Alberta Electric System Operator
3000, 240 4 Avenue SW
Calgary, AB • T2P 4H4
aeso.ca

Alberta Risk-Based Compliance Monitoring Program (ARCMP)

Contents

1. Introduction

Pursuant to Section 23(1)(b)(c) of the *Transmission Regulation*, the Independent System Operator, operating as the Alberta Electric System Operator (AESO), has the mandate to monitor the compliance of electricity market participants[1] (entity) with reliability standards[2] (Alberta Reliability Standards or ARS). Pursuant to Section 103.12 of the ISO Rules, the AESO is required to establish monitoring programs, processes, and procedures for monitoring entity compliance. The Alberta Risk-Based Compliance Monitoring Program (ARCMP) exists to fulfill these obligations relative to ARS.

2. Purpose and Risk-Based Compliance Monitoring

This document defines the AESO's risk-based compliance monitoring framework for performing its compliance monitoring function for ARS. The AESO prioritizes monitoring and oversight on areas which pose the highest reliability and security risks to the Interconnected Electric System[3] (IES) in Alberta. The AESO develops a customized compliance oversight plan (COP) for each entity which is commensurate with the risk it poses to the IES. The ARCMP incorporates IES risks, entity risks, and entity compliance history information into the AESO's compliance monitoring of ARS in a formal and transparent manner. This approach leverages concepts from the North American Electric Reliability Corporation's (NERC) Enterprise Reliability Organization (ERO) Compliance Monitoring and Enforcement Program (CMEP); incorporates Alberta specific considerations; and where possible, simplifies the assessment process that exists in other jurisdictions to minimize administrative burden and optimize resource utilization for stakeholders.

The ARCMP is a critical element of the compliance and enforcement framework in Alberta. Pursuant to Section 21.1 of the *Electric Utilities Act*, if the AESO suspects that an entity has contravened an ARS, it must refer the matter to the Market Surveillance Administrator (MSA)[4].

The AESO's risk-based and periodic application of compliance monitoring processes encourages entities to change behaviours, improve practices to comply with ARS, and supports the AESO in delivering on its mandate to direct the safe, reliable, and economic operation of the IES.

3. Applicability

The ARCMP is applicable to the compliance monitoring of approved and in effect ARS for all entities.

4. Stakeholders

The ARCMP has three stakeholders:

- the AESO in its role as the compliance monitor of ARS;
- the entities that must comply with the ARS; and
- the MSA in its role as the enforcement agency.

[1] As defined by the *Electric Utilities Act*, SA 2003, c E-5.1
[2] As defined by the *Transmission Regulation*, AR 86/2007, s. 19
[3] As defined by the *Electric Utilities Act*, SA 2003, c E-5.1
[4] As defined by the *Alberta Utilities Commission Act,* SA c A-37.2, Division 2

5. Registration

Each entity is required to register with the AESO and confirm its applicable functional entity types in accordance with the Alberta Reliability Standard Functional Model and Criteria for Registration. Registration provides the AESO with information on the functional role(s) of an entity, its impact on the reliability of the IES, and indicates the applicability of ARS for that entity. It is the responsibility of each entity to be aware of its legislative obligations. Pursuant to Section 20.8(b) of the *Electric Utilities Act*, an entity is required to comply with all ARS in effect.

For additional information on registration, see the Alberta Reliability Standard Functional Model and Criteria for Registration[5] and the Alberta Reliability Standard Registration Guide[6].

6. ARCMP Overview

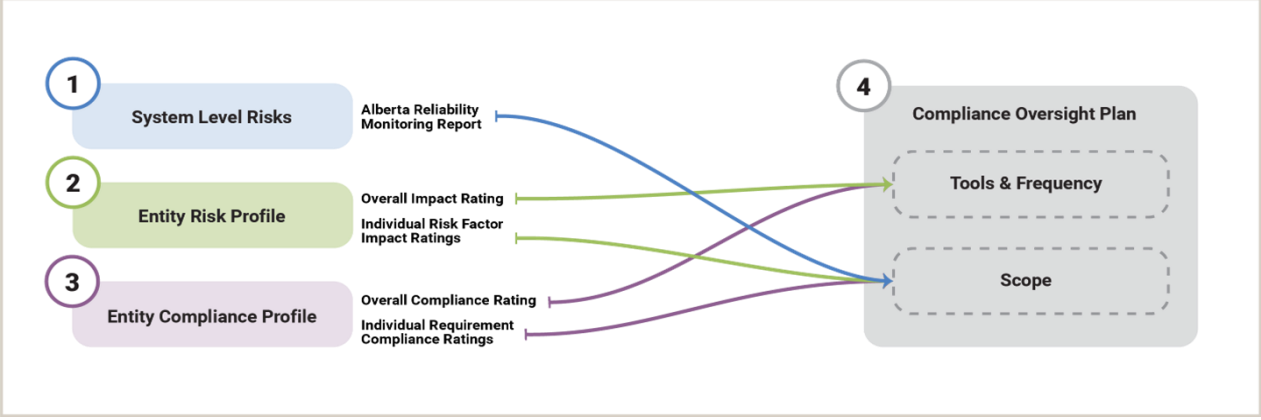
The ARCMP is composed of four components:

1. System Level Risks
2. Entity Risk Profile
3. Entity Compliance Profile
4. Compliance Oversight Plan (COP)

The first three components consider areas of risk to the IES, the results of which are used to inform the fourth component, a customized entity specific COP that communicates the ARS requirements the AESO intends to monitor, tools, and frequency for that entity. The AESO assesses system level (i.e., IES) risks and the results are applied to all entities. Components 2 to 4 are executed at the registered entity level, regardless of whether multiple entities are owned by a single parent company.

A material change in any of the outputs from components 1, 2, or 3 may trigger the need to update an entity's COP. Figure 1 below illustrates the components and results.

Figure 1: ARCMP Components



[5] AESO Website, ARS Compliance Monitoring
[6] AESO Website, ARS Compliance Monitoring

7. ARCMP Components

7.1 System Level Risks

The System Level Risks component periodically assesses and captures the inherent risk and relative importance of each ARS requirement to reliability posed by non-compliance. The AESO uses the results to identify priority issues and ensure its compliance oversight is focused on high-risk requirements to maintain reliability with a more efficient use of resources.

The System Level Risks component focuses on three types of risk:

1. Inherent reliability risks – risks inherent to the operation and maintenance of the IES leverage the Alberta Risk Ratings (ARR) correlated or assigned to each requirement.
2. Emerging risks – risks inherent to changes to the IES or the environment in which it operates (e.g., changes in the generation mix due to decarbonization, climate change resulting in more extreme weather events, the geopolitical climate inducing more frequent and severe cyber-attacks against critical infrastructure, etc.). These risks change over time and the AESO uses this information to inform the priority of related requirements.
3. Implementation risks – risks inherent to the poor implementation of ARS, which can lead to reliability and security risks. These types of risks include inadequate implementation of new, amended, and existing ARS that are identified during the standards development, implementation, and compliance monitoring phases of the ARS Development Lifecycle. These risks change as implementation matures and the AESO uses this information to inform the priority of related requirements.

7.1.1 Inputs

The AESO uses a variety of internal and external sources of information to identify System Level Risks, including, but not limited to:

- Subject matter expertise and the AESO's continuous monitoring of the operation of the IES to identify Alberta specific emerging risks.
- ARRs to identify the prioritized list of ARS requirements.
- NERC's ERO Enterprise CMEP Implementation Plan (IP) and WECC's Reliability Risk Priorities reports to identify potential emerging risks.
- Suspected ARS contraventions of entities to identify implementation risks related to existing ARS.
- Subject matter expertise to identify implementation risks related to new or amended ARS. AESO considerations include ARS complexity, stakeholder feedback during development and implementation results of advanced self-certification, and any other factors deemed relevant to implementation.

7.1.2 Process

The AESO:

1. Monitors and reviews NERC and WECC for releases of the NERC ERO CMEP IP and the WECC Reliability Risk Priorities reports to determine whether the identified risks and mitigating standards and requirements apply in the Alberta context and whether the AESO needs to add any additional, or eliminate, Alberta specific emerging risks.
2. Monitors the IES for Alberta-specific emerging risks which can be mitigated through ARS compliance.

3. Reviews the AESO's compliance monitoring results to identify widely contravened ARS requirements to identify risks related to widespread implementation issues of existing ARS.
4. Reviews and monitors the development, stakeholder feedback, and implementation of new or revised ARS to identify requirements which have a high probability of poor implementation.

7.1.3 Outputs

The output of the System Level Risks process is the Alberta Emerging Reliability Risk Priorities Report which contains the following:

1. A list of the risks identified through the System Level Risks process.
2. The source of each identified risk (e.g., NERC, WECC, actual or predicted implementation issues, etc.).
3. A short explanation of the reasoning behind including the risk.
4. A mapping of ARS requirements to the risks identified through the System Level Risks process.

The AESO posts the Alberta Emerging Reliability Risk Priorities Report on its website[7], including subsequent updates and version changes. The AESO notifies stakeholders of the posting via the AESO's stakeholder newsletter for information and transparency purposes only. No feedback or additional data will be requested by the AESO from stakeholders.

7.1.4 Scheduling

The AESO executes the System Level Risk process at least once every year. The AESO may execute the process more frequently in response to a material change related to one of the inputs.

7.2 Entity Risk Profile

The Entity Risk Profile quantifies the overall impact of a specific entity on the IES. An entity's impact on the IES is primarily established by its footprint (e.g., the number and "size" of its facilities), and the services it provides to the IES (e.g., Remedial Action Schemes (RAS), blackstart, etc.).

The Entity Risk Profile component leverages NERC's ERO Risk Factors and AESO subject matter experts consider unique characteristics of the IES to identify Alberta Risk Factors applicable to the Alberta context. Each Alberta Risk Factor describes an aspect of an entity's footprint and defines criteria or thresholds for determining the relative impact of the entity in according to the Alberta Risk Factor (e.g., None, Low, Medium, High), an explanation of the risk factor's determination, and includes an indication of specific risk factor prioritization (i.e., relative importance) for the purposes of determining an entity's overall risk rating.

To reduce administrative burden, the AESO uses the Alberta Risk Factors to assess the impact of each entity on its reliability impact to the IES using information held by the AESO. The AESO provides the entity with an opportunity to correct any inaccuracies in the information used during the assessment. If the AESO's information is incomplete, the AESO may solicit very specific and targeted information from the entity to assess its impact. The AESO may update the Alberta Risk Factors periodically in response to changes to the inputs.

[7] AESO Website, ARS Compliance Monitoring

7.2.1 Inputs

The AESO uses the following combination of inputs in the Entity Risk Profile component:

- NERC ERO Risk Factors and assessment criteria and WECC ERO Risk Factors as the starting point for defining the Alberta Risk Factors.
- The AESO's subject matter expertise to define Alberta Risk Factors and associated assessment criteria.
- Information held by the AESO to assess each entity.
- Feedback and information from each entity to validate the completeness and accuracy of the information the AESO used in the assessment.

7.2.2 Processes

Alberta Risk Factors Determination Process

The AESO:

1. Monitors and reviews NERC and WECC ERO Risk Factors changes and updates to consider relevance in the Alberta context that would precipitate any material changes to the Alberta Risk Factors, assessment criteria, or risk factor prioritization.
2. Monitors and reviews changes to the state of the IES that would precipitate a material change to the Alberta Risk Factors, assessment criteria, or risk factor prioritization.
3. Tracks and reviews lessons learned through the processes, including each Entity Risk Assessment, to identify potential changes to the assessment criteria or need to implement a risk factor prioritization.
4. Updates the Alberta Risk Factors, evaluation criteria, and risk factor prioritization based on need.

Entity Risk Assessment Process

The AESO evaluates each entity using the Alberta Risk Factors as follows:

1. Reviews information, held by the AESO, about the entity being evaluated.
2. Uses the information to assess the entity against the assessment criteria for each Alberta Risk Factor and assigns the entity a risk rating for each factor (e.g., None, Low, Medium, High).
    a. The AESO may exercise professional judgement to assign a risk rating that deviates from the defined assessment criteria. If an alteration occurs, the AESO documents the rationale and tracks the reasons for alterations to ensure consistency across entities. The AESO may incorporate the outcomes directly into future revisions of the Alberta Risk Factors.
3. Assesses the entity using the Alberta Risk Factors, the risk factor prioritization, and professional judgment to assign a single overall risk rating for the entity (e.g., Low, Medium, High)
4. Tracks the outcomes of overall risk rating assignments to ensure consistency across entities and leverages historical ratings to develop more detailed guidance for future assessments.
5. Shares the Entity Risk Profile with the entity for validation and provides the entity an opportunity to provide additional information or corrections.
6. Reviews feedback provided by the entity, seeks clarification, if required, updates the risk ratings if warranted, finalizes the Entity Risk Profile, and issues it to the entity as part of its COP.

7.2.3 Outputs

Alberta Risk Factors Determination Process Outputs

The outputs of the Entity Risk Profile process are:

1. The table of Alberta Entity Risk Factors Criteria and an explanation regarding any deviation from the NERC ERO Risk Factors.

   The AESO posts the Alberta Entity Risk Factors Criteria on its website[8], including subsequent updates and version changes. The AESO notifies stakeholders of the posting via the AESO's stakeholder newsletter. The AESO provides the Alberta Risk Factors to stakeholders for information and transparency purposes only. No feedback or additional data will be requested by the AESO from stakeholders.

2. Each entity's individualized Entity Risk Profile – documented in its COP – contains the following:
   a. The table of Alberta Risk Factors.
   b. The entity's risk rating for each Alberta Risk Factor, the information used by the AESO in the assessment, and reasons that the AESO altered the rating, if relevant.
   c. The entity's overall Entity Risk rating.

7.2.4 Scheduling

The AESO executes both the Alberta Risk Factors Definition process and the Entity Risk Assessment process at least once every three years. The AESO may execute either process more frequently in response to a material change related to one of the inputs.

7.3 Entity Compliance Profile

The Entity Compliance Profile is an assessment of an entity's risk to reliability and security based on its compliance performance. An entity's compliance history serves as an indicator of performance risk (i.e., the number and magnitude of suspected contraventions identified through compliance monitoring activities and/or audits and compliance related events). Compliance history is the primary indicator of future compliance performance and the best indicator of the effectiveness of an entity's compliance culture, internal compliance program, and internal controls.

The Entity Compliance Profile leverages NERC's concepts of Performance Considerations, incorporates stakeholder feedback, and accounts for differences that exist in the Alberta context.

Performance Considerations

The AESO uses the following performance considerations to determine an entity's compliance profile:

1. Compliance history – the AESO considers the entity's performance during the last two compliance monitoring plan executions, including the number and severity (e.g., Low, Medium, High) of suspected contraventions. The AESO uses professional judgement to assess severity risk to the IES based on the length, extent, and nature of each suspected contravention (e.g., documentation oversight versus incorrect implementation, etc.). Proactive self-reporting and mitigation, in addition to well designed

[8] AESO Website, ARS Compliance Monitoring

and implemented internal controls should lead to self-reported contraventions that result in minimal duration and extent and are therefore factored positively into the assessment. The AESO may use severity ratings to prioritize monitoring of ARS requirements with the poorest performance history (i.e., the requirements with greatest number of high severity suspected contraventions detected during a compliance monitoring activity). The AESO documents reasons for assigning severity risk for each suspected contravention for consistency and for development of guidance for future assessments. The AESO does not provide the detailed assessment to the entity or ask the entity for feedback. If the AESO is aware of information that indicates that the MSA has disagreed with the AESO's assessment of an entity's compliance, the AESO accounts for this in the compliance history assessment.

2. Events – where the AESO is aware of events including, but not limited to, misoperations, generator and transmission forced outages, and cyber security incidents that should have been mitigated by compliance with an ARS requirement(s), the AESO considers the event as part of the entity's compliance performance.

The AESO continuously gathers compliance history and event data through compliance monitoring activities and entities have an opportunity to have compliance performance assessed or reassessed, through the course of the AESO's compliance monitoring processes.

The AESO reviews the considerations on an ongoing basis and may make future enhancements to the process by modifying or adding additional performance considerations.

Demonstrated Exceptional Performance

The AESO completes the compliance history and event reviews, and uses the following criteria for determining demonstrated exceptional performance:

1. The AESO calculates the number of high and medium severity suspected contraventions detected during an AESO compliance monitoring audit or activity for each entity for the two most recent compliance monitoring plan executions.

2. The entities in the top 25th percentile for each Entity Risk Profile rating (i.e., Low, Medium, High) that have the fewest high and medium suspected contraventions identified during an AESO compliance monitoring audit or activity have demonstrated exceptional performance. If the AESO has no applicable compliance monitoring history to assess for specific entities, the demonstrated exceptional performance category does not apply.

The AESO tracks the outcomes of exceptional performance determinations and assesses the effectiveness of the criteria at least once every three years. The results of the AESO's assessment may result in future enhancements to this criteria and performance determinations.

7.3.1 Inputs

The Entity Compliance Profile component relies solely on the following information available to the AESO from past compliance monitoring activity and system events:

- Compliance History – the AESO uses the results of the last two compliance monitoring plan executions to determine the entity's performance for applicable ARS requirements.
    - Self-reports and mitigation plans – the AESO encourages each entity to provide the AESO with a copy of self-reports and mitigation plans it has submitted to the MSA – self-reports from the most recent two compliance monitoring program executions, and ongoing through ARCMP

implementation. Providing this information to the AESO ensures that each entity's compliance history is complete and that the AESO factors in relevant information in its assessment that are indicators of an effective compliance culture and internal controls, and a complete and accurate compliance monitoring activity scope.

- Events – the AESO uses information regarding events it is aware of, which should have been mitigated by compliance with ARS requirements to determine the entity's performance for the affected ARS requirements.

7.3.2 Processes

Compliance History Assessment

The AESO:

1. Documents the results of the compliance history – at the time of initial assessment and following the conclusion of future compliance monitoring activities – including the suspected contraventions under each ARS requirement, the length, extent, and nature of each suspected contravention, as well as whether the suspected contravention appears to have been self-reported prior to the commencement of a compliance monitoring activity.
2. Uses professional judgement as well as statistics on the outcome of past compliance history assessments and any guidance the AESO has developed for this process to assign a severity to each suspected contravention and documents the rationale for the assignment.

Event Assessment

As part of the initial assessment and – in future – after becoming aware of an event which involves one or more entities and appears to be related to ARS compliance, the AESO:

1. Reviews the event to determine whether compliance with one or more ARS requirements should have mitigated the event. The review may result in triggering a compliance monitoring activity of the entity by the AESO.
2. If the review determines that the occurrence of the event indicates non-compliance with one or more ARS requirements, the AESO refers the suspected contravention to the MSA, and adds a suspected contravention of the appropriate severity to the entity's compliance history. The AESO reassesses the entity's overall performance at that time.

The AESO shares the Entity Compliance Profile result with the entity for transparency purposes only. Since the assessment relies on information generated by the AESO, no entity feedback is required.

7.3.3 Outputs

The output of the Entity Compliance Assessment is an indication of an entity's demonstrated exceptional performance determination (yes/no) in its COP.

7.3.4 Scheduling

The AESO executes the Compliance History and Event Assessment processes following the completion of a compliance monitoring activity or event review, respectively. The AESO assesses compliance history and

calculates the exceptional performance determination at least once every three years. The AESO may calculate the exceptional performance determination more frequently, if needed.

7.4 Compliance Oversight Plan (COP)

The COP component combines the outputs of the first three components (System Level Risks, Entity Risk Profile, and Entity Compliance Profile) and defines a customized, entity specific COP (i.e., the tools used to monitor compliance, the frequency and schedule of monitoring, and the scope of ARS requirements the AESO intends to monitor). The AESO has defined the frequency of oversight tools for each combination of entity risk and compliance profile as shown in Table 1 (below). The AESO uses professional judgement to select the exact monitoring frequencies for each entity from the ranges in Table 1 based on factors such as the number of applicable ARS requirements, the duration since the entity's last audit and the AESO's anticipated resource availability.

The AESO will not apply multiple tools in the same year except for spot audits (e.g., self-certification process will not occur in the same year as a scheduled audit), nor will the AESO necessarily apply a tool in every year.

The following table provides a list of options for tools, potential frequency, and an indication of guidelines for ARS requirement scope. For clarity, not all tools listed for a specific risk rating will be used for every entity's COP:

Table 1: Oversight Tools and Frequency

Entity Risk Rating	Tool Options	Frequency Potential	ARS Requirement Scope
1. High	Audit (onsite or offsite)	2-3 years	Subset of applicable requirements
	Self-certification with evidence	1-3 years	Subset of applicable requirements or targeted requirement(s)
	Self-certification without evidence	1-2 years	Subset of applicable requirements
	Spot audit	Event or complaint driven	Targeted requirement(s)
2. High with demonstrated exceptional performance	Audit (onsite or offsite)	3-4 years	Subset of applicable requirements
	Self- certification with evidence	2-3 years	Subset of applicable requirements or a targeted requirement(s)
	Self-certification without evidence	2-3 years	Subset of applicable requirements
	Spot audit	Event or complaint driven	Targeted requirement(s)
3. Medium	Audit (onsite or offsite)	3-4 years	Subset of applicable requirements
	Self-certification with evidence	2-3 years	Subset of applicable requirements or a targeted requirement(s)
	Self-certification without evidence	1-2 years	Subset of applicable requirements
	Spot audit	Event or complaint driven	Targeted requirement(s)
4. Medium with demonstrated exceptional performance	Audit (onsite or offsite)	3-5 years	Subset of applicable requirements
	Self- certification with evidence	3-4 years	Subset of applicable requirements or a targeted requirement(s)
	Self-certification without evidence	2-3 years	Subset of applicable requirements
	Spot audit	Event or complaint driven	Targeted requirement(s)
5. Low	Self-certification with evidence	3-4 years	Subset of applicable requirements or a targeted requirement(s)
	Self-certification without evidence	1-2 years	Subset of applicable requirements
	Spot audit	Event or complaint driven	Targeted requirement(s)

Entity Risk Rating	Tool Options	Frequency Potential	ARS Requirement Scope
6. Low with demonstrated exceptional performance	Self-certification with evidence	3-5 years	Subset of applicable requirements or a targeted requirement(s)
	Self-certification without evidence	2-3 years	Subset of applicable requirements
	Spot audit	Event or complaint driven	Targeted requirement(s)

7.5 Tools and Processes

The AESO uses the compliance monitoring tools listed above in Table 1. The AESO will develop and provide additional guidance to entities for each of the tools listed, as the ARCMP implementation advances. Below is a description of each of the tools.

7.5.1 Audit (onsite or offsite)

Audits provide assurance that ARS requirements are being complied with by applicable entities and the highest risks, identified by the AESO through the ARCMP processes, are managed appropriately. Audits are also an opportunity for the AESO and entity to develop and maintain effective relationships and demonstrate cooperation and commitment that directly supports the reliability and security of the IES.

7.5.2 Spot Audit

The AESO may conduct a spot audit of an entity, onsite or offsite, triggered by (but not limited to):

- newly identified entity specific risk posed to the IES.
- events such as misoperations, generator and transmission forced outages, and cyber security incidents that may have potential impacts to compliance with ARS.
- information or a complaint about an entity that may have potential impacts to compliance with ARS.
- a need to verify the results of an entity's self-certification.
- reasonable suspicion of non-compliance.

ARCMP Audit Process

The AESO has established the ARCMP Audit Process[9] as a companion document to the ARCMP. The ARCMP Audit Process provides an entity with the information it requires to understand the steps involved in an audit.

7.5.3 Self-Certification

Self-certification provides assurance that ARS requirements are being complied with and encourages an entity to develop a robust internal compliance program that includes periodic reviews of its compliance status with applicable ARS requirements and mechanisms to internally detect and correct non-compliance. Self-certification requires an entity to provide a declaration to the AESO and certify its compliance status with the applicable ARS requirements – scope determined as part of the ARCMP processes – for a specific period and if not compliant, provide disclosure to the AESO. The AESO conducts self-certifications with evidence or without evidence on a frequency determined by the AESO as part of the COP.

[9] AESO Website, ARS Compliance Monitoring

Self-certification without evidence

Self-certification without evidence requires the entity to declare its compliance status with the ARS requirements in scope for a specific period.

Self-certification with evidence

Self-certification with evidence requires the entity to declare its compliance status and submit evidence to demonstrate its compliance with the ARS in scope for a specific period.

ARCMP Self-Certification Process

The AESO has established the ARCMP Self-Certification Process[10] as a companion document to the ARCMP. The ARCMP Self-Certification Process provides an entity with the information it requires to understand the steps involved in self-certification.

[10] AESO Website, ARS Compliance Monitoring

8. Revision History

The AESO's Compliance Department revises this document, as needed. The AESO notifies entities of revisions through the stakeholder update process.

Revision	Effective Date	Description/Details
Version 1.0	June 1, 2024	Published on **AESO** website
Version 1.1	August 30, 2024	• Amended Table 1, Medium with Demonstrated Exceptional Performance, Frequency Potential, Self-Certification Without Evidence from 1-2 years to 2-3 years • Amended Section 7.5.4, Advanced Self-Certification, removed reference to declaration statement signed by entity's company officer

Version 1.2	February 21, 2025	• Minor administrative and grammatical changes for clarity
		• Amended section 7 to reflect minor process changes that occurred during ARCMP implementation
		  ○ Section 7.2 – removed references to mapping Alberta Risk Factors to ARS requirements
		  ○ Section 7.3 – removed reference to most recent compliance history being weighted more heavily in compliance performance assessment
		  ○ Section 7.3.3 – removed reference to the AESO providing a list of contraventions in the Compliance Oversight Plan
		• Amended section 7.5 to remove references to legacy processes and added references to the ARCMP Audit and Self-Certification Processes