Introduction

This tool is designed to cover all the relevant control areas of ISO / IEC 27001:2013. All sorts of organisations and
Because it is a general tool, you may find the language challenging at times, but just because you find a section
Please note , completing this tool does not in itself confer ISO/IEC 27001:2013 certification. The findings here must be confirmed as part of a formal audit / assessment visit. **However, it could be used as part of a voluntary adoption of ISO27001:2103, which is the route a private practitioner is likely to take.**

Feedback is very important to us - if there is any way in which we can improve this risk management tool please do send us your ideas to info@pwtraining.com.

The steps involved in using this tool

Before you start the CHECK LIST

1. Work out who you need to involve	Work with relevant business stakeholders what the appropriate scope of the assessment is. Remember this is about your Information Security Management System (ISMS) - everything to do with the digital part of your private practice - computers, data, mobile phones, phones, faxes, client records etc.
2. Collect evidence	Identify and centralise as much evidence as possible. This can include policy documents, process documents, interview transcripts etc.

RISK ASSESSMENT CHECK LIST

4. Review control areas.	**Start with item A.5** and work through to the end. Only when you have finished should you answer questions 1 - 4. The best way to complete this tool is to open the document as an Excel file and work on your screen - start bty saving it to your hard drive and don't forget to save it regularly. If you prefer to work on it as a paper version (not recommended as it is very long) we also have included it as a PDF version. Work through the checklist, reviewing the evidence for each control and determining how compliant it is with the requirements. Work out which areas are most and least relevant to your private practice. Work out if there are any areas that have not been included that you need to consider (additional lines have been included in section 19 and you can add additional ones).
5. Determine level of compliance.	On completion of the review, total up the items needing most attention, those flagging up the highest risks and start there.

Post Assessment

6. Record areas of weakness	Make a note of any areas where compliance is unsuitable or nor relevant to your practice and check this over with your supervisor or other professional person to ensure that you have not misunderstood the task.
7. Determine improvement plan	For each area of weakness, work with relevant professionals to determine how the control can be improved.
8. Schedule re-assessment	Arrange a date to review weak areas to set a target for improvement plans.

Lifecycle Review

9. ISMS Review Schedules	Ensure that the ISMS is re-assessed on a regular basis, ideally once every 12 months.

Did you find this tool too challenging and need some help?
PWT can mentor you and help you to reflect on the items covers in this tool.

T: +44 (0) 1273 700 911
M: +44 (0) 7880 501 116
E: info@pwtraining.com
W: www.pwtraining.com

An ISO27001 Check List for Risk Management, adapted by Philippa Weitz for counsellors and psychotherapists to adopt voluntarily under ISO 27002

ISO 27001: 2013 Ref No.	Title	ISO 27001 Control	TASK 1: What this means to you? What do you need to think about, What extra help or resources might you need?	TASK 2: assess how relevant this item is to your private practice: NON-APPLICABLE, FAIRLY IMPORTANT, VERY IMPORTANT	TASK 2: assess the risk level to your practice: LOW, MEDIUM, HIGH	TASK 3: Create your personalised action plan	ACTION: Choose: - COMPLETED - PROGRESS - TO DO
1	**The organisation and its context - this includes a one-person private practice**						
1.1	Have the internal & external issues that are relevant to the Information Security Management System (ISMS), and that impact on the achievement of its expected outcome been determined?						
2	**Needs and expectations of interests parties**						
2.1	Has the organisation determined the interested parties that are relevant to the ISMS?						

An ISO27001 Check List for Risk Management, adapted by Philippa Weitz for counsellors and psychotherapists to adopt voluntarily under ISO 27002

ISO 27001: 2013 Ref No.	Title	ISO 27001 Control	TASK 1: What this means to you? What do you need to think about, What extra help or resources might you need?	TASK 2: assess how relevant this item is to your private practice: NON-APPLICABLE, FAIRLY IMPORTANT, VERY IMPORTANT	TASK 2: assess the risk level to your practice: LOW, MEDIUM, HIGH	TASK 3: Create your personalised action plan	ACTION: Choose: - COMPLETED - PROGRESS - TO DO
2.2	Have the requirements of these interested parties been determined, including legal, regulatory and contractual requirements?						
3	**Scope of the ISMS - Information Security Management System**						

An ISO27001 Check List for Risk Management, adapted by Philippa Weitz for counsellors and psychotherapists to adopt voluntarily under ISO 27002

ISO 27001: 2013 Ref No.	Title	ISO 27001 Control	TASK 1: What this means to you? What do you need to think about, What extra help or resources might you need?	TASK 2: assess how relevant this item is to your private practice: NON-APPLICABLE, FAIRLY IMPORTANT, VERY IMPORTANT	TASK 2: assess the risk level to your practice: LOW, MEDIUM, HIGH	TASK 3: Create your personalised action plan	ACTION: Choose: - COMPLETED - PROGRESS - TO DO
3.1	Have the boundaries and applicability of the ISMS been determined to establish its scope, taking into consideration the external and internal issues, the requirements of interested parties and the interfaces and dependencies with other organisations?						
3.2	Is the scope of the ISMS documented?						
4	**Leadership and Management Commitme**						

An ISO27001 Check List for Risk Management, adapted by Philippa Weitz for counsellors and psychotherapists to adopt voluntarily under ISO 27002

ISO 27001: 2013 Ref No.	Title	ISO 27001 Control	TASK 1: What this means to you? What do you need to think about, What extra help or resources might you need?	TASK 2: assess how relevant this item is to your private practice: NON-APPLICABLE, FAIRLY IMPORTANT, VERY IMPORTANT	TASK 2: assess the risk level to your practice: LOW, MEDIUM, HIGH	TASK 3: Create your personalised action plan	ACTION: Choose: - COMPLETED - PROGRESS - TO DO
	Is the organisation's leadership committed to the ISMS demonstrated by:						
4.1	~ Establishing the information security policy and objectives, in consideration of the strategic direction of the organisation, and in promotion of continual improvement?						
4.2	~ Ensuring the integration of the ISMS requirements into its business processes?						

An ISO27001 Check List for Risk Management, adapted by Philippa Weitz for counsellors and psychotherapists to adopt voluntarily under ISO 27002

ISO 27001: 2013 Ref No.	Title	ISO 27001 Control	TASK 1: What this means to you? What do you need to think about, What extra help or resources might you need?	TASK 2: assess how relevant this item is to your private practice: NON-APPLICABLE, FAIRLY IMPORTANT, VERY IMPORTANT	TASK 2: assess the risk level to your practice: LOW, MEDIUM, HIGH	TASK 3: Create your personalised action plan	ACTION: Choose: - COMPLETED - PROGRESS - TO DO
4.3	~ Ensuring resources are available for the ISMS, and directing and supporting individuals, including management, who contribute to its effectiveness?						
4.4	~ Communicating the importance of effective information security and conformance to ISMS requirements?						
A5	**Management of Information Security Policy**						
A5.1	**Information security policy**	**To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.**					

An ISO27001 Check List for Risk Management, adapted by Philippa Weitz for counsellors and psychotherapists to adopt voluntarily under ISO 27002

ISO 27001: 2013 Ref No.	Title	ISO 27001 Control	TASK 1: What this means to you? What do you need to think about, What extra help or resources might you need?	TASK 2: assess how relevant this item is to your private practice: NON-APPLICABLE, FAIRLY IMPORTANT, VERY IMPORTANT	TASK 2: assess the risk level to your practice: LOW, MEDIUM, HIGH	TASK 3: Create your personalised action plan	ACTION: Choose: - COMPLETED - PROGRESS - TO DO
A5.1.1.1	Policies for Information Security	1. Do information security policies exist that provide a framework for setting objectives, and demonstrate commitment to meeting requirements and for continual improvement?					
A5.1.1.2	Policies for Information Security	2. Are all policies approved by management?					
A5.1.1.3	Policies for Information Security	3. Are policies properly communicated to employees?					
A5.1.2.1	Review of the policies for information security	1. Are the information security policies subject to review?					
A5.1.2.2	Review of the policies for information security	2. Are the reviews conducted at regular intervals?					
5.1.2.3	Review of the policies for information security	3. Are reviews conducted when circumstances change?					
A6	**Organization of information security**						

T: +44 (0) 1273 700 911
M: +44 (0) 7880 501 116
E: info@pwtraining.com
W: www.pwtraining.com

An ISO27001 Check List for Risk Management, adapted by Philippa Weitz for counsellors and psychotherapists to adopt voluntarily under ISO 27002

ISO 27001: 2013 Ref No.	Title	ISO 27001 Control	TASK 1: What this means to you? What do you need to think about, What extra help or resources might you need?	TASK 2: assess how relevant this item is to your private practice: NON-APPLICABLE, FAIRLY IMPORTANT, VERY IMPORTANT	TASK 2: assess the risk level to your practice: LOW, MEDIUM, HIGH	TASK 3: Create your personalised action plan	ACTION: Choose: - COMPLETED - PROGRESS - TO DO
A6.1	**Internal organization**	**To manage information security within the organization.**					
A6.1.1	Information security roles and responsibilities	Are responsibilities for the protection of individual assets, and for carrying out specific security processes clearly identified and defined and communicated to the relevant parties?					
A6.1.2	Segregation of duties	Are duties and areas of responsibility separated, in order to reduce opportunities for unauthorised modification or misuse of information, or services?					
A6.1.3.1	Contact with authorities	1. Is there a procedure documenting when, and by whom, contact with relevant authorities (law enforcement etc.) will be made?					

An ISO27001 Check List for Risk Management, adapted by Philippa Weitz for counsellors and psychotherapists to adopt voluntarily under ISO 27002

ISO 27001: 2013 Ref No.	Title	ISO 27001 Control	TASK 1: What this means to you? What do you need to think about, What extra help or resources might you need?	TASK 2: assess how relevant this item is to your private practice: NON-APPLICABLE, FAIRLY IMPORTANT, VERY IMPORTANT	TASK 2: assess the risk level to your practice: LOW, MEDIUM, HIGH	TASK 3: Create your personalised action plan	ACTION: Choose: - COMPLETED - PROGRESS - TO DO
A6.1.3.2	Contact with authorities	2. Is there a process which details how and when contact is required?					
A6.1.3.3	Contact with authorities	3. is there a process for routine contact and intelligence sharing?					
A6.1.4	Contact with special interest groups	Do relevant individuals within the organisation maintain active membership in relevant special interest groups?					
A6.1.5	Information security in project management	Do all projects go through some form of information security assessment?					
A6.2	**Mobile devices and teleworking**						
A6.2.1.1	Mobile device policy	1. Does a mobile device policy exist?					
A6.2.1.2	Mobile device policy	2. Does the policy have management approval?					

An ISO27001 Check List for Risk Management, adapted by Philippa Weitz for counsellors and psychotherapists to adopt voluntarily under ISO 27002

ISO 27001: 2013 Ref No.	Title	ISO 27001 Control	TASK 1: What this means to you? What do you need to think about, What extra help or resources might you need?	TASK 2: assess how relevant this item is to your private practice: NON-APPLICABLE, FAIRLY IMPORTANT, VERY IMPORTANT	TASK 2: assess the risk level to your practice: LOW, MEDIUM, HIGH	TASK 3: Create your personalised action plan	ACTION: Choose: - COMPLETED - PROGRESS - TO DO
A6.2.1.3	Mobile device policy	3. Does the policy document address additional issues from using mobile devices (e.g. theft, use of open wireless hotspots etc.)?					
A6.2.2.1	Teleworking	1. Is there a policy for teleworking?					
A6.2.2.2	Teleworking	2. Does the policy have management approval?					
A6.2..3	Teleworking	3. Is there a set process for remote workers to get access?					
A6.2.2.4	Teleworking	4. Are teleworkers given advice and equipment to protect their assets?					
A7	**Human resources security**						

T: +44 (0) 1273 700 911
M: +44 (0) 7880 501 116
E: info@pwtraining.com
W: www.pwtraining.com

An ISO27001 Check List for Risk Management, adapted by Philippa Weitz for counsellors and psychotherapists to adopt voluntarily under ISO 27002

ISO 27001: 2013 Ref No.	Title	ISO 27001 Control	TASK 1: What this means to you? What do you need to think about, What extra help or resources might you need?	TASK 2: assess how relevant this item is to your private practice: NON-APPLICABLE, FAIRLY IMPORTANT, VERY IMPORTANT	TASK 2: assess the risk level to your practice: LOW, MEDIUM, HIGH	TASK 3: Create your personalised action plan	ACTION: Choose: - COMPLETED - PROGRESS - TO DO
A7.1	**Prior to employment**	**To ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities.**					
A7.1.1.1	Screening	1. Are background verification checks carried out on all new candidates for employment?					
A7.1.1.2	Screening	2. Are these checks approved by relevant management authority?					
A7.1.1.3	Screening	3. Are the checks compliant with relevant laws, regulations and ethics?					
A7.1.1.4	Screening	4. Are the level of checks required supported by business risk assessments?					

An ISO27001 Check List for Risk Management, adapted by Philippa Weitz for counsellors and psychotherapists to adopt voluntarily under ISO 27002

ISO 27001: 2013 Ref No.	Title	ISO 27001 Control	TASK 1: What this means to you? What do you need to think about, What extra help or resources might you need?	TASK 2: assess how relevant this item is to your private practice: NON-APPLICABLE, FAIRLY IMPORTANT, VERY IMPORTANT	TASK 2: assess the risk level to your practice: LOW, MEDIUM, HIGH	TASK 3: Create your personalised action plan	ACTION: Choose: - COMPLETED - PROGRESS - TO DO
A7.1.2.1	Terms and conditions of employment	1. Are all employees, contractors and third party users asked to sign confidentiality and non-disclosure agreements?					
A7.1.2.2	Terms and conditions of employment	2. Do employment / service contracts specifically cover the need to protect business information?					
A7.2	**During employment**	**To ensure that employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their normal work, and to reduce the risk of human error.**					
A7.2.1.1	Management responsibilities	1. Are managers (of all levels) engaged in driving security within the business?					

An ISO27001 Check List for Risk Management, adapted by Philippa Weitz for counsellors and psychotherapists to adopt voluntarily under ISO 27002

ISO 27001: 2013 Ref No.	Title	ISO 27001 Control	TASK 1: What this means to you? What do you need to think about, What extra help or resources might you need?	TASK 2: assess how relevant this item is to your private practice: NON-APPLICABLE, FAIRLY IMPORTANT, VERY IMPORTANT	TASK 2: assess the risk level to your practice: LOW, MEDIUM, HIGH	TASK 3: Create your personalised action plan	ACTION: Choose: - COMPLETED - PROGRESS - TO DO
A7.2.1.2	Management responsibilities	2. Does management behaviour and policy drive, and encourage, all employees, contractors and third party users to apply security in accordance with established policies and procedures?					
A7.2.2	Information security awareness, education, and training	Do all employees, contractors and third party users undergo regular security awareness training appropriate to their role and function within the organisation?					
A7.2.3.1	Disciplinary process	1. is there a formal disciplinary process which allows the organisation to take action against employees who have committed an information security breach?					
A7.2.3.2	Disciplinary process	2. Is this communicated to all employees?					

An ISO27001 Check List for Risk Management, adapted by Philippa Weitz for counsellors and psychotherapists to adopt voluntarily under ISO 27002

ISO 27001: 2013 Ref No.	Title	ISO 27001 Control	TASK 1: What this means to you? What do you need to think about, What extra help or resources might you need?	TASK 2: assess how relevant this item is to your private practice: NON-APPLICABLE, FAIRLY IMPORTANT, VERY IMPORTANT	TASK 2: assess the risk level to your practice: LOW, MEDIUM, HIGH	TASK 3: Create your personalised action plan	ACTION: Choose: - COMPLETED - PROGRESS - TO DO
A7.3	**Termination or change of employment**	**To ensure that employees, contractors and third party users exit an organization or change employment in an orderly manner.**					
A7.3.1.1	Termination or change of employment responsibilities	1. Is there a documented process for terminating or changing employment duties?					
A7.3.1.2	Termination or change of employment responsibilities	2. Are any information security duties which survive employment communicated to the employee or contractor?					
A7.3.1.3	Termination or change of employment responsibilities	3. Is the organisation able to enforce compliance with any duties that survive employment?					
A8	**Asset management**						
A8.1	**Responsibility for assets**	**To achieve and maintain appropriate protection of organizational assets.**					

An ISO27001 Check List for Risk Management, adapted by Philippa Weitz for counsellors and psychotherapists to adopt voluntarily under ISO 27002

ISO 27001: 2013 Ref No.	Title	ISO 27001 Control	TASK 1: What this means to you? What do you need to think about, What extra help or resources might you need?	TASK 2: assess how relevant this item is to your private practice: NON-APPLICABLE, FAIRLY IMPORTANT, VERY IMPORTANT	TASK 2: assess the risk level to your practice: LOW, MEDIUM, HIGH	TASK 3: Create your personalised action plan	ACTION: Choose: - COMPLETED - PROGRESS - TO DO
A8.1.1.1	Inventory of assets	1. Is there any inventory of all assets associated with information and information processing facilities?					
A8.1.1.2	Inventory of assets	2. Is the inventory accurate and kept up to date?					
A8.1.2	Ownership of assets	All information assets must have a clearly defined owner who is aware of there responsibilities. Is this the case?					
A8.1.3.1	Acceptable use of assets	1. Is there an acceptable use policy for each class / type of information asset?					
A8.1.3.2	Acceptable use of assets	2. Are users made aware of this policy prior to use?					
A8.1.4	Return of assets	Is there a process in place to ensure all employers / external users return the organisation's assets on termination of their employment, contract, or agreement?					

T: +44 (0) 1273 700 911
M: +44 (0) 7880 501 116
E: info@pwtraining.com
W: www.pwtraining.com

An ISO27001 Check List for Risk Management, adapted by Philippa Weitz for counsellors and psychotherapists to adopt voluntarily under ISO 27002

ISO 27001: 2013 Ref No.	Title	ISO 27001 Control	TASK 1: What this means to you? What do you need to think about, What extra help or resources might you need?	TASK 2: assess how relevant this item is to your private practice: NON-APPLICABLE, FAIRLY IMPORTANT, VERY IMPORTANT	TASK 2: assess the risk level to your practice: LOW, MEDIUM, HIGH	TASK 3: Create your personalised action plan	ACTION: Choose: - COMPLETED - PROGRESS - TO DO
A8.2	**Information classification**	**To ensure that information receives an appropriate level of protection.**					
A8.2.1.1	Classification guidelines	1. Is there a policy governing information classification?					
A8.2.1.2	Classification guidelines	2. Is there a process by which all information can be appropriately classified?					
A8.2.2	Labelling of information	Is there a process or procedure for ensuring information classification is appropriately marked on each asset?					
A8.2.3.1	Handling of assets	1. Is there a procedure for handling each information classification?					
A8.2.3.2	Handling of assets	2. Are users of information assets made aware of this procedure?					
A8.3	**Media handling**	**To prevent unauthorized disclosure, modification, removal or destruction of assets, and interruption to business activities.**					

An ISO27001 Check List for Risk Management, adapted by Philippa Weitz for counsellors and psychotherapists to adopt voluntarily under ISO 27002

ISO 27001: 2013 Ref No.	Title	ISO 27001 Control	TASK 1: What this means to you? What do you need to think about, What extra help or resources might you need?	TASK 2: assess how relevant this item is to your private practice: NON-APPLICABLE, FAIRLY IMPORTANT, VERY IMPORTANT	TASK 2: assess the risk level to your practice: LOW, MEDIUM, HIGH	TASK 3: Create your personalised action plan	ACTION: Choose: - COMPLETED - PROGRESS - TO DO
A8.3.1.1	Management of removable media	1. Is there a policy for the management of removable media?					
A8.3.1.2	Management of removable media	2. Is there a process covering how removable media is handled?					
A8.3.1.3	Management of removable media	3. Are the policies and procedures communicated to all employees using removable media?					
A8.3.2	Disposal of media	Is there a formal procedure governing how removal media is disposed of?					
A8.3.3.1	Physical media transfer	1. Is there a documented policy and process detailing how physical media should be transported?					
A8.3.3.2	Physical media transfer	2. Is media in transport protected against unauthorised access, misuse or corruption?					
A9	**Access Control**						

An ISO27001 Check List for Risk Management, adapted by Philippa Weitz for counsellors and psychotherapists to adopt voluntarily under ISO 27002

ISO 27001: 2013 Ref No.	Title	ISO 27001 Control	TASK 1: What this means to you? What do you need to think about, What extra help or resources might you need?	TASK 2: assess how relevant this item is to your private practice: NON-APPLICABLE, FAIRLY IMPORTANT, VERY IMPORTANT	TASK 2: assess the risk level to your practice: LOW, MEDIUM, HIGH	TASK 3: Create your personalised action plan	ACTION: Choose: - COMPLETED - PROGRESS - TO DO
A9.1	**Business requirement for access control**	**To control access to information.**					
A9.1.1.1	Access control policy	1. is there a documented access control policy?					
A9.1.1.2	Access control policy	2. Is the policy based on business requirements?					
A9.1.1.2	Access control policy	3. is the policy communicated appropriately?					
A9.1.2	Access to networks and network services	Are controls in place to ensure users only have access to the network resources they have been specially authorised to use and are required for their duties?					
A9.2	**User access management**	**To ensure authorized user access and to prevent unauthorized access to information systems.**					
A9.2.1	User registration and de-registration	Is there a formal user registration process in place?					

An ISO27001 Check List for Risk Management, adapted by Philippa Weitz for counsellors and psychotherapists to adopt voluntarily under ISO 27002

ISO 27001: 2013 Ref No.	Title	ISO 27001 Control	TASK 1: What this means to you? What do you need to think about, What extra help or resources might you need?	TASK 2: assess how relevant this item is to your private practice: NON-APPLICABLE, FAIRLY IMPORTANT, VERY IMPORTANT	TASK 2: assess the risk level to your practice: LOW, MEDIUM, HIGH	TASK 3: Create your personalised action plan	ACTION: Choose: - COMPLETED - PROGRESS - TO DO
A9.2.2	User access provisioning	Is there formal user access provisioning process in place to assign access rights for all user types and services?					
A9.2.3	Management of privileged access rights	Are privileged access rights separately managed and controlled?					
A9.2.4	Management of secret authentication information of users	Is there a formal management process in place to control allocation of secret authentication information (e.g. passwords)?					
A9.2.5.1	Review of user access rights	1. Is there a process for asset owners to review access rights to their assets on a regular basis?					
A9.2.5.2	Review of user access rights	2. Is this review process verified?					
A9.2.6	Removal or adjustment of access rights	Is there a process to ensure user access rights are removed on termination of employment or contract, or adjusted of change of role?					

An ISO27001 Check List for Risk Management, adapted by Philippa Weitz for counsellors and psychotherapists to adopt voluntarily under ISO 27002

ISO 27001: 2013 Ref No.	Title	ISO 27001 Control	TASK 1: What this means to you? What do you need to think about, What extra help or resources might you need?	TASK 2: assess how relevant this item is to your private practice: NON-APPLICABLE, FAIRLY IMPORTANT, VERY IMPORTANT	TASK 2: assess the risk level to your practice: LOW, MEDIUM, HIGH	TASK 3: Create your personalised action plan	ACTION: Choose: - COMPLETED - PROGRESS - TO DO
A9.3	**User responsibilities**	**To prevent unauthorized user access, and compromise or theft of information and information processing facilities.**					
A9.3.1 .1	Use of secret authorisation information including passwords	1. Is there a policy document covering the organisation's practice in how secret authentication information must be handled?					
A9.3.1.2	Use of secret authorisation information including passwords	2. Is this communicated to all users?					
A9.4	**System and application access control**	**To prevent unauthorized access to operating systems.**					
A9.4.1	Information access restriction	Is access to information and application system functions restricted in line with the access control policy?					

An ISO27001 Check List for Risk Management, adapted by Philippa Weitz for counsellors and psychotherapists to adopt voluntarily under ISO 27002

ISO 27001: 2013 Ref No.	Title	ISO 27001 Control	TASK 1: What this means to you? What do you need to think about, What extra help or resources might you need?	TASK 2: assess how relevant this item is to your private practice: NON-APPLICABLE, FAIRLY IMPORTANT, VERY IMPORTANT	TASK 2: assess the risk level to your practice: LOW, MEDIUM, HIGH	TASK 3: Create your personalised action plan	ACTION: Choose: - COMPLETED - PROGRESS - TO DO
A9.4.2	Secure log-on procedures	Where the access control policy requires it, is access controlled by a log-on procedure?					
A9.4.3.1	Password management system	1. Are password systems interactive?					
A9.4.3.2	Password management system	2. Are complex passwords required?					
A9.4.4	Use of privileged utility programs	The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled. Are privileged utility programmes restricted and monitored?					
A9.4.5	Access control to program source code	Is access to the source code od the Access Control System protected?					
A10	**Cryptography**						
A10.1	**Cryptographic controls**						

An ISO27001 Check List for Risk Management, adapted by Philippa Weitz for counsellors and psychotherapists to adopt voluntarily under ISO 27002

ISO 27001: 2013 Ref No.	Title	ISO 27001 Control	TASK 1: What this means to you? What do you need to think about, What extra help or resources might you need?	TASK 2: assess how relevant this item is to your private practice: NON-APPLICABLE, FAIRLY IMPORTANT, VERY IMPORTANT	TASK 2: assess the risk level to your practice: LOW, MEDIUM, HIGH	TASK 3: Create your personalised action plan	ACTION: Choose: - COMPLETED - PROGRESS - TO DO
A10.1.1	Policy on the use of cryptographic controls	Is there a policy on the use of cryptographic controls?					
A10.1.2	Key management	Is there a policy governing the whole lifecycle of cryptographic keys?					
A11	**Physical and environmental security**						
A11.1	**Secure areas**	**To prevent unauthorized physical access, damage and interference to the organization's premises and information.**					
A11.1.1 .1	Physical security perimeter	1. Security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) shall be used to protect areas that contain information and information processing facilities. Is there a designated security perimeter?					

An ISO27001 Check List for Risk Management, adapted by Philippa Weitz for counsellors and psychotherapists to adopt voluntarily under ISO 27002

ISO 27001: 2013 Ref No.	Title	ISO 27001 Control	TASK 1: What this means to you? What do you need to think about, What extra help or resources might you need?	TASK 2: assess how relevant this item is to your private practice: NON-APPLICABLE, FAIRLY IMPORTANT, VERY IMPORTANT	TASK 2: assess the risk level to your practice: LOW, MEDIUM, HIGH	TASK 3: Create your personalised action plan	ACTION: Choose: - COMPLETED - PROGRESS - TO DO
A11.1.1.2	Physical security perimeter	2. Are sensitive or critical information areas segregated and appropriately controlled?					
A11.1.2	Physical entry controls	Do secure areas have suitable entry controls to ensure that only authorized personnel have access?					
A11.1.3.1	Securing offices, rooms and facilities	1. Have offices, rooms, and facilities been designed and configured with security in mind?					
A11.1.3.2	Securing offices, rooms and facilities	2. Do processes for maintaining security (e.g. locking filing cabinets, clearing desks) exist?					
A11.1.4	Protecting against external and environmental threats	Have physical protection measures to protect from natural disasters, accidents or malicious attacks been implemented?					
A11.1.5.1	Working in secure areas	1. do secure areas exist?					

An ISO27001 Check List for Risk Management, adapted by Philippa Weitz for counsellors and psychotherapists to adopt voluntarily under ISO 27002

ISO 27001: 2013 Ref No.	Title	ISO 27001 Control	TASK 1: What this means to you? What do you need to think about, What extra help or resources might you need?	TASK 2: assess how relevant this item is to your private practice: NON-APPLICABLE, FAIRLY IMPORTANT, VERY IMPORTANT	TASK 2: assess the risk level to your practice: LOW, MEDIUM, HIGH	TASK 3: Create your personalised action plan	ACTION: Choose: - COMPLETED - PROGRESS - TO DO
A11.1.5.2	Working in secure areas	2.Where they do exist, do secure areas have suitable policies and processes?					
A11.1.5.3	Working in secure areas	3. Are the policies and procedures enforced and monitored?					
A11.1.6.1	Delivery, and loading areas	Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access. 1. Are there separate delivery /loading areas?					
A11.1.6.2	Delivery, and loading areas	2. Is access to these areas controlled?					
A11.1.6.2	Delivery, and loading areas	3. Is access from these loading areas isolated from information processing facilities?					

T: +44 (0) 1273 700 911
M: +44 (0) 7880 501 116
E: info@pwtraining.com
W: www.pwtraining.com

An ISO27001 Check List for Risk Management, adapted by Philippa Weitz for counsellors and psychotherapists to adopt voluntarily under ISO 27002

ISO 27001: 2013 Ref No.	Title	ISO 27001 Control	TASK 1: What this means to you? What do you need to think about, What extra help or resources might you need?	TASK 2: assess how relevant this item is to your private practice: NON-APPLICABLE, FAIRLY IMPORTANT, VERY IMPORTANT	TASK 2: assess the risk level to your practice: LOW, MEDIUM, HIGH	TASK 3: Create your personalised action plan	ACTION: Choose: - COMPLETED - PROGRESS - TO DO
11.2	**Equipment security**	**To prevent loss, damage, theft or compromise of assets and interruption to the organization's activities.**					
A11.2.1	Equipment siting and protection	1. Are environmental hazards identified and considered when equipment locations are selected?					
A11.2.12	Equipment siting and protection	2. Are the risks from unauthorised access / passers-by considered when siting equipment?					
A11.2.2.1	Supporting utilities	Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities. 1. Is there a UPS system or back-up generator?					
A11.2.2.2	Supporting utilities	2. Have these been tested within an appropriate timescale?					

An ISO27001 Check List for Risk Management, adapted by Philippa Weitz for counsellors and psychotherapists to adopt voluntarily under ISO 27002

ISO 27001: 2013 Ref No.	Title	ISO 27001 Control	TASK 1: What this means to you? What do you need to think about, What extra help or resources might you need?	TASK 2: assess how relevant this item is to your private practice: NON-APPLICABLE, FAIRLY IMPORTANT, VERY IMPORTANT	TASK 2: assess the risk level to your practice: LOW, MEDIUM, HIGH	TASK 3: Create your personalised action plan	ACTION: Choose: - COMPLETED - PROGRESS - TO DO
A11.2.3.1	Cabling security	1. Have risk assessments been conducted over the location of power and telecommunications cabling?					
A11.2.3.2	Cabling security	2. Are they located to protect from interference, interception or damage?					
A11.2.4	Equipment maintenance	Is there a rigorous equipment maintenance schedule?					
A11.2.5.1	Removal of assets	1. Is there a process controlling how assets are removed from the site?					
A11.2.5.2	Removal of assets	2. is this process enforced?					
A11.2.5.3	Removal of assets	3. Are there spot checks?					
A11.2.6.1	Security of equipment and assets off-site	1. Is there a policy covering the security of assets off-site?					
A11.2.6.2	Security of equipment and assets off-site	2. is this policy widely communicated?					
A11.2.7.1	Secure disposal or re-use of equipment	1. Is there a policy covered how information assets may be reused?					

An ISO27001 Check List for Risk Management, adapted by Philippa Weitz for counsellors and psychotherapists to adopt voluntarily under ISO 27002

ISO 27001: 2013 Ref No.	Title	ISO 27001 Control	TASK 1: What this means to you? What do you need to think about, What extra help or resources might you need?	TASK 2: assess how relevant this item is to your private practice: NON-APPLICABLE, FAIRLY IMPORTANT, VERY IMPORTANT	TASK 2: assess the risk level to your practice: LOW, MEDIUM, HIGH	TASK 3: Create your personalised action plan	ACTION: Choose: - COMPLETED - PROGRESS - TO DO
A11.2.7.2	Secure disposal or re-use of equipment	2. Where data is wiped, is this properly verified before reuse / disposal?					
A11.2.8.1	Unattended user equipment	1. Does the organisation have a policy around how unattended user equipment should be protected?					
A11.2.8.2	Unattended user equipment	2. Are technical controls in place to secure equipment that has been inadvertently left unattended?					
A11.2.9.1	Clear desk and clear screen policy	1. Is there a clear desk / clear screen policy?					
A11.2.9.2	Clear desk and clear screen policy	2. Is this well enforced?					
A12	**Operations security**						
A12.1	**Operational procedures and responsibilities**	**To ensure the correct and secure operation of information processing facilities.**					
A12.1.1.1	Documented operating procedures	1. Are operating procedures well documented?					

An ISO27001 Check List for Risk Management, adapted by Philippa Weitz for counsellors and psychotherapists to adopt voluntarily under ISO 27002

ISO 27001: 2013 Ref No.	Title	ISO 27001 Control	TASK 1: What this means to you? What do you need to think about, What extra help or resources might you need?	TASK 2: assess how relevant this item is to your private practice: NON-APPLICABLE, FAIRLY IMPORTANT, VERY IMPORTANT	TASK 2: assess the risk level to your practice: LOW, MEDIUM, HIGH	TASK 3: Create your personalised action plan	ACTION: Choose: - COMPLETED - PROGRESS - TO DO
A12.1.1.2	Documented operating procedures	2. Are the procedures made available to all users who need them?					
A12.1.2	Change management	Is there a controlled change management in place?					
10.1.3	Capacity management	Is there a capacity management process in place?					
10.1.4	Separation of development, test and operational facilities	Development, test, and operational facilities shall be separated to reduce the risks of unauthorized access or changes to the operational system. Doe this happen in your organisation?					

T: +44 (0) 1273 700 911
M: +44 (0) 7880 501 116
E: info@pwtraining.com
W: www.pwtraining.com

An ISO27001 Check List for Risk Management, adapted by Philippa Weitz for counsellors and psychotherapists to adopt voluntarily under ISO 27002

ISO 27001: 2013 Ref No.	Title	ISO 27001 Control	TASK 1: What this means to you? What do you need to think about, What extra help or resources might you need?	TASK 2: assess how relevant this item is to your private practice: NON-APPLICABLE, FAIRLY IMPORTANT, VERY IMPORTANT	TASK 2: assess the risk level to your practice: LOW, MEDIUM, HIGH	TASK 3: Create your personalised action plan	ACTION: Choose: - COMPLETED - PROGRESS - TO DO
A12.2	**Protection from malware**	**Malware is an umbrella term used to refer to a variety of forms of hostile or intrusive software, including computer viruses, worms, trojan horses, ransomware, spyware, adware, scareware, and other malicious programs. It can take the form of executable code, scripts, active content, and other software**					
A12.2.1	Controls against malware	1. Are processes in place to detect malware?					
A12.2.2	Controls against malware	2. Are processes to prevent malware spreading in place?					
A12.2.3	Controls against malware	3. Does the organisation have a process and capacity to recover from a malware infection?					
A12.3	**Back-up**	**To maintain the integrity and availability of information and information processing facilities.**					

An ISO27001 Check List for Risk Management, adapted by Philippa Weitz for counsellors and psychotherapists to adopt voluntarily under ISO 27002

ISO 27001: 2013 Ref No.	Title	ISO 27001 Control	TASK 1: What this means to you? What do you need to think about, What extra help or resources might you need?	TASK 2: assess how relevant this item is to your private practice: NON-APPLICABLE, FAIRLY IMPORTANT, VERY IMPORTANT	TASK 2: assess the risk level to your practice: LOW, MEDIUM, HIGH	TASK 3: Create your personalised action plan	ACTION: Choose: - COMPLETED - PROGRESS - TO DO
A12.3.1.1	Information back-up	1. Is there an agreed back-up policy?					
A12.3.1.2	Information back-up	2. does the organisation's back-up policy comply with the relevant legal frameworks?					
A12.3.1.3	Information back-up	3. Are back-ups tested?					
A12.4	**Logging and Monitoring**	**To detect unauthorized information processing activities.**					
A12.4.1	Event logging	Audit logs recording user activities, exceptions, and information security events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring. Are appropriate event logs maintained and regularly reviewed?					
A12.4.2	Protection of log information	Are logging facilities protected against tampering and unauthorized access?					

An ISO27001 Check List for Risk Management, adapted by Philippa Weitz for counsellors and psychotherapists to adopt voluntarily under ISO 27002

ISO 27001: 2013 Ref No.	Title	ISO 27001 Control	TASK 1: What this means to you? What do you need to think about, What extra help or resources might you need?	TASK 2: assess how relevant this item is to your private practice: NON-APPLICABLE, FAIRLY IMPORTANT, VERY IMPORTANT	TASK 2: assess the risk level to your practice: LOW, MEDIUM, HIGH	TASK 3: Create your personalised action plan	ACTION: Choose: - COMPLETED - PROGRESS - TO DO
A12.4.3	Administrator and operator logs	Are system administrator and system logs maintained, protected and regularly reviewed?					
A12.4.4	Clock synchronization	Are all the clocks of all relevant information processing systems within an organization or security domain synchronized with an agreed accurate time source?					
A12.5	**Control of operational software**						
A12.5.1	Installation of software on operational systems	Is there a process in place to control the installation of software onto operational systems?					
A12.6	**Technical vulnerability management**						
A.12.6.1.1	Management of technical vulnerabilities	1. Does the organisation have access to updated and timely information on technical vulnerabilities?					

T: +44 (0) 1273 700 911
M: +44 (0) 7880 501 116
E: info@pwtraining.com
W: www.pwtraining.com

An ISO27001 Check List for Risk Management, adapted by Philippa Weitz for counsellors and psychotherapists to adopt voluntarily under ISO 27002

ISO 27001: 2013 Ref No.	Title	ISO 27001 Control	TASK 1: What this means to you? What do you need to think about, What extra help or resources might you need?	TASK 2: assess how relevant this item is to your private practice: NON-APPLICABLE, FAIRLY IMPORTANT, VERY IMPORTANT	TASK 2: assess the risk level to your practice: LOW, MEDIUM, HIGH	TASK 3: Create your personalised action plan	ACTION: Choose: - COMPLETED - PROGRESS - TO DO
A.12.6.1.2	Management of technical vulnerabilities	2. Is there a process to risk assess and react to any new vulnerabilities as they are discovered?					
A.12.6.2	Restrictions of software installations	Are there processes in place to restrict how users install software?					
A.12.7	**Information systems audit considerations**						
A.12.7.1.1	Information systems audit controls	1. Are information systems subject to audit?					
A.12.7.1.2	Information systems audit controls	2. Does the audit process ensure business disruption in minimised?					
A13	**Communications security**						
A.13.1	**Network Security management**	**To ensure the protection of information in networks and the protection of the supporting infrastructure**					
A13.1.1	Network controls	Is there a network management process in place?					

An ISO27001 Check List for Risk Management, adapted by Philippa Weitz for counsellors and psychotherapists to adopt voluntarily under ISO 27002

ISO 27001: 2013 Ref No.	Title	ISO 27001 Control	TASK 1: What this means to you? What do you need to think about, What extra help or resources might you need?	TASK 2: assess how relevant this item is to your private practice: NON-APPLICABLE, FAIRLY IMPORTANT, VERY IMPORTANT	TASK 2: assess the risk level to your practice: LOW, MEDIUM, HIGH	TASK 3: Create your personalised action plan	ACTION: Choose: - COMPLETED - PROGRESS - TO DO
A13.1.2.1	Security of network services	1. Does the organisation implement a risk management which identifies all network services and services agreement?					
A13.1.2.2	Security of network services	2. Is security mandated in agreements and contracts with service providers (in-house and outsourced)?					
A13.1.2.3	Security of network services	3. Are security related Service Level Agreement (SLA)'s mandated?					
A13.1.3	Segregation in networks	Groups of information services, users, and information systems shall be segregated on networks. Does the network topology enforce this?					
A.13.2	**Information transfer**						
A.13.2.1.1	Information transfer policies and procedures	1. Do organisational policies govern how information is transferred?					

An ISO27001 Check List for Risk Management, adapted by Philippa Weitz for counsellors and psychotherapists to adopt voluntarily under ISO 27002

ISO 27001: 2013 Ref No.	Title	ISO 27001 Control	TASK 1: What this means to you? What do you need to think about, What extra help or resources might you need?	TASK 2: assess how relevant this item is to your private practice: NON-APPLICABLE, FAIRLY IMPORTANT, VERY IMPORTANT	TASK 2: assess the risk level to your practice: LOW, MEDIUM, HIGH	TASK 3: Create your personalised action plan	ACTION: Choose: - COMPLETED - PROGRESS - TO DO
A.13.2.1.2	Information transfer policies and procedures	2. Are procedures for how data should be transferred made available to all employees?					
A.13.2.1.3	Information transfer policies and procedures	3. Are relevant technical controls in place to prevent non-authorised forms of data transfer?					
A.13.2.2	Agreements of information transfer	Do contracts with external parties and agreements within the organisation detail the requirements for securing business information in transfer?					
A.13.2.3	Electronic messaging	Do security policies cover the use of information transfer whilst using electronic messaging systems?					
A.13.2.4.1	Confidentiality and non-disclosure agreements	1. Do employees, contractors and agents sign confidentiality and non-disclosure agreements?					

An ISO27001 Check List for Risk Management, adapted by Philippa Weitz for counsellors and psychotherapists to adopt voluntarily under ISO 27002

ISO 27001: 2013 Ref No.	Title	ISO 27001 Control	TASK 1: What this means to you? What do you need to think about, What extra help or resources might you need?	TASK 2: assess how relevant this item is to your private practice: NON-APPLICABLE, FAIRLY IMPORTANT, VERY IMPORTANT	TASK 2: assess the risk level to your practice: LOW, MEDIUM, HIGH	TASK 3: Create your personalised action plan	ACTION: Choose: - COMPLETED - PROGRESS - TO DO
A.13.2.4.2	Confidentiality and non-disclosure agreements	2. Are these agreements subject to regular review?					
A.13.2.4.3	Confidentiality and non-disclosure agreements	3. Are records of the agreements maintained?					

An ISO27001 Check List for Risk Management, adapted by Philippa Weitz for counsellors and psychotherapists to adopt voluntarily under ISO 27002

ISO 27001: 2013 Ref No.	Title	ISO 27001 Control	TASK 1: What this means to you? What do you need to think about, What extra help or resources might you need?	TASK 2: assess how relevant this item is to your private practice: NON-APPLICABLE, FAIRLY IMPORTANT, VERY IMPORTANT	TASK 2: assess the risk level to your practice: LOW, MEDIUM, HIGH	TASK 3: Create your personalised action plan	ACTION: Choose: - COMPLETED - PROGRESS - TO DO
A.14	**System acquisition, development and maintenance**						
A.14.1	**Security requirements of information systems**	**To ensure that security is an integral part of information systems.**					
A14.1.1.1	Information security requirements analysis and specification	1. Are information security requirements specified when new systems are introduced?					
A14.1.1.2	Information security requirements analysis and specification	2. When systems are being enhanced or upgraded, are security requirements specified and addressed?					
A14.1.2	Security application services on public networks	Do applications which send information over public networks appropriately protect the information against fraudulent activity, contract dispute, unauthorised discloser and unauthorised modification?					

An ISO27001 Check List for Risk Management, adapted by Philippa Weitz for counsellors and psychotherapists to adopt voluntarily under ISO 27002

ISO 27001: 2013 Ref No.	Title	ISO 27001 Control	TASK 1: What this means to you? What do you need to think about, What extra help or resources might you need?	TASK 2: assess how relevant this item is to your private practice: NON-APPLICABLE, FAIRLY IMPORTANT, VERY IMPORTANT	TASK 2: assess the risk level to your practice: LOW, MEDIUM, HIGH	TASK 3: Create your personalised action plan	ACTION: Choose: - COMPLETED - PROGRESS - TO DO
A.14.1.3	Protecting application services transactions	Are controls in place to prevent incomplete transmission, misrouting, unauthorised message alteration, unauthorised disclosure, unauthorised message duplication or replay attacks?					

An ISO27001 Check List for Risk Management, adapted by Philippa Weitz for counsellors and psychotherapists to adopt voluntarily under ISO 27002

ISO 27001: 2013 Ref No.	Title	ISO 27001 Control	TASK 1: What this means to you? What do you need to think about, What extra help or resources might you need?	TASK 2: assess how relevant this item is to your private practice: NON-APPLICABLE, FAIRLY IMPORTANT, VERY IMPORTANT	TASK 2: assess the risk level to your practice: LOW, MEDIUM, HIGH	TASK 3: Create your personalised action plan	ACTION: Choose: - COMPLETED - PROGRESS - TO DO
A.14.2	**Security in development and support processes**	**To maintain the security of application system software and information.**					
A.14.2.1.1	Secure development policy	1. Does the organisation develop software or systems?					
A.14.2.1.2	Secure development policy	2. If so, are there policies mandating the implementation and access of security controls?					
A.14.2.2	System change control procedures	Is there a formal change control procedure?					
A.14.2.3	Technical review of applications after operating system changes	Is there a process to ensure a technical review is carried out operating systems are changed?					
A.14.2.4	Restrictions on changes to software packages	Is there a policy in place which mandates when and how software packages can be changed and modified?					
A.14.2.5	Secure system engineering principles	Does the organisation have documented principles on how systems must be engineered to ensure security?					

T: +44 (0) 1273 700 911
M: +44 (0) 7880 501 116
E: info@pwtraining.com
W: www.pwtraining.com

An ISO27001 Check List for Risk Management, adapted by Philippa Weitz for counsellors and psychotherapists to adopt voluntarily under ISO 27002

ISO 27001: 2013 Ref No.	Title	ISO 27001 Control	TASK 1: What this means to you? What do you need to think about, What extra help or resources might you need?	TASK 2: assess how relevant this item is to your private practice: NON-APPLICABLE, FAIRLY IMPORTANT, VERY IMPORTANT	TASK 2: assess the risk level to your practice: LOW, MEDIUM, HIGH	TASK 3: Create your personalised action plan	ACTION: Choose: - COMPLETED - PROGRESS - TO DO
A.14.2.6.1	Secure development environment	1. has a secure development environment been established?					
A.14.2.6.2	Secure development environment	2. Do all projects utilise the secure development environment appropriately during the system development lifecycle?					
A.14.2.7.1	Outsourced development	1. Where development has been outsourced is this supervised?					
A.14.2.7.2	Outsourced development	2. Is externally developed code subject to a security review before deployment?					
A.14.2.8	System security testing	Where systems or applications are developed, are they security tested as part of the development process?					
A.14.2.9	System acceptance testing	Is there an established process to accept new systems / applications, or upgrades, into production use?					
A.14.3	**Test data**						

An ISO27001 Check List for Risk Management, adapted by Philippa Weitz for counsellors and psychotherapists to adopt voluntarily under ISO 27002

ISO 27001: 2013 Ref No.	Title	ISO 27001 Control	TASK 1: What this means to you? What do you need to think about, What extra help or resources might you need?	TASK 2: assess how relevant this item is to your private practice: NON-APPLICABLE, FAIRLY IMPORTANT, VERY IMPORTANT	TASK 2: assess the risk level to your practice: LOW, MEDIUM, HIGH	TASK 3: Create your personalised action plan	ACTION: Choose: - COMPLETED - PROGRESS - TO DO
A.14.3.1	Protection of test data	1. Is there a system for selecting test data?					
A.14.3.1	Protection of test data	2. Is test data suitably protected?					
A.15	**Supplier relationships**						
A.15.1	**Information security in supplier relationships**						
A.15.1.1.1	Information security policy for supplier relationships	1. Is information security included in contracts established with suppliers and service providers?					
A.15.1.1.2	Information security policy for supplier relationships	2. is there an organisation-wide risk management approach to supplier relationships?					
A.15.1.2.1	Addressing security within supplier agreements	1. Are suppliers provided with documented security requirements?					
A.15.1.2.2	Addressing security within supplier agreements	2. Is supplier access to information assets & infrastructure controlled and monitored?					

T: +44 (0) 1273 700 911
M: +44 (0) 7880 501 116
E: info@pwtraining.com
W: www.pwtraining.com

An ISO27001 Check List for Risk Management, adapted by Philippa Weitz for counsellors and psychotherapists to adopt voluntarily under ISO 27002

ISO 27001: 2013 Ref No.	Title	ISO 27001 Control	TASK 1: What this means to you? What do you need to think about, What extra help or resources might you need?	TASK 2: assess how relevant this item is to your private practice: NON-APPLICABLE, FAIRLY IMPORTANT, VERY IMPORTANT	TASK 2: assess the risk level to your practice: LOW, MEDIUM, HIGH	TASK 3: Create your personalised action plan	ACTION: Choose: - COMPLETED - PROGRESS - TO DO
A.15.1.3	Information and communication technology supply chain	Do supplier agreements include requirements to address information security within the service and product supply chain?					
A.15.2	**Supplier service delivery management**						
A.15.2.1	Monitoring and review of supplier services	Are suppliers subject to regular review and audit?					
A.15.2.2	Managing changes to supplier services	Are changes to the provision of services subject to a management process which includes security and risk assessment?					
A.16	**Information security incident management**						
A16.1	**Management of information security incidents and improvements**						

An ISO27001 Check List for Risk Management, adapted by Philippa Weitz for counsellors and psychotherapists to adopt voluntarily under ISO 27002

ISO 27001: 2013 Ref No.	Title	ISO 27001 Control	TASK 1: What this means to you? What do you need to think about, What extra help or resources might you need?	TASK 2: assess how relevant this item is to your private practice: NON-APPLICABLE, FAIRLY IMPORTANT, VERY IMPORTANT	TASK 2: assess the risk level to your practice: LOW, MEDIUM, HIGH	TASK 3: Create your personalised action plan	ACTION: Choose: - COMPLETED - PROGRESS - TO DO
A.16.1.1	Responsibilities and procedures	Are management responsibilities clearly defined and documented in the incident management processes?					
A.16.1.2.1	Reporting information security events	1. Is there a process for timely reporting of information security events?					
A.16.1.2.2	Reporting information security events	2.is there a process for reviewing and acting on reported information security events?					
A.16.1.3.1	Reporting security weaknesses	1. Is there a process for reporting of identified information security weaknesses?					
A.16.1.3.2	Reporting security weaknesses	2. Is this system widely communicated?					
A.16.1.3.3	Reporting security weaknesses	3. Is there a process for reviewing and addressing reports in a timely manner?					

An ISO27001 Check List for Risk Management, adapted by Philippa Weitz for counsellors and psychotherapists to adopt voluntarily under ISO 27002

ISO 27001: 2013 Ref No.	Title	ISO 27001 Control	TASK 1: What this means to you? What do you need to think about, What extra help or resources might you need?	TASK 2: assess how relevant this item is to your private practice: NON-APPLICABLE, FAIRLY IMPORTANT, VERY IMPORTANT	TASK 2: assess the risk level to your practice: LOW, MEDIUM, HIGH	TASK 3: Create your personalised action plan	ACTION: Choose: - COMPLETED - PROGRESS - TO DO
A.16.1.4	Assessment of and decisions on information security events	Is there a process to ensure information security events are properly assessed and classified?					
A.16.1.5	Response to information security incidents	Is there an incident response process which reflects the classification and severity of information security incidents?					
A.16.1.6	earning from information security incidents	Is there a process or framework which allows the organisation to learn from information security incidents and reduce the impact / probability of future events?					
A.16.1.7.1	Collection of evidence	1. Is there a forensic readiness policy?					
A.16.1.7.2	Collection of evidence	2. In the event of a an information security incident is relevant data collected in a manner which allows it to be used as evidence?					

An ISO27001 Check List for Risk Management, adapted by Philippa Weitz for counsellors and psychotherapists to adopt voluntarily under ISO 27002

ISO 27001: 2013 Ref No.	Title	ISO 27001 Control	TASK 1: What this means to you? What do you need to think about, What extra help or resources might you need?	TASK 2: assess how relevant this item is to your private practice: NON-APPLICABLE, FAIRLY IMPORTANT, VERY IMPORTANT	TASK 2: assess the risk level to your practice: LOW, MEDIUM, HIGH	TASK 3: Create your personalised action plan	ACTION: Choose: - COMPLETED - PROGRESS - TO DO
A.17	**Information security aspects of business continuity managem**						
A17.1	**Information security aspects**	**To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.**					
A.17.1.1	Planning information security	Is information security included in the organisation's continuity plans?					
A.17.1.2	Implementing information security	Does the organisation's information security function have documented, implemented and maintained processes to maintain continuity of service in an adverse situation?					
A.17.1.3	Verify, review and evaluate information security continuity	Are continuity plans validated and verified at regular intervals?					
A.17.2	**Redundancies**						

An ISO27001 Check List for Risk Management, adapted by Philippa Weitz for counsellors and psychotherapists to adopt voluntarily under ISO 27002

ISO 27001: 2013 Ref No.	Title	ISO 27001 Control	TASK 1: What this means to you? What do you need to think about, What extra help or resources might you need?	TASK 2: assess how relevant this item is to your private practice: NON-APPLICABLE, FAIRLY IMPORTANT, VERY IMPORTANT	TASK 2: assess the risk level to your practice: LOW, MEDIUM, HIGH	TASK 3: Create your personalised action plan	ACTION: Choose: - COMPLETED - PROGRESS - TO DO
A.17.2.1	Availability of information processing facilities	Do information processing facilities have sufficient redundancy to meet the organisations availability requirements?					
A.18	**Compliance**						
A.18.1	**Compliance with legal requirements**	**To avoid breaches of any law, statutory, regulator or contractual obligations and of any security requirements**					
A.18.1.1.1	Identification of applicable legislation and contractual requirements	1. Has the organisation identified and documented all relevant statutory, regulatory, or contractual requirements related to security?					
A.18.1.1.2	Identification of applicable legislation and contractual requirements	2. Is compliance documented?					
A.18.1.2.1	Intellectual property rights (IPR)	1. Does the organisation keep a record of all intellectual property rights and the use of proprietary software products?					

An ISO27001 Check List for Risk Management, adapted by Philippa Weitz for counsellors and psychotherapists to adopt voluntarily under ISO 27002

ISO 27001: 2013 Ref No.	Title	ISO 27001 Control	TASK 1: What this means to you? What do you need to think about, What extra help or resources might you need?	TASK 2: assess how relevant this item is to your private practice: NON-APPLICABLE, FAIRLY IMPORTANT, VERY IMPORTANT	TASK 2: assess the risk level to your practice: LOW, MEDIUM, HIGH	TASK 3: Create your personalised action plan	ACTION: Choose: - COMPLETED - PROGRESS - TO DO
A.18.1.2.2	Intellectual property rights (IPR)	2. Does the organisation monitor for the use of unlicensed software?					
A.18.1.3	Protection of records	Are records protected from loss, destruction, falsification and unauthorised access or release in accordance with legislative, regulatory, contractual, and business requirements?					
A.18.1.4.1	Privacy and protection of personally identifiable information	1. Is personal data identified and appropriately classified?					
A.18.1.4.2	Privacy and protection of personally identifiable information	2. Is personal data protected in accordance with relevant legislation?					

An ISO27001 Check List for Risk Management, adapted by Philippa Weitz for counsellors and psychotherapists to adopt voluntarily under ISO 27002

ISO 27001: 2013 Ref No.	Title	ISO 27001 Control	TASK 1: What this means to you? What do you need to think about, What extra help or resources might you need?	TASK 2: assess how relevant this item is to your private practice: NON-APPLICABLE, FAIRLY IMPORTANT, VERY IMPORTANT	TASK 2: assess the risk level to your practice: LOW, MEDIUM, HIGH	TASK 3: Create your personalised action plan	ACTION: Choose: - COMPLETED - PROGRESS - TO DO
A.18.1.5	Regulation of cryptographic controls	Are cryptographic controls protected in accordance with all relevant agreements, legislation and regulations.					
A.18.2	**Information security reviews**						
A.18.2.1.1	Independent review of information security	1. Is the organisation's approach to managing security subject to regular independent review?					
A.18.2.1.2	Independent review of information security	2. Is the implementation of security controls subject to regular independent review/					
A.18.2.2.1	Compliance with security policies and standards	1. Does the organisation instruct managers to regularly review compliance with policies and procedures within their area of responsibility?					
A.18.2.2.2	Compliance with security policies and standards	2. Are records of these reviews maintained?					

An ISO27001 Check List for Risk Management, adapted by Philippa Weitz for counsellors and psychotherapists to adopt voluntarily under ISO 27002

ISO 27001: 2013 Ref No.	Title	ISO 27001 Control	TASK 1: What this means to you? What do you need to think about, What extra help or resources might you need?	TASK 2: assess how relevant this item is to your private practice: NON-APPLICABLE, FAIRLY IMPORTANT, VERY IMPORTANT	TASK 2: assess the risk level to your practice: LOW, MEDIUM, HIGH	TASK 3: Create your personalised action plan	ACTION: Choose: - COMPLETED - PROGRESS - TO DO
A.18.2.3	Technical compliance review	Does the organisation regularly conduct technical compliance reviews of its information systems?					
A.19	**Other areas of security and confidentiality not included that relate to your private p**						
A.19.1	**Other areas of security and confidentiality o consider**						
A.19.1.1	Additional item to consider (please change this box)						
A.19.1.2	Additional item to consider (please change this box)						

T: +44 (0) 1273 700 911
M: +44 (0) 7880 501 116
E: info@pwtraining.com
W: www.pwtraining.com