Aona

NDB serious-harm and remedy exercise

Australian privacy officers, incident responders and security leaders

Read the complete guide on aona.ai

For information and an entity covered by the NDB scheme, assess whether unauthorised access, disclosure or loss is likely to cause serious harm and whether remedial action prevents that risk. Suspected eligible breaches need prompt assessment. The 30-calendar-day assessment rule is not permission to delay required notification.

Two fictional AI-submission scenarios separate evidence of disclosure from the serious-harm and remediation decision.

All people, events, risks and timeline entries are invented. No actual eligible-breach determination, provider response or notification has occurred.

Your review

Reviewer: _____ Date: _____

Organisation or team: _____

☐ **Establish disclosure and coverage**

Identify the actual information, entity, account, path and recipients before deciding applicability.

☐ **Evidence harm and mitigation**

Record why serious harm is likely or not, and what completed remedy actually prevented.

☐ **Separate the two timing duties**

Track suspicion/assessment and the later belief/notification decision without treating 30 days as a universal notice period.

Checked items record your review, not a compliance approval or an installed-product test result.

Notes and next actions

Decision and scope: _____

Evidence to collect: _____

Owner and next review date: _____

Review matrix

Decision point	Stipulated example facts	Illustrative outcome
Scenario A: disclosure	Sensitive personal details reached an uncontrolled external recipient.	Proceed to harm and remedy assessment; the application label alone is not the conclusion.

Decision point	Stipulated example facts	Illustrative outcome
Scenario A: likely harm	The exercise stipulates a credible threat assessed as making serious harm more probable than not.	Likely-serious-harm condition is assumed met for teaching, not inferred from a log alone.
Scenario A: remedy	No completed action prevents that stipulated risk.	Follow the eligible-breach notification path, subject to applicable exceptions.
Scenario B: blocked input	Reliable fictional evidence establishes no transmission and no other disclosure on the assessed path.	No breach is established from that blocked submission; document the evidence and remaining scope.
Unknown facts	Recipient access or remedy effectiveness remains unverified.	Assess promptly; take all reasonable steps within the applicable 30-calendar-day assessment period.
Conclusion reached	Reasonable grounds to believe an eligible breach exist in the scenario.	Notify as soon as practicable where required; do not wait for day 30.

Two different timing questions

- **Suspect:** Record the grounds and assess promptly
- **Assess:** Likely serious harm and remedial action
- **Believe eligible:** Apply notice duties as soon as practicable

The 30-day assessment rule is separate.

Fictional evidence timeline

Day 0: employee reports the suspected AI disclosure; incident owner records the grounds for suspicion.
Day 1: team secures the payload/account facts and requests recipient information.
Day 2: the exercise stipulates evidence of uncontrolled disclosure and likely serious harm; effective remediation is not established.
Day 2 onward: the authorised owner follows the eligible-breach notice path as soon as practicable, subject to the actual rules and exceptions.
Day 30: not a permission to wait; the separate assessment requirement concerns all reasonable steps to complete a suspected-breach assessment.

No real notice is drafted or sent by this fixture. Apply the actual entity, information and evidence before making a real decision.

Ndb fictional evidence timeline

Stage	Fictional event	Meaning
Day 0	Grounds for suspicion recorded	Start prompt assessment
Day 1	Payload and recipient facts sought	Evidence gathering
Day 2	Likely serious harm and ineffective remedy stipulated	Illustrative eligible-breach path

Stage	Fictional event	Meaning
After conclusion	Notice owner acts as soon as practicable if required	Do not wait for day 30

Sources and scope

Sources checked 2026-09-21. Review the current requirements and your actual agreement before using this workbook for a real decision. General information, not professional approval or a completed control test. It does not determine NDB eligibility, prove every copy was removed or notify the OAIC and affected individuals.

OAIC: Quick reference guide for responding to data breaches. Serious-harm and remedial-action assessment, reasonable steps to complete suspected-breach assessment within 30 calendar days and notification as soon as practicable when required.

OAIC: When to report a data breach. Eligible data-breach conditions, likely serious harm and remedial action; not every disclosure is automatically notifiable.