

WHiSSPR Report: Quebec Law 25 Assessment (2026)

Assessing the Governance Capacities of the Act respecting the protection
of personal information in the private sector, as amended by Law 25

Mark Lizar

WHiSSPR Report: Quebec Law 25 Assessment (2026)

White Hat Identity, Surveillance, Security, Privacy and Risk (WHiSSPR) Report

Full Title: Assessing the Governance Capacities of the Act respecting the protection of
personal information in the private sector, as amended by Law 25

Author: Mark Lizar

Published by: Global Privacy Rights

Lab: Transparency Lab

Published: 2026

License: Global Privacy Rights, Copyright 2026

Source assessed: *Act respecting the protection of personal information in the private sector*, chapter P-39.1, official English consolidated text current to 10 June 2026, read in full. The amendments assessed were enacted by the *Act to modernize legislative provisions as regards the protection of personal information*, 2021, chapter 25, commonly called Law 25, in force in stages from 22 September 2022 to 22 September 2024.

WHiSSPR rating method (TPI v2) defaults - Scoring orientation: ordinal categories on the ANCR TPI scale. +1 dynamic, in context. 0 present but static or out of context. -1 present but obstructed. -3 non-operable. - Indicator family: Kantara ANCR Transparency Performance Indicators (TPI). - No composite is defined and none should be inferred. The ratings are ordinal categories rather than measurements on a continuous scale, so arithmetic across them, including any weighted sum, does not produce a comparable figure. - Assurance ladder: a contract reaches level 3 when accountability behind each identifier traces to a named party under a named instrument. It reaches dynamic secure level 4 when the access itself is credentialed at the point of request, logged to a party that is not the requester, actively approved rather than standing, and bounded in time and scope.

About WHiSSPR Reports

A WHiSSPR Report, White Hat Identity, Surveillance, Security, Privacy and Risk, is an audit of the privacy and security of identity surveillance. The order of the letters is the method, and each stage is answered before the next is asked.

- **Identity.** Which identifiers the instrument reaches, what the actual scope of disclosure of each is when checked against permissions and exposure rather than against what is claimed, and whether any official or contractual use is named, because only a named use supports a claim of legitimate status.
- **Surveillance.** What observation the instrument permits against those identifiers. Who can see, what is emitted, what is retained, what is inferable.
- **Security, meaning the security of that surveillance.** Not whether unauthorised access occurs, but whether the authorised access is accountable.
- **Privacy risk.** The residual once the first three are known, recorded rather than resolved.

Applied to a statute rather than to a contract, the output is a ceiling and a floor: the best assurance any contract made under the Act could claim, and the worst it guarantees.

WHiSSPR uses the Kantara Initiative Data Controller Identity Record schema and Transparency Performance Indicators to assess transparency performance and measure operational accountability.

Sourcing

Every quotation in this report was matched literally against the official English consolidated text published by the Éditeur officiel du Québec, which carries the notation that the document has official value. Every finding that a term is absent or that a term appears a stated number of times rests on a search of the whole English text, not only the sections quoted.

Quebec statutes are enacted in French and English and both versions are official. Where the two could differ in legal effect at a clause cited here, the comparison has not been made, and that limit is recorded in Unresolved.

The Subject

Title	Act respecting the protection of personal information in the private sector, chapter P-39.1
Amended by	Act to modernize legislative provisions as

	regards the protection of personal information, 2021, chapter 25 (Law 25)
Legislature	National Assembly of Québec
Regulator	Commission d'accès à l'information
Nature	Binding statute in force, not guidance and not a bill. The operative verb is “must”
In force	In three stages: 22 September 2022, 22 September 2023, 22 September 2024
Text assessed	Consolidated English text current to 10 June 2026
Scope	Personal information collected, held, used or communicated in the course of carrying on an enterprise within the meaning of article 1525 of the Civil Code

This is the only instrument in the WHiSSPR series so far that is law and in force. Bill C-36 is at second reading and China’s AI Safety Governance Framework 3.0 is guidance. What Law 25 asks for is already owed.

Executive Summary

The central finding: **Quebec is the only jurisdiction assessed that requires the accountable person to be identified to the public before any interaction, and it still gives the individual no evidence of what they were told.**

Section 3.1 requires that “The title and contact information of the person in charge of the protection of personal information must be published on the enterprise’s website”. Neither Bill C-36 nor China’s Framework 3.0 requires anything comparable. Section 8 requires the disclosure to be made “when the information is collected”, which binds it to the event rather than leaving it readily available at no stated time. Section 8.1 requires an enterprise using identification, location or profiling technology to “first inform” the person.

And then the record stops. The word “receipt” appears four times in the Act. Every one concerns the receipt of a request or of a decision of the Commission, and one of them is the sharpest finding in this report: section 54 requires the Commission to send its decision “by any means providing proof of the date of receipt”. **The Act requires proof of receipt when the regulator communicates with a party, and requires none when an enterprise gives notice to an individual.**

What the Act does well

1. Published accountability, at the top of the enterprise. Section 3.1: the person exercising the highest authority holds the function by default, may delegate it only in writing, and the title and contact must be published.
2. Notice bound to the collection event. Section 8: the enterprise “must, when the information is collected and subsequently on request, inform that person” of purposes, means, rights of access and rectification, and the right to withdraw consent.
3. Notice before profiling. Section 8.1 requires an enterprise collecting by technology that can identify, locate or profile to “first inform” the person of the use of the technology and “of the means available to activate the functions”.
4. Consent quality defined and enforced. Section 14 requires consent to be “clear, free and informed and be given for specific purposes”, requested for each purpose, presented separately in writing, valid “only for the time necessary”, and closes with: “Consent not given in accordance with this Act is without effect.”
5. Confidentiality by default. Section 9.1 requires the highest level of confidentiality by default “without any intervention by the person concerned”.
6. Automated decisions answered to a person. Section 12.1 requires disclosure at the time of the decision, and on request the information used, “the reasons and the principal factors and parameters”, and an opportunity to submit observations “to a member of the personnel of the enterprise who is in a position to review the decision”.
7. Transfer assessed against the receiving State. Section 17 requires a privacy impact assessment before communicating outside Québec, taking into account “the legal framework applicable in the State in which the information would be communicated”.
8. A remedy the individual can bring. Section 93.1: where an infringement is intentional or results from gross fault, “the court shall award punitive damages of not less than \$1,000”.

What it does not do

1. It creates no record of the disclosure. Nothing requires the notice under section 8 or section 8.1 to be recorded, versioned, timestamped or retained, and nothing gives the individual a copy.
2. It publishes a policy without a version history. Section 8.2 requires a confidentiality policy to be published and requires notice of any amendment, and requires no superseded version to remain retrievable. What was in force on a given day cannot be established later from the Act’s own requirements.
3. It logs the wrong disclosures. Section 18 second paragraph requires an entry of every communication made under subparagraphs 6 to 9.1. Communications to the Director of Criminal and Penal Prosecutions, to police, and to public bodies sit at subparagraphs 2, 3 and 5, outside the entry requirement.

4. It exempts the main surveillance vector from its own default. Section 9.1 second paragraph: “The first paragraph does not apply to privacy settings for browser cookies.”
5. It names no controller. The word “controller” appears zero times. The Act’s subject is the “person carrying on an enterprise”, which does not map onto ISO/IEC 29100 or the GDPR vocabulary without translation, and there is no controller identity record of any kind.

Conclusion

Quebec has legislated the addressee and not the evidence. The individual is told who is accountable, told at the moment of collection, told before profiling begins, and given a statutory cause of action with a minimum award. What the individual cannot do is prove any of it. **Law 25 gives the individual a cause of action and nothing to bring to it.**

Comparative Analysis Framework

1. Bill C-36, the Protecting Privacy and Consumer Data Act, 45-1, first reading, assessed in the companion WHiSSPR report of 21 September 2026
2. China’s AI Safety Governance Framework 3.0, TC260, September 2026, assessed in the companion WHiSSPR report of 23 September 2026
3. EU GDPR, Regulation 2016/679: Articles 12 to 14, Articles 37 to 39, Articles 40 to 42
4. Convention 108, in force with 55 Parties, and Convention 108+ (CETS 223), not yet in force, at 34 of the 38 ratifications required. Council of Europe Treaty Office, 23 September 2026
5. ISO/IEC 29100, privacy framework; ISO/IEC 29184:2020, online privacy notices and consent; ISO/IEC TS 27560:2023, consent record information structure

The Three Questions

1. How much notice and transparency is actually required?

More than any other instrument in this series, and it is required in three distinct places.

Before any interaction. Section 3.1 publishes the title and contact information of the person in charge. Section 3.2 requires detailed information about the enterprise’s governance policies and practices to be “published in simple and clear language on the enterprise’s website”. Section 8.2 requires a published confidentiality policy for any enterprise collecting through technological means, and notice of any amendment to it.

At the collection event. Section 8 binds the disclosure to the moment: “when the information is collected”. Four items are mandatory, and three more are owed where applicable, including “the name of the third person for whom the information is being

collected” and “the possibility that the information could be communicated outside Québec”. A further three are owed on request, including “the duration of the period of time the information will be kept” and the contact information of the person in charge.

Before the technology acts. Section 8.1 requires an enterprise using identification, location or profiling technology to “first inform” the person, and defines profiling as collection and use “to assess certain characteristics of a natural person, in particular for the purpose of analyzing that person’s work performance, economic situation, health, personal preferences, interests or behaviour”.

So the operative answer is that Quebec requires disclosure before identification, at collection, and before profiling, in clear and simple language, from a named and published accountable person. It requires no version, no timestamp, no integrity value and no copy for the individual. The content obligation is the strongest assessed. The evidence obligation is absent.

2. Will consent still be valid?

Valid in law, unprovable in practice, and Quebec says so more precisely than the others.

Section 14 is the strongest consent provision in the comparison. It requires consent to be clear, free and informed, given for specific purposes, “requested for each such purpose, in clear and simple language”, presented separately from other information where written, time limited, and it voids what does not comply: “Consent not given in accordance with this Act is without effect.”

Nothing requires that consent to be recorded. Section 8.3 then deems consent from the act of providing information in accordance with section 8. So the Act defines a demanding standard for consent, deems consent in a common case, and creates no artefact by which either the standard or the deeming can be tested afterwards. An enterprise that meets section 14 in full and one that ignores it produce the same evidence for the individual, which is none.

The asymmetry in section 18 is worth stating beside this. An enterprise must make an entry of communications to a person with compulsion powers, to debt recovery agents, and for the recovery of its own claims. It need make no entry of the consent that authorised everything else.

3. Are there privacy officers to implement the Act?

Yes, and this is where Quebec separates from every other instrument assessed.

Section 3.1 does three things no comparator does. It vests the function in “the person exercising the highest authority” by default, so accountability starts at the top rather than at a designated functionary. It permits delegation only “in writing”. And it requires the title and contact information to be published on the website, or made available by other appropriate means where there is no website.

Section 3.2 requires the governance policies to be “approved by the person in charge”, which gives the role a decision to make rather than a mailbox to hold. Section 3.3 requires that the person in charge be consulted “from the outset” of any project requiring a privacy impact assessment. Section 18.3 requires a mandatory to notify the person in charge of any violation or attempted violation without delay and to allow verification.

What section 3.1 does not do is qualify the role, protect its independence, or protect the holder from dismissal. Compare Bill C-36, where section 8(1) makes the contact available only on request and the provision has not developed in twenty five years.

Stage 1: Identity

Which identifiers the Act reaches

Identifier	Where required	Disclosed to the individual
The person in charge of the protection of personal information	s.3.1, third paragraph: title and contact “must be published on the enterprise’s website”	Published, before any interaction
The enterprise as accountable party	s.3.1, first paragraph: “Any person carrying on an enterprise is responsible”	Named in the policy under s.8.2, not as a record
The third person for whom information is collected	s.8, second paragraph	Required where applicable
Third persons to whom information is communicated	s.8, second paragraph: names or categories	Categories are sufficient
The controller	No provision. The term appears zero times	No provision

Accountability analysis

Finding. Quebec identifies the accountable human before the interaction and does not identify the accountable entity as a record. The published contact under section 3.1 is a title and a contact point on a web page. It is not resolvable, not versioned, not machine readable, and carries no integrity value, so it cannot be cited as it stood on a given day.

Comparison. GDPR Articles 13 and 14 require the identity and contact details of the controller as a condition attached to collection, and Articles 37 to 39 govern the data protection officer’s designation, position and tasks including independence. Quebec requires publication, which GDPR does not, and omits independence, which GDPR has. ISO/IEC 29184:2020 treats identification of the PII controller as notice content, and

ISO/IEC TS 27560:2023 specifies a structure in which that identification could be recorded. The Act references no standard.

Asymmetry. The individual can find out today who is accountable at any Quebec enterprise with a website. The individual cannot establish what that enterprise told them yesterday.

Stage rating: 0, present but static or out of context. The identity disclosure is present, publicly reachable before identification, and higher than either comparator. It is static, unversioned and not machine readable, which is what holds it at 0 rather than +1.

Stage 2: Surveillance

What observation the Act permits

Finding. Consent is the rule under section 14 and section 12, and the exceptions are narrower than the federal equivalents. Section 12 permits use for another purpose without consent in five cases only: a consistent purpose, clear benefit to the person, fraud prevention and security assessment, delivery of a product or service requested, and de-identified study or research. The Act then constrains the first: a consistent purpose “must have a direct and relevant connection with the purposes for which the information was collected. However, commercial or philanthropic prospection may not be considered a consistent purpose.”

That last sentence removes marketing from the consistent purpose route by name. Bill C-36’s legitimate interest exception at section 18(3) has no equivalent sentence, and permits disclosure as well as collection and use.

A limit worth naming. Section 9.1 requires the highest level of confidentiality by default “without any intervention by the person concerned”, which is a stronger formulation than data protection by design, because it names the outcome rather than the process. Its second paragraph then reads: “The first paragraph does not apply to privacy settings for browser cookies.” The default is exempted at precisely the point where most commercial observation of individuals actually happens.

Openness and transparency analysis

Finding. Three publication duties and one event-bound duty. Section 3.2 publishes the governance practices. Section 8.2 publishes the confidentiality policy and requires notice of amendments. Section 3.1 publishes the accountable contact. Section 8 binds disclosure to the collection event, and section 8.1 binds it to the point before profiling technology is used.

Gap. Three defects survive.

1. **No version and no evidence.** Section 8.2 requires a policy and a notice of amendment. Nothing requires superseded versions to remain retrievable, nothing requires a publication time or an integrity value, and nothing records that any notice was given. The amendment notice exists without a version history to attach it to.
2. **Cross-border disclosure is a possibility, not a destination.** Section 8 requires the person to be informed of “the possibility that the information could be communicated outside Québec”. The section 17 assessment that determines where, to whom and under what protection is conducted by the enterprise and disclosed to no one. The individual learns that a transfer may happen, not that one did, and not to which State.
3. **Retention is on request.** The period of time the information will be kept sits in section 8’s third paragraph, owed on request rather than at collection.

Stage rating: 0, present but static or out of context. The content required is the strongest in the comparison and section 8.1 is in context. Nothing is recorded, so no disclosure can be tested after the event, which is what holds the stage at 0.

Stage 3: Security of the Surveillance

This stage asks whether authorised access is accountable, not whether unauthorised access occurs.

Who may access, and what is recorded

Route	Provision	Entry required	Notice to the individual
The enterprise’s attorney	s.18(1)	No	No
Director of Criminal and Penal Prosecutions	s.18(2)	No	No
Police and bodies for prevention, detection or repression of offences	s.18(3)	No	No
Communication required by an Act or collective agreement	s.18(4)	No	No
A public body exercising its functions	s.18(5)	No	No

Route	Provision	Entry required	Notice to the individual
A person with power to compel	s.18(6)	Yes	No
Urgency threatening life, health or safety	s.18(7)	No	No
Study, research or statistics	s.18(8)	Yes	No
Debt recovery on behalf of others	s.18(9)	Yes	No
Recovery of the enterprise's own claim	s.18(9.1)	Yes	No

Finding. Section 18, second paragraph: “A person carrying on an enterprise must make an entry of every communication made under subparagraphs 6 to 9.1 of the first paragraph.” The Act therefore does require a log of some non-consensual disclosures, which is more than Bill C-36 requires and more than the Framework requires of its providers.

The gap is which ones. Subparagraphs 2, 3 and 5 are the state routes: the prosecution service, the police, and public bodies. They sit outside the entry requirement. The disclosures with the greatest consequence for an individual are the ones the Act does not require to be written down.

Where the entry goes. The entry is made by the enterprise and held by the enterprise. Nothing requires it to be lodged with a party that is not the discloser, nothing requires it to be shown to the individual, and nothing sets a threshold, a time bound or an approval for the access it records. Whether the section 27 access right reaches the entry is not stated in the Act and is recorded in Unresolved.

Against the assurance ladder. Level 4 requires access that is credentialed at the point of request, logged to a party that is not the requester, actively approved rather than standing, and bounded in time and scope. Section 18 satisfies none of the four for the state routes and one of the four, partially, for the commercial routes.

Incident disclosure is the exception that proves the point. Section 3.5 requires the Commission and the affected individuals to be notified promptly where a confidentiality incident presents a risk of serious injury, and gives the Commission power to order notification where it is not given. Quebec will compel an enterprise to tell an individual that their information escaped. It will not require the enterprise to tell them that it was handed over.

Stage rating: -1, present but obstructed. Measured for rights access, an entry requirement exists and reaches the commercial routes, which lifts this above the non-

operable rating recorded for both comparators. It excludes the state routes, is held by the discloser, and carries no notice to the individual, so what is present is obstructed.

Stage 4: Privacy Risk

The residual, recorded rather than resolved.

Risk	Provision	Severity
Notice given with no record, so compliance and non-compliance are indistinguishable afterwards	ss.8, 8.1, 14	High
Policy amendable with no retained version history	s.8.2	High
State disclosure without entry or notice	s.18(2), (3), (5)	High
Browser cookies exempt from confidentiality by default	s.9.1, second paragraph	High
Transfer assessment conducted and held by the transferring enterprise	s.17	Medium
Portability excludes inferred information	s.27, third paragraph	Medium
Person in charge without qualification, independence or dismissal protection	s.3.1	Medium
Consent deemed from the act of providing information	s.8.3	Medium

Enforcement, and the position it creates

Quebec's enforcement is the strongest assessed. Section 90.12 sets the maximum monetary administrative penalty at "\$50,000 in the case of a natural person and, in all other cases, \$10,000,000 or, if greater, the amount corresponding to 2% of worldwide turnover for the preceding fiscal year". The penal offence reaches "\$15,000 to \$25,000,000, or, if greater, the amount corresponding to 4% of worldwide turnover". The Commission may inquire on its own initiative or on an anonymous complaint (s.81), may demand information from any person "whether subject to this Act or not" (s.81.3), and may order protective measures on an incident (s.81.4). Reprisals against complainants are forbidden and presumed from adverse employment measures (ss.81.1, 81.2).

And section 93.1 gives the individual a direct route: “the court shall award punitive damages of not less than \$1,000”. Not a discretion, a floor.

The residual risk is therefore not weak law. It is a strong right with no evidence behind it. An individual who believes they were not told what section 8 requires, or that their consent did not meet section 14, must prove a negative about a conversation that left no artefact. The enterprise holds its own policies, its own impact assessments and its own section 18 entries. The individual holds a cause of action and a statutory minimum award.

Stage rating: -1, present but obstructed. The rights, the remedy and the penalties are present and are the strongest in the comparison. They are obstructed by the absence of any artefact with which to exercise them.

Consent Validity Analysis

Requirement	Law 25	Recorded?
Clear, free and informed	s.14	No
Specific to each purpose	s.14	No
Requested separately in writing	s.14	No
Time limited to the purpose	s.14	No
Express for sensitive information	s.12, first paragraph	No
Withdrawable	s.8(4)	No
Void if non-compliant	s.14, fourth paragraph	Not applicable

Consent under Law 25 is valid in law and unprovable in practice. Section 14’s closing sentence makes non-compliant consent “without effect”, which is a strong sanction attached to a fact nobody is required to record. The sanction is real and the trigger is unevicenced.

The Opening

Quebec has already built the two things that are hardest to legislate, and neither comparator has either.

1. **A published accountable identity, before identification** (s.3.1). This is the Kantara Data Controller Identity Record’s core content, required by statute and already in place across the Quebec private sector.
2. **A notice bound to the collection event** (ss.8, 8.1). This is the trigger a notice record needs, and it exists.

What is missing is the artefact. ISO/IEC TS 27560:2023 specifies an information structure for a record of a notice and consent event. Applied to section 8, it would produce a record referencing a version of the section 8.2 policy, carrying the section 3.1 contact, timestamped at the collection event, and given to the individual as a receipt. Nothing in Law 25 forbids it. Section 3.3's requirement that a project allow information to be communicated "in a structured, commonly used technological format" already contemplates machine-readable output.

Two routes exist without amending the Act. A government regulation under section 3.5 already determines the content and terms of incident notices, which establishes the pattern of prescribing notice content by regulation. And the Commission's guidance and order powers reach the practices of an enterprise directly.

The one thing that would change the position most is also the smallest: require the section 8 disclosure to carry a version reference and be issued to the person as a record. Everything else in Quebec's architecture is already there.

Impact Analysis

Burden on enterprises. Law 25 asks for a published contact, published governance practices, a published policy, privacy impact assessments for systems projects and for every transfer outside Québec, incident procedures and a register, and confidentiality by default. These are real obligations, and they are proportionate by the Act's own terms at sections 3.2 and 3.3. The marginal cost of adding a record to the notice already required is small next to the assessments already mandated.

Burden on individuals. The individual is asked to read a policy, recognise that profiling technology is in use, and bring an action if wronged. Quebec asks less of the individual than any comparator and still requires them to carry the evidential burden alone.

Cross-border position. Section 17 assesses the receiving State's legal framework before a transfer, which is the structure Convention 108+ Article 14 contemplates and which Bill C-36 does not have. The assessment is held by the transferring enterprise and published to no one, so a counterparty, a regulator in the receiving State, or the individual cannot see what was concluded. Quebec does the analysis that supports transborder cooperation and keeps the result private.

Recommendations

To the Government of Québec, by regulation where possible:

1. Section 8: require the disclosure to reference the version of the confidentiality policy in force at the moment of collection, and to be issued to the person concerned as a record they retain.
2. Section 8.2: require superseded versions of the confidentiality policy to remain retrievable, each carrying a publication time and an integrity value.
3. Section 18, second paragraph: extend the entry requirement to subparagraphs 2, 3 and 5, and require the entry to be disclosable to the person concerned where lawful and after any investigative constraint lapses.
4. Section 9.1: remove the browser cookie exemption, or bound it to a stated and time limited technical justification.
5. Section 17: require the conclusion of the transfer assessment, not the assessment itself, to be stated in the section 8 disclosure, naming the State and the instrument relied on.
6. Section 3.1: add qualification, independence and dismissal protection for the person in charge, so that the published contact carries a protected role behind it.
7. Section 27: state whether the access right reaches the section 18 entries.

To the Commission d'accès à l'information:

8. Treat the absence of any record of a section 8 disclosure as a matter going to compliance with section 8 itself, since a duty that leaves no trace cannot be supervised.
9. Specify the record structure against ISO/IEC TS 27560:2023 so that a Quebec notice record is interoperable rather than a provincial format.

To standards bodies and implementers:

10. Section 3.1 is the closest thing in North American law to a mandatory published controller identity. Treat it as the entry point for a controller identity record profile that can be met by a statute already in force.

Methodology

The official English consolidated text of chapter P-39.1, current to 10 June 2026, was retrieved from the Éditeur officiel du Québec and read in full. Term counts were taken across the whole text. Each stage was rated on the ordinal ANCR TPI scale after the preceding stage was answered, in the order the method requires. Comparisons to Bill C-36 and to China's AI Safety Governance Framework 3.0 are drawn from the companion WHiSSPR reports of 21 and 23 September 2026, which were produced on the same method.

No composite score is given and none should be inferred.

Unresolved

Item	Status
Whether the French text differs in legal effect at the clauses cited, starting with sections 3.1, 8.1 and 18	Not checked. Both versions are official
Whether the section 27 access right reaches the entries required by section 18, second paragraph	Not stated in the Act. No decision of the Commission on the point was sought for this report
Whether any regulation made under section 3.5 prescribes notice content beyond incidents	Not checked
Decisions of the Commission applying sections 8, 14 or 18 since 22 September 2023	Not surveyed. This report assesses the statute, not its application
The Act respecting Access to documents held by public bodies, chapter A-2.1, as amended by the same Law 25	Outside scope. This report assesses the private sector Act only
Convention 108 Parties and Convention 108+ ratifications	Checked. Council of Europe Treaty Office, 23 September 2026: ETS 108 shows 55 ratifications or accessions and no signature outstanding; CETS 223 shows 34 ratifications and 12 signatures not followed by ratification, against the 38 required

Assessment Framework Version: WHiSSPR v2.0 (2026)