CHARTERED PROFESSIONAL ACCOUNTANTS CANADA

Practitioner Guidance

THE IMPACT OF AN EVENT OF AN UNCONTROLLED NATURE ("FORCE MAJEURE EVENT") ON WEBTRUST FOR CERTIFICATION AUTHORITIES ENGAGEMENTS, REPORTING AND SEAL ISSUANCE

Release Date 28 February 2023

Table of Contents

Section One – Introduction

Background

In 2020, COVID-19 impacted businesses worldwide and forced practitioners to work differently as they were unable to physically attend a client location due to local, national and global restrictions. In response to this pandemic, The WebTrust/PKI[1] Assurance Task Force (Task Force) developed non-authoritative guidance (guidance) to highlight matters to consider when planning, performing and reporting on WebTrust engagements in that restrictive environment. The guidance was prepared for use by those practitioners enrolled in the CPA Canada WebTrust for Certification Authorities program and was developed based on the circumstances at the time of publishing. CPA Canada continue to monitor the effects of the global pandemic with a goal of modifying or withdrawing the guidance as appropriate.

In 2023, the impact of COVID-19 restrictions on the work of a practitioner has been, for the most part, eliminated. Although the conditions creating the need for the temporary COVID seal have passed, CPA Canada and the Task Force recognize there may be some circumstances where practitioner report qualifications can be the direct result of an inability to perform certain tests due to the events of uncontrolled nature and/or imposed restrictions related to such events.

Force Majeure Events

With this in mind, CPA Canada has modified the prior COVID-19 related document to deal with a Force Majeure event. Force Majeure generally describes those uncontrollable events that are not the fault of any party and that make it difficult or impossible to carry out normal business. Typically, a Force Majeure event includes natural causes (fire, storms, floods), governmental or societal actions (war, invasion, civil unrest, labour strikes), and infrastructure failures (transportation, energy) for example.

Purpose and Applicability

This guidance has not been issued under the authority of the Auditing and Assurance Standards Board (AASB). CPA Canada and its boards and committees are not responsible for any errors, omissions or results obtained from the use of this guidance. It has not been adopted, endorsed, approved, disapproved or otherwise acted upon by any board, committee, the governing body or membership of CPA Canada or any provincial Institute/Ordre.

1 Public Key Infrastructure.

This guidance considers assurance standards issued up to January 31, 2023 and does not address all aspects of the standards applicable to the types of engagements covered by this guidance. It is intended to be used in conjunction with relevant standards set out in the *CPA Canada Handbook – Assurance*,[2] by the American Institute of Certified Public Accountants (AICPA)[3] and in the International Auditing and Assurance Standards Board's (IAASB) *Handbook of International Quality Control, Auditing, Review, Other Assurance, and Related Services Pronouncements* (IAASB Handbook).[4] The publication date of this guidance should also be considered when determining the applicability of recently issued standards and WebTrust Principles and Criteria (Principles and Criteria).

This guidance is not a substitute for understanding the Principles and Criteria and assurance standards relevant to the engagement. Practitioners are expected to use professional judgment in determining whether the material in the guidance is both appropriate and relevant to the circumstances of each assurance engagement to report on policies and controls at a Certification Authority (CA).

Background on CPA Canada's WebTrust Seals

For 23 years, CPA Canada has administered a WebTrust for CA program where, upon submission of an unqualified report by an enrolled WebTrust practitioner, CPA Canada has issued a WebTrust Seal (Seal) to be placed on the CA's website that is linked to the unqualified practitioner report. The program rules require that assurance engagements be completed within 15 months of the end of the prior engagement period (three months from the end of the subsequent 12-month engagement period) in order to maintain the Seal. If an engagement is not completed within the 15-month period, the underlying Seal expires, and the related link no longer works.

In scenarios where practitioner reports have been qualified, no Seal has traditionally been provided; where required, the CA is required to make the reports publicly available (often through links on their website).

Potential Issues as a Result of a Force Majeure Event

The effects of a Force Majeure event on CAs may result in two distinct types of issues that will impact the execution and/or results of the related WebTrust engagement:

2 Canadian Standard on Assurance Engagements (CSAE) 3000, *Attestation Engagements Other than Audits or Reviews of Historical Information* and CSAE 3001, *Direct Engagements.*

3 AICPA Statement on Standards for Attestation Engagements (SSAE) No. 18, *Attestation Standards: Clarification and Recodification,* and specifically:
- AT-C Section 105, *Concepts Common to All Attestation Engagements*
- AT-C Section 205, *Examination Engagements*

4 International Standard on Assurance Engagements (ISAE) 3000 (Revised), *Assurance Engagements Other than Audits or Reviews of Historical Financial Information.*

1. **Scope limitation:** an inability by the practitioner to obtain evidence of control performance by the CA due to inability to access client premises/records
2. **Control deficiencies:** controls not being performed or not being performed effectively by the CA

There could be instances where both a scope limitation and control deficiencies may be identified in the current circumstances. Each will impact the engagement and related assurance report differently and are discussed further below.

Scope Limitation

The occurrence of a Force Majeure event is likely to impact the way in which a WebTrust practitioner plans and performs testing procedures to support an assurance opinion.

As a result of restricted/limited access to a CA's physical premises and a CA's management, the completion of necessary procedures required to assess whether certain key controls are implemented and operating effectively may be more challenging.

The extent of the impact on engagements will vary depending on a number of factors, including but not limited to:

- timing of the assurance engagement
- knowledge of the client and familiarity with their premises
- relevant laws and regulations for the specific jurisdiction (i.e., as it pertains to event lockdowns or other restrictions)
- relevant policies and procedures adopted by the client and/or the practitioner in response to Force Majeure events

In some cases, the practitioner may be able to perform alternative procedures to evaluate the effectiveness of controls.

Section 2 highlights potential use of alternative techniques to gather evidence since in many cases practitioners are able to adapt their approach to obtain the evidence required. However, if this is not possible, the practitioner will be prevented from issuing an unqualified report in a timely manner.[5]

5 CSAE 3000, paragraph 66, AT-C 205, paragraph 68 and ISAE 3000 paragraph 66, note that if the practitioner is unable to obtain sufficient appropriate evidence, a scope limitation exists and the practitioner is required to issue a qualified conclusion, disclaim a conclusion, or withdraw from the engagement, where withdrawal is possible under applicable laws or regulation, as appropriate.

Typically, a qualified report, for any reason, results in no seal issuance by CPA Canada. However, where access and travel restrictions caused by the global pandemic specifically prevent practitioners from obtaining sufficient appropriate evidence, a temporary CPA Canada WebTrust Seal (Force Majeure Seal) may be issued.

Control Deficiencies

Force Majeure event measures may also create a scenario where the CA is unable to perform (or appropriately perform) certain controls that are required by the various WebTrust engagements. Section 3 highlights, among other things, factors that may impact the effective operation of CA controls and potential areas of challenge in control implementation and operating effectiveness. In the absence of suitable compensating controls, deficiencies of key controls would result in a qualified (or adverse) opinion.[6]

Although deficiencies in controls may be due to the effects of a Force Majeure event on the CA, in this case, the qualification does not relate to an inability to test certain controls, but rather to the fact that the key controls are actually deficient and therefore no temporary a Force Majeure event Seal will be issued.

This non-authoritative guidance discusses these issues in further detail and provides factors for practitioners to consider when conducting and reporting on WebTrust engagements in the current environment. Section 4 of this guidance specifically addresses practitioner reporting considerations for a Force Majeure event-related scope limitations, a Force Majeure event-related control deficiencies and the new temporary Force Majeure Seal that may apply in certain circumstances where a Force Majeure event-related scope limitation exists.

6 CSAE 3000, paragraph 74(b) and ISAE 3000, paragraph 74(b) note that the practitioner is required to express a qualified conclusion or adverse conclusion when, in the practitioner's professional judgment, the subject matter information is materially misstated. The same issue is addressed in ATC-205 paragraphs 68 and 70.

Acknowledgements

This guidance has been prepared by the WebTrust/PKI Assurance Task Force for use by those practitioners enrolled by CPA Canada to perform WebTrust engagements. The Task Force operates under CPA Canada's oversight and is comprised of members who are experienced in PKI and assurance. The Task Force develops the Principles and Criteria to perform WebTrust engagements. The Principles and Criteria are drafted to address elements subject to an assurance engagement in the guidelines and requirements created and updated by the CA/Browser Forum. The Task Force provides periodic updates to the Principles and Criteria based on updates from the CA/Browser Forum. All public Task Force documents and resources on CPA Canada's practitioner qualification and guidance can be found at www.cpacanada.ca/webtrust.

Members of the Task Force are:

- Timothy Crawford, *BDO USA, LLP* (co-Chair)
- Daniel J. Adam
- Donoghue Clarke, *Ernst & Young LLP*
- Chris Czajczyc, *Deloitte LLP*
- Adam Fiock, *BDO USA, LLP*
- Eric Lin, *Ernst & Young LLP*
- Zain Shabbir, *KPMG LLP*
- Donald E. Sheehy

CPA Canada Support

- Anna-Marie Christian, Director Emerging Issues & Strategic Partnerships
- David Chin, Principal, WebTrust (co-Chair)
- Lilia Dubko, Manager, Assurance Programs

Section Two – Testing Relevant Controls Remotely

Potential Impact of Physical Access Limitations

In the current environment, practitioners may be prevented from physically visiting a client CA's primary and secondary locations as a result of government-imposed health and safety measures, including travel and access restrictions.

Accordingly, traditional in-person walkthroughs and testing of certain controls will likely be impacted, such as physical and environmental security controls as well as controls that require live attendance of the practitioner.

For WebTrust for CA engagements, the following are some areas where it may be difficult for the CAs to provide evidence of control performance in traditional ways if physical access is not available:

- security of CA facilities and assets
- security of third-party access
- physical asset classification and management
- physical access controls
- CA key generation and destruction ceremonies
- CA key transportation witnessing (e.g., transportation of HSMs (Hardware Security Modules) from primary site to disaster recovery site)
- HSM key migration ceremonies
- logical security assessments or scans requiring on-site presence (e.g., internal IPs)

Potential Use of Alternative Techniques to Gather Evidence

In assessing the usefulness of alternative techniques, the practitioner should consider matters such as:

- availability of other (local) practitioners in examination of foreign operations
- availability, integrity and reliability of alternative evidence
- familiarity with use of technology in performance of assurance procedures
- ability to obtain evidence of the operating effectiveness of controls during affected period at a later point in time
- existence of mitigating or compensating controls

Depending on the nature of the control, virtual reviews may be inappropriate or unreliable. If alternative procedures cannot be performed, the practitioner may need to limit the scope of the assurance opinion.

Use of Local Practitioners to Examine Foreign Operations

In cases where CA premises are accessible but where the practitioner does not have a local office and travel restrictions are preventing a site visit to the CA's premises, a practitioner may need use the work of another practitioner to obtain the necessary evidence at the foreign operation.

In doing so, the practitioner is required to follow applicable professional standards on using the work of another practitioner, including that the practitioner should:

- evaluate whether the work of another practitioner is adequate for the practitioner's purposes
- where relevant, inform CPA Canada about team members from the local practitioner who are considered key team members as part of the identification of members of the WebTrust engagement team (WebTrust requirement)

Alternative Technique for Physical Inspection: Use of Video

The practitioner may consider the use of video walkthroughs/livestreams to make certain observations related to the implementation and operating effectiveness of CA controls (e.g., to observe physical and environmental access controls at a CA's data centre). The use of video technology as a sole source of evidence can be influenced by a number of factors, based on risk and the ability to obtain corroborative evidence. These factors include, but are not limited to:

- **familiarity with the CA's operations and physical environment:** The practitioner may be more comfortable using video evidence where they have visited the facility previously. Conversely, the practitioner may be uncomfortable using video evidence for new clients.
- **who is controlling the device(s), and how and where the cameras are directed:** If the practitioner is not in control, there is a risk that the video footage may be manipulated.
- **legal and site restrictions on the use of such technology:** The practitioner should consider the existence of privacy legislation and that shared data centres may not permit the hosting of photography or video footage outside the CA facility.
- **whether the practitioner is able to clearly see what is being observed through the video footage:** If the video lacks resolution, then it may not be a reliable source of evidence.
- **risk tolerance of the practitioner/firm with placing reliance on video evidence**

Practitioners should maintain an appropriate level of professional skepticism and carefully evaluate the quality of electronic records and documentation.

To mitigate some of the risks identified above with virtual observations, additional procedures/considerations might include, but are not limited to:

- **geo-tagging of the live stream:** Where available, this helps with specific location identification inside a data centre.
- **corroboration of the live stream from existing camera feeds within the facility:** This helps address room-to-room movements and data centre identification.
- **use of staff that are experienced and familiar with client premises**
- **use of other evidence to corroborate video footage:** For example, in a root key generation, the practitioner may be able to obtain sufficient evidence with respect to a number of controls for a root key generation by reviewing an electronic copy of the script and the video of the generation. Because it may be difficult to transmit live video feed inside a high-security area, it may be necessary to review video of the key generation after the fact.

Alternative Techniques for Documentation and Other Evidence Gathering

The practitioner requires a great deal of supporting documentation from a CA. If the CA's employees are working remotely, the practitioner needs to consider whether sufficient appropriate evidence is likely to be available to support the WebTrust opinion. Even when CA personnel are working remotely, evidence may still be able to be generated and provided to a practitioner.

Reliability of Electronic Evidence and Documentation

The practitioner is required to evaluate whether the information is sufficiently reliable for the engagement. Where the client is an existing client, procedures such as the ones mentioned in this section, when combined with the inspection of relevant documents, records, or electronic files, may enable the practitioner to confirm that the CA controls in operation during a prior period are also in place in the current period. Use of such procedures and inspection will also help the practitioner to understand how changes in the system since the prior period were designed and implemented. However, in a scenario where this is a new client, there may be greater risk in accepting electronic evidence only.

Although the practitioner is not responsible for authenticating the documents themselves, the practitioner needs to exercise professional skepticism when considering their reliability as evidence. For example, the practitioner needs to consider the reliability of scanned or otherwise reproduced source documents and whether the document is faithful in form and content to the original. The following techniques may be considered for assessing reliability:

- Consider whether the electronic document reflects the entire content of the original and includes all signatures.
- Ensure the document is final and not draft documentation.
- Consider the processes (and controls) management has put into place over the conversion and maintenance of hard-copy documents to an electronic format.

If the practitioner has concerns about the authenticity of documentation, the practitioner should obtain additional corroborating evidence if available or consider the need to inspect the original source at a later time, but still in advance of the report date.

Section Three – Control Deficiencies

One of the most important considerations for practitioners conducting a WebTrust engagement in the current environment relates to understanding the impact of a Force Majeure event on the CA's operations, systems, risks and controls.

This section discusses when the practitioner is able to test the operating effectiveness of controls and identifies significant control exceptions caused by the CA not performing or modifying certain key controls due to a Force Majeure event occurring.

Management's Responsibility for Controls and Identification of Force Majeure Event-Related Changes

When there are significant changes to systems and controls, management is responsible for identifying and assessing new risks that might arise from system changes. Management is also responsible for making modifications to controls – or designing and implementing new controls – to mitigate assessed risks.

Where changes have been made as a result of the effects of a Force Majeure event, the timing and reasons for the changes should be noted by management (e.g., if there were government-mandated lockdowns in the CA's country during the period covered by the engagement or other imposed lockdowns or distancing requirements that created the need for the change). Information that describes the changes in controls and procedures should be approved by authorized personnel prior to implementation and full records of the changes should be maintained for assurance purposes. This will assist the practitioner in assessing possible areas where the potential for deficiencies in controls resulting from changes may exist. This is discussed in the paragraphs that follow.

Factors That May Impact the Effective Operation of CA Controls

It is important that the practitioner carefully discuss with management all changes to the CA's operations, systems and controls resulting from a Force Majeure event to assess whether all relevant new risks have been identified and addressed. A new risk could result, for example, from the introduction of remote access software to enable employees to work from home. Depending on whether CAs relax remote access permissions in the current environment, significant deficiencies could be identified related to certain expected controls in a PKI operation. When there are significant modifications to deal with the impacts arising from a Force Majeure event, a practitioner will likely need to reassess engagement and control risks. The practitioner may also have to design and perform different procedures, vary the timing of planned procedures, or perform further procedures in response to the reassessed risks.

In addition to the introduction of procedural changes, existing controls may not be performed in the current circumstances or may not be performed effectively due to the effects of the health and safety issues caused by a Force Majeure event. This may be the case for physical and environmental security controls and operations controls where trusted personnel are typically on-site.

The extent of the impact of a Force Majeure event may vary depending on a number of circumstances, for example:

- geographical location of primary and secondary sites
- operational shutdowns
- reduction or changes in personnel especially those in trusted roles, potentially resulting in segregation of duties issues and/or knowledge gaps
- ability/allowability for certain controls to be performed remotely
- degree of human interaction required vs. automation of controls
- time period within which specific controls need to be performed
- existence of mitigating controls

Regardless of the impact of a Force Majeure event, the practitioner's responsibility to obtain sufficient appropriate evidence to support the opinion in the WebTrust engagement is unchanged.

Potential Areas of Challenge in Control Implementation and Operating Effectiveness

There may be areas where existing/traditional controls need to be modified or may not be enforced in the current environment. Depending on the individual facts and circumstances of the CA, several WebTrust for CA control areas may be impacted, such as:

- personnel security
- physical and environmental security
- operations management
- system access management
- business continuity
- key generation, destruction, and transport

In addition, public CAs are required to have engagements performed and practitioner reports provided that use the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security criteria. Several criteria have time-sensitive elements (and a need for trusted roles) that could be impacted by remote working arrangements and other Force Majeure event limitations. These include, for example:

- certificate revocation
- key generation
- network and certificate security requirements criteria
- trusted roles, delegated third parties, and system accounts
- vulnerability detection and patch management

Practitioner Report Considerations

This is addressed in more detail in Section 4. In dealing with a deficiency in the implementation or operating effectiveness of the control, the practitioner should determine the following:

- **timing and/or the period over which the deficency(ies) exists:** This will determine whether the deficiency(ies) identified should be reported as being COVID-19-related or not.
- **significance of the deficency(ies) as it pertains to achievement of the relevant criterion being reported upon:** The significance will determine whether the issue will be reported using:
  - a qualified or an adverse opinion or
  - an emphasis of matters / other matters paragraph.

Modified Assertion[7]

Where deficiencies in controls exist, it has become more common to have the management assertion modified to reflect the control deficiencies and related criteria that were not met as a result. In addition, where there are significant impacts caused by a Force Majeure event, consideration should be given to adding additional commentary in the assertion that deals with the significant changes caused by a Force Majeure event and the period in which these changes were in effect. That would include, for example:

- effects of a Force Majeure event on the CA, its operations, and technologies used in providing CA services
- disclosure of all significant changes to CA systems and related controls due to a Force Majeure event

7 In CPA Canada and International Standards, the word statement is used in the standard rather than assertion.

An example of a modified assertion is provided in the reporting guidance is set out in the article titled **Practitioner Qualification and Guidance**.

Management Representation Letters

During this pandemic, the practitioner may request management to make additional representations. Those additional representations may relate to any of the following:

- effects of a Force Majeure event on the CA, its operations, and technologies used in providing CA services
- any communications to customers and business partners about changes in CA service level agreements or commitments
- disclosure of all significant changes to CA systems and related controls due to a Force Majeure event
- identification and assessment of new risks arising from changes to systems and related controls

Section Four – Qualified Practitioner Reports and Temporary Force Majeure Event Seal

This section covers practitioner reports that are qualified as a result of:

- a scope limitation due to inability to access client premises/records
- deficiencies in controls as a result of a Force Majeure event

This section also introduces the new temporary Force Majeure event Seal that CPA Canada will issue in limited circumstances for a pre-determined period and with specific conditions.

Scope Limitation Due to Inability to Access Client Premises/ Records

As a result of being unable to access client locations/records due to a Force Majeure event-related conditions, practitioners may be unable to obtain sufficient evidence with respect to the Principles and Criteria. Due to the limitation in scope of the engagement, practitioners may be unable to issue an unqualified report and receive the traditional Seal.

Factors to Consider in Determining Whether a Force Majeure Event-Related Scope Limitation Exists

The key issue in determining and evidencing whether the scope limitation is due to the impact of a Force Majeure event depends on whether:

- the scope restriction is caused by government-imposed travel/access restrictions during a Force Majeure event restriction period; and
- as a result of the restriction, the practitioner is unable to obtain sufficient evidence through traditional and/or alternative techniques or procedures

Impact of a Force Majeure Event-Related Scope Limitation

An engagement that has been directly impacted by Force Majeure event, and has specifically affected the practitioner's ability to obtain sufficient and appropriate evidence, will result in a qualified report and should contain a separate paragraph that would be headed, for example, Basis for Qualified Opinion – Scope Limitation Due to a Force Majeure event. This paragraph would then detail the locations that could not be attended, the controls that could not be tested and the criteria that could not be satisfied as part of the engagement.

A Temporary Force Majeure Event Seal Issuance and Replacement of Traditional Seal

Limitations caused by an inability to physically attend due to a Force Majeure event-related restriction differ from traditional scope limitations and, as such, are being considered differently by CPA Canada for a limited time from a Seal issuance perspective.

A temporary Force Majeure event Seal is being introduced to recognize the extraordinary circumstances caused by the Force Majeure event pandemic and is not intended to replace the traditional Seal. To recognize the temporary nature of the circumstances, a temporary Force Majeure event Seal is permitted to remain on a CA's website for a maximum of six months from the end date of the period examined.

The process for obtaining a temporary Force Majeure event Seal will follow the same process as that followed to obtain a traditional Seal for unqualified reports using the same seal request form with additional information provided. The documentation should note that:

- the practitioner report has been qualified
- the qualification is directly related to Force Majeure event scope restrictions only and is disclosed in the practitioner's report
- there are no qualifications with respect to control deficiencies during the period

When a CA has been granted a temporary Force Majeure event Seal, it is expected that the practitioner will be able to perform the procedure(s) that could not be completed initially which gave rise to the scope limitation before the temporary Force Majeure event Seal expires (six months from the end of the period examined). A renewal reminder will be issued to the practitioner when there are three months remaining in the life of the temporary Force Majeure event Seal. Where the practitioner is able to perform such procedures and is able to subsequently issue an unqualified report for the CA, the unqualified report could then be submitted to CPA Canada to obtain the traditional Seal. Where the practitioner is not able to perform such procedures and is not able to subsequently issue an unqualified report for the CA, the temporary Force Majeure event Seal will be deactivated at the expiry date.

Control Deficiencies as a Result of a Force Majeure Event

If deficiencies of controls are a direct result of issues caused by a Force Majeure event, consideration could be given to setting them out in a separate basis for qualification paragraph in the practitioner report.

The qualification section may be separately identified as, for example, Basis for Qualified Opinion – Control Deficiencies Due to a Force Majeure event. Consider the following example:

Basis for Qualified Opinion – Control Deficiencies Due to a Force Majeure event
During our procedures, we noted the following deficiencies that occurred during the period in which, due to a Force Majeure event, government-imposed access restrictions were in force at the primary location from March 2023 to July 2023, which caused a qualification of our opinion:

Item	Observation	Relevant WebTrust Criteria
1	We noted that electronic dual-custody multi-factor entrance and exit controls to the secure PKI stopped working in April 2020 and were unable to be repaired until the end of July 2020 when third-party suppliers were able to supply and install new equipment. This caused WebTrust Principles and Criteria for Certification Authorities v2.2, Criterion 3.4 to not be met.	3.4: The CA maintains controls to provide reasonable assurance that: • physical access to CA facilities and equipment is limited to authorised individuals, protected through restricted security perimeters, and is operated under multiple person (at least dual custody) control; • CA facilities and equipment are protected from environmental hazards; • loss, damage or compromise of assets and interruption to business activities are prevented; and • compromise of information and information processing facilities is prevented.

Item	Observation	Relevant WebTrust Criteria
2	Traditionally, the disaster recovery plan testing is conducted in May of each year. The plan is then amended in June of each year, if required, based on the results of testing. The disaster plan was not tested in May 2020. Additionally, physically secure disaster recovery facilities were not available. This caused WebTrust Principles and Criteria for Certification Authorities v2.0, Criterion 3.8 to not be met.	3.8: The CA maintains controls to provide reasonable assurance of continuity of operations in the event of a disaster. Such controls include, at a minimum: • the development and testing of a CA business continuity plan that includes a disaster recovery process for critical components of the CA system; • the storage of required cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location; • the storage of backups of systems, data and configuration information at an alternate location; and • the availability of an alternate site, equipment and connectivity to enable recovery. The CA maintains controls to provide reasonable assurance that potential disruptions to Subscribers and Relying Parties are minimised as a result of the cessation or degradation of the CA's services.

The opinion paragraph would separate qualifications due to a Force Majeure event-related issues from other qualifications, if appropriate.

Seal

No traditional Seal or a temporary Force Majeure event Seal is issued to a CA where a control deficiency is identified that is sufficient to cause a qualified or adverse opinion.

Conclusion

The impact of a Force Majeure event on the engagement will depend on individual facts and circumstances of the CA and related engagement. It will vary depending on a number of factors including but not limited to geographic location of the CA and practitioner, government-imposed health and safety measures, and timing of the engagement. The issues and related response should be assessed on a case-by-case basis. CPA Canada will continue to monitor the effects of the global pandemic and modify or withdraw this guidance as appropriate. Please visit our website for the latest updates and resources at www.cpacanada.ca/webtrust.