Date: 21 January 2026

To:
Reliability Panel
Australian Energy Market Commission
Level 15, 60 Castlereagh Street
Sydney NSW 2000

From:
VeriConneX Pty Ltd
Level 8/140 Bourke Street
Melbourne, VIC 3000

vericonnex.com.au

To the Chair of the Reliability Panel,

VeriConneX appreciates the opportunity to contribute to the Reliability Panel's review of the Template for Compliance Programs. As the developer of COMET, Australia's leading GPS (Generator Performance Standards) compliance management platform, with more than 3GW of generation and storage assets under management across two dozen generators, we bring practical, evidence-based insights from real-world implementation of compliance programs across diverse technologies.

This review comes at a critical juncture in Australia's energy transition. As our grid becomes increasingly dominated by inverter-based resources with new and evolving performance characteristics, effective compliance frameworks are a critical tool for maintaining system security and reliability.

Why a robust compliance management framework is important

Recent grid failures in Australia and globally show that market operators, network providers, and asset owners must collaborate to maintain grid security and reliability in an increasingly complex landscape. Owners of large generation and storage assets must ensure their plants meet technical standards and don't destabilise the grid or neighboring assets. As inverter-based technologies proliferate and older conventional generation reach end of life, emerging challenges—subsynchronous oscillations, inertia and frequency control, voltage instability, and power quality issues—are complicating power system operations. The consequences are real: from West Murray Zone connection problems in Australia to the 2025 Iberian blackout that hit Spain and Portugal.

Significant disparity exists between asset owners who proactively manage compliance and those who take reactive or passive approach to compliance - the Template should establish proactive practices as the industry standard to ensure all participants contribute equally to system security.

Today's compliance challenge is implementation, not documentation

Asset owners consistently report one key challenge: unclear assessment methods in the current template for demonstrating compliance with performance standards. Some methods are too vague and high-level; others are too prescriptive or inapplicable to modern generation and storage assets. In our view:

"an outcomes-focused template that sets clear objectives while letting industry determine the best methods to achieve them is the best way forward."

While the current Template provides a useful foundation, the main challenge facing the industry is not the lack of guidance but the implementation of compliance programs. Many asset owners are insufficiently managing GPS compliance on an ongoing basis, discovering non-compliance issues only

when something goes (badly) wrong or during intermittent AEMO or NSP audits. This reactive approach creates unnecessary risk for both individual assets and the broader power system.

We believe the updated Template can and should play an important role to support this implementation gap by providing clearer direction on what constitutes an effective, active compliance program versus a “document and park for as long as we can” approach.

Addressing the implementation gap: from testing-focused to monitoring-enabled compliance

The traditional compliance template remains heavily weighted toward periodic on-site testing. This testing-centric paradigm made sense when it was developed, but modern technologies now enable a fundamentally better approach: automated continuous monitoring *complemented* by targeted testing. The traditional testing approach is expensive (in some cases accounting for 60% or more of compliance costs), risky (staged tests can complicate system operations), insufficiently frequent (every 3-7 years), and invasive (requiring outages and specific operating conditions).

Asset owners and their engineering teams recognise these issues. However, many asset teams remain constrained by organisational inertia, tight operating budgets that haven't historically included monitoring platforms, complex contractual and outsourcing arrangements and the temptation to defer costly testing when immediate OPEX pressures mount. Engineers also understand that continuous monitoring delivers superior outcomes—complete event coverage rather than periodic sampling, earlier detection of performance drift, and validation using real system conditions rather than artificial staged tests.

What's needed is regulatory clarity that establishes continuous automated monitoring as the preferred foundation for modern compliance programs, with periodic testing serving its proper role: validating performance at edge conditions that may not occur naturally or frequently, and providing targeted verification following plant changes. The Updated Template should provide this clarity, giving asset owners and their technical teams the regulatory confidence to implement approaches they already know deliver better security outcomes at lower cost.

Four pillars of effective compliance programs

Based on our operational experience providing compliance management services to, and working closely with, Australia’s leading Asset Owners, we have concluded that effective compliance programs rest on four pillars:

1. Monitoring - Continuous monitoring of plant performance under both normal and abnormal conditions is essential. All necessary technologies exist today: metering, data management systems, high-speed internet connectivity, and cloud-based analytics platforms. While monitoring alone is insufficient (edge conditions may not be reached), it is a foundational capability to ensure plants behave as expected and to identify performance drift early.

2. Testing - Periodic testing remains important for verifying performance at edge conditions that may not occur naturally. However, testing should be viewed as a necessary complement to continuous monitoring, and not be relied upon as the sole method for assessing compliance. Testing is intrusive, costly, infrequent, and cannot cover all scenarios (e.g., actual fault ride-through).

3. Modelling - Model validation or benchmarking must be performed periodically to ensure accurate models are available for detailed investigations. Model validation for significant grid events is good

practice, particularly for voltage control, frequency control and fault ride-through. Model data should be validated and documented regularly.

4. Reporting and Documentation - The current reactive approach (records available on-demand, 7-year retention) tacitly encourages Asset owners to “look the other way” - the best Asset owners do not do this. All Asset owners should have positive obligations to document their compliance status regularly and make this available to AEMO and the AER, similar to how publicly listed companies publish annual reports. This would transform compliance from reactive to proactive, support more reliable operation of our grid, and improve transparency to AEMO and the NSPs.

Our key recommendations

Our recommendations address this implementation gap while reflecting the technological and economic realities of modern power systems:

1. **Strengthen continuous monitoring preference** - Make continuous monitoring the preferred approach for modern power systems, reflecting both cost-effectiveness and superior security outcomes. The revised Principle 3 should explicitly state continuous monitoring is preferred, not merely an option to "consider."
2. **Add a Plant Performance change management framework** - Any hardware or software changes (which can impact the response of a plant relative to its GPS obligations) should be undertaken under a defined change management framework. We recommend adding a new Principle 6 and corresponding methodology for hardware and software change verification.
3. **Provide technology-specific guidance** - Different technologies genuinely require different approaches. The Template should distinguish between synchronous plant, grid-following IBR, and grid-forming IBR, as well as address battery degradation and hybrid systems explicitly.
4. **Provide guidance based upon connection context** - i.e. transmission connected, distribution connected power plants
5. **Provide guidance for material inverter based loads** - specifically assets like datacentres and hydrogen electrolysers
6. **Add three new methodologies:** Automated event detection and assessment (reflecting best practise), Generator Performance change verification protocol and Risk-based compliance framework
7. **Update cost guidance** - Reflect that continuous monitoring now delivers superior outcomes at comparable or lower cost than using traditional periodic testing alone.
8. **Establish positive reporting obligations** - Move beyond on-demand record provision to regular documented compliance status reporting.

A General Comment on Maintaining Flexibility and Enabling Innovation in Compliance

While the Template should provide clear guidance on compliance objectives and outcomes, it must avoid over-prescription of specific methodologies or technologies. The Template should establish what needs to be achieved—ongoing assurance of compliance with performance standards—while preserving flexibility in how asset owners demonstrate that compliance. This outcomes-focused approach is essential for several reasons:

First, it enables innovation in compliance methodologies. As technologies evolve and new approaches emerge (such as the shift from periodic testing to continuous automated monitoring), asset owners must have the freedom to adopt superior methods without waiting for regulatory approval.

Second, different technologies and operational contexts genuinely require different approaches - a one-size-fits-all prescription would either be too restrictive for some or inadequate for others.

Third, excessive prescription risks entrenching incumbent approaches and creating barriers to more effective, efficient compliance solutions.

The Template's role is to establish principles, define minimum requirements, and provide guidance on suitable approaches - not to mandate specific vendors, technologies, or detailed procedures. AEMO and NSPs should similarly focus their oversight on compliance outcomes and evidence quality, rather than prescribing particular implementation approaches. This preserves competitive pressure for better solutions while maintaining robust system security outcomes.

The Reliability Panel has an opportunity to actively improve grid security by nudging compliance from reactive to proactive

In 2026, modern technologies and approaches are available to address the implementation challenge. It has become cost effective to move grid compliance activities from once every 24 months to once every 24 hours through:

- **Automatic detection** of every relevant system event across high-speed monitoring data
- **Immediate assessment** of plant responses against registered performance standards
- **Alerting operators** to potential non-compliance within days rather than months or years
- **Detailed documentation of compliance** with complete event coverage and audit-ready records
- **Integrated model validation** through comparison of measured to modelled performance

Our experience across diverse plant types proves that continuous automated monitoring is not just technically feasible but economically superior to traditional approaches, typically reducing compliance review effort by 75-80% while providing earlier detection and complete coverage.

"It's 'too hard' or 'too expensive' is simply not true in 2026."

The updated Template should provide regulatory recognition of this transformation, establishing clear guidance for continuous monitoring with automated assessment, field testing as an essential function, modelling and documentation as the best practice for modern power systems.

Our detailed responses to the questions proposed in the review are attached below.

Yours faithfully,

Aditya Upadhye,
Managing Director, VeriConneX

Question 1: Effectiveness of the Template in providing guidance for compliance programs

What are stakeholders' experiences of using the Template?

The current Template provides a useful foundation for developing compliance programs, particularly its structure of compliance principles and performance standard methodologies. However, our experience across more than 3GW of generation and storage assets reveals a significant gap between the Template's guidance and the practical implementation of effective, ongoing compliance programs.

The Template's primary limitation is its heavy orientation toward periodic testing regimes. Many asset owners interpret it as endorsing a "test every 3-5 years and document the results" approach, when continuous automated monitoring complemented by targeted testing delivers superior security outcomes at comparable or lower cost.

Moreover, recommended compliance assessment methods are often too high-level and don't translate well to new renewable plants connecting to the grid. This ambiguity leads asset owners to interpret requirements differently—some taking minimal approaches—resulting in inconsistent methodologies across the industry.

Does the current Template provide useful guidance to help parties with their obligations under the NER?

Yes, but incomplete.

While the Template outlines what performance standards must be addressed and offers compliance methodologies, it falls short in key areas:

Implementation guidance: The Template doesn't clearly distinguish between "active" compliance programs and passive "document only" approaches. This contributes to significant disparity in industry practices—some asset owners maintain robust proactive programs while others discover non-compliance only during audits or failures.

Insufficient emphasis on monitoring: While acknowledging continuous monitoring as an option, the Template doesn't convey that for modern power systems, continuous monitoring should be the foundation of compliance programs, not merely an alternative to periodic testing.

Technology and cost mismatch: The Template doesn't reflect how modern technologies have transformed compliance. Traditional staged testing remains expensive (~60% of compliance costs), while continuous monitoring has become affordable and can reduce overall costs while delivering superior outcomes.

What opportunities are there to improve the Template to provide better guidance in relation to compliance with NER technical performance standards?

VeriConneX has identified four key opportunities to provide better guidance.

1. Establish continuous monitoring as the preferred foundation

The Template should explicitly state that continuous automated monitoring represents best practice where practicable. The revised Template should update Principle 3 to state continuous monitoring is preferred (not merely an option), include methodologies for automated event detection and assessment, and clarify its advantages: complete event coverage, earlier detection of performance drift, and validation using real system conditions.

2. Provide clearer implementation guidance

The Template should distinguish programs providing genuine ongoing assurance from those satisfying minimum documentation requirements. This includes guidance on assessment frequency, clarifying that "instituting and maintaining" means active ongoing monitoring (not reactive reviews), and emphasising the four pillars: Monitoring, Testing, Modelling, and Reporting/Documentation.

3. Clarify complementary roles of testing and monitoring

The Template should articulate that monitoring provides continuous assurance and identifies drift early, testing validates edge conditions and verifies plant changes, modelling must be periodically validated, and reporting should be proactive rather than reactive ("available on demand").

4. Include technology-specific and risk-based guidance

The Template should address how methodologies differ by technology (synchronous vs grid-following vs grid-forming IBR), provide risk-based frameworks focusing effort where it matters most, include plant performance change management (especially software/firmware updates), and integrate with broader asset management programs.

Question 2: Proposed assessment principles and rationale

Do you agree with the proposed high level assessment criteria?

Yes.

We strongly support the Panel's proposed assessment criteria and believe they provide an appropriate framework for evaluating updates to the Template. The three criteria - safety, security and reliability; innovation and flexibility; and principles of good regulatory practice - collectively address the key considerations for effective compliance frameworks.

Safety, security and reliability: This criterion correctly prioritises system security outcomes while recognising the need for efficiency. We particularly support the Panel's articulation that the Template should "promote efficient testing regimes" while "minimising the risk that consumers bear the cost of overly onerous testing regimes." This balance is critical - effective compliance shouldn't be unnecessarily expensive.

Innovation and flexibility: This criterion appropriately recognises that the Template must accommodate evolving technologies without constraining innovation. As our grid transforms from synchronous-dominated to IBR-dominated, the Template must support compliance approaches that work across diverse technology types while remaining adaptable to future developments.

Principles of good regulatory practice: We strongly endorse this criterion, particularly the Panel's emphasis on balancing prescription with flexibility. The Template should be clear enough to guide effective compliance programs and support the AER's enforcement function, while remaining flexible enough to accommodate legitimate differences in plant types and operations.

Are there additional criteria the Panel should consider or criteria included here that are not relevant?

Yes.

The proposed criteria are comprehensive and appropriate. However, we suggest one refinement to strengthen the framework:

Add explicit consideration of implementation effectiveness: While "principles of good regulatory practice" touches on this, we recommend making implementation effectiveness a more explicit focus. The Template's success should be measured not just by how well it's written, but by whether it actually drives better compliance behaviour across the industry.

This would involve assessing whether the Template:

- Encourages proactive rather than reactive compliance approaches
- Promotes early detection of potential non-compliance rather than discovery during audits or failures
- Facilitates regular compliance monitoring rather than periodic assessments
- Supports a culture where asset owners actively monitor and report their compliance status

This refinement would help ensure the Template addresses the implementation gap we've identified - the disparity between asset owners who proactively manage compliance and those who take reactive or passive approaches. The Template should explicitly nudge the industry toward practices that genuinely improve system security, not just satisfy minimum documentation requirements.

Beyond this refinement, the proposed criteria appropriately capture the key considerations for this review.

Question 3: Proposed revised compliance principles

Do you agree with the revised compliance principles?

Yes, and Principle 3 should be strengthened.

We support the Panel's consolidation and modernisation of the compliance principles. The revised principles are clearer, more concise, and better aligned with contemporary compliance practice. Several specific improvements stand out:

Principle 1 (Materiality and efficiency): The consolidation of the existing Principles 3 and 6 is excellent, and the explicit reference to the NEO provides valuable guidance on how to balance costs, risks, and materiality. This principle appropriately recognises that compliance programs should be proportionate and efficient.

Principle 2 (Frequency of testing): The two-part structure effectively addresses both variable and stable plant parameters. This distinction remains relevant and helps registered participants design appropriate testing regimes.

Principle 4 (Efficacy of compliance program): We strongly support the addition of "A Registered Participant should review and update its compliance program(s) periodically." This reinforces that compliance programs are living documents requiring ongoing attention, not one-time exercises.

Principle 5 (Good electricity industry practice): Maintaining explicit reference to "good electricity industry practice" is essential, as this concept underpins the entire compliance framework.

However, we believe **Principle 3 (Role of continuous plant monitoring)** requires strengthening to reflect current best practice and technological capabilities.

Recommended enhancement to Principle 3

The current proposed wording states continuous monitoring should be "considered" where practicable. We recommend strengthening this to establish continuous monitoring as the **preferred approach** for modern compliance programs:

Proposed revised Principle 3:

> "Subject to Principle 1, registered participants should institute continuous monitoring regimes that analyse plant performance during events, disturbances and normal operation to demonstrate ongoing compliance against performance standards. Where continuous monitoring is not practicable, registered participants should clearly document the reasons and implement alternative monitoring and testing regimes that provide equivalent assurance of ongoing compliance."

Rationale for this strengthening:

Modern technologies have fundamentally transformed what's possible in compliance monitoring. High-speed metering, data management systems, internet connectivity, and cloud-based analytics platforms are now widely available and affordable. The capabilities exist today to move compliance activities from "once every 24 months" to "once every 24 hours" through automated event detection, immediate assessment, and complete event coverage.

Continuous monitoring delivers superior outcomes for system security:

- **Complete coverage** rather than periodic sampling
- **Earlier detection** of performance drift or degradation
- **Real system conditions** rather than artificial staged tests
- **Lower overall cost** compared to traditional testing-focused approaches
- **Reduced risk** by avoiding intrusive staged tests that can complicate outage coordination and thereby, system operations

The Template should provide clear regulatory recognition of this transformation. Asset owners and their engineering teams already recognise these benefits, but many remain constrained by organisational inertia, tight budgets, or uncertainty about regulatory expectations. The Template can remove this uncertainty by establishing continuous monitoring as the expected foundation for modern compliance programs.

This doesn't mean mandating specific vendors or technologies—the principle of good regulatory practice requires maintaining flexibility in how continuous monitoring is implemented. Rather, it means establishing the regulatory expectation that where monitoring infrastructure exists or can be reasonably implemented, it should form the foundation of compliance programs, with periodic testing serving its proper complementary role: validating performance at edge conditions and following plant changes.

Are there any key concepts that are not currently outlined in the compliance principles that should be included?

Yes.

We recommend adding a **new Principle 6 addressing plant performance change management**, particularly for software and firmware updates:

Proposed new Principle 6 (Plant performance change management):

> "Where plant performance may be affected by hardware modifications, software updates, or firmware changes, registered participants must assess whether such changes could impact compliance with performance standards. These may include changes that are not material for an application under NER Cl. 5.3.9. Changes assessed as potentially affecting performance must be verified through appropriate testing, monitoring, or modelling before or immediately after implementation, with results documented in accordance with the compliance program."

Rationale:

Modern IBR plant is increasingly software-defined, where firmware updates and other settings changes can fundamentally alter performance characteristics in ways that would be impossible for synchronous plant. A firmware update to a wind farm or battery system can change frequency response, voltage control behaviour, or fault ride-through performance without any physical modifications to equipment.

This creates a compliance challenge not adequately addressed in the current principles. Asset owners need clear guidance that:

- Software and firmware changes must be treated with the same rigour as hardware modifications
- Changes must be assessed for potential performance impacts before implementation
- Changes assessed as potentially affecting performance require verification
- This verification should occur promptly, not deferred to the next scheduled periodic test

This principle would fill a critical gap in the compliance framework as our grid becomes increasingly dominated by software-defined plants. It recognises that for IBR, maintaining compliance requires robust change management processes that traditional synchronous plant do not need to the same degree.

Additional consideration: Risk-based compliance frameworks

While not necessarily requiring a separate principle, the Template could benefit from explicitly acknowledging risk-based approaches within the existing principles. The current Principle 1 (Materiality

and efficiency) touches on this, but could be enhanced to more clearly state that compliance programs should focus effort and resources where they matter most for system security.

This could involve:

- More frequent monitoring and testing of performance standards critical to system security
- Recognition that not all performance standards carry equal risk if non-compliant
- Flexibility to adjust monitoring intensity based on plant characteristics, operating patterns, and system conditions

However, we recognise this concept may be better addressed through guidance in the Template body rather than adding another principle, as the principles should remain high-level and concise.

Question 4: Structure and form of the Template

Do stakeholders support the Panel's proposed approach to revise the Template structure based on plant type to include schedule 5.2, schedule 5.3 and schedule 5.3a plant?

Yes.

We strongly support the Panel's proposed approach to structure the Template by plant type (schedule 5.2, 5.3, and 5.3a). This structure offers several important advantages:

Clarity and ease of use: Organising the Template by plant type creates clear, separate sections that registered participants can navigate directly to their relevant plant. This reduces confusion and makes it easier to identify applicable compliance methodologies.

Alignment with the NER structure: Structuring the Template to mirror the schedules in the NER creates logical consistency between the regulatory framework and the compliance guidance. Registered participants familiar with their obligations under schedule 5.2, 5.3, or 5.3a can easily find the corresponding Template guidance.

Technology-appropriate guidance: Different plant types have fundamentally different technical characteristics, operating profiles, and appropriate compliance approaches. Separating guidance by plant type allows the Template to provide methodologies tailored to each technology without forcing a one-size-fits-all approach that would be either too restrictive for some or inadequate for others.

Future adaptability: As the NER continues to evolve and potentially adds new plant categories or further refines existing categories, the plant-type structure provides a clear framework for incorporating these changes into the Template.

Do stakeholders have any suggestions for how the Template should provide guidance to different plant types?

Yes, we have five suggestions.

1. Provide technology-specific methodologies where appropriate

While maintaining technology neutrality as a general principle, the Template should explicitly recognise where different technologies require different compliance approaches. Specifically:

For schedule 5.2 plant, distinguish between **Synchronous plant** (traditional generators, synchronous condensers), **Grid-following IBR** (most current wind, solar, and battery systems), **Grid-forming IBR** (emerging technology) and **Hybrid systems** (combinations of different technologies at a single site) where applicable - including continuous monitoring of control system responses and validation against manufacturer specifications.

For schedule 5.3 plant, address:

- **Large inverter-based loads** (data centres, hydrogen electrolysers): Provide methodologies appropriate for large, controllable loads with power electronics interfaces

For schedule 5.3a plant (HVDC links):

- Recognise that while HVDC links share inverter-based characteristics with other IBR, their continuous operation, system-critical role, and typically extensive built-in monitoring may warrant different compliance approaches

2. Address connection context differences

Compliance approaches may appropriately differ based on connection arrangements:

- **Transmission-connected plant**: Typically have sophisticated monitoring infrastructure and direct relationships with AEMO and TNSPs. This may also include plants (e.g.: > 5 MW) connecting to a DNSP's sub-transmission network.
- **Distribution-connected plant**: May have different monitoring capabilities and work primarily through DNSPs

The Template should acknowledge these differences and provide appropriate guidance for each context.

3. Recognise plant-specific characteristics

Beyond technology type and connection context, provide guidance on how compliance methodologies should account for:

- **Plant size and materiality**: A 30 MW solar farm versus a 500 MW wind farm may warrant different monitoring, testing and modelling intensity
- **Operating patterns**: Baseload versus peaking versus intermittent plant
- **Age and degradation**: Battery degradation, turbine aging, and equipment wear
- **Retrofit and upgrade cycles**: How compliance should be managed through plant lifecycle changes

4. Provide clear cross-references

Where similar compliance methodologies apply across different plant types, use clear cross-references rather than duplicating content. This maintains the clarity of the plant-type structure while avoiding unnecessary repetition.

5. Include worked examples

The Template would benefit from including brief worked examples showing how registered participants should apply the guidance for different plant types. For instance:

- How a BESS operator might demonstrate compliance with frequency control requirements where it participates in the ancillary services market
- How a hybrid system with multiple DUIDs validate its active power control performance

These examples, which should be framed as potential approaches - not 'thou shalt' methodologies, would help clarify the Template's intent and support consistent application across the industry.

Do stakeholders propose any alternative approaches to revising the Template structure to accommodate additional plant types and align with the revised NER?

No, rather we'd ask you to consider two enhancements.

We do not propose alternative structural approaches. The Panel's proposed plant-type structure appropriately balances clarity, alignment with the NER, and practical usability.

However, we would encourage the consideration of two enhancements to strengthen the proposed structure:

Enhancement 1: Include a summary cross-reference table

Include an upfront summary table that maps each access standard to the plant types it applies to and the relevant Template section. This would help registered participants quickly confirm they've identified all applicable requirements. For example:

Access Standard	Applies to	Template Section
S5.2.5.1 Reactive Power Capability	Generating systems, Integrated resource systems, Synchronous condensers	2.1
S5.3a.8 Reactive Power Capability	HVDC links	4.3

This cross-reference would be particularly valuable during the transition period as industry adapts to the restructured Template and revised NER.

Enhancement 2: Maintain technology-neutral language in principles

While the plant-type structure provides necessary differentiation in methodologies, the compliance principles (discussed in Question 3) should remain technology-neutral and applicable across all plant types. This ensures the fundamental concepts - materiality, efficiency, continuous monitoring, good industry practice - apply consistently regardless of technology while allowing methodologies to differ appropriately.

The proposed plant-type structure provides the right foundation for an effective, modern Template that serves the increasingly diverse NEM participant base.

Question 5: Testing and monitoring regimes for schedule 5.3 plant and schedule 5.3a plant

In general terms, what kinds of tests and monitoring regimes are included in existing compliance programs for schedule 5.3 plant (certain loads and distribution networks) and schedule 5.3a plant (HVDC links)? Is there a consistent structure for these programs that can be leveraged for the Template?

We believe so.

While our direct operational experience is primarily with schedule 5.2 plant (generation and storage), we observe several common patterns in compliance approaches for schedule 5.3 and 5.3a plant based on industry engagement and technical collaboration.

We note some common elements—continuous monitoring where technically and economically feasible, periodic testing of protection systems, model validation following significant events—there is likely less standardisation in compliance programs for schedule 5.3 and 5.3a plant compared to a schedule 5.2 plant. This reflects both the relatively recent formalisation of technical standards for these plant types and their diverse characteristics.

The Template can provide valuable standardisation while maintaining necessary flexibility for different plant types and scales.

Are there any existing methodologies in the Template that would be appropriate to apply for new plant types?

Yes, several.

Several existing methodologies in the Template are readily adaptable to schedule 5.3 and 5.3a plant. These include the ones specified for **Reactive power capability testing** (current S5.2.5.1 methodologies), **Voltage disturbance response** (current S5.2.5.4 methodologies), and **Quality of electricity generated** (current S5.2.5.2 methodologies).

Some methodologies such as those for Fault ride-through may need to be adapted or enhanced.

Are there any specific testing or monitoring methodologies that are unique to a specific plant type that the Panel should consider including in the Template?

We do not have any comment on this question.

Question 6: Appropriateness of existing testing and monitoring regimes

Despite the extensive changes to the technical requirements in Schedule 5.2, which existing testing and monitoring regimes in the Template are likely to remain suitable for new plant?

Many of the fundamental testing and monitoring approaches in the existing Template remain sound and appropriate for new plant, though some will benefit from refinement to reflect the evolution of the access standards.

The key is distinguishing between methodologies that remain fit-for-purpose and those requiring updates.

Methodologies that remain broadly suitable

Continuous high-speed monitoring approaches: The Template's emphasis on continuous monitoring using high-speed recorders remains highly appropriate and, if anything, has become more important as the grid becomes increasingly IBR-dominated.

These approaches provide complete event coverage, validate performance under real system conditions, and identify performance drift early—exactly what's needed for modern compliance programs.

Event-based compliance validation: Methodologies that investigate plant performance during actual system disturbances remain appropriate and should be strengthened. Approaches that analyse plant trips during significant disturbances, assess responses during major events, and validate models against real system behaviour align well with the revised access standards.

Protection system testing: Methodologies for routine testing and calibration of protection systems through secondary injection, circuit breaker timing verification, and performance assessment during events remain fundamentally sound across all plant types.

Sub-system testing approaches: The Template's recognition that relevant sub-systems should be routinely tested remains valid. Control systems, auxiliary power systems, and protection relays all benefit from periodic verification regardless of the specific access standard requirements.

Methodologies requiring refinement or clarification

While these methodologies remain fundamentally sound, some aspects need updating:

Model validation frequency and triggers: The Template should more explicitly emphasise ongoing model validation, particularly for IBR where control system behaviour is software-defined. The current emphasis on validation "following plant changes" remains appropriate but should be strengthened to ensure models remain current and accurate when benchmarked against real-world events.

Testing frequency guidance: Some suggested testing frequencies in the existing Template (e.g., "every 3 years," "every 5 years") were appropriate when established but may need reconsideration given:

- The increasing sophistication and affordability of continuous monitoring

- The rate of change in IBR control systems and firmware
- The growing criticality of certain performance standards (e.g., fault ride-through, system strength)

The Template should provide more nuanced guidance on how testing frequency should be determined based on plant characteristics, technology type, and availability of continuous monitoring.

Technology-neutral language: The Template's move toward technology-neutral language was appropriate, but the revised Template should reinstate technology-specific guidance where genuinely necessary to address the distinct characteristics of synchronous plant, grid-following IBR, and grid-forming IBR.

Are there any specific details about existing testing or monitoring regimes in the Template that should be amended to account for the rule changes listed above? For example, should the suggested frequency of testing of particular methodologies be amended for more effective compliance programs?

Yes, several specific amendments would better align the Template with revised access standards and contemporary best practice. But as a preface...

Given the grid's rapid evolution and diverse new technologies, prescribing specific methodologies has limited value—it's horses for courses. What works for a large 500kV hybrid power plant may be impractical or excessive for a small sub-transmission solar farm. Flexibility in methodologies is preferable, provided the overarching principles remain intact.

Several cross-cutting improvements would enhance the Template

Strengthen the monitoring-testing relationship: More clearly establish that continuous monitoring should be the foundation where available, with testing validating edge conditions and plant changes. The current Template treats these as alternative approaches rather than complementary activities.

Introduce risk-based frequency guidance: Rather than prescribing fixed testing intervals, provide principles for determining appropriate frequency based on:

- Criticality of the performance standard to system security
- Plant technology and likelihood of performance drift
- Availability and quality of continuous monitoring
- Plant operating patterns and system conditions

Address software and firmware changes: Establish clear expectations that software and firmware updates must trigger compliance validation, not just physical plant changes. For IBR, a firmware update can fundamentally alter performance even without hardware modification.

Clarify model validation expectations: Strengthen requirements for ongoing model validation, particularly following significant system events that provide good validation opportunities. This should include the requirement to identify and log ‘good modelling events’. Current models should be validated against actual performance and updated when discrepancies are identified.

These amendments would modernise the Template to reflect both the revised access standards and contemporary best practice in compliance management, while preserving the fundamental soundness of existing methodologies.

In addition to the above improvements and to answer the question more directly...

1. Reactive power capability (S5.2.5.1)

- Clarify that testing should address the revised voltage range requirements (from 90% to 110% of nominal voltage)
- Explicitly address temperature derating requirements introduced in the revised standard
- Consider that with continuous SCADA monitoring of reactive power output, the testing frequency could be extended to every 5 years for plant with robust monitoring, while maintaining 3 years where monitoring is limited

2. Voltage disturbance response (S5.2.5.4)

- Clarify the definition and measurement of "continuous uninterrupted operation" as revised in the Access Standards Package 1 rule and how it applies in a real-world setting
- For plant with continuous high-speed monitoring, clarify that assessment should occur for all voltage disturbances exceeding specified thresholds, not just those causing trips
- Strengthen the expectation that continuous monitoring should be the primary method, with periodic testing serving to validate edge conditions not naturally encountered

3. Fault ride-through and reactive current injection (S5.2.5.5 and new S5.2.5.5A)

- Update methodologies to reflect the new S5.2.5.5A requirements for reactive current injection, including the revised rise time , settling time , and commencement time requirements for reactive current
- For plant with continuous high-speed monitoring, establish that every significant fault event should be assessed, not just those causing trips

4. Frequency protection and Frequency control (S5.2.5.3 and S5.2.5.11)

- Clarify that assessment should include both fast frequency response (FFR) and governor/primary frequency response where plant provides these services
- Consider reducing testing frequency from every 3 years to every 5 years where comprehensive continuous monitoring is in place and regularly validated

5. Voltage and reactive power control (S5.2.5.13)

- Update methodologies to address multiple modes of operation (voltage control, reactive power control, power factor control) and validation of mode transitions
- Consider that for plant with continuous monitoring of voltage and reactive power response during system events, testing frequency could be adjusted based on the frequency of suitable validation events
-

6. Instability detection and response (S5.2.5.10)

- Substantially revise to address the new requirements for instability detection and response applicable to all plant types
- Develop new methodologies appropriate for validating:
  - Detection of oscillations or unstable operation
  - Contribution factor of the assessed plant when instability is detected
- Distinguish between approaches appropriate for synchronous plant versus IBR

Question 7: Suggestions for new testing or monitoring regimes

Are stakeholders aware of any new testing or monitoring regimes that could contribute to making more effective compliance programs for performance standards made under the amended access standards?

Yes, we recommend three new methodologies that reflect current best practice and technological capabilities:

1. Automated event detection and assessment methodology

Rationale: Modern compliance programs increasingly rely on automated systems to identify and assess compliance-relevant events from continuous monitoring data. This represents a fundamental shift from manual, periodic reviews to automated, near-real-time compliance assessment.

Proposed methodology:

Method: Automated event detection and compliance assessment

Suitable for: All performance standards where continuous high-speed monitoring is available, particularly S5.2.5.3 (frequency response), S5.2.5.4 (voltage disturbance), S5.2.5.5 (fault ride-through), S5.2.5.13 (voltage control), and S5.2.5.14 (active power control).

Description:

- Implement automated systems that continuously analyse high-speed monitoring data (typically 20-100ms resolution) to detect events requiring compliance assessment
- Configure automated detection algorithms for:
  - Frequency deviations beyond operational tolerance bands
  - Voltage disturbances exceeding specified thresholds
  - Fault events and voltage sags
  - Significant changes in system conditions
  - Plant trips or abnormal operating conditions
- Automatically assess plant performance against registered performance standards for each detected event
- Generate alerts when potential non-compliance is detected or when plant response differs from expected behaviour
- Maintain comprehensive records of all detected events, assessments, and outcomes

Frequency: Continuous operation with automated daily, weekly, or monthly summary reporting as appropriate to the plant and its operating patterns.

Compliance assessment basis:

- Consistency with registered performance standards
- Consistency with validated plant models
- Consistency with historical plant performance (to identify drift or degradation)
- Immediate alerting of potential non-compliance for investigation

Benefits:

- Complete event coverage rather than periodic sampling
- Early detection of performance issues or drift
- Immediate visibility of potential non-compliance
- Reduced reliance on manual data review
- Comprehensive documentation for audit purposes
- Lower overall compliance costs compared to manual periodic reviews

This methodology recognises that technology has advanced significantly since the Template was last updated. Automated event detection and assessment tools are now readily available and affordable, and represent best practice for modern compliance programs.

2. Plant performance change verification protocol

Rationale: As noted in our response to Question 3, modern IBR plant is increasingly software-defined. Firmware and software updates can fundamentally alter plant performance characteristics. The Template should include explicit methodologies for verifying compliance following such changes.

Proposed methodology:

Method: Plant performance change verification

Suitable for: All performance standards, but particularly critical for IBR plant where software/firmware changes can affect performance.

Description:

- Keep record of R2 model and model parameters (for example, in the Power System Design and Setting Data Sheet (PSDS)) as the starting record of 'as-commissioned' plant design
- Record of any change to plant design (software and hardware) to the records in the PSDS
- Record assessment prior to implementation of the change and note its materiality
- Verification test results or monitoring data
- Confirmation of continued compliance or identification of new performance limitations
- Updates to plant models if performance characteristics changed
- Notification to AEMO/NSP if performance has changed materially

Frequency: Triggered by any plant change, particularly software/firmware updates.

Compliance assessment basis:

- Continued compliance with registered performance standards post-change
- Consistency with plant models
- No unintended performance degradation

This methodology fills a critical gap in the current Template by explicitly addressing how compliance should be managed through the plant lifecycle, particularly for software-defined IBR.

3. Risk-based compliance monitoring framework

Rationale: Not all performance standards carry equal risk to system security if non-compliant, and not all plant types or operating patterns present the same risk profile. A risk-based framework allows compliance programs to focus effort where it matters most.

Proposed methodology:

Method: Risk-based compliance monitoring

Suitable for: All performance standards, as an overarching framework for determining monitoring intensity and testing frequency.

Description:

Risk assessment factors:

Performance standard criticality:

- System security impact if non-compliant (e.g., fault ride-through more critical than some power quality aspects)
- Consequences of non-compliance (credible contingency events, system strength, voltage stability)
- Current system needs (e.g., frequency control more critical in low-inertia conditions)

Plant characteristics:

- Technology type and likelihood of performance drift
- Plant age and operating history
- Complexity of control systems
- Recent performance record

Monitoring capability:

- Availability and quality of continuous monitoring
- Frequency of natural validation opportunities (system events)
- Sophistication of automated assessment tools

Risk-based monitoring intensity:

High-risk combinations (critical standard + limited monitoring + history of issues):

- More frequent testing (e.g., every 2-3 years rather than 5 years)
- Enhanced continuous monitoring with automated alerting
- Mandatory assessment of every relevant system event
- More frequent model validation

Medium-risk combinations (standard criticality or monitoring):

- Standard testing frequencies (e.g., every 3-5 years)
- Continuous monitoring where available
- Assessment of major system events
- Periodic model validation

Low-risk combinations (less-critical standard + comprehensive monitoring + strong performance history):

- Extended testing intervals (e.g., every 5-7 years)
- Reliance primarily on continuous monitoring
- Assessment of significant events
- Model validation as opportunities arise

Documentation requirements:

- Risk assessment methodology and results
- Justification for monitoring intensity decisions
- Regular review and update of risk assessments (e.g., annually or following significant events)

Frequency: Risk assessment updated annually or following significant changes to plant, system conditions, or performance history.

Compliance assessment basis:

- Appropriate monitoring intensity relative to assessed risk
- Ongoing compliance demonstrated through monitoring and testing proportionate to risk
- Regular reassessment of risk factors

This framework recognises that a one-size-fits-all approach to compliance monitoring is neither efficient nor optimal for system security. By focusing effort where risks are highest, compliance programs can be both more effective and more efficient.

Are there any commonly used regimes that are not currently listed in the Template?

Yes, but with the exception of continuous monitoring, which we feel like we've covered, we believe the template is fit for purpose.

Question 8: Reflecting changes in technology and cost in the Template

Does the current Template appropriately consider all technology types? If not, how can the Template be amended to better reflect newer technologies?

No, the template does not. We'd recommend the committee consider a layered approach.

The current Template does not adequately address the full range of technology types now prevalent in the NEM. While the 2019 review removed technology-specific language to achieve neutrality, this has inadvertently created gaps where technology-specific guidance is genuinely necessary. The Template requires updating to explicitly address distinct technology characteristics while maintaining appropriate neutrality where technologies can be treated equivalently.

Rather than attempting comprehensive technology neutrality, the Template should adopt a layered approach:

Layer 1: Technology-neutral principles and methodologies applicable across all plant types (continuous monitoring, event investigation, protection testing, model validation)

Layer 2: Technology-category specific guidance distinguishing between:

- Synchronous plant (generators and synchronous condensers)
- Grid-following IBR (most current wind, solar, and battery systems)
- Grid-forming IBR (emerging but increasingly important)
- Hybrid systems (combinations of multiple technologies)

Layer 3: Technology-specific considerations within categories where genuinely necessary

This layered approach maintains appropriate neutrality while providing necessary specificity where technology differences genuinely require different compliance approaches.

Have the costs of the compliance methods listed in the Template changed significantly?

Yes, significantly.

The relative costs of compliance methods have changed substantially since the Template was developed, and even since the 2019 review. These cost shifts have important implications for which methodologies the Template should emphasise.

Staged testing costs remain high

Traditional staged testing continues to be expensive, typically accounting for 60% or more of total compliance costs:

Direct costs:

- Test planning and coordination with AEMO/NSPs
- Specialist testing personnel and equipment
- Plant downtime and lost revenue during testing
- Post-test analysis and reporting
- Travel and logistics for remote sites

Indirect costs and risks:

- System security risks during staged tests that stress the network
- Potential for test-induced plant damage or trips
- Disruption to plant operations and maintenance schedules
- Opportunity costs when testing requires specific system conditions

For large-scale testing (e.g., fault ride-through validation, partial load rejection), costs can range from $50,000 to $200,000+ per event, with additional costs if tests must be repeated due to unsatisfactory results or unfavourable system conditions.

Continuous monitoring costs have decreased dramatically

In contrast, the costs of implementing comprehensive continuous monitoring have fallen significantly:

Infrastructure costs (declining):

- High-speed metering equipment costs have decreased substantially
- Data storage costs have fallen dramatically with cloud computing
- Communications infrastructure (internet connectivity) has become ubiquitous and affordable
- Many modern plants now have monitoring infrastructure installed as standard

Platform costs (increasingly affordable):

- Cloud-based compliance monitoring platforms have emerged offering subscription-based pricing
- Typical costs: $20,000-$50,000 per year for comprehensive monitoring across large plants
- Costs scale efficiently across multiple sites
- Platform costs are often comparable to or lower than conducting a single staged test

Operational costs (decreasing):

- Automated event detection eliminates manual data review
- Automated compliance assessment reduces engineering review time by 75-80%
- Real-time alerting enables faster response to potential issues
- Comprehensive documentation reduces audit preparation time

The economic case has shifted decisively

The economic comparison between traditional testing-focused programs and modern monitoring-enabled programs has fundamentally changed:

Traditional approach (testing every 3 years):

- Periodic testing: $150,000-$400,000 per cycle
- Manual compliance reviews: $30,000-$60,000 per year
- Three-year cost: $240,000-$580,000
- *Result*: Periodic sampling, delayed issue detection, incomplete event coverage

Modern approach (continuous monitoring + targeted testing):

- Continuous monitoring platform: $60,000-$150,000 over three years
- Reduced periodic testing (focused on edge conditions): $50,000-$100,000 per cycle
- Three-year cost: $110,000-$250,000
- *Result*: Complete event coverage, immediate issue detection, superior compliance assurance

The modern approach typically costs 40-60% less than traditional approaches while delivering substantially better outcomes for system security. This cost shift should be explicitly recognised in the Template.

What changes, if any, could be made to the Template to reflect updated information on the costs of testing and compliance regimes?

We would recommend seven changes.

Several specific changes would help the Template reflect current cost realities and guide registered participants toward more cost-effective compliance approaches:

1. Update the guidance on continuous monitoring

The Template's current Section 1.4 acknowledges continuous monitoring has "a number of benefits" and is "increasingly becoming a more affordable option." This understates the current reality. The revised Template should:

- State explicitly that continuous monitoring, by leveraging existing infrastructure at each plant, now typically costs less than traditional periodic testing approaches while delivering superior outcomes
- Note that the cost advantage of monitoring has increased significantly as technologies have matured
- Clarify that "affordable" is not just for large plant—monitoring solutions now scale effectively to smaller installations
- Establish continuous monitoring as the expected foundation for compliance programs, with testing serving a complementary rather than primary role

2. Provide cost-benefit guidance for methodology selection

The Template should include guidance on considering costs and benefits when selecting compliance methodologies:

Factors favouring continuous monitoring:

- Plant operates regularly, providing natural validation opportunities
- High-speed metering infrastructure exists or can be readily installed
- Performance standards are amenable to event-based validation
- Multiple performance standards can be monitored through a single platform
- Plant size and importance justify monitoring investment (though threshold continues to decline)

Factors favouring periodic testing as primary approach:

- Plant operates infrequently (dry-stored, rarely dispatched)
- Performance standards require edge conditions unlikely to occur naturally
- Monitoring infrastructure would be disproportionately expensive relative to plant materiality
- Regulatory or contractual requirements mandate specific testing

This guidance would help registered participants make informed, cost-effective decisions about compliance approaches.

3. Adjust suggested testing frequencies based on monitoring availability

While engineering judgement and risk assessment approaches should remain the driver of testing frequency for all plant, we believe that testing can be less frequent when monitoring is in place. Therefore the Template should differentiate suggested testing frequencies based on whether comprehensive continuous monitoring is in place, for example:

With comprehensive continuous monitoring:

- Many performance standards: Test every 5-7 years (extended from current 3-5 years)

- Rationale: Continuous monitoring provides ongoing assurance, reducing need for frequent testing
- Testing focuses on edge conditions and follows plant changes
- Natural system events provide regular validation

Without comprehensive continuous monitoring:

- Many performance standards: Test every 3-4 years (maintain or slightly increase frequency)
- Rationale: Periodic testing is the primary validation method
- More frequent testing needed to provide reasonable assurance

This differentiation would create appropriate incentives for monitoring adoption while ensuring adequate validation for those not yet monitoring.

4. Acknowledge the total cost of compliance programs

The Template should recognise that compliance program costs include:

- Direct testing and monitoring costs
- Engineering review and assessment time
- Documentation and record-keeping
- Audit preparation and response
- Remediation of identified issues
- Opportunity costs (plant downtime, lost revenue)

Methodologies that reduce total program costs while improving effectiveness should be explicitly preferred. The Template can note that automated continuous monitoring typically reduces engineering review time by 75-80% compared to manual periodic reviews, representing significant cost savings.

5. Address scale and materiality considerations

Cost considerations vary with plant scale and materiality. The Template should acknowledge that:

For very large, critical assets (e.g. > 200MW:

- Comprehensive monitoring clearly essential
- Advanced platforms with automated assessment mandatory
- Investment in sophisticated testing justified

For large, material plant (e.g., 30-200MW):

- Comprehensive monitoring clearly cost-justified
- Advanced platforms with automated assessment appropriate
- Investment in sophisticated testing also warranted where needed

For medium-scale plant (e.g., 5-30MW):

- Monitoring increasingly cost-effective
- Balance between platform sophistication and cost
- Targeted testing focused on critical performance standards

For small plant (e.g., <5MW):

- Cost considerations more constraining

- May rely more heavily on manufacturer validation and periodic testing
- Simpler monitoring approaches where implemented

However, the threshold where monitoring becomes cost-effective continues to decrease as technologies mature and platform costs decline.

6. Recognise monitoring as infrastructure investment

The Template should note that monitoring infrastructure, once implemented, provides value beyond compliance:

- Asset health monitoring and predictive maintenance
- Performance optimisation and revenue maximisation
- Rapid fault diagnosis and reduced outage duration
- Validation of ancillary service provision
- Support for operational decision-making

These co-benefits further improve the economic case for monitoring investment. Compliance programs that leverage monitoring infrastructure deliver better outcomes at lower total cost to the business.

7. Update the technology cost narrative

Finally, the Template should update its narrative about technological change and costs:

- Acknowledge that monitoring technologies have matured significantly
- Note that cloud-based platforms have transformed economics
- Recognise that costs continue to decline while capabilities improve
- Emphasise that "it's too expensive" is no longer valid for most plant in 2026
- Establish expectation that future reviews will continue tracking cost evolution

By explicitly addressing cost changes, the Template can guide registered participants toward compliance approaches that are both more effective for system security and more economical for asset owners. The current Template's cost assumptions, while reasonable when established, no longer reflect market realities and may inadvertently encourage outdated, more expensive approaches.

The fundamental message should be: continuous automated monitoring is now the most cost-effective foundation for compliance programs, delivering superior system security outcomes at lower total cost than traditional periodic testing approaches. The Template should clearly convey this reality.