Konfydence

Outsmart Scams - Together

Behavioral Evidence Template (Audit-Ready, 1-Pager)

Purpose

This template documents *behavior-based security awareness activities* to support audit and compliance discussions (e.g. NIS2 Article 21, ISO/IEC 27001:2022 Annex A.6.3).
It focuses on **observable behavior and learning outcomes**, not individual performance.

⚠ Important wording:
This template supports audit evidence. It does not claim certification or compliance.

Section 1 — Session Overview

- **Organization / Unit:**
- **Date:**
- **Format:** (Workshop / Simulation / Game-based session / Hybrid)
- **Participants:** (Number, roles or teams – no individual names)
- **Facilitator:**

Section 2 — Scenarios Practiced *(Tick or list those used)*

Scenario Type	Description
Authority-based	e.g. executive or manager request
Urgency-based	time pressure, “act now”
Trust-based	known sender / familiar platform
Mixed triggers	multiple HACK elements

Example scenarios used:

- ☐ Executive payment request under time pressure
- ☐ IT account / MFA reset request
- ☐ Supplier invoice with changed bank details
- ☐ Other: ______________________

Section 3 — Decision Patterns Observed (Group-Level)

(No individual tracking)

For each scenario, document:

- **Most common first reaction:**
  ☐ Immediate action ☐ Pause ☐ Verification ☐ Escalation
- **Key confusion points:**
  (e.g. authority vs. verification responsibility)
- **Trigger(s) identified:** ☐ Hurry ☐ Authority ☐ Comfort ☐ Emotional pressure

Section 4 — Discussion & Learning Outcomes

Key discussion themes:

- What felt convincing?
- What made verification feel difficult?
- When did people hesitate — and why?

Learning outcomes observed:

- ☐ Increased recognition of urgency manipulation
- ☐ Improved willingness to verify
- ☐ Clearer escalation behavior
- ☐ Better shared language around risk (e.g. HACK)

Section 5 — Follow-Up Actions

(Optional but powerful for auditors)

- ☐ Policy clarified
- ☐ Internal process reinforced
- ☐ Additional training scheduled
- ☐ Scenario added to next session
- ☐ No follow-up required at this time

Section 6 — Evidence Mapping (Optional Callout)

Supports:

- **NIS2 Article 21(2)(g)** – Security awareness & training
- **ISO/IEC 27001:2022 Annex A.6.3** – Awareness, education, training

Evidence type:

✓ Training activity
✓ Behavioral discussion
✓ Continuous improvement indicator

Footer (important)
This document captures *reasonable, proportionate effort* to address human-related cyber risk through structured awareness and behavior-based learning.