MONTHLY DPO SUPPORT PACK · C7

Breach drill record

Fictional organisation, illustrative only, not a client case study. Quillmarrow Supplies Pte. Ltd. (fictional) is invented. All people are shown by role only.

Organisation	Quillmarrow Supplies Pte. Ltd. (fictional)
Document	C7 · Breach drill record
Version	1.0
Date	22 January 2027 (illustrative)
Prepared by	Alex Lew, reviewer and sign-off
Client approver (role)	Head of Operations (DPO)
Label	Fictional organisation, illustrative only, not a client case study

The scenario in this record was simulated and never happened. No notification or customer message was actually sent as part of the exercise.

1. Purpose and scope

The tabletop exercise tested Quillmarrow's breach management plan, B11 v1.0, from initial vendor notification through containment, assessment, a separate decision to notify, preparation of communications and evaluation of lessons.

The exercise followed **C.A.R.E.: Contain, Assess, Report, Evaluate**, as set out in the PDPC Guide on Managing and Notifying Data Breaches under the PDPA. It was conducted remotely on 21 January 2027 and lasted 90 minutes.

The exercise tested how participants would respond to a reported compromise of web-shop accounts. It did not test live systems or require a real incident response. The simulated assessment and decision below are recorded separately, as required by B11.

2. Participants and roles

Participant	Role in the exercise
Head of Operations (DPO)	Led the exercise response, opened the simulated incident record and led the assessment.
COO	Participated in the response and management discussion.
Head of Customer Service	Participated in discussion of customer information and communications.
IT Manager	Participated in the discussion of ShopCloud and containment.
Head of Marketing	Participated in the discussion of communications.
Managing Director (MD)	Joined for the simulated decision step with the DPO.
The reviewer	Facilitated and observed the exercise; made no decisions for Quillmarrow.

The times in the timeline are simulated scenario times, not the times at which actions occurred during the 90-minute exercise.

3. Scenario

On **Day 1 at 09:10**, Fictional ShopCloud (DV-02) tells Quillmarrow that a credential-stuffing attack has accessed **620 web-shop customer accounts**.

The account information comprises names, delivery addresses, phone numbers and order histories. Quillmarrow does not hold payment card data. Participants work from the information available in the scenario and identify what they would need to establish before completing the assessment.

The exercise considers containment with ShopCloud, the scale and potential harm, the notification decision and a possible customer message. The scenario is a test only; it is not a record of an actual attack or breach.

4. Timeline

Simulated time	What happened	Who	B11 step
Day 1, 09:10	ShopCloud reports that an attack accessed 620 customer accounts.	ShopCloud to Quillmarrow	Receive report
Day 1, 09:25	The incident record is opened.	DPO	Record and coordinate
Day 1, 10:00	Containment is agreed: ShopCloud forces password resets and blocks the attacking addresses.	DPO and ShopCloud	Contain
Day 1, 11:00	Assessment begins.	DPO	Assess
Day 2, 15:00	Assessment is completed: 620 individuals are affected; significant harm is considered unlikely on the data involved, subject to lawyer confirmation.	DPO	Assess
Day 2, 16:00	A separate decision is recorded: notify the PDPC on the basis of significant scale. A voluntary customer message with password advice is prepared.	MD and DPO	Decide and prepare to report
Day 3, 12:00	The simulated PDPC notification draft is ready.	Quillmarrow response team	Prepare to report
No later than Day 5	Simulated deadline for PDPC notification, calculated as 3 calendar days after the Day 2 assessment.	Quillmarrow	Report, if notifiable

The timeline records the intended exercise response. The draft and message were exercise materials; nothing was actually sent.

5. Assessment

The DPO completed the simulated assessment on **Day 2 at 15:00**. It recorded the facts and assessment separately from the subsequent notification decision.

Assessment point	Exercise finding
Event	ShopCloud reported a credential-stuffing attack involving web-shop accounts.
Data involved	Names, delivery addresses, phone numbers and order histories. Quillmarrow does not hold payment card data.
Scale	620 individuals; the scenario exceeds the significant-scale threshold of 500 or more individuals.
Harm	Significant harm was considered unlikely on the data involved. This view is to be confirmed with a Singapore-qualified lawyer.
Containment	ShopCloud was to force password resets and block the attacking addresses.

The rules used in the exercise are:

- A data breach is notifiable if it results in, or is likely to result in, significant harm to affected individuals, or is of a significant scale (affects 500 or more individuals).
- The organisation must assess whether a breach is notifiable in a reasonable and expeditious manner.
- If notifiable, notify the PDPC as soon as practicable and no later than 3 calendar days after assessing that the breach is notifiable.
- Where significant harm is likely, notify affected individuals as soon as practicable, on or after notifying the PDPC, subject to the exceptions in the Act.

- A data intermediary processing on Quillmarrow's behalf must notify Quillmarrow without undue delay after it has credible grounds to believe a breach occurred.
- Keep the assessment (facts, scale, harm) separate from the decision to notify (who decides, when, reasons).

The simulated harm view is not a legal conclusion. Quillmarrow should confirm the application of the rules to an actual incident with a Singapore-qualified lawyer.

6. Decision to notify

At **Day 2, 16:00**, the MD and DPO made and recorded the simulated decision separately from the assessment.

Decision point	Recorded exercise decision
PDPC	Notifiable on the basis of significant scale: 620 individuals were affected.
Timing	Notify the PDPC as soon as practicable and no later than **Day 5**, 3 calendar days after the assessment on Day 2.
Affected individuals	On the exercise's harm view, notification to individuals was not required on the harm test, subject to confirmation with a Singapore-qualified lawyer.
Voluntary message	A customer message with password advice was prepared voluntarily.
Draft notification	The simulated PDPC notification draft was ready on Day 3 at 12:00.

No PDPC notification or customer message was actually sent. The exercise does not establish what the decision would be in a real event; that would depend on its facts and Quillmarrow's assessment at the time.

7. What worked

The exercise followed the response from vendor report to containment, assessment and decision. The DPO opened a simulated incident record shortly after the report and led the assessment. Containment was discussed with ShopCloud, including password resets and blocking the attacking addresses.

Participants identified the number of affected individuals and used it in the separate decision to notify. The simulated notification draft was ready on Day 3, ahead of the Day 5 deadline. A voluntary customer message with password advice was also prepared.

The exercise exposed weaknesses in the existing plan and form before a real incident. Those findings are recorded below rather than treated as completed fixes.

8. What went wrong

1. **Calendar-day timing was initially wrong.** Participants first counted 3 working days rather than calendar days for the PDPC notification deadline. The correct exercise deadline was Day 5.
2. **ShopCloud's incident contact was not available.** Nobody had the contact to hand during the exercise, creating a potential delay in reaching the vendor.
3. **There was no named deputy decision-maker.** The MD was simulated as unreachable for two hours, and B11 v1.0 did not name a deputy.
4. **Assessment and decision were initially combined.** Participants first wrote the facts and the notification decision in one box. They need separate records so that the assessment, decision, timing and reasons can be followed.

9. Lessons and actions

The following actions are covered by **DA-14**, owned by the DPO and due **15 February 2027**. At 31 January 2027, DA-14 was **Open, on track**.

Lesson	Action	Owner	Due	Tracker ref
Count the notification period in calendar days.	Add a calendar-day reminder to the B11 v1.1 form.	DPO	15 February 2027	DA-14

Lesson	Action	Owner	Due	Tracker ref
The vendor’s incident contact must be accessible during a response.	Add the ShopCloud incident contact to B11 v1.1.	DPO	15 February 2027	DA-14
The plan needs a deputy if the MD is unavailable.	Include the COO as deputy decision-maker in B11 v1.1.	DPO	15 February 2027	DA-14
Assessment and decision need to be recorded separately.	Reinforce the separate assessment and decision records in B11 v1.1.	DPO	15 February 2027	DA-14

The MD approved B11 v1.1 on **12 February 2027**. This later approval does not alter the DA-14 status recorded at 31 January.

10. Sign-off

Record approved by: Head of Operations (DPO), 22 January 2027

Noted by: Managing Director, 12 February 2027

The next drill is planned for **July 2027**.

About this sample

Fictional organisation, illustrative only, not a client case study. Quillmarrow Supplies Pte. Ltd., its people, vendors, findings and dates are invented. Nothing in this document reports a client result.

I personally review and sign off every deliverable. You appoint your own DPO. I support them.

This is practical compliance support, not legal advice. For legal advice, use a Singapore-qualified lawyer.

What's not included

- Acting as, being named as or replacing your DPO.
- Legal advice, legal representation or submitting regulatory notifications on your behalf.
- Certification or a guarantee of compliance.
- An emergency hotline or a substitute for your own incident-response arrangements.
- Forensic investigation, penetration testing, security engineering or administering your systems.
- Holding your customer database or making changes to live systems.
- Rebuilding the whole PDPA programme, a new AI governance review or a major new project (these need a separate scope and quote).
- Healthcare-sector work or on-site delivery.

Questions about this sample: DM @alewyl1 on X, or ask for a free intro call (coffee chat).