



Internal Affairs
Te Tari Taiwhenua

DRAFT

Testing and Monitoring Requirements

Online Casino Gambling Technology

DISCUSSION DRAFT v1.0 September 2026

Contents

Contents	2
Introduction	3
Approved Independent Testing Laboratories	4
Market Entry Testing Requirements	5
Licence Application	5
Licensed (Day One)	6
Ongoing Testing Requirements	7
Internal Testing Requirements	7
Development Process	7
Testing Process	8
Release Process	8
External Testing Requirements	9
Random Number Generators	9
Games	11
Live Dealer Operations	12
Gambling Platform	13
Periodic Testing Requirements	13
Game Testing and Platform Certification	13
Information Security	14
Ongoing Monitoring Requirements	16
Live RTP Monitoring	16
System Monitoring and Reporting	16

Introduction

The purpose of this document is to specify the requirements for operators to test and monitor online casino gambling technology under section 80 of the **Online Casino Gambling Act 2026** (the Act).

Section 80 empowers the Secretary to require operators to monitor and test online casino gambling technology and specify how this is done, including the type and frequency of monitoring and testing, who must conduct that monitoring and testing, and the certification and documentation that must be provided to the Secretary.

This document should be read in conjunction with the **Online Casino Gambling Regulations 2026** (the Regulations) and the **Online Casino Gambling Minimum Standards 2026** (Minimum Standards).

While we expect operators to ensure they are always compliant with their legislative obligations, these testing requirements set out how operators are able to provide compliance assurance to the Secretary at licensing and on an ongoing and periodic basis. In developing these requirements, the Secretary has taken a risk-based approach taking into account:

- the likelihood of non-compliance occurring;
- the impact of non-compliance; and
- the means available to assess compliance and the burden imposed by the approach.

The requirements specified in this document apply to all operators, from **[DATE]**.

Approved Independent Testing Laboratories

1. The following Independent Test Laboratories (ITLs) are approved under section 80(11)(b) to conduct the external monitoring and testing specified in these testing and monitoring requirements:
 - 1.1 Test Houses approved by the [UK Gambling Commission](#)
 - 1.2 Independent Testing Labs registered with the [Alcohol and Gaming Commission of Ontario](#)
 - 1.3 Accredited Test Facilities who provide testing service for land-based gambling in New Zealand being:
 - 1.3.1 Gaming Labs International Australia
 - 1.3.2 Quality Assurance Laboratories PTY Ltd
 - 1.3.3 BMM Australia PTY Ltd

Market Entry Testing Requirements

Licence Application

2. A person who is notified under section 16(4) of the Act that they may apply for a licence to conduct online casino gambling in New Zealand (a licence) must satisfy the Secretary that they are, amongst other requirements, willing and able to comply with the duties and requirements under the Act¹.
3. To assist the Secretary in making this determination, an applicant must provide the Secretary with a Game and Random Number Generator (RNG) Register **[a template Game and RNG register is currently under development]**.
4. The Game and RNG register must confirm that every game (including live dealer games) and RNG the applicant intends to offer has been tested by an approved ITL and found to comply with one (or more) of the following:
 - 4.1 the applicable Regulations and Minimum Standards in accordance with the Ongoing Testing Requirements; or
 - 4.2 the [Alcohol and Gaming Commission of Ontario's Standards for Internet Gaming](#); or
 - 4.3 the [UK Gambling Commission's Remote Gambling and Software Technical Standards](#).
5. In addition, an applicant must also provide a list of critical technology² providers they intend to use (this will align with what is stated in the Game and RNG Register), along with a brief summary of the products and services they are providing, and the production data centre and cloud hosting locations for each. Applicants should sight and retain evidence of each provider's ISO/IEC 27001 certificate, statements of applicability, or equivalent independent assurance for their production data centres and cloud hosting.
6. If an applicant operates in another jurisdiction that requires a [third-party annual security audit](#), or equivalent security assurance, the applicant must also provide the most recent audit report or evidence of that assurance.

¹ Section 19(1)(b) Online Casino Gambling Act 2026

² Critical technology includes games, random number generators, and components of the gambling platform that accept, process, determine the outcome of, display, and log details about customers bets.



Licensed (Day One)

7. In response to being granted a licence, an operator must provide the Secretary with:
 - 7.1 an updated Game and RNG Register; and
 - 7.2 a letter signed by the Operator's Chief Executive Officer (or equivalent) and Chief Compliance Officer (or equivalent) confirming that all Online Casino Gambling Technology (OCGT) complies with all applicable Regulations and Minimum Standards.
8. The letter must expressly confirm compliance of the gambling platform and all supporting technology, including underlying infrastructure, network devices, operating systems, databases, gaming software, and other applications. The confirmation must also cover any OCGT provided by third parties.
9. These documents must also confirm that every game (including live dealer games) and RNG made available and operational on the gambling platform on the licence start date has been tested by an approved ITL and found to comply with one (or more) of the following:
 - 9.1 the applicable Regulations and Minimum Standards in accordance with the Ongoing Testing Requirements; or
 - 9.2 the [Alcohol and Gaming Commission of Ontario's Standards for Internet Gaming](#); or
 - 9.3 the [UK Gambling Commission's Remote Gambling and Software Technical Standards](#).
10. A game or RNG made available and operational on the gambling platform on the licence start date is not required to undergo further external testing against the applicable Regulations and Minimum Standards in accordance with the Ongoing Testing Requirements if it has been externally tested by an approved ITL, and found to comply with one of the following standards before a licence is granted:
 - 10.1 the [Alcohol and Gaming Commission of Ontario's Standards for Internet Gaming](#); or
 - 10.2 the [UK Gambling Commission's Remote Gambling and Software Technical Standards](#).
11. Any new game or RNG introduced after the licence start date, or any update to an existing game or RNG that affects, or may affect, the fairness of the game or RNG, must be externally tested in accordance with the Ongoing Testing Requirements to verify compliance with all applicable Regulations and Minimum Standards.

Ongoing Testing Requirements

12. All OCGT must be tested to ensure it complies with all applicable Regulations and Minimum Standards.
13. Where compliance can be readily observed through use of the operator's gambling platform, or where a change does not impact game fairness (**minor change**), an operator may only need to undertake internal testing to confirm compliance, provided the operator complies with the Internal Testing Requirements.
14. Where an update affects, or may affect, the fairness of a game or RNG (**major change**), the operator must ensure that the game or RNG is re-tested by an approved ITL in accordance with the External Testing Requirements.
15. Operators must ensure that all **new** games and RNGs are adequately tested by an approved ITL in accordance with the External Testing Requirements.
16. To ensure compliance with the above requirements (paragraphs 13-**Error! Reference source not found.**), an operator must ensure that, as part of Game Testing and Platform CertificationGame Testing and Platform Certification, an approved ITL reviews the operator's internal development, testing, and release control processes for games released and changes undertaken during the relevant certification period.
17. The operator must also receive confirmation from an ITL that the operator has correctly categorised each relevant change as major or minor, and whether the operator has complied with the applicable **Error! Reference source not found.** and **Error! Reference source not found.** requirements.
18. Where OCGT is supplied by a third party, the operator remains responsible for ensuring that the technology complies with all applicable Regulations and Minimum Standards, and that it has been tested in accordance with these testing requirements.

Internal Testing Requirements

19. Internal testing of OCGT is permitted only where the operator complies with the following best practice guidelines governing the development, testing, and release control of OCGT.
20. Operators certified to ISO/IEC 27001 are likely to have information security management processes and procedures that support compliance with these best practice guidelines. However, certification does not remove the requirement to demonstrate compliance with these guidelines as part of Game Testing and Platform Certification.
21. Where an operator does not comply with these guidelines the OCGT must be tested by an approved ITL.

Development Process

22. **Source Code Security:** Source code must be maintained in a secure, access-controlled environment with an auditable log of all access to prevent unauthorised manipulation and maintain code integrity.
23. **Version Control:** Older versions of source code, including retirement dates, must be retained to ensure a full audit trail and rollback capability in case of system failure or compliance investigation.
24. **Access Control:** Access for developers must be strictly controlled based on the principle of minimum privilege, granting only the access necessary for the specific role.
25. **Documentation:** Source code must be accompanied by comprehensive technical documentation suitable for independent review and future maintenance.
26. **Code Quality:** Source files need sufficient commenting, legibility, and structure to permit static code analysis and confident functional review by external parties.
27. **Segregation of Duties:** Write access to the core platform source code must be restricted from personnel focused only on game-specific development to prevent unauthorised modification of critical systems.
28. **Peer Review:** Changes to critical modules must be peer-reviewed by suitably skilled, independent developers to ensure alignment with documentation and quality standards before being merged.

Testing Process

29. **Environment Separation:** Development, testing, and production environments must be logically and physically segregated to prevent development bugs or unauthorised code from accidentally entering the live system.
30. **Personnel Separation:** Testing should be performed by separate staff to those who developed the product to ensure an impartial and objective assessment of the product's functionality and compliance.
31. **Independent Assessment:** An independent assessment of changes must be performed using tools (such as file comparison utilities or equivalent) to verify that only documented and approved changes were made to the code base.

Release Process

32. **Change Management Plan:** The migration of any new OCGT, or any change to existing technology, into the operational environment must be supported by a documented change management plan. The plan must ensure that appropriate testing, change control mechanisms, approvals, and authorisations are in place. The change management plan must be managed by a person with the necessary proficiency and expertise to oversee the change and make decisions.
33. **Change Management Documentation:** The following must be recorded in the change management documentation:
 - 33.1 unique change ID

- 33.2 game number/RNG identifier
 - 33.3 delivery channel(s)
 - 33.4 description of change
 - 33.5 justification for major or minor change classification
 - 33.6 for minor changes: confirmation they have been internally tested and the changes documented
 - 33.7 for major changes: confirmation of adequate ITL certification
 - 33.8 relevant manager / change board authorisation for change
 - 33.9 other particulars as required by the licence holder's internal change management requirements.
34. **Emergency Changes:** Emergency fixes and patches may be deployed immediately to address critical security or integrity failures (e.g., a zero-day exploit or severe bug causing over or underpayment). However, where this change is considered major it must be followed by formal certification by an ITL within 60 days to verify the change did not introduce new issues.

External Testing Requirements

35. In addition to any internal testing, the following OCGT must be externally tested and certified by an approved ITL against the applicable Regulations and Minimum Standards before release into the operational environment and whenever a major change occurs:
- 35.1 Random Number Generators;
 - 35.2 Games;
 - 35.3 Live Dealer Operations; and
 - 35.4 Underlying systems that support the gambling platform.
36. Recognising that OCGT may have previously been tested by an approved ITL for use in another regulated jurisdiction, the ITL may take that prior testing into account when determining the additional testing that may be required to certify whether the OCGT complies with the Regulations and Minimum Standards.
37. Any prior testing relied on must be relevant to the applicable Regulations and Minimum Standards and provide sufficient assurance for determining compliance with these testing requirements.

Random Number Generators

38. An operator must ensure that every RNG used in connection with its gambling platform is tested against **Minimum Standard 14** by an approved ITL before release into the operational environment and after any major change.

39. An operator must not use an RNG in the operational environment unless the operator holds current certification from an approved ITL confirming that the RNG complies with Minimum Standard 14.
40. Before relying on certification that an RNG complies with Minimum Standard 14 an operator must ensure that the approved ITL has:
 - 40.1 reviewed the RNG's design documentation to understand its intended implementation and functional specifications within the gambling platform.
 - 40.2 researched the specific RNG algorithm or hardware being used to determine whether there are any publicly known weaknesses or vulnerabilities that could be exploited to manipulate outcomes.
 - 40.3 reviewed the source code to verify that the RNG has been implemented in accordance with the RNG documentation, and that there are no unauthorised or accidental deviations.
 - 40.4 performed advanced statistical testing on both the raw RNG output and the final scaled or mapped data to assess randomness, independence, uniformity, and unpredictability.
 - 40.5 conducted testing using recognised statistical test standards, such as the DIEHARD test suite, the National Institute of Standards and Technology (NIST) test suite, or an equivalent test suite that provides a comparable level of rigour.
 - 40.6 used datasets of sufficient size and quality to ensure statistically valid and reliable results.

Documentation:

41. An RNG test report must contain sufficient detail to demonstrate the testing performed and the results obtained, including the software version tested, testing methodology, test dates, and any limitations, assumptions, or conditions relevant to the certified use of the RNG (for example, acceptable degrees of freedom). The test report is not required to be provided to the Secretary unless requested but must be retained by the operator for seven years and made available on request.
42. The following information must also be recorded in the operator's Game and RNG Register:
 - 42.1 RNG name or description and unique reference;
 - 42.2 RNG type, including whether it is hardware, software, or a combination of both
 - 42.3 developer name and, where different, supplier name;
 - 42.4 version number tested;
 - 42.5 intended use of the RNG;
 - 42.6 name of the ITL that conducted the testing;
 - 42.7 date of testing;

- 42.8 date from which the RNG became, or is intended to become, active;
 - 42.9 test report or certificate reference;
 - 42.10 digital signature or other unique software identifier, where applicable;
 - 42.11 any limitations or conditions relating to the certified use of the RNG; and
 - 42.12 jurisdiction(s) for which the testing was conducted and the testing requirements or standards applied.
43. The operator must provide the Game and RNG Register to the Secretary every three months, at the same time as the quarterly report required under regulation 33 of the Regulations.

Games

44. Games must be tested against the following Regulations and Minimum Standards by an approved ITL before release into the operational environment and after any major changes that affects, or may affect, the fairness of a game:
- 44.1 Game Design and Features: **Regulation 14** and **Minimum Standard 10**.
 - 44.2 Informed Decision Making: **Regulation 22** and **Minimum Standard 13**.
 - 44.3 Jackpot Systems (if applicable): **Minimum Standard 9**.
 - 44.4 Peer-peer games (if applicable): **Minimum Standard 16**.
45. Because each game may differ in functionality, configuration, and integration, the requirements above indicate the Regulations and Minimum Standards likely to be relevant to external testing. The applicable scope must be determined on a case-by-case basis, following a substantive review of the game.
46. Before relying on certification that a game complies with the applicable Regulations and Minimum Standards an operator must ensure that the approved ITL has:
- 46.1 reviewed the game design and mathematical model to confirm that they are accurate, internally consistent, and reflected in the game rules and customer-facing information.
 - 46.2 confirmed that the theoretical Return to Player (RTP) has been correctly calculated and is consistent with the game rules and prize tables.
 - 46.3 confirmed, through a statistically significant volume of simulated or actual game play, that the observed RTP is consistent with the expected RTP and within the tolerance permitted by the game's volatility.
 - 46.4 reviewed the software and source code to verify that the game design, mathematical model, game rules, prize tables, RTP, and game features have been accurately implemented.
 - 46.5 tested that all advertised prizes and game features occur as expected, including through emulation testing where game outcomes are forced, and manual play testing where appropriate.

Documentation:

47. A game test report must contain sufficient detail to demonstrate the testing performed and the results obtained, including, but not limited to, the digital signature, the software version number, the RTP value(s). The test report is not required to be provided to the Secretary unless requested but must be retained by the operator for seven years and made available on request.
48. The following information must also be recorded in the operator's Game and RNG Register:
 - 48.1 game name and unique identifier;
 - 48.2 game type and generation;
 - 48.3 developer name and, where different, supplier name;
 - 48.4 software version tested;
 - 48.5 details of any game or game version that the game supersedes, where applicable;
 - 48.6 RTP value or range;
 - 48.7 name of the ITL that conducted the testing;
 - 48.8 date of testing;
 - 48.9 date from which the game became, or is intended to become, active;
 - 48.10 test report or certificate reference;
 - 48.11 where applicable, any feature that would need to be turned off or its setting adjusted for the game to be compliant with the applicable standard;
 - 48.12 digital signature or other unique software identifier;
 - 48.13 gambling platform channel or channels covered by the testing; and
 - 48.14 jurisdiction for which the testing was conducted and the testing requirements or standards applied.

Live Dealer Operations

49. Live dealer operations must be tested against **Minimum Standard 15** by an appropriately qualified and independent body, such as a regulator or an approved ITL. The testing must be conducted by inspection before the live dealer operations are made available through the operator's gambling platform and at least once every 12 months thereafter.
50. If live dealer operations have been inspected for international regulatory purposes by an appropriately qualified and independent body within the previous 12 months, a separate inspection is not required, provided the previous inspection included sufficient testing to demonstrate compliance with Minimum Standard 15.

Documentation:

51. Inspection reports are not required to be provided to the Secretary unless requested. However, the operator must retain each inspection report and make it available to the Secretary on request.
52. The following information must also be recorded in the operator's Game and RNG Register:
 - 52.1 details of each game offered through the live dealer operations; and
 - 52.2 the date of the most recent inspection of the live dealer operations.

Gambling Platform

53. Integration testing is required following any update to the underlying systems that support the gambling platform, such as a game server or operating system, where the update may affect the fairness of a significant number of games available through the gambling platform.
54. The integration testing must include the retesting of a representative sample of affected games. The sample must be sufficiently broad to include each game type and generation and must not be restricted to games with similar characteristics.

Periodic Testing Requirements

Game Testing and Platform Certification

55. Six months after being granted a licence, an operator must obtain a Game Testing and Platform Certification from an approved ITL. This certification independently validates that:
 - 55.1 the operator's market-entry confirmation was supported by appropriate evidence;
 - 55.2 a representative sample of prior testing met the market-entry requirements;
 - 55.3 ongoing testing, monitoring, and release controls are operating effectively following launch; and
 - 55.4 systems and functions not subject to external testing requirements, including player account management, payments, player wallets, and responsible gaming controls, are integrated, secure and operating as required.
56. Before relying on a Game Testing and Platform Certification issued by an approved ITL, an operator must ensure that the ITL has:
 - 56.1 reviewed a sample of market entry games, RNGs, and associated test reports to confirm that evidence of prior ITL testing exists and that it meets these testing requirements.
 - 56.2 reviewed the operator's internal development, testing, and release control processes for games released, and changes undertaken, since the

licence was granted or previous certification, to confirm whether the operator has complied with the applicable Internal Testing and External Testing requirements set out in this document, and correctly classified each relevant change.

- 56.3 confirmed that live Return to Player (RTP) monitoring is in place and implemented in accordance with these testing requirements.
 - 56.4 validated the full list of operational games is included in the Game and RNG Register.
 - 56.5 reviewed wider platform functionality that is not subject to external ITL testing required on 'Day One' under these testing requirements to ensure it is integrated and operating as intended, including, but not limited to:
 - 56.5.1 limit setting;
 - 56.5.2 breaks in play, time-outs and pop-up alerts;
 - 56.5.3 self-exclusion;
 - 56.5.4 customer support availability;
 - 56.5.5 identity and age verification;
 - 56.5.6 customer location;
 - 56.5.7 display of information and game rules to customers.
 - 56.6 confirmed compliance with the applicable incident/event notification requirements.
 - 56.7 completed the Game Testing and Platform Certification Template **[under development]**
- 57. Where any non-compliance has been identified and subsequently corrected, the details must be recorded in the Game Testing and Platform Certification Template to ensure transparency.
 - 58. Following the initial Game Testing and Platform Certification, the operator must obtain Game Testing and Platform Certification on a periodic basis.
 - 59. Unless otherwise specified by the Secretary, each periodic certification must be obtained within 12 months after the previous certification.
 - 60. The Secretary may specify a different frequency or scope of certification for an operator, including the size or composition of any sample to be reviewed, having regard to the level of compliance identified during the previous certification.
 - 61. The operator must provide the completed template to the Secretary within 20 working days after the date by which the periodic certification was required to be obtained.

Information Security

Quarterly Vulnerability Scans and Annual Penetration Testing

- 62. Operators must undertake quarterly vulnerability scans and annual penetration testing of all critical OCGT, including:

- 62.1 electronic systems that record, store, process, share, transmit or retrieve sensitive customer information, for example, debit card details, authentication information, customer account balances
 - 62.2 electronic systems that generate, transmit, or process random numbers used to determine the outcome of games or virtual events
 - 62.3 electronic systems that store results or the current state of a customer's gamble
 - 62.4 points of entry to and exit from the above systems (other systems that can communicate directly with core critical systems)
 - 62.5 communication networks that transmit sensitive customer information.
63. Vulnerability scans may be undertaken by the operator or an independent and suitably qualified person. Annual penetration testing must be undertaken by an independent and suitably qualified person.
64. If vulnerability scans are undertaken by the operator, the operator must ensure that the independent specialist conducting the annual penetration testing reviews the scope, methodology, results, and remediation of those scans and confirm whether they were adequately performed.

Annual Security Review

65. Operators must undergo an annual security review conducted by an independent and suitably qualified person to confirm compliance with **Minimum Standard 17**. The first annual security review must occur within six months of being granted a licence.
66. An operator that holds current ISO/IEC 27001:2022 certification is not required to undergo a full annual security review, provided the scope of the certification covers all the operator's OCGT.
67. An independent and suitably qualified person must review the scope of the certification and the Statement of Applicability to confirm that:
- 67.1 all the operator's online casino gambling technology is within the scope of the certification; and
 - 67.2 all controls specified in **Minimum Standard 17** are included in the Statement of Applicability.
68. If any online casino gambling technology is outside the scope of the certification, or any control specified in Minimum Standard 17 is not included in the Statement of Applicability, those matters must be separately assessed as part of the annual security review.

Documentation:

69. Unless significant non-compliance is identified, the operator is not required to provide the annual security review report to the Secretary. However, the operator must retain the report for seven years and make it available to the Secretary on request.
70. If significant non-compliance is identified, the operator must provide the report to the Secretary within seven days.

Ongoing Monitoring Requirements

Live RTP Monitoring

71. Operators must ensure that the actual RTP of each relevant game is monitored against its theoretical RTP on an ongoing basis.
72. Monitoring must be sufficiently granular to identify discrepancies that may not be apparent from aggregated results. It must measure performance both in aggregate and, where applicable, by primary stake level, gambling platform channel, base game, and distinct game feature, including bonus features, progressive jackpots, skill components, and gamble options.
73. The methodology and allowable RTP tolerance for each game must take account of the game's volatility and volume of play. For a game or product for which a single theoretical RTP does not apply, the operator must monitor relevant performance measures, including hit rates and outcome distributions, against the designed probabilities and published odds.
74. Live RTP monitoring may be undertaken by a game supplier or another person that holds the necessary game transaction data. Where monitoring is undertaken by another person, the operator must ensure that it receives the monitoring results and is promptly notified of any material discrepancy identified.
75. Any material discrepancy identified through live RTP monitoring must be reported in accordance with the applicable incident and event notification requirements outlined in System Monitoring and Reporting.

Documentation:

76. The operator must retain records that demonstrate the monitoring performed, including the methodology and tolerances used, the monitoring period and game data covered, the results obtained, and any material discrepancies identified.
77. These records are not required to be provided to the Secretary unless requested but must be retained by the operator and made available to the Secretary on request.

System Monitoring and Reporting

78. Operators must continuously monitor OCGT for events that may affect its security, integrity, availability, or correct operation, or the fairness of online casino gambling.
79. The monitoring must be sufficient to identify and promptly flag the following types of events, where relevant:
 - 79.1 failures of identity or age verification technology;
 - 79.2 failures of technology used to implement self-exclusion, limits, breaks in play, time-outs, alerts, or other harm-minimisation controls;

- 79.3 unplanned outages affecting access to the gambling platform, games, customer accounts, or transactions;
- 79.4 payment processing errors or failures;
- 79.5 errors or malfunctions affecting RNGs, game logic, game outcomes, RTP, jackpots, or the calculation or payment of winnings;
- 79.6 unauthorised access to, or the disclosure, alteration, loss, or destruction of, customer or financial information;
- 79.7 compromises of customer accounts;
- 79.8 attacks on the gambling platform or supporting systems, including credential-stuffing, bot, or denial-of-service attacks;
- 79.9 the release or operation of a game, RNG, or software version that has not undergone the testing required by these testing requirements;
- 79.10 failures of systems operated by a supplier that materially affect the gambling platform or other online casino gambling technology; and
- 79.11 any other event that may materially affect the security, integrity, availability, or correct operation of online casino gambling technology, or the fairness of online casino gambling.

Documentation:

- 80. In addition to notifying the Secretary of any serious incident under regulation 35 of the Regulations, the operator must notify the Secretary of any other event identified through monitoring that has had, or could reasonably be expected to have, a material adverse effect on the security, integrity, availability, or correct operation of online casino gambling technology, or the fairness of online casino gambling.
- 81. The notification must include:
 - 81.1 the date and time of the event;
 - 81.2 how and when the event was identified;
 - 81.3 the online casino gambling technology affected;
 - 81.4 the known or estimated effect of the event; and
 - 81.5 any other information reasonably necessary to explain the nature and effect of the event.
- 82. The operator must provide the notification as soon as possible and no later than five working days after becoming aware of the event.
- 83. If complete information is not available within five working days, the operator must provide an initial notification containing the information available at that time and the expected date of a further report. The operator must provide the further report as soon as the remaining information becomes available.

