Grant Thornton

An instinct for growth™

Self-assessment questionnaire

QUESTION	YES	?	NO
Governance			
Do you have appropriate organizational structures, policies and processes in place to help you understand, assess and systematically manage security risks to the network and information systems that support your essential services?			
Is there an effective metrics dashboard and system in place to communicate both your ongoing activities and completed efforts to executive management and shareholders?			
Cyber risk assessment			
Can the organization effectively identify, assess and understand its security risks?			
Are risk assessments conducted to identify, quantify and prioritize risks against criteria for risk acceptance?			
Business resilience and systems security – BCP / DRP			
Does the organization build resilience against cyberattack and system failure into the design, implementation, operation and management of the systems that support the delivery of your essential services?			
Does the organization review and ensure that effective controls are in place around the security operations and architecture of your various levels and platforms, including email, internet activity, patching procedures, intrusion detection and prevention systems, security monitoring and threat intelligence?			
Application security			
Does the organization conduct independent testing and scanning of applications before they are deployed into the production environment? Do you have a defect management process to improve application security by addressing reported issues and bugs?			
Does the organization run static code analysis and dynamic code reviews—either internally or through third parties—before software releases?			
Third party risk management			
Does the organization evaluate and manage security risks that arise as a result of dependencies on external suppliers to the network and information systems that support the delivery of essential services? This includes ensuring that appropriate measures are employed where third party services			
Does the organization retain the contractual right to audit suppliers? Do the contractual clauses provide suppliers with minimum cybersecurity standards and controls they must adhere to?			

QUESTION	YES	?	NO
Identity and access management			
Does the organization review who has access to systems and functions supporting the delivery of essential services on a regular basis to ensure segregation of duties?			
Does the organization maintain an effective access management process that provides access only on "a need to know" basis?			
HR security			
Does the organization conduct screening and reference checks before staff members commence employment? Does it revoke all access upon an employee's termination date?			
Do your staff members have appropriate awareness, knowledge and skills to maintain the security of the network and information systems that support your delivery of essential services?			
Data security management and privacy			
Do you protect the data that you store or transmit electronically from actions that may cause disruption to essential services, such as unauthorized access, modification or deletion?			
Does the organization have the proper controls to classify, handle, store, retain and destroy data as required?			
Does the organization have the proper administrative, physical and technical controls to ensure that employees and third parties are only provided access to data on a need-to-know basis and in accordance with applicable privacy laws and standards?			
Physical security			
Does the organization have a formal physical security program (including CCTV, door ajar alarms) to protect staff and organizational assets?			
Does the organization have the proper environmental controls for its different data centres, including UPS and diesel generators to support continuous operations?			
Security standards compliance			
Have you identified relevant security standards for the organization as part of industry, regulatory or practical requirements?			
Do you perform audits to ensure compliance with relevant legal, regulatory, security and industry requirements?			
Incident response and investigation			
Does the organization have a formalized and well-communicated incident response management plan?			
Does the organization monitor the security status of the networks and systems supporting the delivery of essential services to detect potential security problems and track the ongoing effectiveness of protective security measures?			

West
Shane Troyer
T +1 604 443 2148
E Shane.Troyer@ca.gt.com

Central
Sandy Boucher
T +1 416 339 7027
E Sandy.Boucher@ca.gt.com

East
Leah White
T +1 902 491 7718
E Leah.White@ca.gt.com