of Applicability with all of the Information Security Annex. A controls that are in place. This was evidenced against their statement of applicability, Statement of Applicability, Version 8, January 2023.

The Risk Assessment Process is clearly defined in the ISMS Policy, Version 13, dated January 2023 under section 8 refers to the Risks Assessment Methodology and the most significant risk was identified within the Risk Register as unauthorised access to customer data. This is sampled below from the :

Asset/Asset Group: Critical information for Clients
Threat: Unauthorised access
Information Security aspect affected – C, I, A: Confidentiality
Current controls in place and implemented: 1. All hardcopy customer files held securely. 2. All electronically held files in access-controlled directories. All reports to be written directly to these directories.
Known vulnerabilities to be addressed: 1. Data Transmission,
Vulnerability rating (1 to 5): 3
Probability rating (1 to 5): 2
Impact rating (1 to 5): 5
Risk Value (V x P x I): 30
Risk Evaluation: Continue with Policies and Procedures.
Comments and links to SOA for Risk Treatment Action details: Information only to be shared over secure networks. Reduce the holding of hard copy files unless there is a specific reason to keep them.
Link to SOA: A.8.3.1, A.8.3.2, A.8.3.3, A.9.3, A.13.1.1, A.13.1.2, A.13.1.3, A.14.1.2.

The company is mobilising their system to Advice Pro on 10th February 2023 which will be penetration tested annually carried out by external service provider.

The Statement of Applicability was noted to have identified controls to mitigate risks following the identification, analysis, and evaluation. The Statement of Applicability was evidenced - Statement of Applicability, Version 8, January 2023 and has been created in line with Annex A. This is detailed in Clause 6 of this report.

Clause 9: Performance Evaluation

Performance Evaluation (Monitoring, Measuring and Analysing) has been established and defined and is tied in with the Objectives and Targets. Continuous monitoring is undertaken observing each part of the service provision. A CAPA Log was evidenced at the audit. This is designed to document internal audit and risk assessment outcomes, concerns, problems, incidents, breaches and suggestions, who is responsible for the management of each individual issue, completion target dates and corrective action taken. They do not require pen testing due to them using Advice Pro which is a fully-managed, secure web-based case management system developed specifically for advice organisations. It captures client details and casework information over a wide range of matter types. Advice Pro is 27001 compliant and conducts pen testing.

They have an Internal Audit Schedule in place that fully covers the requirements of ISO 27001. Evidenced were the following audits:
• Dated: 25-03-2022
• Auditor: CD
• Area: Current system
• Findings: Further review of Defacto transfer plans
• Dated: 13-12-2022
• Auditor: CD
• Area: Defacto, EDBS, Admin Function
• Findings: Build more admin support into ISO functions going forward – ISSG documents and these records and audit actions too.
• Dated: 13-12-2022
• Area: SoA plus
• Auditor: CD
• Findings: New system purchased – Advice Pro – installation starts 10.2.23, training plan for all staff, customisation systems, ISO27001 held, penetration tested, etc. SOA and ISO files adjusted re new information, migration period and forward plans for Advice Pro. Completion should be finalised by end of February – staff trained, case systems customised for MWM, critical case information uploaded, further documents uploaded where needed to meet GDPR requirements of archiving, over 7 years of age will be destroyed. ISSG function within management team agenda will cover off this and CD will lead with TJ on overseeing all the above and reporting back next meeting

The internal audits were conducted and written up with adequate detail. There is adequate information recorded and they represent adequate examples of internal audits.

Management reviews are conducted monthly. Evidenced were minutes from their most recent management review.
Date of meeting: 26-01-2023
Attendees: CD, LH, DD, TJ.
The minutes followed the requirements of the 27001 standard. There is a good level of detail in the minutes relating to actions that need to be taken, and who is responsible.

Clause 10: Improvement

Performance Evaluation (Monitoring, Measuring and Analysing) has been established and defined. Continuous monitoring is undertaken observing each part of the service. They document and monitor any actions that need to be actioned in their management review minutes and this was evidenced at the audit.
The following entry was noted:
• 26-01-2023: LH to send ACE evaluation to SPO's and discuss evaluation with Lesley Holland (RRO Gov). Carried over as no feedback from Lesley.
• 26-01-2023: LH to speak to Scott Harcus and offer a different variant of the family contract that would incorporate ACE's. - Sent everything incl delivery plan, nothing specific sent back. Chris had exchange with Scott about 31st March. Business plan. Yasmin has been spoken to regarding this matter. No further forward with outcome.
• 26-01-2023: LH to discuss potentially delivering ACE's in different establishment for potential contract expansion/development. Going to wait until a better relationship has been established with HMP B'Ham. Timing is everything.
The entries documented and evidenced at the stage 2 audit are findings raised at management reviews.

Section E: Legal Compliance

They are fully aware of their legal and regulatory obligations. They have documented their legal and regulatory register. This includes:
• Data Protection Act 2018
• Employment Agency Act 2003
• Freedom of Information Act 2000
• Computer Misuse Act 1990
• Human Rights Act 1998
• Equality Act 2010
• Terrorism Act 2006

• Counter-Terrorism and Security Act 2015
• Counter-Terrorism Act 2008
This list will be reviewed at least annually for the Management Review but they will monitor for alerts from various business sources.
Any changes or additions notifications will prompt an analysis of the impact on their business and make appropriate changes for compliance.
The senior team, led by the MD are ultimately responsible for all compliance issues. The MD attended the audit throughout.
Employers' Liability Insurance is in place via Aviva, expiring 3-06-2023.

Relevant SoA controls: A18.1 (A18.1.1 / A18.1.5) A18.2

No enforcement actions have been received.

Section F: Use of the Certification Mark

The Certification Mark will be used on the website. It will be used within the BAB guidelines.

Closing Meeting

The closing meeting was attended by Chris Dyer (MD) Tracy Jennings (Business Administrator). The findings raised were discussed and accepted as reflective of the audit. As part of the closing meeting, a discussion was held in regard to the date of the next audit by BAB in line with the Certification cycle. The client was advised that the date suggested was to be considered a pencilled in date and not a formal booking, this date and audit duration (ie number of days) would be confirmed by the audit booking team closer to the date of the audit.
The suggested date for the next audit is w/c 5-02-2023.

Non-Conformities and Opportunities for Improvement

	Type	Clause	Summary
No Non-Conformances Found			
OFI-1	OFI	7	(27001) The company would benefit from raising Data Protection compliant CCTV signage on the perimeter of their building. This was raised as an Opportunity for improvement.
OFI-2	OFI	7	(27001) The company would benefit from delivering an ISMS focused awareness training with its workforce. This was raised as an Opportunity for improvement.
OFI-3	OFI	8	(27001) The company would benefit from hosting Business Continuity Plan desktop exercise with its workforce. This was raised as an Opportunity for improvement.

= Major Non-Conformity
= Minor Non-Conformity
= Opportunity for Improvement

If non-conformances have been raised throughout this assessment, you are required to provide the following to assist in the closure of these to **compliance@british-assessment.co.uk**.

Major Non-conformance (Recertification Assessment) – Provide evidence within 10 days of the assessment
Major Non-Conformance (Surveillance Assessment) – Provide evidence within 28 days of the assessment
Minor Non-Conformances – Provide a corrective action plan within 28 days detailing how you intend to rectify in preparedness for the next assessment together with a root cause analysis.
Important Note: If this assessment represented a "Stage 2" (Initial) assessment, certification cannot be granted until such time that the corrective action plan has been received.

Certification Cycle Assessment Plan (from to 3)

Business function/Process	Stage Two Audit	1st Surveillance Audit	2nd Surveillance Audit	Recertification Audit
Context of the organisation	P	P	P	P
Leadership	P	P	P	P
Planning	P	P	P	P
Support	P	P	P	P
Operation	P	P	P	P
Performance Evaluation	P	P	P	P
Improvement	P	P	P	P
Client Site Visit	tbc	tbc	tbc	tbc

P = Planned, = Done, = Excluded

Plan for next Assessment

Time	Assessment Activity
09.00	Arrive on site
	Opening Meeting
	Overview of Company Review:- Context of the Organisation Review non-conformities, observations, recommendations from previous audit.
	Leadership
	Planning for the management systems including risk Including Statement of Applicability
	Support
	Operation
	Performance Evaluation
	Improvement
	Performance Evaluation
	Customer Communication
	Internal Audits
	Legal Compliance
	Use of Certification Mark (where applicable)
	Auditor collating information and preparing for closing meeting.
	Closing Meeting

Assessment Notes

a. The assessment was based on sampling and therefore non-conformities may exist which have not been identified.

b. If you wish to distribute copies of this report external to your organisation then all pages must be included.

c. The British Assessment Bureau, its staff and agents shall keep all information relating to your organisation confidential and secure and shall not disclose any such information to any third party except that in the public domain or required by law or relevant accreditation bodies. The British Assessment Bureau staff agents and accreditation bodies have signed individual confidentiality undertakings and will only receive confidential information on a 'need to know' basis.

d. This report and related documents have been prepared for and only for the British Assessment Bureau client and for no other purpose. As such the British Assessment Bureau does not accept or assume any responsibility (legal or otherwise) or accept any liability for or in connection with any other purpose for which the Report may be used or to any other person to whom the Report is shown or in to whose hands it may come and no other persons shall be entitled to rely on the Report.

e. The management system documentation included the necessary policies, procedures, process descriptions etc, required by the standard.

Complexity Statements

1) Type(s) of business and regulatory requirements	Organization works in critical business sectors
Critical business sectors are sectors that may affect critical public services that will cause risk to health, security, economy, image and government ability to function that may have a very large negative impact to the country	
2) Process and tasks	Standard but non-repetitive processes, with high number of products or services
3) Level of establishment of the MS	ISMS is already well established and/or other management systems are in place
4) IT infrastructure complexity	Few or highly standardized IT platforms, servers, operating systems, databases, networks, etc.
5) Dependency on outsourcing and suppliers, including cloud services	Little or no dependency on outsourcing or suppliers
6) Information System development	None or a very limited in-house system/application development

PIN: **198411**	Date: **06 February 2023**	Organisation: **Mentoring West Midlands Community Interest Company**	
CONFIDENTIAL		Document: **Audit Summary Report**	Version **27**