

Security Awareness Software: Selection, Requirements, and Workflow

- - Define requirements, evaluate vendors, implement, and operate awareness software as a human-risk control
- - Human risk dominates breaches; AI-driven social engineering is scaling fast
- - For awareness managers, IT, security, L&D, compliance, and educators
- - Roadmap: capability map, requirements, scoring, workflow, rollout, metrics, ethics
- - You leave with a requirements matrix, scorecard, workflow blueprint, and 30/60/90 plan



Why Awareness Platforms Matter in 2026

Phish-prone Percentage (PPP) Over Time

Sustained training drives lasting risk reduction



Baseline Susceptibility

33.2% globally; 39.5% at 10,000+ employee enterprises; 54% in large healthcare



- **Human risk now tops tech gaps:** 91% struggle with compliance; only 28% pair training with monitoring



- **Baseline phishing susceptibility:** 33.2% globally; 39.5% at 10,000+ employee enterprises; 54% in large healthcare



- **Sustained training works:** PPP falls 40% by 90 days, 87% by 12 months, stabilizing near 3.9%



- **Market converging on Human Risk Management:** awareness, simulation, analytics, control linkage



- **Programs stall without an owner,** cadence, and metrics beyond completion

Building the Business Case and Mapping Market Categories



- **Frame spend as human-risk reduction:** tie phishing susceptibility, report rate, time-to-report to exposure



- **Drivers:** ransomware and BEC losses, cyber-insurance mandates, NIS2/DORA proof, 17.1% phishing spike since late 2025



- **Market:** USD 6.74B in 2026, ~16.8% CAGR; software platforms growing faster than services



- **Categories:** legacy suites (KnowBe4, Proofpoint, Cofense), adaptive behavior platforms (Hoxhunt, SoSafe, CybSafe), simulation specialists, M365-native AST



- **Lead with executive metrics:** susceptibility trend, report rate, report-to-click ratio, credential submission, time-to-report, repeat clickers



Legacy Awareness Suites



Adaptive Behavior Platforms



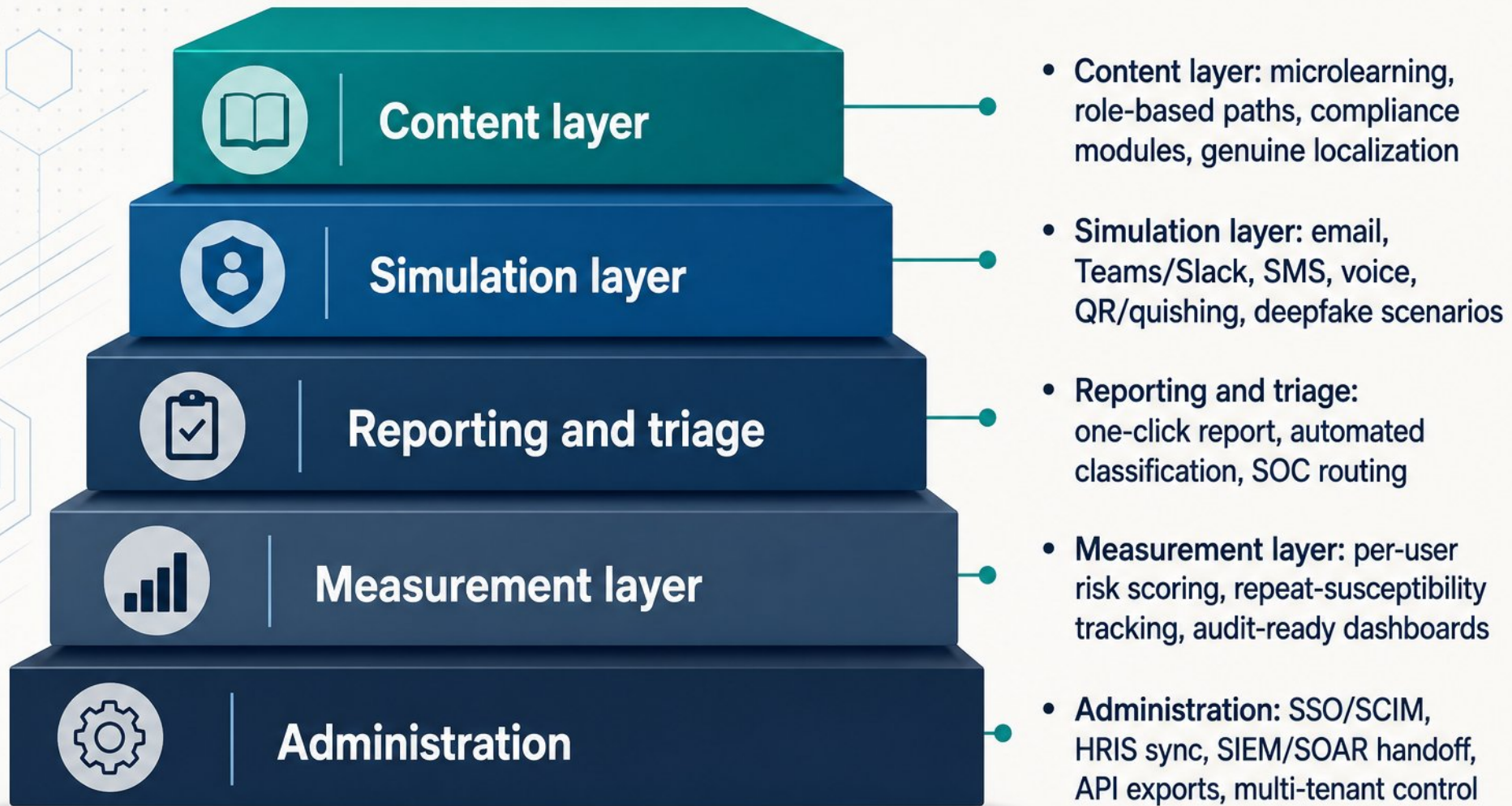
Simulation Specialists



M365-Native Options



Core Capability Map: What Awareness Platforms Actually Do



Requirements Gathering and Stakeholder Alignment



- Map stakeholders and decision rights early: security, IT, L&D, compliance, legal, privacy, HR, works councils, business owners



- Translate business and risk goals into functional and non-functional requirements, not feature wish lists



- Separate must-haves: mandated compliance evidence, reporting and triage workflow, localization, accessibility, identity integration



- Name constraints before vendor contact: budget, admin headcount, implementation window, data residency, procurement rules



- Document everything in a traceable matrix so every score and demo question maps to a stated need





Selection Criteria, Weighted Scorecards, and Total Cost of Ownership



- Fix weights before the first vendor demo — never after



- Customize by risk profile: measurement 25%, realism 20%, content 18%



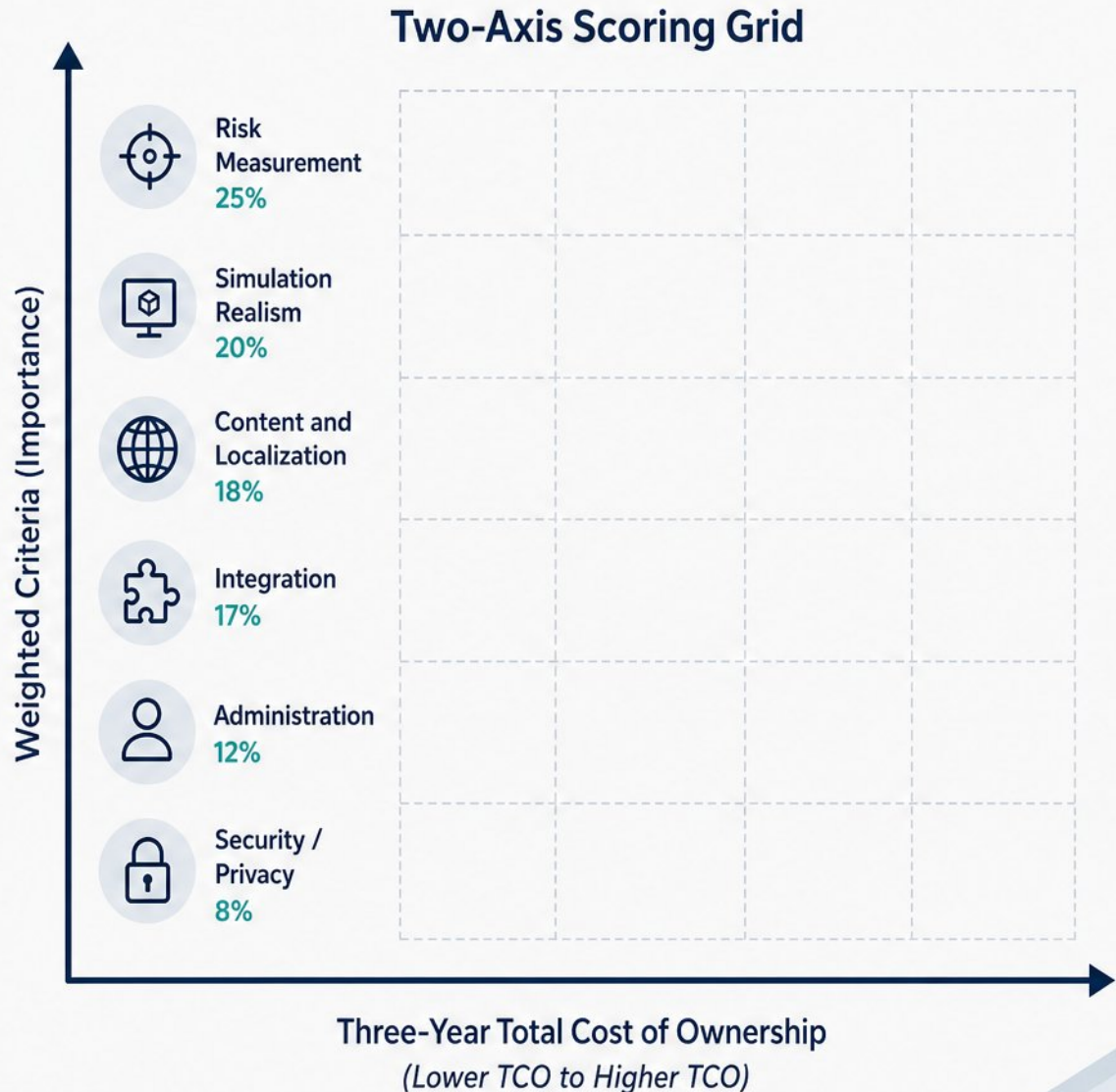
- Score every vendor independently during RFI phase



- Model three-year TCO: subscriptions, add-ons, integration, admin labor



- Watch auto-renewals, seat minimums, escalation clauses, exit terms



Running a Pilot That Produces Evidence, Not Anecdotes



PILOT DESIGN CARD



HIGH-RISK COHORT

Focus on roles most exposed to risk



30-45 DAY DURATION

Two simulation rounds plus follow-up training



BASELINE FIRST

Capture a clear starting point before launching



PRE-AGREED SUCCESS CRITERIA

Defined in writing before the pilot starts



- Design the pilot as a structured experiment, success criteria agreed in writing



- Recruit 100-200 staff from finance, executive admin, IT, legal, or sales



- Run at least 30-45 days: two simulation rounds plus follow-up training



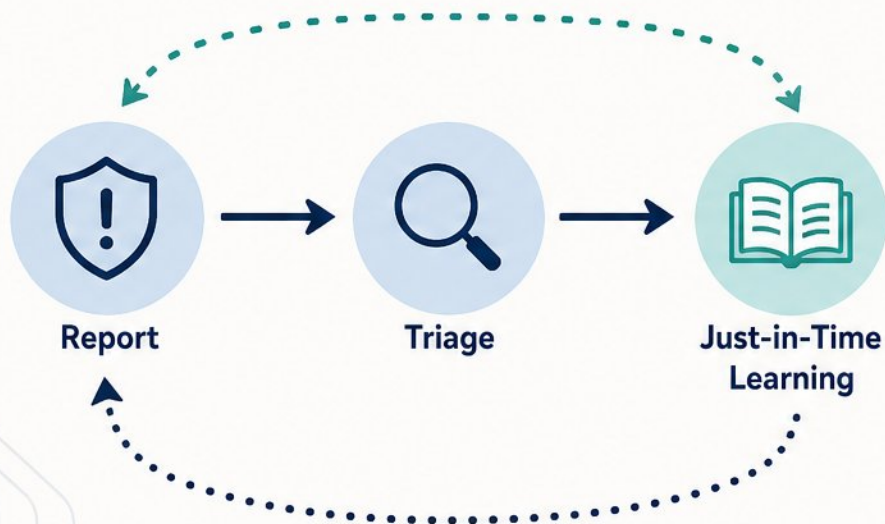
- Baseline first: click rate, target reduction, completion, report-rate gain



- Measure the unglamorous: build time, AD user-load, post-click page, triage handling

Workflow Design: From Campaign Calendar to Behavior Change

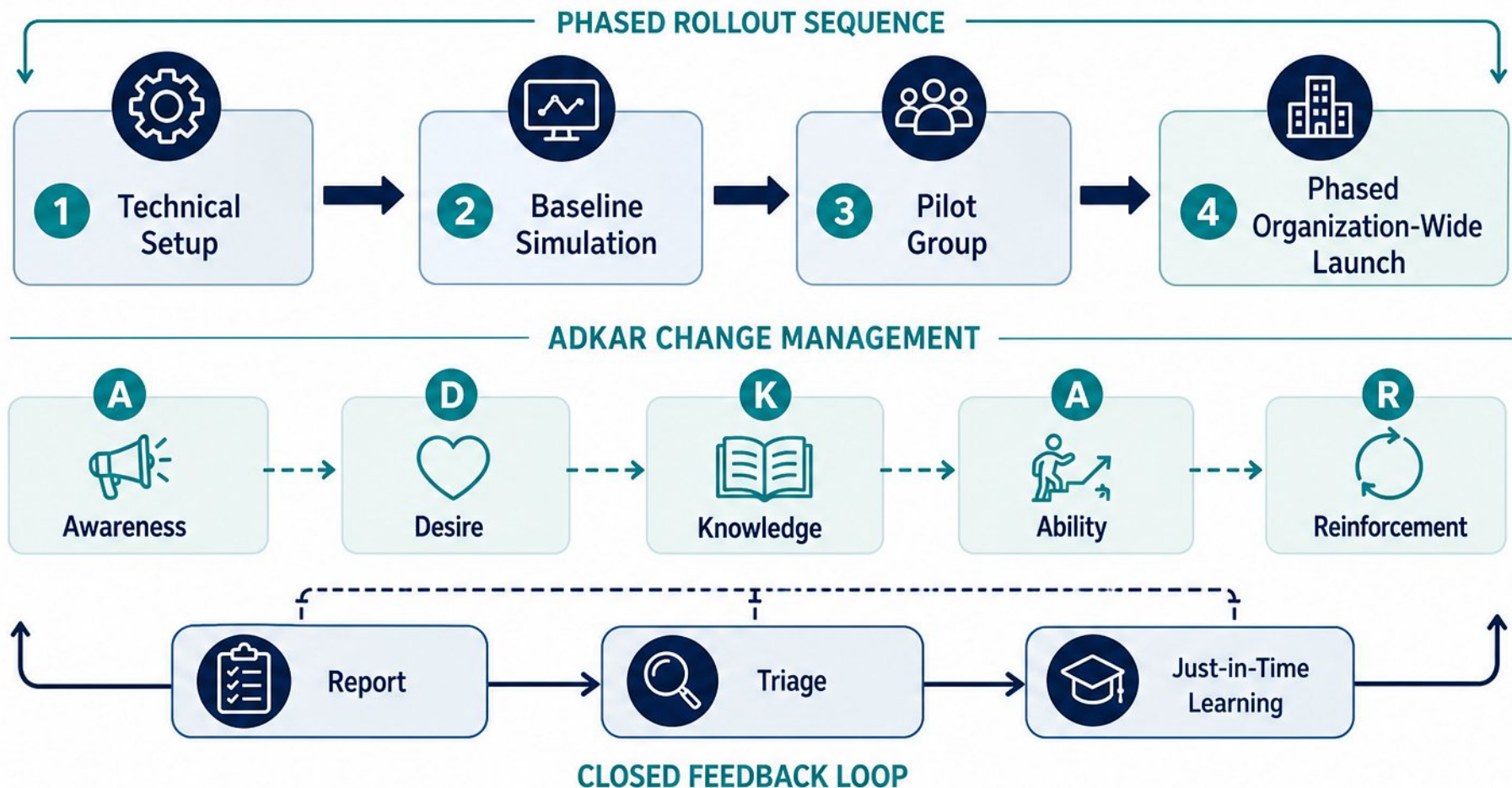
Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
											
Training Assignment	Training Assignment	Training Assignment	Training Assignment	Training Assignment	Training Assignment	Training Assignment	Training Assignment	Training Assignment	Training Assignment	Training Assignment	Training Assignment
											
Simulation	Simulation	Simulation	Simulation	Simulation	Simulation	Simulation	Simulation	Simulation	Simulation	Simulation	Simulation
 Tax Season Focus		 Quarter Close Focus		 Summer Focus			 Quarter Close Focus		 Year-End Focus		



- ✓ Build a 12-month calendar: one training assignment + one simulation per month
- ✓ Cadence is the top driver; skipping months causes non-linear damage
- ✓ Tune themes to seasonality: tax season, quarter close, year-end cycles
- ✓ Segment by role and risk tier: monthly for critical roles, quarterly for staff
- ✓ Close the loop: JIT micro-training under 10 minutes, never punitive emails
- ✓ Automate assignments, reminders, escalations; no re-testing within 30 days

Implementation, Change Management, and User Adoption

- Sequence rollout: technical setup, baseline simulation, pilot, then phased launch
- Allow a realistic 90-day timeline for large enterprises
- Apply ADKAR: awareness, desire, knowledge, ability, reinforcement
- Reduce friction: SSO, SCIM sync, one-click reporting, API connections—no MX changes
- Enable champions and managers before launch; publish a written no-blame policy

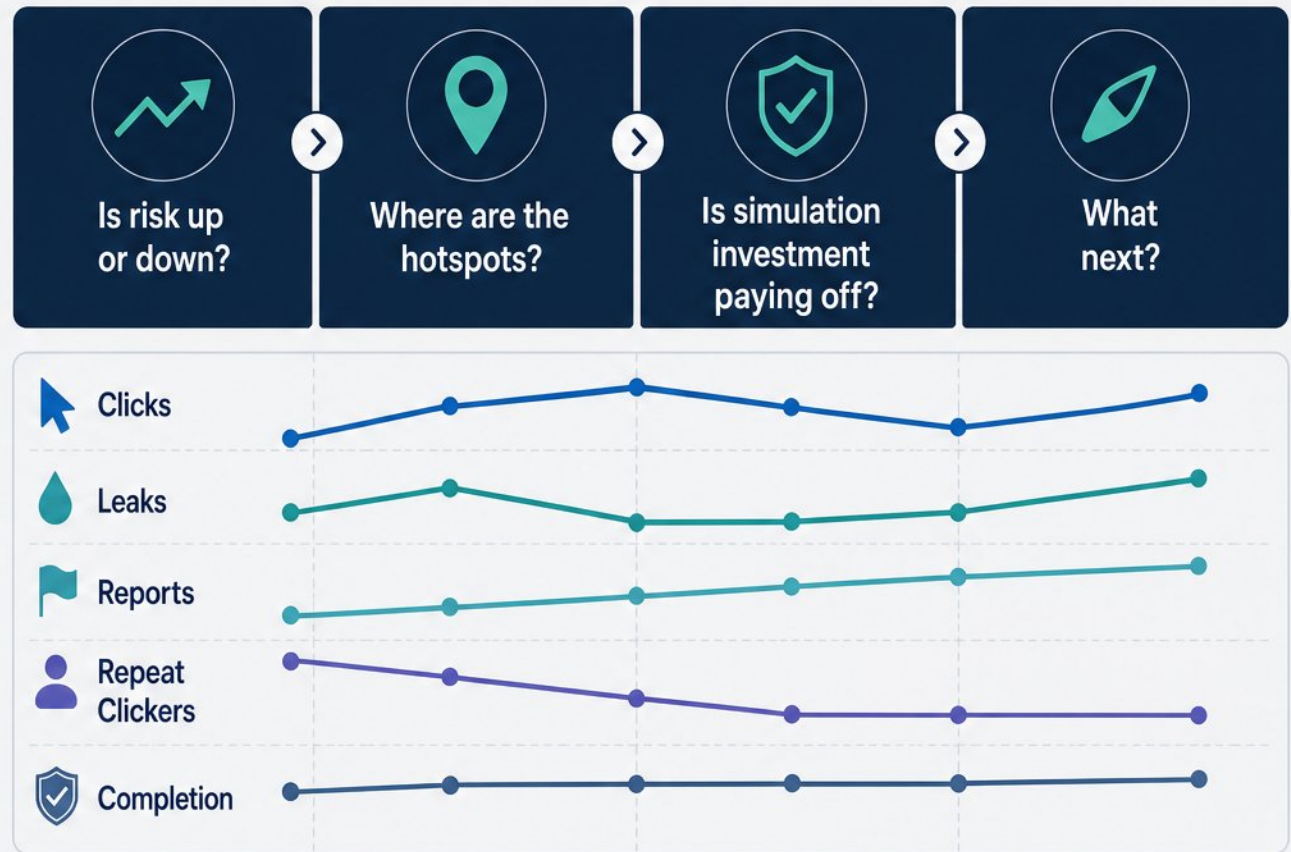


Measurement, Dashboards, and Continuous Improvement



- ✓ Track click, leak, report, and time-to-report together — never click rate alone
- ✓ Report rate leads culture: 30–50% at 12 months, 50%+ by 24 months
- ✓ 100% completion with 25% clicks is a compliance record, not security
- ✓ One dashboard answers four questions in under a minute
- ✓ Read trends against difficulty mix to separate resilience from template familiarity

ONE DASHBOARD. FOUR QUESTIONS. CLEAR ANSWERS.



Risk, Compliance, and Ethical Guardrails

- Legal basis: legitimate interest under GDPR Art. 6(1)(f), documented via a signed LIA — never employee consent
- Run a DPIA where simulation and scoring amount to systematic monitoring; honor works-council co-determination (BetrVG §87)
- Minimize data: collect only delivery, click, report, completion events; never store real credentials; auto-anonymize after 30–90 days
- Design ethically: no layoff, health, or finance bait; no public shaming; no disciplinary use of a single click
- Keep an audit-ready compliance dossier: LIA, security policy, works-council records, vendor DPA, retention schedule, aggregated reports



Case Walkthroughs: Small Regulated Firm, Global Enterprise, Education and Nonprofit



- Small regulated firm: lean team, one platform, compliance evidence and phishing triage
- Global enterprise: multi-tenant admin, dozens of languages, works-council consultation, SIEM/SOAR integration
- Education and nonprofit: low budgets, high turnover, low reporting baselines
- Platform matters less than discipline: monthly cadence, progressive difficulty, just-in-time training
- Unifying training and simulation cut admin load ~30% and cleaned up audit reporting



Your Takeaway Toolkit and 30/60/90-Day Action Plan



Toolkit 1:

requirements matrix
tracing each goal
to owners



Toolkit 2:

weighted scorecard
with fixed weights
and 3-year TCO



Toolkit 3:

workflow blueprint –
calendar, segmentation,
triage, reporting



1–30 Days



Days 1–30:
sponsorship,
matrix, RFI,
baseline simulation



31–60 Days



31–60:
pilot high-risk
cohort



61–90 Days



61–90:
score, negotiate,
decide



Beyond launch: named owner, quarterly steering, escalation thresholds, annual re-baseline

GOVERNANCE AND GUARDRAILS



Policy



LIA/DPIA



Audit Dossier

PersonWise.

PersonWise • AI digital-human course platform



Scan the code or click anywhere to watch this course live, with voice Q&A

personwise.ai/t/6f352676/public