PIEVC Engineering Protocol for Climate Change Infrastructure Vulnerability Assessment

Part I

April 2009

For further information about this ***Engineering Protocol*** or the ***National Engineering Vulnerability Assessment*** **Project** please contact the PIEVC Secretariat at Engineers Canada:

David Lapp, P.Eng.
Manager, Professional Practice
Engineers Canada

1100-180 Elgin Street
Ottawa, Ontario, Canada
K2P 2K3

david.lapp@engineerscanada.ca

(613) 232-2474 Ext. 240

Table of Contents

Part I – Background, Overview and Guidance

List of Figures

Part I – Background, Overview and Guidance

1 Introduction and Scope

This document is intended to guide practitioners through the ***PIEVC Engineering Protocol for Climate Change Infrastructure Vulnerability Assessment*** (the Protocol). The Protocol is a step-by-step process to assess the impact of climate change on infrastructure. Information developed through this assessment process will assist owners and operators to effectively incorporate climate change adaptation into design, development and management of their existing and planned infrastructure. This protocol has been successfully utilized to assess four categories of infrastructure:

1. Buildings
2. Roads and associated structures
    - Culverts
    - Surface
    - Bridges
    - Etc.
3. Stormwater and wastewater treatment and collection systems
4. Water resource systems and other water management infrastructures
    - Potable water collection
    - Treatment and distribution
    - Water control dams
    - Retention and flood control structures
    - Etc.

The Protocol describes a step-by-step process of risk assessment and engineering analysis for evaluating the impact of climate change on infrastructure. The observations, conclusions and recommendations derived from the application of this protocol provide a framework to support effective decision-making about infrastructure operation, maintenance, planning and development.

This Protocol has been developed for owners and operators to assess public infrastructure. However, the principles and steps will be similar for assessing privately owned infrastructure.

The Protocol was developed with funding contributions from Natural Resources Canada. Engineers Canada (the business name of the Canadian Council of Professional Engineers) owns the intellectual property that is the Protocol. It may be used in Canada for Canadian-based infrastructure without charge, provided the user signs a license agreement with Engineers Canada. The Protocol may be used internationally for infrastructures located outside Canada subject to the payment of a license fee and a license agreement with Engineers Canada.

The Public Infrastructure Engineering Vulnerability Committee (PIEVC) is a national steering committee set up by Engineers Canada in 2005. This committee consists of senior representatives from Federal, provincial and municipal levels of government in Canada along with several non-government organizations. It oversees the National Engineering Vulnerability Assessment project, a long term initiative of the Canadian engineering profession to assess the

vulnerability of public infrastructures to the impacts of future changes in climate. This information is a vital input to propose adjustments and amendments to infrastructure codes and standards and related engineering practices.

Note that Engineers Canada provides the Secretariat for the PIEVC and is responsible for all legal and administrative agreements relating to the use of the Protocol.

PIEVC is supported by infrastructure Expert Working Groups consisting of engineers and other technical experts with design and operations experience in the particular infrastructure category as well as climate scientists and other subject matter experts. PIEVC currently has four such groups as follows:

1. Buildings
2. Roads and associated structures
3. Stormwater and wastewater systems
4. Water resource management systems

This document is divided into three main sections:

1. Description of the processes and organization for planning engineering vulnerability assessments of public infrastructure
2. Presentation of the basic principles of risk management that are applicable to this work, along with technical references
3. Procedural description of the five steps involved in executing the Protocol.

The document includes worksheets to record the work completed at each step.

2 Vulnerability Assessment Planning and Execution

Engineering vulnerability assessments normally involve one or, at most, a few individual infrastructures rather than an entire inventory. The individual infrastructure(s) should be carefully selected to provide a representative sample of the inventory. If significant vulnerabilities are detected, and there is widespread variability in nature and severity of vulnerabilities, it may be necessary to assess all individual infrastructures in an inventory to determine what adaptive actions are required for an individual infrastructure.

PIEVC has developed a five-phase process for planning and executing vulnerability assessments, including:

- Phase I – Initial Contact and Preliminary Discussions
- Phase II – Project Scoping and License Agreement
- Phase III – Procurement of Expertise
- Phase IV – Engineering Vulnerability Assessment
- Phase V – Conclusions and Recommendations

These phases are briefly described in the following sections and are presented graphically in

Figure 1.

Note that the engineering vulnerability assessment of an individual infrastructure or group of infrastructures is referred to as the "Project" for the remainder of this document.

2.2 Phase I - Initial Contact and Preliminary Discussions

Discussion for a Project may be initiated in a number of ways:

- The PIEVC Secretariat approaches an owner or operator or their representative (the "Project Partner") and negotiate a Project. The Project Partner may be represented on one of PIEVC's various committees or may be approached due to some unique features of the infrastructure or its location;

- A potential Project Partner may approach PIEVC with a unsolicited proposal;

- The PIEVC Secretariat issues a Request for Expression of Interest to infrastructure owners, soliciting their interest in a Project; or

- Consultants may identify potential infrastructure assessment sites and approach the infrastructure owner and the PIEVC Secretariat with an unsolicited proposal.

The Protocol is the intellectual property of Engineers Canada, and owners/operators of infrastructure, as well as third-party users, (e.g. consultants) may not use it without the permission of Engineers Canada, which is normally granted through the signing of a license agreement. Part of this agreement includes the obligation to share the results of the assessment with the Federal Government of Canada, PIEVC and Engineers Canada.

2.3 Phase II - Project Scoping

Once the potential Project Partner confirms their serious intent to pursue an assessment, the Project enters the Project Scoping and License Agreement phase. During this phase, the project partner and the PIEVC Secretariat:

- Complete the initial stages of the project definition in sufficient detail to complete a project work statement suitable for procurement purposes
- Negotiate and sign a License Agreement between Engineers Canada and the Project Partner;
- Negotiate a memorandum of agreement (MOA) that outlines the roles and responsibilities of Engineers Canada and the Project Partner, as well as terms and conditions that will govern the Project. It includes the License Agreement and may include additional sections that cover any financial obligations between or among the signing parties as well as any additional administrative policies and procedures needed to execute the agreement;
- Normally an outside consultant is required, and arrangements for procuring these

services utilize the procurement policies and procedures of the Project Partner which may include the development of a Request for Proposal (RFP) for cases where a competitive process is required or desired.

The PIEVC Secretariat has generic versions of MOAs, works statements, and RFPs that can help guide this process. These are available through the Secretariat. However, every infrastructure owner has unique management and technical circumstances that may affect the terms and conditions that will guide this process.

Detailed instructions for developing a project definition are integral to this Engineering Protocol and are outlined in Section 8.1 of this document. Project proponents are encouraged to use these procedures and the related worksheets provided under separate cover to guide the project definition process. Obviously, at the project scoping stage, project proponents will not have access to all of the data necessary to complete this step of the engineering protocol. However, the methodology and underlying thought process will significantly aid the project proponent to identify the key components that must be incorporated in the project Work Statement to provide potential consultants with sufficient information to appropriately scope and cost the engineering assessment.

Normally, at the completion of Project Scoping PIEVC and the infrastructure owner will have developed and agreed to three key documents:

1. A Memorandum of Agreement;
2. A Project Work Statement: and
3. A Request for Proposal.

These documents along with this Engineering Protocol will guide the rest of the assessment process.

PIEVC is aware that other project management alternatives may be more suitable in some circumstances. However, in every case the project proponent and PIEVC must clearly articulate the project definition and delineate management responsibilities. In some circumstances the project management tools may differ slightly from those outlined above but the process must always result in similar management system controls for the project.

2.4 Phase III - Procurement of Expertise

Normally, the Project partner will manage the procurement of expertise according to their own policies and procedures.

The RFP developed in Phase II will be used to guide the technical requirements of the process.

During this stage, the PIEVC Secretariat will normally facilitate the formation of a Project Advisory Group consisting of representatives from the:

- Infrastructure owner;

- PIEVC Secretariat;
- Corresponding PIEVC Expert Working Group; and
- Other groups, as appropriate.

One of the roles of the Project Advisory Group is to assist in the evaluation of proposals and to advise the Project Partner that the technical requirements of the work are met and the project team has the requisite mix of expertise and experience to satisfy the requirements.

Representatives from the project oversight group may assist the infrastructure owner evaluate proposal documents.

In some circumstances the Project Partner may deem it appropriate to sole-source the project to a specific consultant. The PIEVC Secretariat and Engineers Canada have no objection to this approach provided that any sole-source contract meets the project management guidelines of the infrastructure owner and written justification is provided to the PIEVC Secretariat.

It is recommended that the Project Partner negotiate a consultant agreement incorporating the Work Statement developed during Phase II.

2.5 Phase IV - Vulnerability Assessment

The PIEVC Engineering Protocol will guide the vulnerability assessment. The protocol is detailed in Sections 3 and 4.

The consultant will provide three key deliverables.

1. Prior to initiating detailed work, it is strongly recommended that the consultant provide an engagement plan outlining their key deliverables, schedule, personnel and management controls governing the vulnerability assessment.
2. Each month, the consultant will provide a written progress report.
3. At project completion the consultant will provide a detailed project report outlining conclusions on the nature and severity of the findings, conclusions on the nature and severity of infrastructure component vulnerabilities and recommendations.

The approved project Work Statement may also identify other key deliverables specific to the particular infrastructure owner or PIEVC needs.

On a regular basis, the consultant will convene a project update teleconference/meeting including the PIEVC project oversight committee.

2.6 Phase V - Conclusions and Recommendations

At the completion of the vulnerability assessment the consultant will provide a set of conclusions and recommendations relating to the climate impact and adaptation of the infrastructure. These conclusions and recommendations will fall into several categories, as outlined in Section 4.5:

1. A report of infrastructure components that have been assessed to be vulnerable.

2. Initial recommendations regarding possible:
    i. Remedial engineering actions;
    ii. Monitoring of structure over a set time period;
    iii. Management actions;
    iv. Additional data collection; or
    v. Additional engineering analysis of particular infrastructure components that may be necessary to determine extent and nature of vulnerabilities.

3. A report on the infrastructure components that have been assessed to have sufficient adaptive capacity to withstand projected climate change impacts; thus requiring no further action at this time.

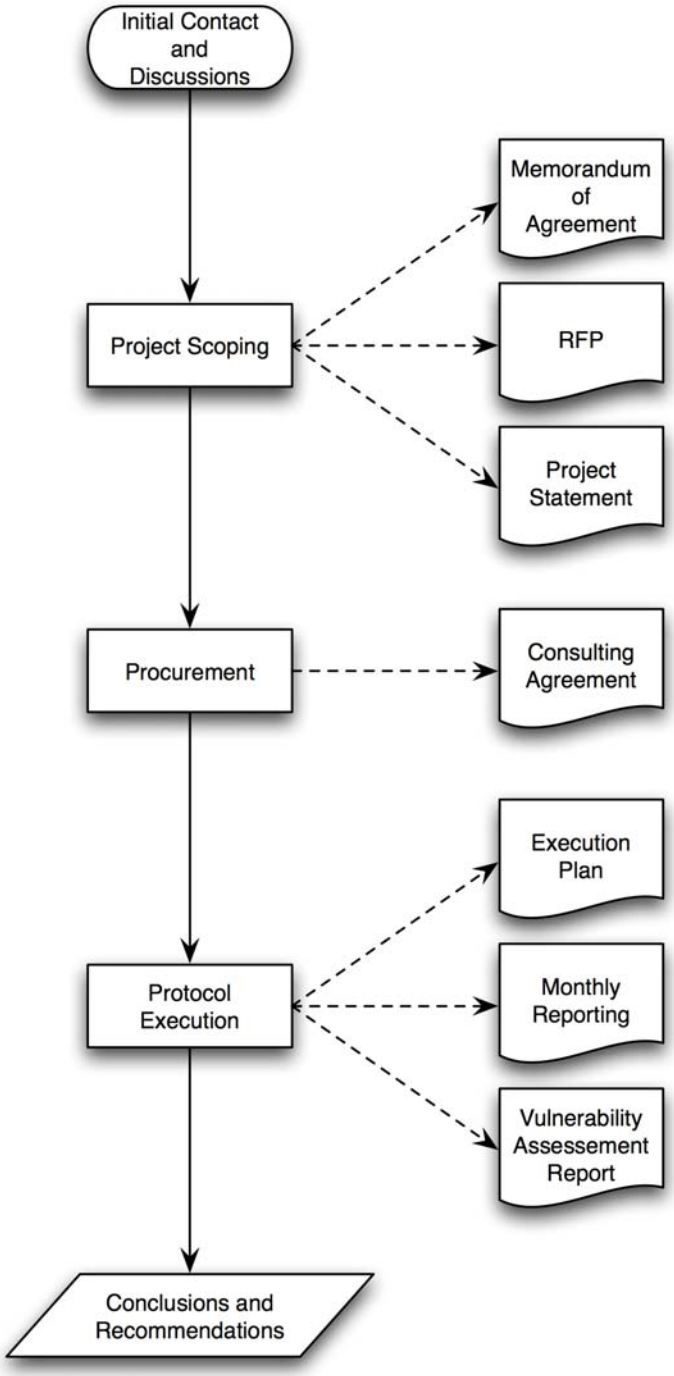
4. A report on data gaps and availability; requiring additional work or studies.

5. Identification of infrastructure components that may be evaluated in the future.

6. A report on other conclusions, trends, insights and limitations.

As part of any License Agreement with Engineers Canada, the Project Partner will forward a copy of the report, including the conclusions and recommendations to Engineers Canada. The findings will be synthesized and incorporated within a ***National Engineering Vulnerability Registry*** that is managed by Engineers Canada. The registry is used to sort, consolidate and analyze engineering vulnerabilities in the four infrastructure categories at the component level.

Figure 1: Overall Project Execution Process



3 Protocol Overview

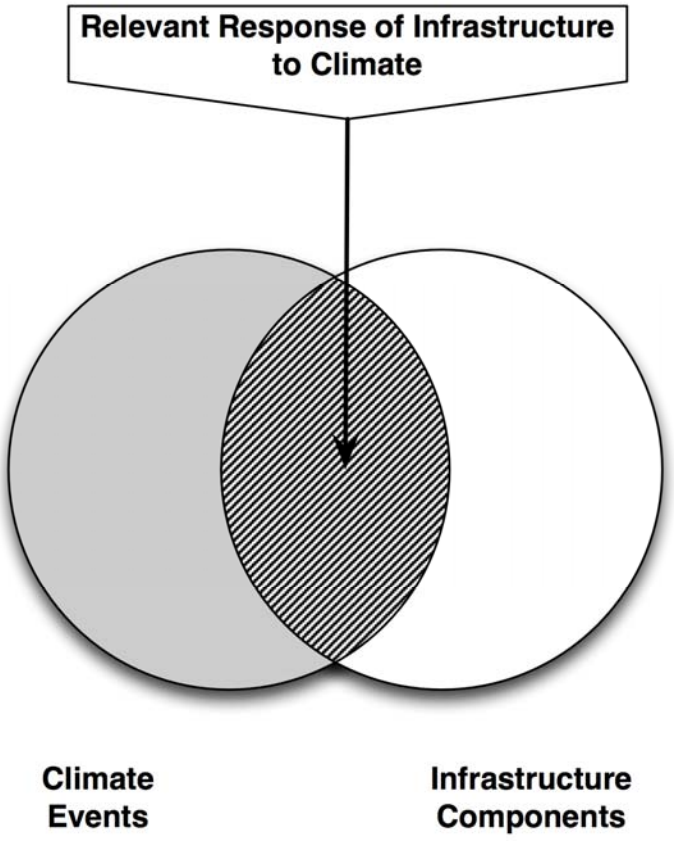
Climate data is used to design infrastructure. Under climate change, historic data may no longer be appropriate. As a result, infrastructure may be vulnerable. Existing infrastructure may not have sufficient resiliency. New infrastructure may not be designed with sufficient load and adaptive capacity.

To assess climate change infrastructure vulnerability, the practitioner must evaluate:

1. The infrastructure;
2. The climate (historic, recent and projected); and
3. Historic and forecast responses of the infrastructure to the climate.

This interaction is depicted in Figure 2.

Figure 2: Venn Diagram Illustrating Relevant Interactions between Climate and Infrastructure



A great deal of information may be available to describe the infrastructure and the climate in the

region. The protocol sets out a procedure to sift the data to develop an understanding of how climate and infrastructure interact to create vulnerability. Not *all* climate and infrastructure data is necessary to complete the protocol. The initial stages of the protocol help the practitioner identify the *key* data necessary to complete the assessment. Throughout the protocol the practitioner is directed to continuously evaluate the availability and quality of data sufficient to support conclusions and recommendations.

The protocol is divided into five steps, as illustrated in Figure 3. Each step of the protocol is described in greater detail in Sections 3.1 through 3.5.

Figure 3: Overview of the Protocol

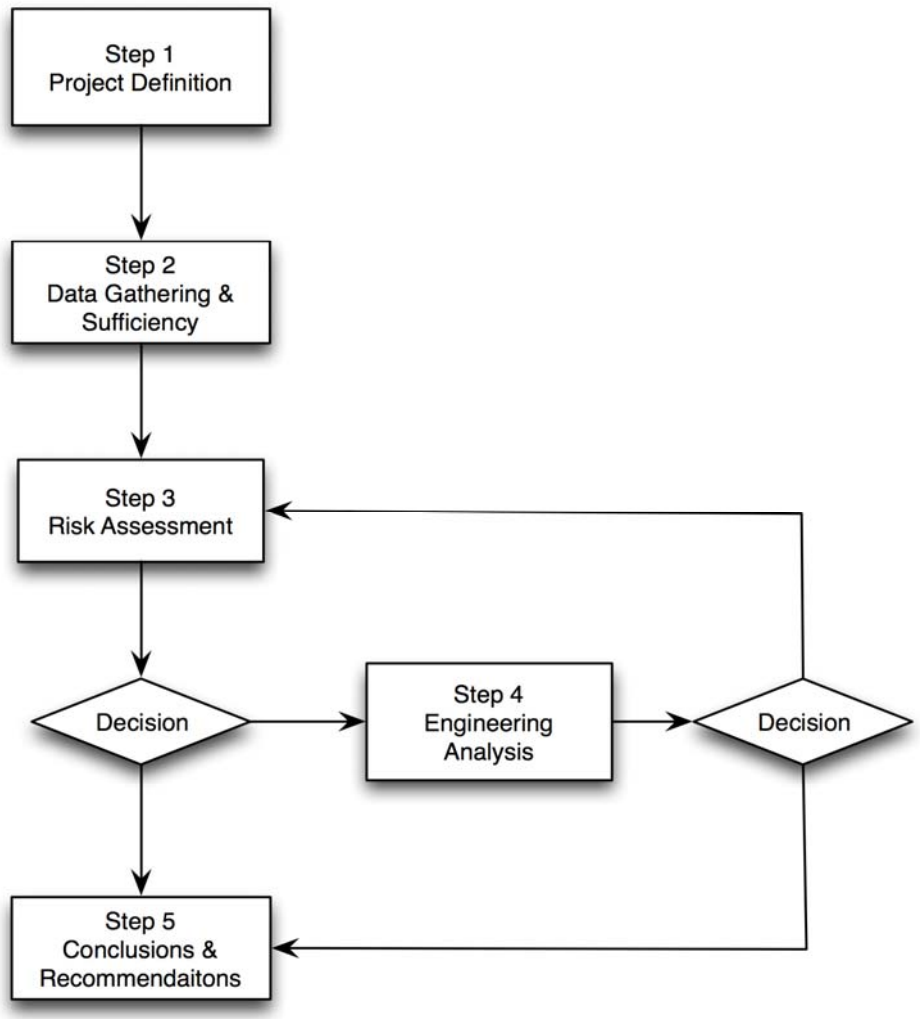
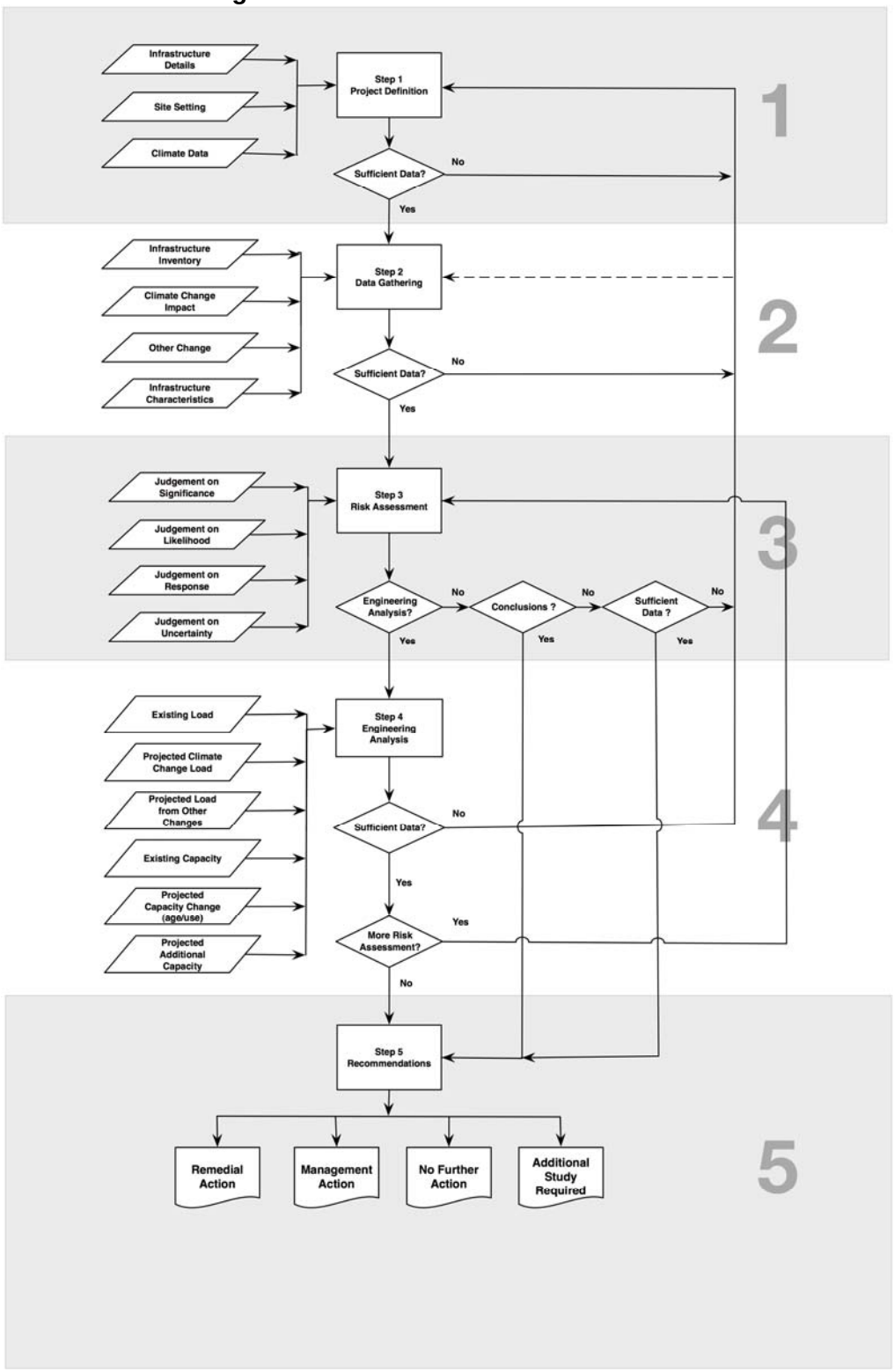


Figure 4 outlines the detailed protocol procedure. Part II of this protocol expands on this flow chart and provides specific procedures for conducting an engineering climate change

infrastructure vulnerability assessment. At the completion of each step of the protocol the practitioner is required to assess data sufficiency and address the need for further, more detailed, analysis. This results in a number of feedback loops within the protocol and significant inter-linkage between steps. The detailed protocol provides guidance on how to answer these questions. However, the practitioner must take care to fully evaluate, and document, each of these key decision points to manage against scope creep and avoid iterations, unless completely justified within the context of the assessment. As general guidance, the practitioner should consider the incremental benefit gained by additional costs of data acquisition or technical analysis. This is a project specific assessment driven by budget, risk and other management factors. If the practitioner is unsure of any of these factors, they are encouraged to work with the Project Partner to ensure that all relevant factors are considered.

Figure 4: Detailed Protocol Flow Chart



3.1 Step 1 - Project Definition

In Step 1 the practitioner will be asked to:

- Develop a general description of:
  - The infrastructure;
  - The location;
  - Historic climate;
  - Load;
  - Age;
  - Other relevant factors; and
- Identify major documents and information sources.

In this step the practitioner defines the boundary conditions for the vulnerability assessment.

3.2 Step 2 - Data Gathering and Sufficiency

In Step 2 the practitioner will be asked to provide more definition about:

1. Which parts of the infrastructure will be assessed; and
2. The particular climate factors that will be considered.

Step 2 is comprised of two key activities:

1. Identification of the features of the infrastructure that will be considered in the assessment:

   - Physical elements of the infrastructure;
     - Number of physical elements;
     - Location(s);
   - Other relevant engineering/technical considerations:
     - Material of construction;
     - Age;
     - Importance within the region;
     - Physical condition;
   - Operations and maintenance practices;
   - Operation and management of the infrastructure;
     - Insurance considerations;
     - Policies;
     - Guidelines;
     - Regulations; and
     - Legal considerations.

2. Identification of applicable climate information. Sources of climate information include, but are not limited to:

   - The National Building Code of Canada, Appendix C, Climate Information;

- Intensity - Duration – Frequency (IDF) curves;
- Flood plain mapping;
- Regionally specific climatic modeling;
- Heat units (i.e. degree-days) (i.e. for agriculture, HVAC, energy use, etc.); and
- Others, as appropriate.

The practitioner will be required to exercise professional judgement based on experience and training. Step 2 is an interdisciplinary process requiring engineering, climatological, operations, maintenance, and management expertise. The practitioner must ensure that the right combination of expertise is represented either on the assessment team or through consultations with other professionals during the execution of the assessment.

3.3 Step 3 - Risk Assessment

In Step 3 the practitioner will identify the interactions between the infrastructure, the climate and other factors that could lead to vulnerability. These include:

- Specific infrastructure components;
- Specific climate change parameter values; and
- Specific performance goals.

The protocol requires the practitioner to identify which elements of the infrastructure are likely to be sensitive to changes in particular climate parameters. They will be required to evaluate this sensitivity in the context of the performance expectations and other demands that are placed on the infrastructure. Infrastructure performance may be influenced by a variety of factors and the protocol directs the practitioner to consider the overall environment that encompasses the infrastructure.

At this point in the protocol the practitioner, in consultation with the Project Partner, management, engineering and operation personnel, will perform a risk assessment of the infrastructure's vulnerability to climate change. The interactions identified will be evaluated based on the professional judgement of the assessment team. The risk assessment will identify areas of key concern.

The practitioner will identify those interactions that need further evaluation. The assessment process does not require that all interactions be subjected to further assessment. In fact, in most assessments most of the interactions considered will ultimately be eliminated from further consideration. Some interactions may clearly present no, or negligible, risk. Some interactions may clearly indicate a high risk and a need for immediate action. Those interactions that do not yield a clear answer regarding vulnerability may be subjected to the further Engineering Analysis as outlined in Section 8.4.

At this stage, the practitioner must also assess data availability and quality. If professional judgment identifies a potential vulnerability that requires data that is not available to the assessment team, the protocol requires that the practitioner revisit Step 1 and/or Step 2 to acquire and refine the data to a level sufficient for risk assessment and/or engineering analysis.

The practitioner may determine that this process requires additional work outside of the scope of the assessment. Such a finding must be identified in the recommendations outlined in Step 5.

This is a key decision point in the Protocol. The practitioner is required to determine:

- Which interactions require additional assessment;
- Where data refinement is required; and
- Initial recommendations about:
  - New research;
  - Immediate remedial action; or
  - Non-vulnerable infrastructure.

3.4 Step 4 - Engineering Analysis

In Step 4 the practitioner will conduct focused engineering analysis on the interactions requiring further assessment, as identified in Step 3.

The protocol sets out equations that direct the practitioner to numerically assess:

- The total load on the infrastructure, comprising:
  - The current load on the infrastructure;
  - Projected change in load arising from climate change effects on the infrastructure;
  - Projected change in load arising from other change effects on the infrastructure;

- The total capacity of the infrastructure, comprising:
  - The existing capacity;
  - Projected change in capacity arising from aging/use of the infrastructure; and
  - Other factors that may affect the capacity of the infrastructure.

Based on the numerical analysis:

- A vulnerability exists when ***Total Projected Load*** exceeds ***Total Projected Capacity***; and
- Adaptive capacity exists when ***Total Projected Load*** is less than ***Total Projected Capacity.***

At this stage the practitioner must make one final assessment about data availability and quality. If, in the professional judgement of the practitioner, the data quality or statistical error does not support clear conclusions from the Engineering Analysis, the protocol directs the practitioner to revisit Step 1 and/or Step 2 to acquire and refine the data to a level sufficient for robust engineering analysis. The practitioner may determine that this process requires additional work outside of the scope of the assessment. Such a finding must be identified in the recommendations outlined in Step 5.

Once the practitioner has established sufficient confidence in the results of the engineering analysis, the protocol reaches another key decision point. The practitioner must decide to either:

- Make recommendations based on their analysis (Step 5); or
- Revisit the risk assessment process based on the new/refined data developed in the engineering analysis (Step 3).

3.5 Step 5 - Recommendations

In Step 5 the practitioner is directed to provide recommendations based on the work completed in Steps 1 through 4. Generally, the recommendations will fall into five major categories:

- Remedial action is required to upgrade the infrastructure;
- Management action is required to account for changes in the infrastructure capacity;
- Continue to monitor performance of infrastructure and re-evaluate at a later time;
- No further action is required; and/or
- There are gaps in data availability or data quality that require further work.

The practitioner may identify additional conclusions or recommendations regarding the veracity of the assessment, the need for further work or areas that were excluded from the current assessment.

4 The Team

4.2 A Multi-Disciplinary Team

When guided by a well-balanced team of qualified professionals, the protocol is a very powerful tool, derived from standard risk management methodologies, tailored to climate change. It is quite common for practitioners to identify data gaps, poor data quality, or lack of relevant tools such as local results from regional climatic models. Often, lack of financial resources or project schedule commitments can affect the ability of the practitioner to completely address these concerns. The protocol allows a number of avenues to proceed when these issues arise. For example,

- The practitioner may identify the data gap and make a recommendation for further work outside of the context of the vulnerability assessment.
- The practitioner may identify the data gap and table any further analysis on the affected parameters.
- The practitioner may infill the missing data based on reasonable professional assumptions and precede with the analysis.

Lack of input data need not deter practitioners from making professionally based judgments and expressing opinions leading to recommendations.

Of paramount importance in addressing the types of questions raised by the protocol is a well-balanced team of professionals dedicated to the execution of the vulnerability assessment. The correct blend of professional and local expertise can support and validate assumptions that allow the practitioner to compensate for missing or poor quality data and account for the lack of other technical resources. Team composition and depth of experience has a very significant bearing on the veracity of the final assessment report. The following expertise is absolutely necessary on the assessment team:

- Fundamental understanding of risk and risk assessment processes;
- Directly relevant engineering knowledge of the infrastructure type;
- Climatic and meteorological expertise/knowledge relevant to the region;
- Hands-on operation experience with the specific infrastructure under assessment;
- Hands-on management knowledge with the specific infrastructure under assessment; and
- Local knowledge and history, especially regarding the nature of previous climatic events, their overall impact in the region and approaches used to address concerns, arising.

We cannot overstate the importance of local knowledge in conducting a vulnerability assessment. Local knowledge, filtered through the overall expertise of the assessment team, more often than not, will compensate for data gaps and provide a solid basis for professional judgment of the vulnerability of the infrastructure.

Throughout this protocol we use the term practitioner. The reader should interpret this to mean the entire assessment team. It is highly unlikely that a project proponent will identify a practitioner with all of the necessary attributes, skills, knowledge and experience in a single person.

4.3 The Team Leader

The team leader should be an experienced professional with demonstrated experience in management of multi-disciplinary projects. In some cases, the team leader may also contribute some of the other technical and professional skills outlined above. However, in all cases the leader must be able to coordinate and prioritize the work of the rest of the team and have sufficient background and experience to consolidate findings from different disciplines and areas of expertise. These attributes are normally developed over years of professional practice. Thus, it is generally inadvisable to assign team leadership to a junior professional.

5 Fundamentals of Risk and Risk Assessment

This PIEVC Engineering Vulnerability Protocol is derived from standard risk assessment processes. As such, there is some advantage to reviewing these concepts prior to initiating a vulnerability assessment to ensure that the entire team and workshop participants have a common understanding of the expectations established by the protocol and of acceptable approaches for addressing questions that the practitioner may identify throughout the exercise.

Risk is defined as the possibility of injury, loss or negative environmental impact created by a hazard. The significance of risk is a function of the *probability* of an unwanted incident and the *severity* of its consequence[1]. In mathematical terms:

$$R = P \times S$$

Where:

R = Risk
P = Probability of a negative event
S = Severity of the event, given that it has happened

In risk assessment, practitioners answer three questions[2]:

1. What can happen?
2. How likely is it to happen?
3. Given that it has happened, what are the consequences?

The PIEVC Protocol guides the practitioner through a process designed to answer these questions.

In risk analysis, practitioners are cautioned to ensure that their assessment of probability does not affect their assessment of severity. Basically, the consequence of an event is independent from the likelihood that the event will occur. By separating probability and severity in this way, the practitioner is able to dissect the factors that contribute to risk. Ultimately, this can yield very useful information to guide recommendations regarding approaches to risk mitigation. Practitioners can identify steps that reduce:

- The probability of an event;
- The severity of an event; or
- Both.

5.2 Hazard Identification – What can happen?

In this protocol, hazards are identified as interactions between identified climatic events and components of the infrastructure. The practitioner identifies conceivable climatic events that could occur in the region within the timeframe of the vulnerability assessment.

[1] Paul R. Amyotte, P.Eng. & Douglas J. McCutcheon, P.Eng.; ***Risk Management – An Area Of Knowledge For All Engineers***; Engineers Canada, 2006
[2] Tim Bedford and Roger Cooke; ***Probabilistic Risk analysis: Foundations and Methods***; Cambridge University Press; Fourth Printing 2006

For example, the practitioner could identify that an event of 50 mm of rain in one hour is conceivable during the remaining service life of the infrastructure.

The practitioner will then review the infrastructure and determine the components and sub-components that comprise the infrastructure. This requires professional judgement. If the component analysis is not sufficiently detailed, the assessment may miss potential vulnerabilities. However, if the component analysis is overly detailed, the scope of the assessment can mushroom and become unmanageable or very expensive.

Once the component analysis and climate analysis are completed the practitioner consolidates the lists. The consolidated list yields a set of interactions between climatic events and infrastructure components.

For example, the list may suggest that, during the timeframe of the evaluation, it is conceivable that the 50 mm rain event could impact culverts within the infrastructure system.

As a final step of the hazard identification the practitioner normally will perform a pre-screening of the identified interactions. In essence, they will judge if the identified interactions could conceivably occur. It is imperative that at this stage the assessment the practitioner does not establish a numerical value for the likelihood of the interaction. In essence, they are assessing the reasonableness or conceivability of the interaction. Based on professional judgment, this "sniff test" can significantly reduce the number of interactions considered in further evaluation.

At the end of the hazard analysis, the protocol will yield a set of interactions, or hazards, that will be assessed further for likelihood and severity, finally yielding a value for risk.

Hazard analysis does not identify risks.

Hazard analysis identifies a specific set of circumstances that could potentially result in a negative outcome. In the following analysis, the practitioner will establish just how likely the interaction is and the consequences of the interaction, should it actually occur.

5.3 Probability – How likely is it to happen?

To determine risk, the practitioner must first assign a probability of an interaction occurring. In some circumstances, historical data or statistics are available to guide this assessment. However, more often than not, this guidance is not available. In such cases, the probability can be assigned based on professional judgment. This is a normal procedure in risk assessment. Thus, the lack of measured data should not impose an impediment to completing the vulnerability assessment. Standard risk assessment textbooks state:

> ***Expert judgment techniques are useful for quantifying models in situations in which, because of either cost, technical difficulties or the uniqueness of the situation under study, it has been impossible to make enough observations to quantify the model with "real data".***[2]

This protocol addresses this issue through guidance regarding:

- The composition of the practitioner team; and
- The participants at the Vulnerability Assessment Workshop.

It is important to ensure that sufficient expertise, experience and knowledge be accessed to ensure a balanced and reliable estimate of the probability.

In the Vulnerability Assessment Workshop, participants systematically assess each of the interactions deemed to be conceivable and reasonable by the practitioner. The combined expertise and experience of the workshop participants is designed to yield a pragmatic and realistic estimate of the probability of occurrence of an infrastructure – climate event interaction.

The protocol provides guidance regarding the selection of probability values. The protocol uses a standardized probability scale of 0 to 7, where 0 means that the event will never occur and 7 means that the event is certain. Further, the protocol provides three different approaches to assigning these factors. Finally, the protocol allows the practitioner to use other methods to assess probability, should these methodologies be justified given the circumstances of the current assessment.

5.4 Severity – Given that it has happened, what are the consequences?

The second step in establishing a value for risk is to assess the consequences of an event, given that the event has happened. In some circumstances, historical data or statistics are available to guide this assessment. However, more often than not, this guidance is not available. In such cases, the severity can be assigned based on professional judgment.

It is important to ensure that sufficient expertise, experience and knowledge be accessed to ensure a balanced and reliable estimate of the severity.

In the Vulnerability Assessment Workshop, participants systematically assess each of the interactions deemed to be conceivable and reasonable by the practitioner. The combined expertise and experience of the workshop participants is designed to yield a pragmatic and realistic estimate of the severity of an infrastructure – climate event interaction, should that event ever occur.

The protocol provides guidance regarding the selection of severity values. The protocol uses a standardized severity scale of 0 to 7, where 0 means no negative consequences, should the interaction occur and 7 means significant failure, should the interaction occur. Further, the protocol provides two different approaches to assigning these factors. Finally, the protocol

allows the practitioner to use other methods to assess severity, should these methodologies be justified given the circumstances of the current assessment.

5.5 Risk – What is the significance of the event?

Finally, the practitioner is directed to determine the risk for each interaction. As previously stated, risk is a function of the *probability* of an unwanted incident and the *severity* of its consequence. Logistically, the protocol directs the practitioner to multiply the probability and severity values derived above to establish a value for risk. If the practitioner uses the recommended probability and severity scales, the risk analysis will yield a set of risk values ranging between 0 and 49. Since, the scale factors are unitless, the resulting risk values are also unitless.

The protocol then goes on to help the practitioner define criteria for further screening the risks. Low risk interactions are eliminated from further evaluation. Medium risk interactions are normally subjected to further engineering analysis (Step 4 of the Protocol). High risk interactions are normally passed forward to conclusions and recommendations (Step 5 of the Protocol).

In simple terms, low risk interactions pose minimal threat. Medium risk interactions ***MAY*** be significant and require further refinement and analysis before the practitioner passes final judgement. High risk interactions pose a material threat and require remedial action. The protocol identifies categories of recommendations for high risk items including, but not limited to, management action, retirement, or re-engineering and retrofit.

The concept of tolerance to risk is inherent in the predefined cut-offs identified by the protocol. Basically, the protocol assumes that infrastructure owner accepts a level of risk simply by operating the infrastructure. The owner accepts this level of risk as a normal consequence of the operation and may already have procedures in place to manage the risk. In essence, no activity is risk free, but a minimal level of risk is acceptable. The protocol also assumes that as risk values increase, the owner's tolerance to the risk decreases and they are likely to undertake risk mitigation activities to address the concern and reduce the risk to a level within their risk tolerance. At the highest level, the risk exceeds the boundaries of the owner's risk tolerance and they will take urgent action. The protocol allows the practitioner to adjust the cut-off values, as appropriate, based on their professional judgment and consultation with the infrastructure owner.

5.6 Common Myths and Misconceptions About Risk

It is important for practitioners to understand the implications of common myths and misconceptions about risk. In this protocol, there is a significant level of involvement with laypeople. Understandably, the average layperson does not have a profound technical understanding of risk. Thus, the practitioner has the responsibility to guide the layperson through the process in a technically rigorous manner.

It is important to be able to identify and address the most common problems associated with risk analysis. Some of these common myths and misconceptions include:

"Hazard is risk." It is very common for the average person to confuse the conceivability of an event with its risk. Simply because an event can be conceived does not mean that, in the real world, it will actually occur. Risk assessment considers the likelihood of an event in association with its consequence. Hazard assessment simply asks the question: "What events can I imagine that could result in a negative outcome."

"Probability is risk." Often the average person will confuse the likelihood of an event with risk. Likelihood, or probability, is only one factor that constitutes risk. The severity of the event, should it occur, must also be considered. When probability is confused with risk, the impact of the event is neglected. It is possible to label high probability - low impact events as high risk. This can lead to unnecessary management action. Conversely, it is possible to label high severity – low probability events as low risk, resulting in little or no mitigative action.

"Severity is risk." The average person may confuse the severity of an event with its risk. In this scenario, high severity events are considered to be high risk regardless of their likelihood. Similarly, low severity events are considered to be low risk even though they may occur quite frequently. As above, by neglecting one key factor of risk the actual risk may not be properly assessed or managed.

"Probability and severity are dependent (linked) variables." This misconception is often the most difficult to address with a layperson. It is very challenging for the average person to separate the likelihood of an event from its consequences. For example, if they can conceive of the event, then it must be serious. The problem with this view is that it does not allow the practitioner to assess probabilities and impacts in a clinical manner. Properly executed, a risk assessment must treat severity and probability as independent variables. Although, the average person may see probability and severity as causally linked, the probability of the event is in no way related to the severity of the consequence. Severity does not cause probability, nor does probability cause severity. Probability is a function of frequency. Severity is a function of the physical nature and physics of the infrastructure and climatic event. Risk assesses the combined implications of the two. This perspective allows the practitioner to rank the likelihood of events and the severity of events separately in order to rigorously evaluate the implications.

These concepts are technically complex and outside of the experience of the average person. Therefore it is the practitioner's duty to be vigilant in the execution of the protocol. They must ensure that these myths and misconceptions do not creep into the mindset of the practitioner team or workshop participants and compromise the veracity of the assessment results.

6 The Vulnerability Assessment Workshop

In Step 3 of the protocol, there is a requirement that the practitioner execute a workshop with the practitioner team and representatives from the infrastructure ownership and operations teams. This is the way to draw on the combined experience of the practitioner and people who have direct contact with the infrastructure. This method allows the team to apply professional judgment in a transparent and consistent manner. As stated above, this can be done in a technically rigorous way and yield results that can withstand professional scrutiny.

Where data exists, the practitioner is directly to use it. However, if the data is missing or suspect in any manner, the practitioner is directed to rely on the professional judgment of the practitioner team and workshop participants. Thus, the workshop represents the most important phase of the evaluation.

At the workshop the practitioner reviews the results of their prescreening assessment and invites participants to assess the probabilities and severities of the interactions identified by the practitioner. Although the protocol allows the practitioner to conduct the risk assessment through a series of one-on-one meetings, where necessary; experience to date demonstrates that a properly executed workshop yields the most robust risk analysis. It is therefore strongly recommend that the practitioner use a workshop unless there are significant, compelling and material, reasons to the contrary.

Given the importance of the workshop, it is critical that the right mix of knowledge, experience and professional skills be present. If the practitioner team has been structured properly, the professional skills and experience should be available to the workshop. However, the practitioner team may be missing hands-on experience with this particular infrastructure and local knowledge regarding climatic events and how the infrastructure and operations team responded to those events. Participants at the workshop can fill these gaps. It must be stressed that it is not sufficient to include only management and engineering staff from the infrastructure owner. Operations staff must also participate. It is not uncommon for operations staff and management/engineering staff to have a distinctly different perspective of climate-infrastructure interactions. Events that the management team view to be very significant may already have been encountered and addressed by the operations team.

For example, the management team may view that a severe snow event could prevent operations staff from executing their duties, while the operations staff have already experienced snow events of equal or greater severity and developed methods to address the problems they encountered. As often as not, these procedures are not formally documented and can only be described by the affected staff.

Although these perspectives may seem trivial on the surface, they are very significant indicators of how the staff will respond during severe climatic events that affect their operations responsibilities. This should emerge during the workshop discussions and forms a substantive input to the local knowledge data used by the practitioner to establish the risk profile.

Generally, participants at the workshop should include:

- The practitioner team;

- Representatives from the infrastructure management team;
- Representatives from the infrastructure engineering team;
- Representatives from the infrastructure operations team;
- Local expertise/knowledge regarding severe climatic events in the region and climatic events that may have affected the infrastructure;
- Representatives from the organization providing climate information;
- Representatives from any advisory groups or technical experts who may be supporting the vulnerability assessment; and
- Others deemed necessary by the infrastructure owner or practitioner team.

The workshop should follow a consistent agenda. Given the number of laypeople who may be involved, it is important to provided sufficient background on the exercise to all participants and establish the expected outcomes from the meeting. Generally, the workshop agenda should include:

- A brief presentation on climatic change and the implications for the region;
- A brief presentation on risk and risk assessment;
- A brief presentation on the work completed by the practitioner to date;
    - As a minimum, identifying the key interactions to be considered by workshop participants;
- Introduction of the spreadsheet or matrix developed by the practitioner in compliance with Step 3 of the protocol;
    - Explanation of the infrastructure components and climate events that the practitioner deems to be relevant;
    - Polling of the workshop to determine if potentially relevant infrastructure components or climate events have been missed;
        - At this stage of the process the probability and severity values will not have been entered into the matrix or spreadsheet;
- A tabletop exercise, drawing on the expertise of workshop participants, establishing probability and severity for each relevant interaction identified by the practitioner. This could be done by:
    - Assigning groups to input data to hard copies of the matrix distributed to the workshop;
    - Assigning groups to input data to laptops distributed throughout the workshop;
    - As a single facilitated discussion filling in a master spreadsheet projected to the entire workshop; or
    - Other methods as deemed appropriate.
- If appropriate, a site visit or tour of the infrastructure or of specific components of the infrastructure; and
- A summary of findings arising from the workshop.

Because of the length of the agenda, and the need for rigorous discussion, the practitioner should plan the workshop for one complete eight-hour day.

Given the amount of professional, billable, hours that will be consumed at the workshop, it is critical that the practitioner:

- Carefully plan the event in consultation with the infrastructure management and operations teams;
- Schedule it to maximize productive outcomes;
    - Not before screening analysis is complete or before all necessary and relevant data has been accumulated; and
- Provide as much validated data and background information as possible.

7 Economic Considerations

Economic considerations permeate climate change infrastructure vulnerability assessment.

At the project level, the Project Partner must establish a scope for the project and work that scope within budgetary limitations. This may drive decisions regarding the use of regional climate modeling, which can be expensive, and the overall depth and reach of the assessment. Thus, economics may dictate a smaller, more focused, assessment. Under such constraints, it is the practitioner's responsibility to work with the infrastructure owner to establish a scope of work that both addresses the owner's immediate issues while maximizing the opportunity to extrapolate assessment results to other areas of interest to the infrastructure owner. That is, the practitioner must work with the owner to maximize the "bang for the buck".

During the execution of the assessment, practitioners will often identify data gaps. When this occurs, the practitioner and Project Partner must assess the available mechanisms for obtaining or improving the data. This can also be an expensive exercise and must be evaluated based on the economic return associated with the task. For example, the data may be necessary to fully understand a risk associated with one sub-component of the infrastructure. If this sub-component is deemed to be critical with a significant economic penalty associated with its loss, the team may decide that the costs are justifiable. That is, the cost of the potential risk significantly outweighs the cost of filling the data gap. On the other hand, the data may be desired to characterize a risk that, in the grand scheme of things, is relatively minor. In this case, the team may decide to forego the expense of additional data acquisition. That is, the cost of the potential risk is much less than the cost of filling the data gap. These examples establish economic boundary conditions. During the actual execution of an assessment, significant professional judgment and consultation with the infrastructure owner may be required.

It should be noted that acquiring 100% of the data necessary to support a vulnerability assessment is normally outside of the economic reach of the assessment. Missing data is common and filling the gap can be very expensive. The protocol directs practitioners to use professional judgment to address these issues. One key element of this judgment is the economic implication of the methodologies the practitioner recommends to address the gap.

Finally, the practitioner may identify recommendations to address vulnerabilities identified by the assessment. Once again, the practitioner should take economic factors into consideration. For example, one potential solution to an identified vulnerability could be replacement of the infrastructure, with major capital expenditure. Since the assessment does not normally evaluate the engineering alternatives to address vulnerabilities at any depth, the practitioner should

evaluate the implications of such a recommendation, in consultation with the owner, to assess the economic feasibility. Practitioners must not shy away from reporting identified vulnerabilities, but should take to care state their recommendations within the context of reasonable, economic constraints. In the example above, although full replacement may be ideal other, more cost effective, approaches may be available and should be considered. Ultimately, these considerations will play a role in the final acceptance of the assessment and its recommendations.