

Practice before the request.

Facilitator guide | Agency AI Attack Readiness Kit

Use a 15-minute staff discussion. Choose a facilitator, one reader and a note-taker. Use only fictional names. No client records, credentials, bank details, real transfers or live account changes.

Read the fictional request

A familiar-looking vendor message supplies new payment instructions and a new callback number. It says the usual approver is unavailable and asks for an urgent change.

Ask five questions

1. What exactly changed?
2. Which contact already in approved records verifies it?
3. Who is authorized to approve it?
4. Where is the decision recorded?
5. Who handles an unverified or urgent request?

Discuss, compare, assign

Allow 3 minutes for the scenario, 7 for discussion and 5 to compare with the separate answer guide and assign one next action. A hosted 20-minute version can use the remaining 5 minutes for questions.

Preparation only. A discussion does not test technical controls or establish that an agency is secure. Published October 22, 2026.

Keep a callback card nearby.

Changed instructions? Use a trusted route.

Pause a sensitive change. Use the contact already in approved records, not a new number supplied by the request. Confirm the specific change. Follow the agency approval process. Escalate if it cannot be verified. Retain the decision through the approved process.

Blank payment-change worksheet

Fictional exercise / date: _____

What changed: _____

Trusted contact location (no personal details here): _____

Verification owner: _____

Approver / backup role: _____

Approved decision-record location: _____

Escalation role: _____

Unanswered question: _____

Evidence needed: _____

Follow-up owner / review date: _____

Use roles rather than sensitive details. Store completed records only in an agency-approved location. No real transfer is part of this exercise.

Find the recovery route.

Blank recovery-contact worksheet

Scenario: normal email is unavailable. Do not test a live account.

Approved provider contact-record location: _____

Separate verified contact route location: _____

Agency decision owner / backup role: _____

Offline incident-procedure location: _____

Who verifies the identity of recovery help: _____

Evidence still needed / follow-up date: _____

Questions to bring to your IT provider

Who maintains legitimate email senders and verifies SPF, DKIM and DMARC alignment? What dated evidence supports MFA and privileged-access settings? How are suspicious sign-ins and forwarding rules reviewed? How is recovery arranged when email is unavailable? Who verifies the running website version after an update?

For every unanswered question, name an owner, request evidence and set a review date. Unknown does not mean compromised. Do not change DNS or account access from this worksheet alone.

Do not write passwords, recovery codes, customer records or bank details here. Use the established response provider for a suspected active incident.

Answer guide | keep separate

Expected decisions

Request: identify the specific changed instructions and urgency.

Verification: use an independently trusted route already recorded.

Approval: follow the existing agency authority and backup procedure.

Record: retain the confirmation and decision in the approved location.

Escalation: use the designated owner when verification fails.

A fictional worked outcome

The employee finds the vendor contact in approved records but cannot identify the backup approver. The payment change remains paused. The designated agency owner is assigned to confirm the backup approval procedure before a later rehearsal. This is an example of an unanswered question, not a customer result.

What counts as a narrow observation

Record: “The team located the approved contact record.” Do not expand that into “Our accounts are secure.” Record: “No backup approval role was identified during discussion.” Do not expand that into a breach finding.

Debrief without blame

Which decision was unclear? What evidence would resolve it? Who owns the follow-up? When will we review it? Staff do not need to prove that AI wrote a request before applying the verification procedure.

Share a useful lesson.

Reuse and attribution

You may share this original Cirlet kit at no charge, including in commercial training, with attribution and a link to the canonical page. You may adapt the original exercise text; label changes and retain fictional-example and safety limits. Do not imply Cirlet reviewed an adaptation or that a source endorses it. Third-party material keeps its own rights. Do not sell the unchanged kit as a standalone product.

Suggested attribution

Agency AI Attack Readiness Kit, by Cirlet. Free resources at aicybersecurityforinsuranceagencies.com/readiness-kit.

Sources and boundaries

The trusted-contact principle is informed by FBI IC3, May 15, 2025:

<https://www.ic3.gov/PSA/2025/PSA250515> . The agency exercise and worksheets are Cirlet originals. The advisory documents an impersonation technique, not an attack on a named agency in this kit.

AI assists Cirlet with research, drafting, code and assets. Fictional scenarios are not customer case studies. These materials do not provide emergency response, certification, legal advice or a guarantee against compromise.

Optional scoped help

Cirlet offers the \$750 Agency AI Security Sprint: one website, one email environment and up to two optional AI workflows; agreed checks, prioritized findings, one agreed improvement and handoff. Scope, access and date agreed first. Agreed delivery before billing; no Sprint fee if agreed delivery is not provided. First 30-minute conversation free. Full scope: cirlet.com/security-review .