DRI CANADA · YEAR OF EXERCISE DESIGN

THE GREAT CANADIAN DISASTER

Inject Four Debrief & Inject Five Briefing

A national tabletop exercise testing decision-making, coordination, and continuity under complex, cascading disruptions.

DRI CANADA Train. Prepare. Recover.

DRI CANADA'S YEAR OF EXERCISE DESIGN

May 12, 2026 · 9:00 AM EDT

Test your plans before reality does.

TODAY'S BRIEFING

Agenda

01

Inject Four Recap

Where Day 4 took us — a leak you could not authenticate, a voice that was no longer yours, and a payroll that failed

02

How Teams Responded

Seven submissions, six decisions, and every deadline set by someone else

03

Submission Highlights

Standout thinking from this round's participants

04

Leaderboard

Inject Four preliminary results, with overall standings to follow

05

How the Exercise Ends

Inject Five, the final inject — recovery, accountability and the after-action review

DRI CANADA Train. Prepare. Recover.

INJECT FOUR · MAY 4, 2026 · 6:00 AM EDT

Where Inject Four Left Us

The extortion deadline expired and a sample of data went public — part genuine, part fabricated, part other organizations' — with a second demand on a 24-hour fuse and individuals being named.

Deepfaked officials and counterfeit notices took over the information space, the Monday payment cycle failed, and the relief rotations planned in Inject 3 never arrived.

Then a vendor reported "high confidence" that the recovery environment was clean. Every team was asked to land six decisions on clocks it did not control.

Leak & second demand	unverifiable, mirrored, and naming individuals
Fabricated voices	deepfakes and counterfeit notices in your name
Payments & people	payroll missed; relief rotations did not arrive
The way back	vendor "high confidence"; failback undefined

CURRENT ASSESSMENT

The deferrals ended. Every team notified on credible risk, refused the second demand and declined to reconnect on a vendor's word — and each recorded a position, an authority and a cost. What those decisions cost is the subject of Inject 5.

DRI CANADA Train. Prepare. Recover.

INJECT FOUR

How the Scenario Landed

Seven submissions this round, from three of the participant groups.

Large Corps & Critical Infrastructure

No submission from this group this round. The scenario pressure: reconnect today on a vendor's word, with no failback and forensic help in a national queue.

Federal & Provincial Government

Three submissions. Notified OPC, TBS and the Manitoba Ombudsman on credible risk, set minimum crews, and treated a handful of specialists as the real single point of failure.

Small & Medium Enterprises

No submission from this group this round. The scenario pressure: no card rails, no cash float, and a leak naming customers.

Communities & Local Governments

One submission. Life safety, water and wastewater came first; staff were not disciplined for unsafe travel; and reconnection was limited to isolated testing with stop conditions.

Finance & Insurance

Three submissions. Regulators named and notified, emergency payments run under dual control, and explicit numeric gates set before any reconnection.

DRI CANADA Train. Prepare. Recover.

HOW SUBMISSIONS ARE REVIEWED

Judging Criteria

Decision-Making

Sound, timely choices made under uncertainty and incomplete information.

Continuity of Operations

Practical steps to sustain critical services and protect people.

Coordination

Internal and external communication, escalation, and partner engagement.

Resilience & Recovery

Forward-looking actions that strengthen recovery and reduce future risk.

DRI CANADA Train. Prepare. Recover.

TABLETOP EXERCISE · AFTER-ACTION HIGHLIGHTS

Inject Four: What the Teams Did

Teams faced a leak they could not authenticate, fabricated officials, a failed payroll and pressure to reconnect — here is what they decided, accepted, and learned.

7
submissions received

3
sector groups represented

48 hr
response window

Day 4
point in the scenario

THE SETUP

The scenario every team responded to

A leak you cannot authenticate

A sample release, mirrored faster than it can be taken down: some genuine, some fabricated, some belonging to others. A second demand, and individuals named in public.

A voice that is not yours

Synthetic audio and video of senior officials, counterfeit notices in your branding, and a credential-harvesting site posing as an exposure check.

The money stops

Payroll, benefits, claims, pensions and vendor payments all miss. Cash is scarce, staff are unpaid, and the relief rotations did not arrive.

“High confidence”

A vendor says the recovery environment is clean. Executives, officials and unions want reconnection today — and nobody can prove it, or say how to fail back.

DRI CANADA Train. Prepare. Recover.

1

HOW TEAMS RESPONDED — BY THE NUMBERS

Inject 4 · aggregate view across every submission

INJECT 4 RECAP

7	0	100%	Notify
submissions, across three sector groups	teams paid or negotiated the second demand	declined to reconnect on vendor confidence alone	the universal answer once scope could not be confirmed

Notification: every team replaced “confirmed scope” with credible risk of harm, named its regulator, and committed to say what it could not verify.

Payments: every team stood up manual emergency payments — dual authorization, call-back verification, caps and later reconciliation — with hardship cases first.

The pattern: the governance routes of Inject 3 became positions, with an authority, a time and an accepted cost. Six of seven teams put numbers on minimum crews.

TOP PRIORITIES

How priorities shifted on Day 4

1

Protect people & sustain the workforce

First on every list. Safe sites, pay, fatigue limits and minimum crews came before systems — several teams called the workforce the constraint on everything else.

2

Keep a voice people can trust

With identity under attack, teams moved from one source of truth to several pre-authenticated channels, and corrected only the fabrications that could cause harm.

3

Pay people, then restore — safely

Emergency payroll and benefit payments ran ahead of recovery. Restoration dropped to last place, gated on independent evidence and a tested way back.

Cross-cutting: *restoration was no longer the goal of the response. For most teams it became the last priority — and the one they were most willing to delay.*

DRI CANADA Train. Prepare. Recover.

KEY RISKS IDENTIFIED

The threats teams flagged most

Harm to named individuals

People are being named in a leak that mixes genuine and fabricated records. Fraud, harassment and identity theft were rated high / high at most tables.

Unsafe restoration

A premature reconnect could re-infect the recovery environment and turn one long outage into two. No team could prove the environment was clean.

Crews below minimum

Relief did not arrive and absenteeism is rising. Fatigue and manual error are compounding on five days of backlog.

Missed pay

Unpaid staff face fuel, family and travel barriers. Several teams linked missed pay directly to who would turn up for the next shift.

Fraud in manual payments

Emergency processes run by exhausted people invite duplicates, diverted payments and reconciliation failures.

Collapse of trusted instruction

Deepfakes, spoofed notices and credential harvesting mean staff and the public may act on a counterfeit — or stop trusting the real thing.

DRI CANADA Train. Prepare. Recover.

DECISIONS & AUTHORITY

What got decided — and who decided it

Key decisions made

- Notify affected individuals and regulators on credible risk, stating what cannot be verified
- Refuse the second extortion demand and accept the risk of further release
- Correct only fabrications that create safety, fraud or operational harm — no item-by-item denials
- Run emergency payroll and priority payments by hand, with compensating controls
- Operate to minimum crews and stop lower-priority services first
- Do not require unpaid staff to make unsafe journeys; record them as unavailable, not absent
- Decline reconnection until independent validation and a rollback path exist

Decision authority & structure

- Extortion stayed at the top of the house: Board, CEO, Deputy Minister or Executive Committee
- Notification sat with Privacy / ATIP and Legal, signed off at CEO or senior-official level
- Emergency spending authority rested with the CFO, inside delegated limits
- Restoration required joint CIO / CISO advice and executive risk acceptance
- Workforce decisions were shared between HR, Labour Relations and operations leads
- With external partners in a national queue, teams decided on internal advice rather than wait

DRI CANADA Train. Prepare. Recover.

PEOPLE & PAYMENTS

Minimum crews — and how the money moved

Minimum crews teams named

- Two-person floors for IT Security and the Service Desk — reconnection pauses below that
- Four specialists for earthquake early warning; five for nuclear emergency response
- About 50 people to keep urgent claims and benefit payments moving
- Eight officers per correctional unit; health and EMS at 30% of normal workforce
- Five for incident command; identity and access “fragile if one person drops”
- Eight for emergency payments; four security staff per critical site
- One team listed its critical functions but did not put numbers against them

How emergency payments were controlled

- Two approvers from separate functions on every emergency payment
- Call-back verification through a known, independent contact
- Transaction caps and pre-approved recipient categories
- Last validated or historical payment files as the starting point
- Hardship and life-sustaining payments first; anything unverifiable deferred
- A written commitment where same-day payment was not possible, then reconciliation

DRI CANADA Train. Prepare. Recover.

COMMUNICATIONS

Proving you are you

Internal

Call trees, known call-back numbers, radio nets, code words and in-person briefings. High-risk instructions needed confirmation through a second known-good channel.

External

Say the dataset is mixed and unverified, warn against the fake “check your exposure” site, and point people to channels that existed before the incident.

Discipline

No item-by-item denials. Correct only what creates a safety, fraud or operational risk — and do not let “verified facts only” turn into silence.

Signature move: *the strongest statements gave what is known, what is not, what to do, and the time of the next update — “even if there is no material change.”*

DRI CANADA Train. Prepare. Recover.

LOOKING AHEAD

Cascading risks & decision triggers

Cascading risks teams named

- Re-infection or a second compromise after a premature reconnect
- Further releases, with more individuals named and targeted
- Critical crews falling below the safe minimum as fatigue and absence compound
- Missed pay driving hardship and further absenteeism
- Duplicate or diverted payments in the manual process
- A fabricated instruction causing unsafe action by staff or the public

Triggers teams set for themselves

- Any new indicator of compromise → stop restoration and return to containment
- 24 consecutive hours with zero indicators, plus a tested failback → reconnect in stages
- A critical function below its minimum crew → stop the next service in the order
- Payment failures above 15% for 30 minutes → expand manual processing
- Generator fuel below six hours at a critical facility → conserve and shed services
- External support unavailable for 24 hours → build internal capability rather than wait

DRI CANADA Train. Prepare. Recover.

WHAT WORKED WELL — STRENGTHS

Strengths demonstrated across this round

Deferrals became decisions

The triggers that never fired in Inject 3 were replaced. Teams notified, refused and declined — and wrote down who decided and on what evidence.

Vendor confidence was not enough

No team reconnected on “high confidence.” It was treated as evidence, not authorization, with independent validation and a way back required first.

People came first — in numbers

Minimum crews were named by function, with the first service to stop below the line. Unpaid staff were not ordered to travel unsafely.

Costs accepted out loud

The best submissions named the risk they were accepting — further release, over-notification, longer outage — rather than implying there was none.

WHAT WORKED WELL

Strengths teams saw in themselves

Risk-based, not certainty-based

Teams described a deliberate shift from waiting for confirmed facts to acting on credible evidence and accepted risk.

Governance that held

Tactical, strategic and executive layers stayed distinct, with a clear owner for each of the six decisions.

Functions working as one

Legal, Privacy, HR, Finance and Communications sat inside the response alongside IT and Operations rather than being consulted afterwards.

Plans that survived contact

Tested payment continuity plans and critical-function lists held up under no relief, a failed payment cycle and scarce cash.

Assumptions actively revised

Rotations became minimum crews, one channel became several, and vendor assurance became team-owned restoration criteria.

Pressure resisted

Containment-first held against executives, officials and unions all asking for reconnection today.

DRI CANADA Train. Prepare. Recover.

3

COMMON GAPS — WHERE PLANS FELL SHORT

The weaknesses to carry into your after-action review

INJECT 4 RECAP

Authentication not pre-shared

Six of seven teams said they cannot yet prove a message is really theirs. Call-back lists, code words and alternate channels exist, but were not agreed or exercised in advance.

Thin staffing depth

Six of seven named staffing as a gap: crews not pre-defined, relief with no confirmed alternates, and critical functions resting on a few specialists.

Manual payments under-controlled

Five of seven flagged emergency pay: procedures not understood at the operational level, and real exposure to fraud, duplicates and reconciliation failure.

Recovery criteria unwritten

Four of seven had no documented standard for declaring the recovery environment ready — and the same number flagged reliance on external partners.

SUBMISSION HIGHLIGHTS

Standout thinking from Inject Four

Team A

Vendor confidence treated as “evidence, not authorization”; two-person crew floors; and a notice built to separate confirmed facts from fabricated material.

Team B

The sharpest workforce insight: named specialist crews for earthquake warning and nuclear response, with single experts identified as the real point of failure.

Team C

The most detailed crew model, about 50 people for urgent claims, plus tested payment workarounds and an honest note that readiness criteria are not yet written.

Team F

Eighteen measurable triggers, from generator fuel below six hours to 24 hours without external support, and a refusal to treat a logo or a voice as proof.

Team G

Whole-of-government reach: corrections at eight officers per unit, health at 30% of workforce, and the candour to label its numbers “pure assumption.”

Team H

The clearest reconnection gate: full endpoint visibility, 24 hours with zero indicators and a tested failback — and a statement that names its next update time.

Team J

Numeric triggers, a published service-suspension order, a five-phase restoration with a stop rule, and the risk accepted written beside every decision.

DRI CANADA Train. Prepare. Recover.

ADD YOUR THOUGHTS

Right calls. Real costs.

What did you learn from Inject Four — when every deadline belonged to someone else?

LEADERBOARD — INJECT FOUR

Inject Four Preliminary Results

7 teams · final = average of judges (1–5 scale)

2

4.69

Team C & H

1

4.94

Team J

3

4.62

Team B

Judging in progress

Two judges' scores are still outstanding. Teams A, F, H and J are currently averaged on two of their three scores, so these standings may change.

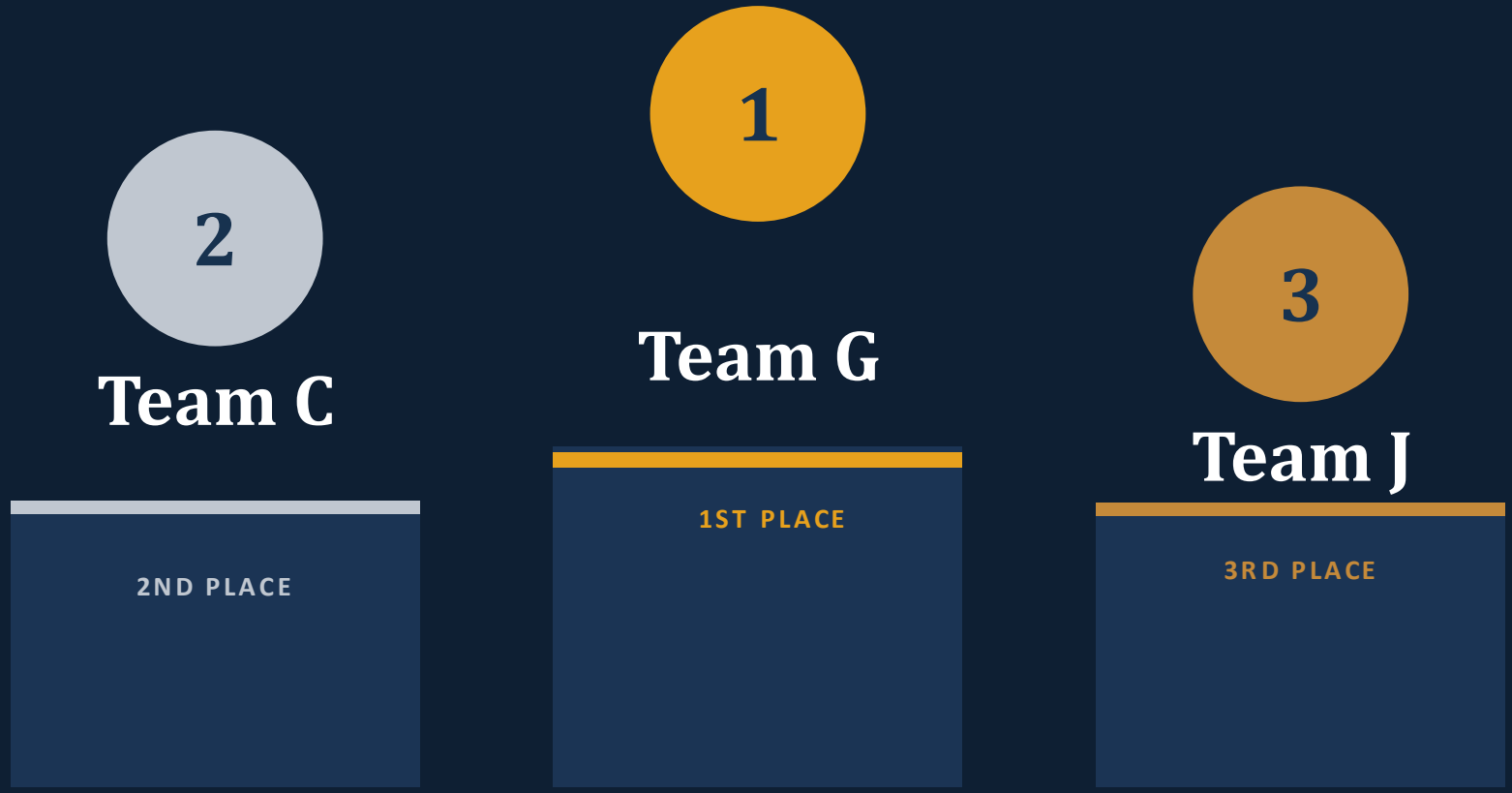
RANK	TEAM	PRELIM
1	**Team J**	4.94
2	**Team C**	4.69
3	**Team H**	4.69
4	**Team B**	4.62
5	**Team G**	4.56
6	**Team F**	4.15
7	**Team A**	3.53

DRI CANADA Train. Prepare. Recover.

THE GREAT CANADIAN DISASTER · STANDINGS

Overall Leaderboard — After Four Injects

Combined results across Injects One to Four · to be confirmed



THE SITUATION RESOLVES

Introducing Inject Five

Eight days on, the power is back, the forensic results are in, and the questions have begun. The final inject closes the scenario: recovery, accountability, and what you will change.

START TIME

9:00 AM EDT

TIME NEEDED

1 hour

DATE

May 12, 2026

The Great Canadian DISASTER

INJECT FIVE · MAY 12, 2026 · 9:00 AM EDT

How the Exercise Ends

It is Day 12. The emergency is over. The incident is not.

The week between went the way you were warned. Power returned unevenly, systems came up in configurations nobody could vouch for, and fuel, parts, IT/OT components and vendor support arrived late or not at all. You worked through it on manual processes and short crews.

This morning the grid is stable across most regions, the national forensic queue has cleared, and your independent assessment is in. Most suppliers are back, but one you depend on is still rationing. Workarounds nearly two weeks old have quietly become the way things are done.

Your executive wants a stand-down date. The people who carried the response are spent, and some are angry. And a board, council, minister, regulator, auditor, union and the media have each asked for an account of what you decided on Day 4.

The core tension: *you made defensible decisions on Day 4, and every one of them still cost something. Now you close out recovery and account for them.*

RISK & RESILIENCE TRENDS

- Supply Chain Disruption
- Critical Infrastructure
- HR Issues
- Regulatory / Legal

PROFESSIONAL PRACTICES

- 6 Plan Implementation
- 8 Exercise, Assessment & Maintenance
- 10 Coordination with External Agencies

DRI CANADA Train. Prepare. Recover.

INJECT FIVE

Where each sector stands on Day 12

Large Corps & Critical Infrastructure

Systems are returning in a sequence nobody planned, one critical supplier is still rationing parts, and the board wants to know why recovery took six days longer than the vendor promised.

Federal & Provincial Government

Ministers and central agencies want a stand-down date, a union grievance is on file, and privacy regulators are asking who was notified and who was missed.

Small & Medium Enterprises

Card rails are back but the cash float is gone, suppliers want paying for two weeks of credit, and customers named in the leak want to know what you did for them.

Communities & Local Governments

Council wants the Day 4 record, residents who evacuated on a fake notice want answers, and crews who ran water and wastewater by hand need rest.

Finance & Insurance

Reconciliation has found duplicate and diverted manual payments, regulators are reviewing notification decisions, and customers are still being phished in your name.

DRI CANADA Train. Prepare. Recover.

THE FINAL INJECT · THREE PARTS, ONE HOUR

What Inject Five Asks of You

No new crises. Close out recovery, stand behind one decision, and leave with improvements somebody owns.

1. **Declaring recovery** [Part 1] What has to be true before you stand down? Which service is last back, and which manual workaround do you retire first?

2. **The supplier that isn't back** [Part 1] One critical dependency is still at reduced capacity. How long can you hold, and what if it never fully returns?

3. **Standing down your people** [Part 1] What do you commit to, on the record, for the staff who carried this — and what is your answer to the grievance?

4. **Accountability** [Part 2] Choose one audience and account for one Day 4 decision from your log: what you knew, what you did not, and whether you would decide the same again.

5. **After-action review** [Part 3] What did your plan assume, what actually happened, and why the difference? What worked and must be kept?

6. **Three commitments** [Part 3] Pick three improvements. Each needs a named role, a due date, and a way to prove it works.

BEFORE YOU RESPOND

What you now know

The recovery environment was not clean. A dormant privileged account sat in the vendor-certified build, and two organizations that reconnected on Day 4 were re-encrypted on Day 6.

The full dataset was published on Day 6: roughly 55% genuine, 30% fabricated and 15% other organizations'. Some people you notified were never affected; some who were have not heard from you. One organization paid and was published anyway.

The fabrications did harm. The fake exposure-check site harvested staff credentials, and a deepfake evacuation notice emptied a community overnight.

Manual payments leaked. About 2% were duplicates, and one was diverted because the call-back number came from the spoofed email.

Your people paid a price: a grievance over staff recorded as absent, two specialists on medical leave, and overtime nobody has funded.

Judge the decision on what you knew then. Judge the plan on what you know now.

DRI CANADA Train. Prepare. Recover.

One last hour.

Three parts. No new crises. Finish well.

> > > >

The Great Canadian DISASTER

Empowering Canada's continuity professionals to build a resilient nation.

Test your plans before reality does.

DRI CANADA Train. Prepare. Recover.