1.	Have all policies been assigned to an owner responsible for review and approve periodically?
2.	Is there a set of information security policies that have been approved by management, published, and communicated to constituents?
3.	Have all information security policies and standards been reviewed in the last 12 months?
4.	Do all projects involving Scoped Systems and Data go through some form of information security assessment?
5.	Is Information classified according to legal or regulatory requirements, business value, and sensitivity to unauthorized disclosure or modification?
6.	Does the policy or procedure for information handling include encryption requirements?
7.	Does the policy or procedure for information handling include electronic transmission security requirements including email, web, and file transfer services?
8.	Is there a policy or procedure for information handling (storing, processing, and communicating) consistent with its classification that has been approved by management, communicated to appropriate constituents, and assigned an owner to maintain and periodically review?
9.	Is all Scoped Data sent or received electronically encrypted in transit while outside the network?
10.	Does Scoped Data sent or received electronically include protection against malicious code by network virus inspection or virus scan at the endpoint?
11.	Are Information security requirements specified and implemented when new systems are introduced, upgraded, or enhanced?
12.	Are new, upgraded, or enhanced systems required to include a determination of security requirements based on the sensitivity of the data?
13.	Is access to applications, operating systems, databases, and network devices provisioned according to the principle of least privilege?
14.	Is there segregation of duties for granting access and approving access to Scoped Systems and Data?
15.	Are unique IDs required for authentication to applications, operating systems, databases, and network devices?
16.	Is there segregation of duties for approving and implementing access requests for Scoped Systems and Data?
17.	Is there a set of rules governing the way IDs are created and assigned?
18.	Does the password policy require a minimum password length of at least eight characters?
19.	Does the password policy define specific length and complexity requirements for passwords?
20.	Is there a password policy for systems that transmit, process, or store Scoped Systems and Data that has been approved by management, communicated to constituents, and enforced on all platforms and network devices? If no, please explain in the 'Additional Information' field.

21.	Are complex passwords (mix of upper-case letters, lower case letters, numbers, and special characters) required on systems transmitting, processing, or storing Scoped Data?
22.	Is access to systems that store, or process scoped data limited?
23.	Does the password policy require initial and temporary passwords to be changed upon next login?
24.	Does the password policy prohibit keeping an unencrypted record of passwords (paper, software file or handheld device)?
25.	Does the password policy prohibit including unencrypted passwords in automated logon processes (e.g., stored in a macro or function key)?
26.	Does the password policy require passwords to be encrypted in transit?
27.	Does the password policy require passwords to be encrypted or hashed in storage?
28.	Does system policy require logoff from terminals, PC, or servers when the session is finished?
29.	Are outside development resources utilized?
30.	Is data input into applications validated?
31.	Are web applications configured to follow best practices or security guidelines (e.g., OWASP)?
32.	Is HTTPS enabled for all web pages?
33.	Are available high-risk web server software security patches applied and verified at least monthly?
34.	Are Web Server and application logs relevant to supporting incident investigation protected against modification, deletion, and/or inappropriate access?
35.	Is there an established incident management program that has been approved by management, communicated to appropriate constituents and an owner to maintain, and review the program?
36.	Is there a formal Incident Response Plan?
37.	Are events on Scoped Systems or systems containing Scoped Data relevant to supporting incident investigation regularly reviewed using a specific methodology to uncover potential incidents?
38.	Does regular security monitoring include malware activity alerts such as uncleaned infections and suspicious activity?
39.	Are there security and hardening standards for network devices, including Firewalls, Switches, Routers and Wireless Access Points (baseline configuration, patching, passwords, Access control)?
40.	Are all network device administrative interfaces configured to require authentication and encryption?
41.	Are default passwords changed or disabled prior to placing network devices into production?
42.	Is there sufficient detail contained in network device logs to support incident investigation?
43.	Are all available high-risk security patches applied and verified on network devices?

44.	Are network technologies used to isolate critical and sensitive systems into network segments separate from those with less sensitive systems?
45.	Is every connection to an external network (e.g., The Internet, partner networks) terminated at a firewall?
46.	Do network devices deny all access by default?
47.	Do the firewalls have any rules that permit 'any' network, sub network, host, protocol, or port on any of the firewalls (internal or external)?
48.	Are encrypted communications required for all remote network connections from external networks to networks containing Scoped Systems and Data?
49.	Is remote administration of organizational assets approved, logged, and performed in a manner that prevents unauthorized access?
50.	Are encrypted communications required for all remote system access?
51.	Are Network Intrusion Detection capabilities employed?
52.	Is Scoped Data sent or received electronically?
53.	Are applications used to transmit, process, or store Scoped Data?
54.	Are controls validated by independent, third party auditors or information security professionals?
55.	Is there a policy that defines network security requirements that is approved by management, communicated to Constituents, and has an owner to maintain and review?
56.	Is there a DMZ environment within the network that transmits, processes, or stores Scoped Systems and Data?
57.	Is there collection of, access to, processing of, or retention of any client scoped Data that includes any classification of non-public personal information or personal data of individuals?
58.	Is client scoped data collected, accessed, transmitted, processed, or retained that can be classified under U.S. State Privacy Regulations? (e.g., CA, MA, NY, NV, WA, CO)
59.	Is client scoped data collected, accessed, transmitted, processed, or retained that can be classified as European Union covered Personal Data, or Sensitive Personal Data (e.g., genetic data, biometric data, health data)?
60.	Is Client scoped data collected, transmitted, processed, or retained that can be classified as Personal Information as defined by Canadian Personal Information Protection and Electronic Documents Act (PIPEDA) or Canadian Provincial Privacy Regulations
61.	Are there contractual obligations and procedures defined to address breach notification to the client including maintenance of record-keeping obligations of all breaches?
62.	Is documentation of data flows and/or data inventories maintained for client scoped privacy data based on data or asset classification?
63.	Is there a designated organizational structure or function responsible for data privacy or data protection as it relates to client-scoped privacy data?
64.	Are regular privacy impact risk assessments conducted? If yes, please provide frequency and scope in 'Additional Information' field.

65.	Does the organization have or maintain internet-facing websites(s), mobile applications, or other digital services or applications that, collect, use, or retain client-scoped private data and are used directly by individuals?
66.	Is personal data collected directly from an individual on behalf of the client?
67.	Are there documented privacy policies and procedures that address choice and consent based on the statutory, regulatory, or contractual obligations to provide privacy protection for client-scoped privacy data?
68.	For client-scoped Data, is personal data provided to the organization directly by the client?
69.	Are there documented policies and operating procedures regarding limiting the personal data collected and its use to the minimum necessary?
70.	Is there a documented data protection program with administrative, technical, and physical and environmental safeguards for the protection of client-scoped Data?
71.	Do fourth parties, (e.g., subcontractors, sub-processors, sub-service organizations) have access to or process client scoped data?
72.	Are there controls in place to ensure that the collection and usage of client scoped data or personal information used or processed by the organization is limited and in compliance with applicable law?
73.	Is there a documented records retention policy and process with defined schedules that ensure that Personal Information is retained for no longer than necessary?
74.	Are policies and procedures in place to address third party privacy obligations including limitations on disclosure and use of client scoped data?
75.	Is there a data privacy or data protection function that maintains enforcement and monitoring procedures to address compliance for its privacy obligations for client-scoped privacy data?
76.	Are there policies and processes in place to address privacy inquiries, complaints, and disputes?
77.	Are network vulnerability scans performed against internal networks and systems?
78.	Are network vulnerability scans performed against internet-facing networks and systems?
79.	Is there a documented process in place to protect against and detect attacks against automatic software update mechanisms?
80.	Do network vulnerability scans occur at least Monthly?
81.	Are server security configuration reviews performed regularly to validate compliance with documented standards?
82.	Are all servers configured according to security standards as part of the build process?
83.	Are all systems and applications patched regularly?
84.	Is there a documented privacy policy and are procedures maintained for the protection of information collected, transmitted, processed, or maintained on behalf of the client?
85.	Are Hypervisor hardening standards applied on all Hypervisors?
86.	Are Hypervisor Standard builds/security compliance checks required?
87.	Are Hypervisors kept up to date with current patches?
88.	Is sufficient information in Hypervisor logs to evaluate incidents?

89.	Are Hypervisors used to manage systems used to transmit, process, or store Scoped Data?
90.	Are there physical security controls for all secured facilities (e.g., data centers, office buildings)?
91.	Are formal business continuity procedures developed and documented?
92.	Does the approved anti-malware policy or program mandate an interval between the availability of a new anti-malware signature update and its deployment no longer than 24 hours?
93.	Is there a documented third-party risk management program in place for the selection, oversight, and risk assessment of Subcontractors (e.g. service providers, dependent service providers, sub-processors)?
94.	Does the third-party risk management program require Confidentiality and/or Non-Disclosure Agreements from Subcontractors?
95.	Does the third-party risk management program require business units to notify if there are new or changed subcontractors?
96.	Do Subcontractors (e.g., backup vendors, service providers, equipment support maintenance, software maintenance vendors, data recovery vendors, hosting providers, etc.) have access to scoped systems and data or processing facilities?
97.	Is the Cloud Service Provider certified by an independent third party for compliance with domestic or international control standards (e.g., the National Institute of Standards and Technology - NIST, the International Organization for Standardization - ISO)?
98.	Are audits performed to ensure compliance with applicable statutory, regulatory, contractual or industry requirements?
99.	Are Constituents required to attend security awareness training?
100.	Is there a policy or process for the backup of production data?