HOME AND COMMUNITY CARE SUPPORT SERVICES

SERVICES DE SOUTIEN À DOMICILE ET EN MILIEU COMMUNAUTAIRE

SPO RISK ASSESSMENT

QUESTIONS AND ANSWERS

Note: Some questions have been edited for clarity. Also, as per the memo released on December 8, 2023 providers are not required to complete the section on Service Experience. As such, questions regarding Service Experience are not included in this document.

General Questions

#	Question	Response
1	What is the process for evaluating the results of the assessments and how and when will it be shared with the SPO?	Each section will be reviewed, and risk levels will be assigned based on the responses. It is anticipated that SPOs will receive a letter communicating their results in spring 2024.
2	Will the Risk Assessment outcome affect future prequalification?	HCCSS, Ontario Health, the Ministry of Health, and system partners are working to modernize home care within Ontario. Future Prequalification processes is part of that work, which is ongoing.
3	Will the Risk Assessment outcome affect future contract amendments?	HCCSS, Ontario Health, the Ministry of Health, and system partners are working to modernize home care within Ontario. Future contract amendments are part of that work, which is ongoing.

Risk Assessment Form

#	Question	Response
4	Would it be possible to provide links or copies of all documents referenced/listed just to ensure providers are referencing the right information while confirming their responses?	Relevant links that are referenced within the Risk Assessment Form are as follows: • Policy and Procedures: Home and Community Care Regulations: Ontario Regulation 187.22: Home and Community Care Services • Information and Privacy Commissioner of Ontario • Personal Health Information Protection Act, 2004

Ontario

5	Do you want information that substantiates / explains a yes or no response?	Please see accompanying addendum (released with this FAQ document), which SPOs can use to provide additional information for selected questions. Further, please note that upon review of submissions HCCSS may connect with your organization directly if clarification is required.
6	If an item is in progress is that classified as a Yes or No?	Please see accompanying addendum (released with this FAQ document), which SPOs can use to provide additional information for selected questions.
7	Are copies of agreements with HCCSS required to be submitted, and if so, please specify what copies are needed.	Copies of agreements with HCCSS are not required.

Policies & Procedures – Human Resources

#	Question	Response
8	**[Regarding question 7B in the Risk Assessment Form]** Could it please be confirmed if obtaining an annual offense declaration from staff coupled with the submission of a vulnerable section check every three (3) years would meet the requirement outlined in 7B.	As per each Services Schedule Section 7.4 Human Resource Requirements, the SPOs must verify that each Service Provider Personnel who will provide Services "has obtained a Canadian Police Information Centre computer check and provides an annual offence declaration". The HCCSS/LHIN Service Agreement does not identify a frequency for recurring police vulnerable sector screening (VSS), and only requires an offence declaration/attestation annually. As such, the situation described in this question seems that it would satisfy the requirement in 7B.
9	**[Regarding question 7B in the Risk Assessment Form]** Is it possible to have the option to clarify why a 'No' response may be entered even though the SPO organization addresses the issue with P&P and through different 'audit/provision of proof 'avenues just not in the same manner as outlined in the question? E.g., Annual College registration requires attestations to renew licensing; This is audited by the SPO and/or VSC are mandatory on a 2 yrs. cycle? Etc.	Please see item H1 in the accompanying addendum (released with this FAQ document), which allows for further explanation of question 7B. Note that the method described in the question may be insufficient for SPOs that employ PSWs.
10	**[Regarding question 7B in the Risk Assessment Form]** To confirm, is the annual attestation completed by	Completion of the annual attestation required through the HCCSS SPO agreement meets contractual requirements, but is completed annually after the vulnerable sector

	health care providers sufficient to comply with the vulnerable sector check/police clearance compliance requirement?	check/police clearance requirement has been met upon hire. In addition, SPOs are required to comply with all applicable laws.
11	**[Regarding question 8B in the Risk Assessment Form]** Could it please be confirmed that if an organization itself looks up/confirms college registration status annually, this would meet the requirement outlined in 8B	Please see item H2 in the accompanying addendum (released with this FAQ document), which allows for further explanation of question 8B.
12	**[Regarding question 8B in the Risk Assessment Form]** Is there opportunity to clarify how the same outcome is accomplished without requiring annual attestation by staff? For example, if an organization verifies with individual professional regulatory colleges annually to ensure up to date licensing in good standing for all clinical staff and does not rely on individual attestation, the answer would be 'no' based on the format of the question, yet the issue is being directly addressed and compliance validated.	Please see item H2 in the accompanying addendum (released with this FAQ document), which allows for further explanation of question 8B.
13	**[Regarding question 8B in the Risk Assessment Form]** To confirm, is an annual college registration sufficient to comply with this compliance requirement?	SPO personnel may be registered annually, but this does not mean they are in good standing with their College. Please respond to Question 8B and as per item H2 in the accompanying addendum (released with this FAQ document), add any additional information that may complete your response.
14	**[Regarding question 10 in the Risk Assessment Form]** Can you list some examples of legislative practices identified in the question?	Examples of legislative requirements would include those related to training and development within SPO agreements with HCCSS, including those found within General Conditions and/or services schedules and subsequent amending agreements. These examples are specific to the agreement with HCCSS. However, all SPOs are required to be in compliance with legislative practices for the province of Ontario (E.g. Information and Privacy Commissioner of Ontario, Personal Health Information Protection Act, 2004).

Policies & Procedures – Home and Community Care Regulations

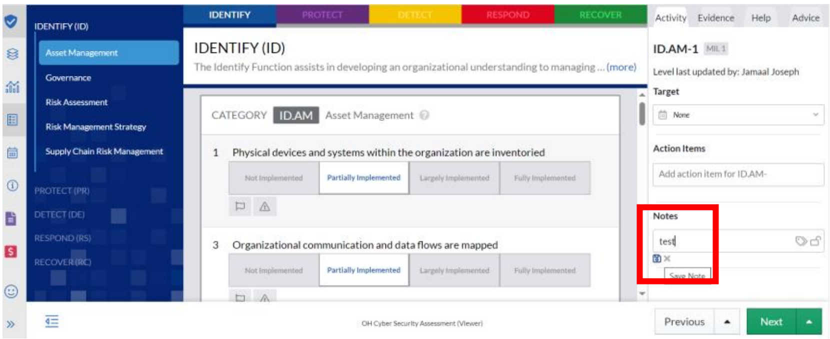
#	Question	Response
15	**[Regarding question 14C in the Risk Assessment Form]** In terms of French Language Services, an organization's webpage is a public domain not exclusively patient facing. Is there an expectation that each SPO provide webpage in both French and English?	Yes, as per an SPO amending agreement distributed in August 2023 "(8) Any websites, webpages, social media and other web-based content maintained by a Service Provider containing information about its services must be available in both English and French." Any portion of an SPO's public facing websites must be bilingual.

Privacy Attestation

#	Question	Response
16	**[Regarding question 16D in the Risk Assessment Form]** With respect to compliance with the 'proposed' requirements is it possible to have the option of partially compliant or compliant with some elements in development/progress? A simple yes/ no answer may not fully reflect what is being done and being put in place to ensure compliance.	Please see item P1 in the accompanying addendum (released with this FAQ document), which allows for further explanation of question 16D.
17	**[Regarding question 16D in the Risk Assessment Form]** Is it possible for the SPO to have opportunity to provide clarification that this is being addressed but not necessarily in the specific format outlined by the question?	Please see item P1 in the accompanying addendum (released with this FAQ document), which allows for further explanation of question 16D.
18	**[Regarding question 16L in the Risk Assessment Form]** Is it possible to have the option of Not-Applicable? If the SPO does not subcontract frontline care delivery services to another agency then answering No implies a lack of compliancy and answering Yes is misleading.	Please see item P2 in the accompanying addendum (released with this FAQ document), which allows for "Not Applicable" to be chosen.
19	**[Regarding question 16L in the Risk Assessment Form]** Does this apply to non-clinical services that may be subcontracted (e.g., afterhours phone service for HCCSS staff to	Subcontracted non-clinical services do not apply to this question.

	contact SPO staff) where there is no direct interaction with clients or access to or retention of client information?	

Cyber Security Assessment – General Questions

#	Question	Response
20	Is it possible to review the questions in advance of submitting responses?	Yes. Once the user is logged into the cyber security assessment, questions can be reviewed and clicked through without entering a response first. Please also see Appendix A within this FAQ document for a list of the questions.
21	When I enter information to Activity\Notes and Evidence tab, they are not being save. Therefore, I am not able to view them or amend them.	Please see the attached screenshot. Upon selecting the Notes tab, a disc icon will be visible underneath. Hover over this tab, and you'll see the option to Save Note. Click here to save your note.  IDENTIFY (ID) The Identify Function assists in developing an organizational understanding to managing ... (more) CATEGORY ID.AM Asset Management 1 Physical devices and systems within the organization are inventoried 3 Organizational communication and data flows are mapped ID.AM-1 MIL 1 Level last updated by: Jamaal Joseph Target None Action Items Add action item for ID.AM- Notes test OH Cyber Security Assessment (Viewer) IDENTIFY (ID) Asset Management Governance Risk Assessment Risk Management Strategy Supply Chain Risk Management PROTECT (PR) DETECT (DE) RESPOND (RS) RECOVER (RC) IDENTIFY PROTECT DETECT RESPOND RECOVER Activity Evidence Help Advice Not Implemented Partially Implemented Largely Implemented Fully Implemented Save Note Previous Next
22	Are we able to download a copy of the Cyber Security Maturity Assessment? If no, can you provide an electronic copy to us?	Please see Appendix A within this FAQ document for a list of the questions within the Cyber Security Maturity Assessment.
23	Why do some cells have "target" listed and others do not?	Targets are not required for this assessment. If they have been selected by the SPO, they can be manually removed by any user with edit access to the assessment. If your organization requires assistance to remove these targets, please contact risk.assessment@ontariohealth.ca.
24	Could the document names be listed under the Activity comments area?	Any comments can be included in the Notes section, including document names.
25	Is any additional information required under the Evidence tab?	Through the Evidence tab, users are able to identify the name and location of evidence that will support the given Maturity Level. Evidence should be retained locally and may be requested during evaluation of the assessment.

26	Is there an expectation that we will require remedial actions by a specific deadline for any individual answers or cumulative sections not deemed to be minimal standard? What is the deadline and what is the impact of not meeting the required score?	It is anticipated that SPOs will receive letters regarding their results in spring 2024. Any remedial actions and related deadlines will be communicated through HCCSS upon review of results.
27	As we are not currently part of the RSOC scope, what is the intended purpose of this assessment? How will the results be used?	The purpose of the SPO Risk Assessment is to ensure compliance with standards regarding privacy, cybersecurity, experience, and the capacity to deliver services. Additionally, it focuses on implementing safeguards for patient safety and maintaining the quality of care. Following the assessment, organizations will receive a letter from Ontario Health, with their results. Shortly after, HCCSS will connect with your organization to support areas of identified risk or any requiring improvement.
28	Please provide an explanation of the scoring system.	The scoring is based on the Maturity Level provided for each question (e.g., Fully implemented, Partially implemented, etc.).
29	What comments/notes/evidence are you looking for in each question? Please provide any specific requirements and examples if possible.	Within the Notes field, users should describe the implemented control to add context to the Maturity Level given. An example could be for ID.RM-1, “Risk management processes are established, managed, and agreed to by organizational stakeholders” that internal processes and accountabilities for risk management are well defined and communicated to all stakeholders within the SPO. Through the Evidence tab, users are able to identify the name and location of evidence that will support the given Maturity Level. Evidence should be retained locally and may be requested during evaluation of the assessment. An example could be the name of a relevant policy, a security control, or applicable technology.
30	How secure is the Axio site?	Please see the Axio webpage at https://axio.com/security-notice/ for relevant information.

Cyber Security Assessment – Specific Questions

#	Question	Response
31	**[Regarding item ID.AM – 3 – Organizational communication and data flows are mapped]** Information flow and system exchanges: Can you please clarify this as I enter the home care site, HPG and upload document. Is this considered a system exchange? How do I respond clearly to this question as a sole provider Physiotherapist?	Yes, that could be considered a system exchange. Business flow processes are related to the flow of data from within your organization as well as also contributed to HPG. Examples could include data uploads, manual data entry and/or document creation.
32	**[Regarding item ID.AM - 5 – Resources (e.g., devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value)]** hardware, In the advice section this is listed “Performing contingency planning on hardware, software, and firmware development can be an effective means of achieving information system resiliency.” I do not develop hardware software of firmware; how do I answer this?	Determining criticality and the value of your digital assets (such as databases, computers, business data, software applications, etc.) are important for contingency planning. This will help to achieve information system resiliency.
33	**[Regarding item ID.AM - 6 – Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established)]** I do not have personal, contractors or third-party personnel, how do I answer this?	Cybersecurity roles and responsibilities are to be documented for the safety and security of your organization as well as organizational data. This can be the responsibility of any number of individuals (e.g., one person or more). This ensures that in the event of a security event or incident it is known whom to contact to address the concern.

Appendix A: Questions within the Cyber Security Maturity Assessment

Viewer Question	Practice Name
IDENTIFY - Asset Management	
ID.AM-1	Physical devices and systems within the organization are inventoried
ID.AM-3	Organizational communication and data flows are mapped
ID.AM-5	Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value
ID.AM-6	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established
IDENTIFY - Governance	
ID.GV-1	Organizational cybersecurity policy is established and communicated
ID.GV-2	Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners
ID.GV-3	Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed
ID.GV-4	Governance and risk management processes address cybersecurity risks
IDENTIFY - Risk Assessment	
ID.RA-5	Threats, vulnerabilities, likelihoods, and impacts are used to determine risk
IDENTIFY - Risk Management Strategy	
ID.RM-1	Risk management processes are established, managed, and agreed to by organizational stakeholders
IDENTIFY - Supply Chain Risk Management	
ID.SC-1	Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders
ID.SC-2	Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process
ID.SC-3	Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.
ID.SC-4	Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.
PROTECT - Identity Management, Authentication and Access Control	
PR.AC-1	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes
PR.AC-2	Physical access to assets is managed and protected
PR.AC-3	Remote access is managed
PR.AC-4	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties
PR.AC-5	Network integrity is protected (e.g., network segregation, network segmentation)
PR.AC-6	Identities are proofed and bound to credentials and asserted in interactions
PROTECT - Awareness and Training	

PR.AT-1	All users are informed and trained
PR.AT-2	Privileged users understand their roles and responsibilities
PR.AT-3	Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities
PR.AT-5	Physical and cybersecurity personnel understand their roles and responsibilities
PROTECT - Data Security	
PR.DS-1	Data-at-rest is protected
PR.DS-2	Data-in-transit is protected
PR.DS-4	Adequate capacity to ensure availability is maintained
PROTECT - Information Protection Processes and Procedures	
PR.IP-5	Policy and regulations regarding the physical operating environment for organizational assets are met
PR.IP-9	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed
PROTECT - Protective Technology	
PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy
PR.PT-3	The principle of least functionality is incorporated by configuring systems to provide only essential capabilities
PR.PT-4	Communications and control networks are protected
DETECT - Anomalies and Events	
DE.AE-1	A baseline of network operations and expected data flows for users and systems is established and managed
DE.AE-2	Detected events are analyzed to understand attack targets and methods
DE.AE-4	Impact of events is determined
DETECT - Security Continuous Monitoring	
DE.CM-1	The network is monitored to detect potential cybersecurity events
DE.CM-2	The physical environment is monitored to detect potential cybersecurity events
DE.CM-4	Malicious code is detected
DE.CM-5	Unauthorized mobile code is detected
DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed
DETECT - Detection Processes	
DE.DP-1	Roles and responsibilities for detection are well defined to ensure accountability
DE.DP-4	Event detection information is communicated
DE.DP-5	Detection processes are continuously improved
RESPOND - Communications	
RS.CO-1	Personnel know their roles and order of operations when a response is needed
RS.CO-2	Incidents are reported consistent with established criteria
RS.CO-3	Information is shared consistent with response plans
RS.CO-4	Coordination with stakeholders occurs consistent with response plans
RESPOND – Analysis	
RS.AN-2	The impact of the incident is understood
RS.AN-3	Forensics are performed
RS.AN-4	Incidents are categorized consistent with response plans

RESPOND – Mitigation	
RS.MI-1	Incidents are contained
RS.MI-2	Incidents are mitigated
RESPOND – Improvements	
RS.IM-1	Response plans incorporate lessons learned
RS.IM-2	Response strategies are updated
RECOVER - Recovery Planning	
RC.RP-1	Recovery plan is executed during or after a cybersecurity incident
RECOVER - Improvements	
RC.IM-2	Recovery strategies are updated
RECOVER - Communications	
RC.CO-3	Recovery activities are communicated to internal and external stakeholders as well as executive and management teams