



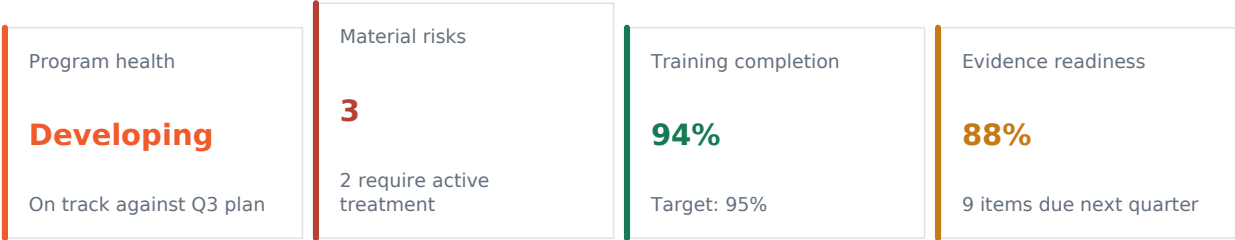
SAMPLE EXECUTIVE REPORT

Quarterly Security Report

A board- and leadership-ready sample report that turns cybersecurity activity into clear decisions, evidence, and next steps.

Quarterly Security Report

Q3 2026 • Illustrative management report. A concise view of program health, material risk, awareness activity, evidence, and decisions requiring leadership attention.



Executive summary

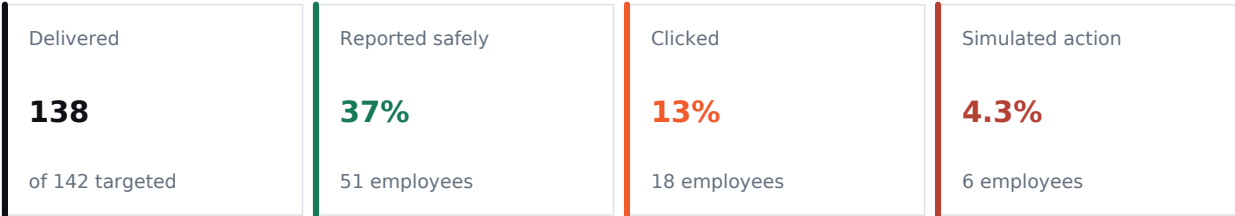
The security program advanced materially this quarter. Core policies are published, employee acknowledgement is near completion, and the first phishing simulation established a baseline for reporting behavior. The highest priorities for next quarter are closing two critical remediation items, completing the incident-response tabletop, and formalizing the vendor-review process for systems that process customer information.

Leadership decision required	Approve the Q4 remediation plan and designate business owners for the customer-data vendor review. Confirm whether the organization will pursue SOC 2 readiness in the next 12 months so evidence collection can be sequenced appropriately.
------------------------------	--

Program scorecard

Area	Current status	Quarter movement	Next action
Governance	Established	Security owner and monthly review cadence in place	Confirm annual policy review calendar
Policies & evidence	Progressing	6 of 7 core policies published; acknowledgements underway	Publish data-handling policy and close acknowledgement gap
Awareness & phishing	Baseline set	First simulation completed; report rate 37%; click rate 13%	Assign targeted refresher and repeat invoice scenario
Risk & remediation	Attention required	2 critical and 8 high items tracked	Close public storage exposure and extension risk
Incident readiness	Planned	Draft response plan completed	Run leadership tabletop in Q4

Phishing simulation results



Interpretation: The first campaign created a measurable baseline. Reporting behavior is encouraging; credential- and benefits-themed requests remain a coaching opportunity. Follow-up learning was assigned to employees who clicked or completed the simulated action. This report evaluates program improvement, not employee discipline.

Quarterly priorities

Priority	Why it matters	Owner	Due
Resolve critical cloud exposure	Reduces risk of unauthorized access to test data and services	Engineering	Oct 11
Complete incident tabletop	Confirms escalation, decision-making, and communication readiness	Executive sponsor	Nov 15
Establish vendor review workflow	Creates consistency for customer-data and material-service providers	Operations	Nov 30
Run phishing refresher campaign	Reinforces reporting behavior and tests learning improvement	Security lead	Dec 12

Report basis	This sample report uses program evidence such as policy publication and acknowledgement records, training completion, phishing simulation outcomes, risk-register status, remediation tracking, and management review notes. It does not represent an audit opinion, certification, or guarantee of compliance.
--------------	---