FalconryTrust
POWERED BY FALCONRY360

FALCONRYTRUST · PLATFORM TOUR

# Dashboard gallery

Eighteen Falconry360 views, from the Board report to a single phishing campaign. One record underneath; each seat sees what it owns and can change.

CONTENTS

# Eighteen views, nine seats, one record.

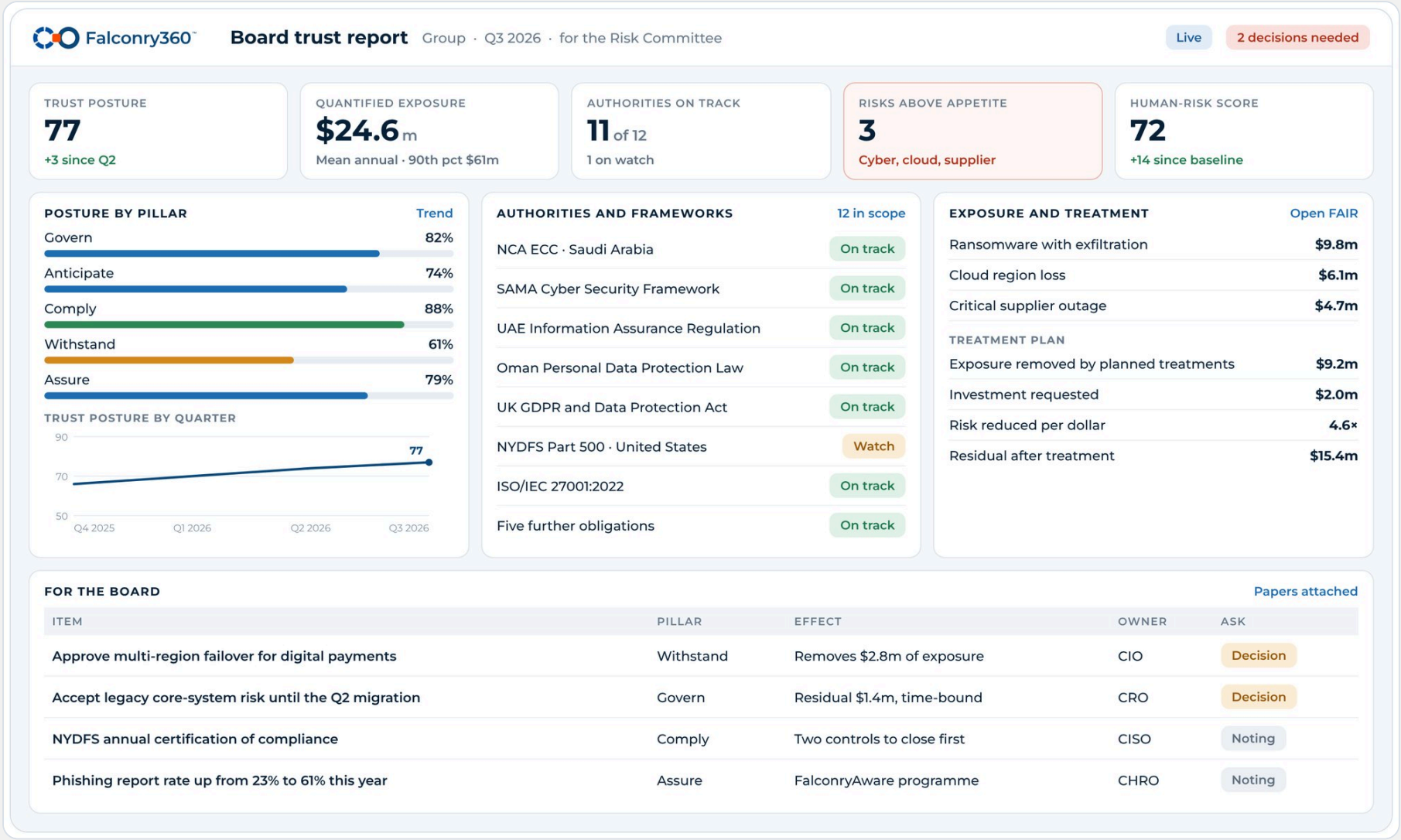
Every view is drawn from the same four masters in Falconry360: the asset master, the supplier master, the control library and the regulatory library. A control tested once moves every view that depends on it.

| VIEW | SEAT | WHAT IT ANSWERS |
|---|---|---|
| 01 **Board trust report** | Board and risk committee | Posture by pillar, quantified exposure, authorities on track and the two decisions the Board is asked to make. |
| 02 **Chief Risk Officer** | CRO | Risk against appetite, top quantified exposures and assurance coverage over the risks that matter. |
| 03 **Cyber trust and privacy** | Enterprise overview | One view across cyber, privacy and technology risk for every entity in the group. |
| 04 **CISO workspace** | CISO | Trust posture, risks above appetite, critical assets, third parties at risk and open findings. |
| 05 **CISO, telecoms group** | CISO · sector view | Readiness by framework, network exposure and human risk for a network operator. |
| 06 **Control library and mapping** | GRC lead | One control tested once, answering every framework that requires it. |
| 07 **DPO workspace** | DPO | Privacy posture, records of processing, rights requests, impact assessments and breach clocks. |
| 08 **CIO workspace** | CIO | Service availability, application estate, change, cloud and the obligations attached to technology. |
| 09 **OT security workspace** | OT security lead | IEC 62443 zones, security levels against target, OTCC compliance and plant findings. |
| 10 **Cyber risk quantification** | CISO and CRO | Loss exceedance, exposure by scenario and the treatments that remove the most exposure per dollar. |
| 11 **Third-party cyber risk** | Procurement and CISO | Supplier tiers, assessments, concentration and the issues due first. |
| 12 **Cyber resilience** | Resilience lead | Recovery against tolerance, playbooks, notification readiness and exercises. |
| 13 **Security awareness programme** | Awareness lead and CHRO | The twelve-month programme, role paths and the behaviour trend across the year. |
| 14 **Phishing simulation** | Awareness lead | One campaign from delivery to follow-up: funnel, clicks by department and reporting speed. |
| 15 **Security awareness overview** | CISO | Report rate, click rate, credential entries and the human-risk score in one place. |
| 16 **AI governance** | AI governance lead | The AI inventory, risk tiers, human oversight and ISO/IEC 42001 readiness. |
| 17 **FalconryX agent activity** | GRC lead and CISO | What the agents drafted, what reviewers accepted, amended or rejected, and the review queue. |
| 18 **Managed Trust service report** | Client sponsor | Service levels, what was delivered this month and the decisions waiting on the client. |

# Board trust report

Posture by pillar, quantified exposure, authorities on track and the two decisions the Board is asked to make.

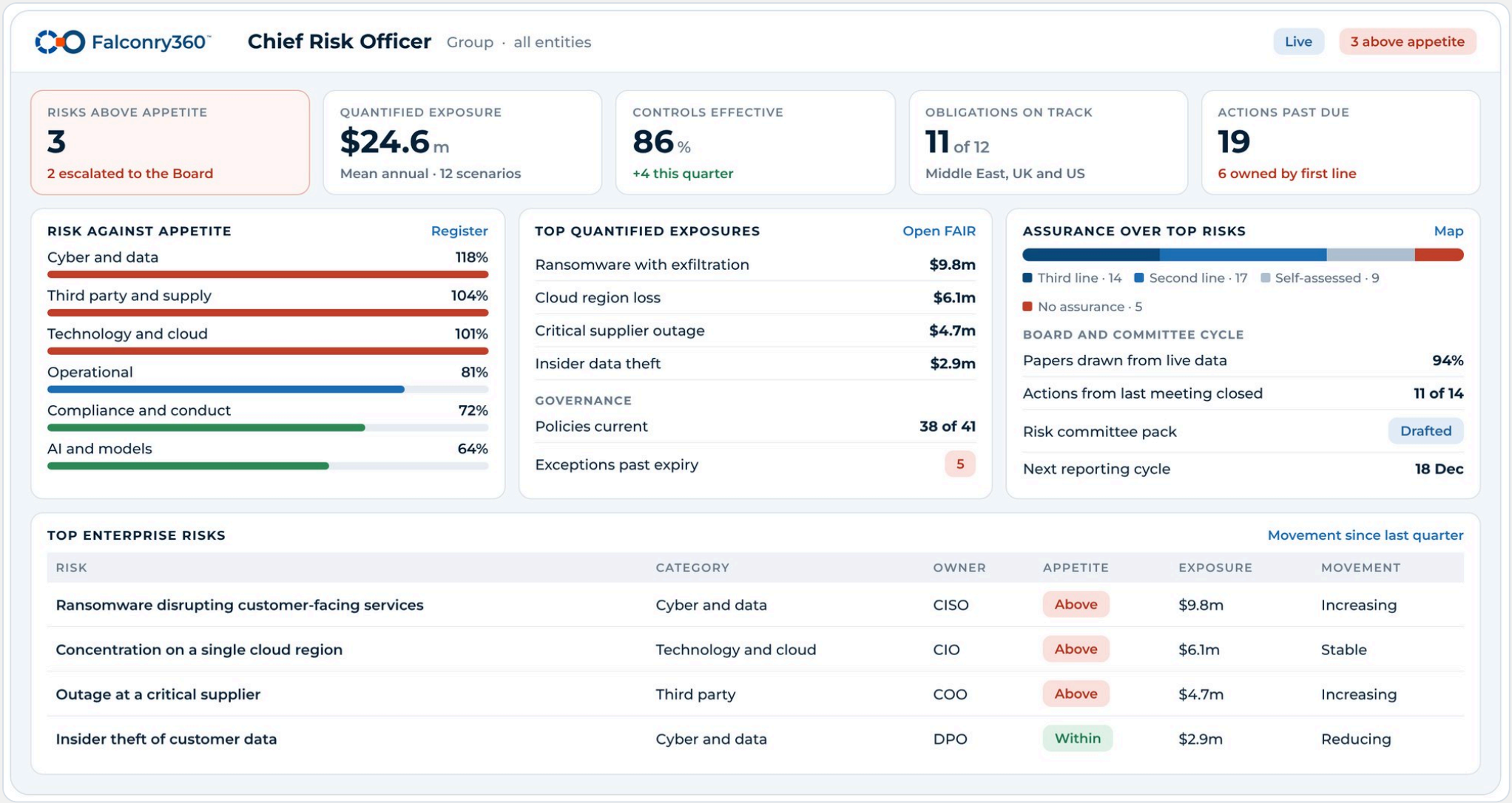
Illustrative Falconry360 view
falconrytrust.com/risk-quantification.html



# Chief Risk Officer

Risk against appetite, top quantified exposures and assurance coverage over the risks that matter.

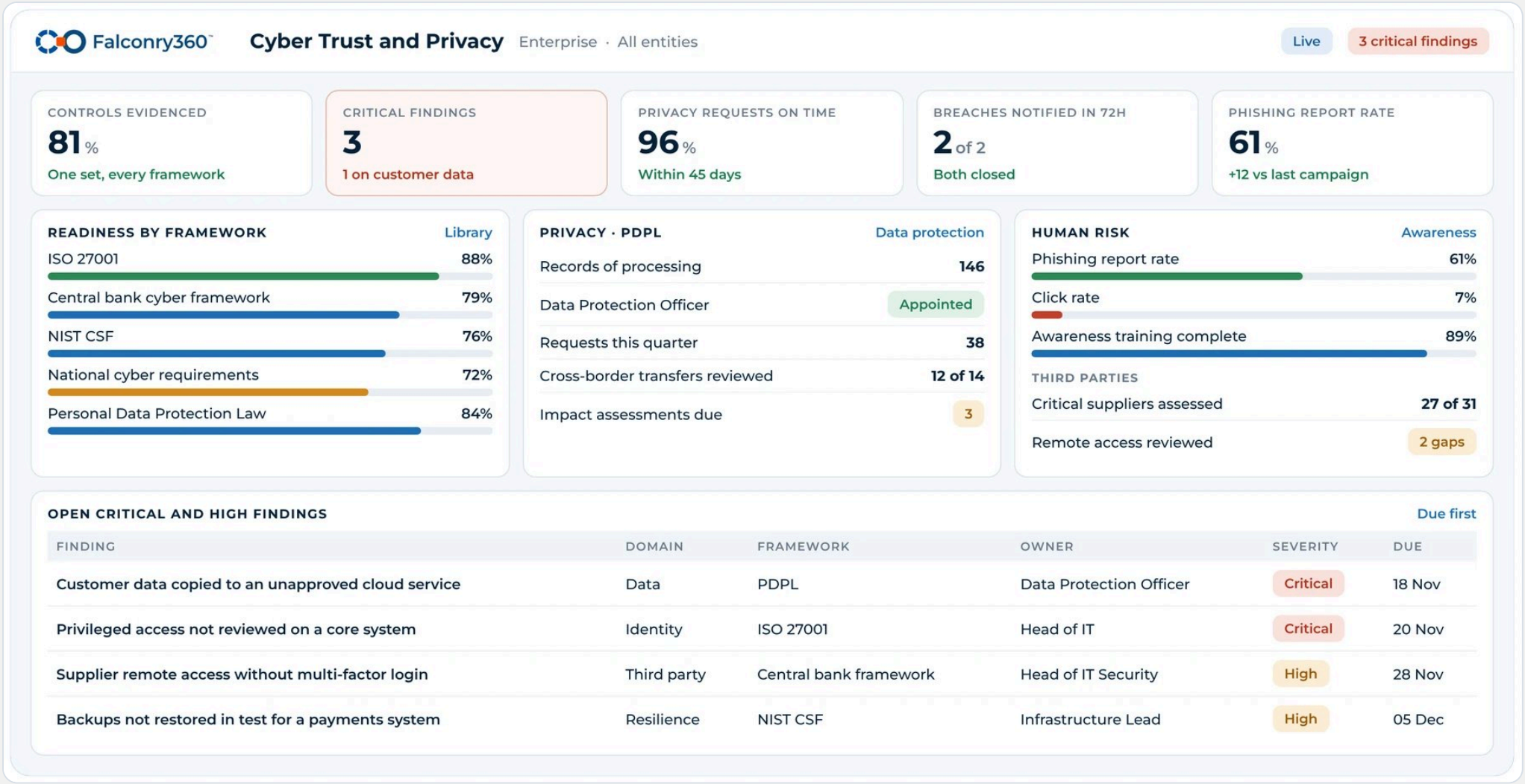
Illustrative Falconry360 view
falconrytrust.com/risk-quantification.html



# Cyber trust and privacy

One view across cyber, privacy and technology risk for every entity in the group.

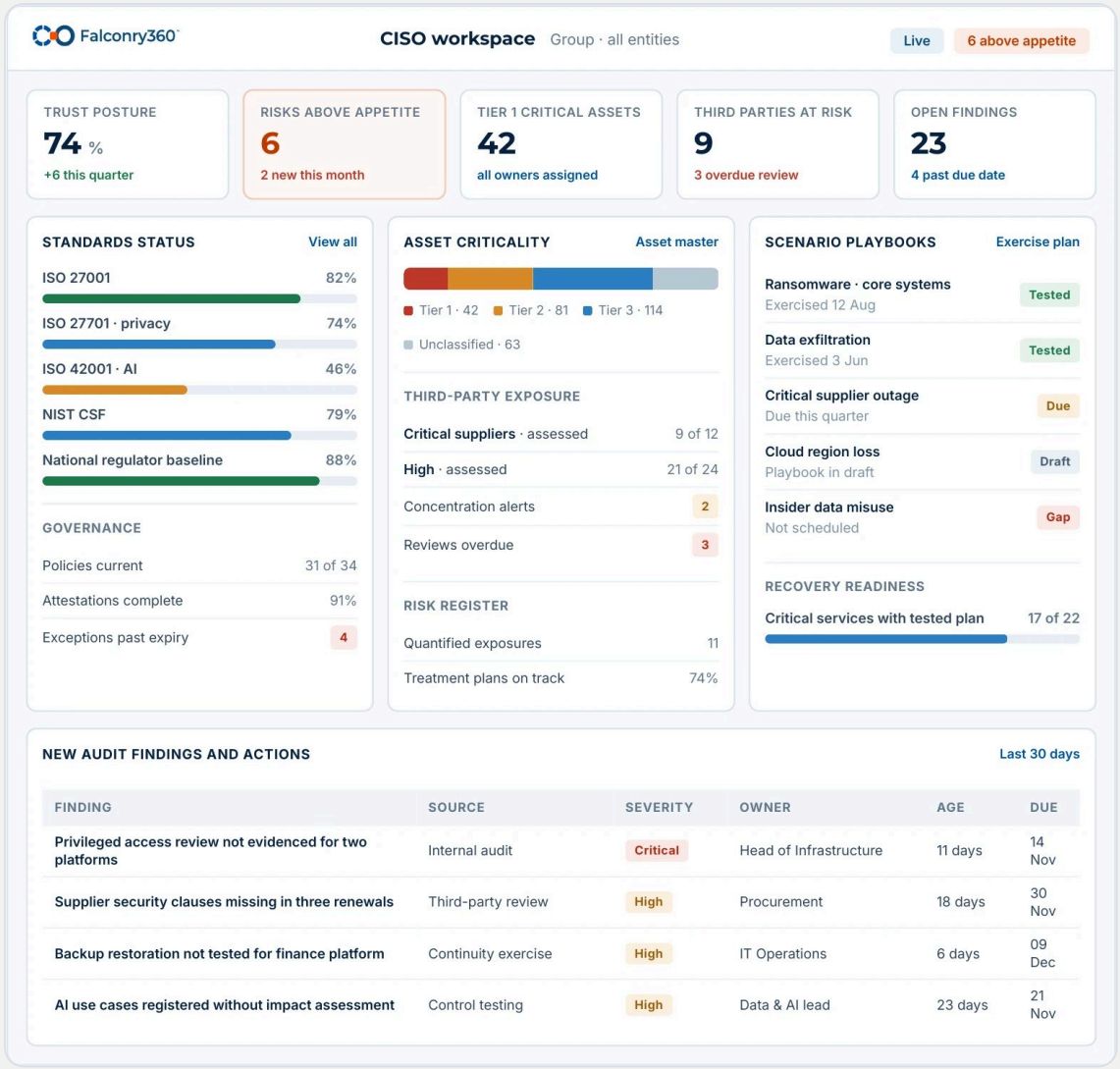
Illustrative Falconry360 view
falconrytrust.com/platform.html



# CISO workspace

Trust posture, risks above appetite, critical assets, third parties at risk and open findings.

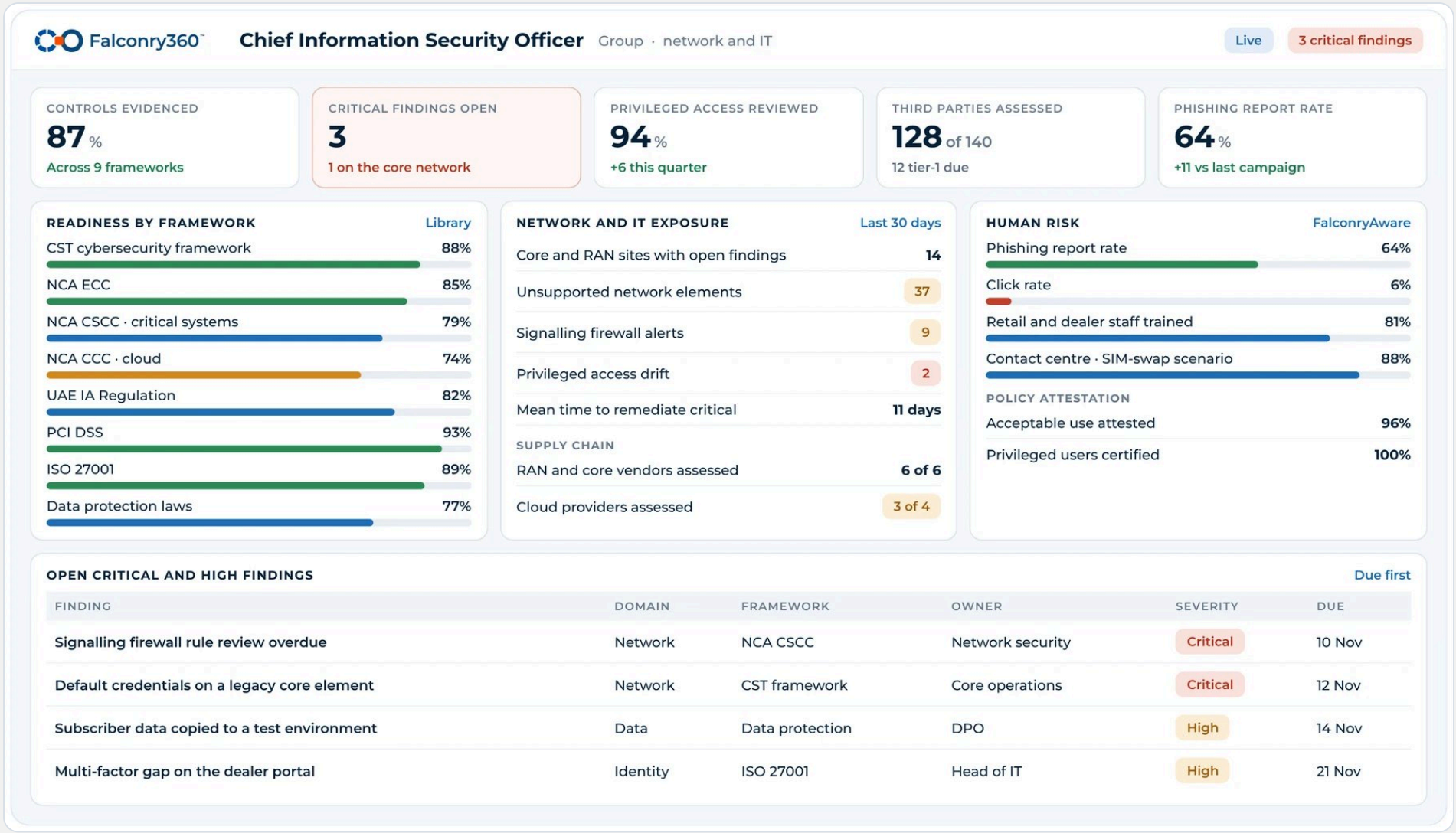
Illustrative Falconry360 view
falconrytrust.com/cyber-security.html



# CISO, telecoms group

Readiness by framework, network exposure and human risk for a network operator.

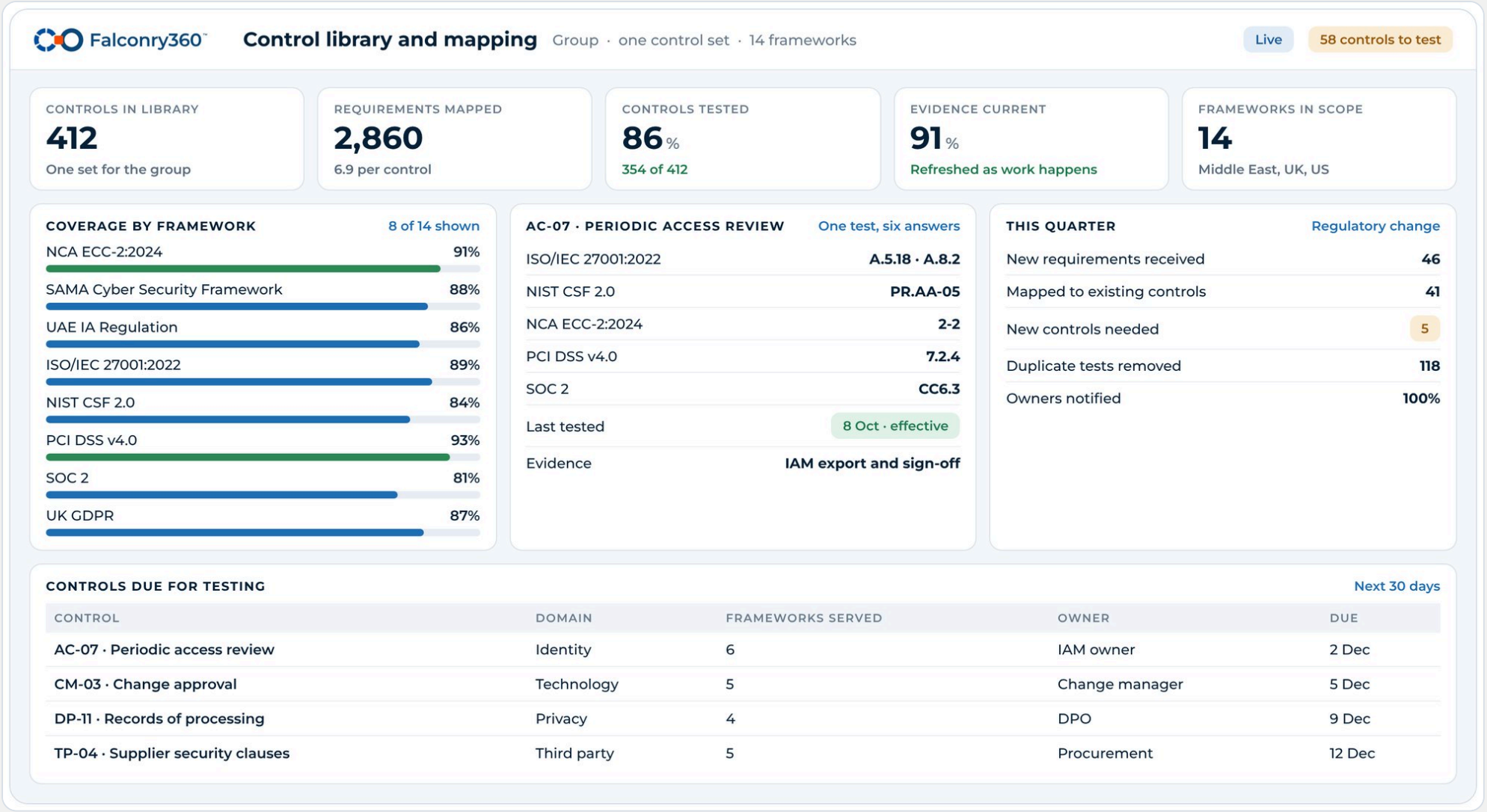
Illustrative Falconry360 view
falconrytrust.com/industries.html



# Control library and mapping

One control tested once, answering every framework that requires it.

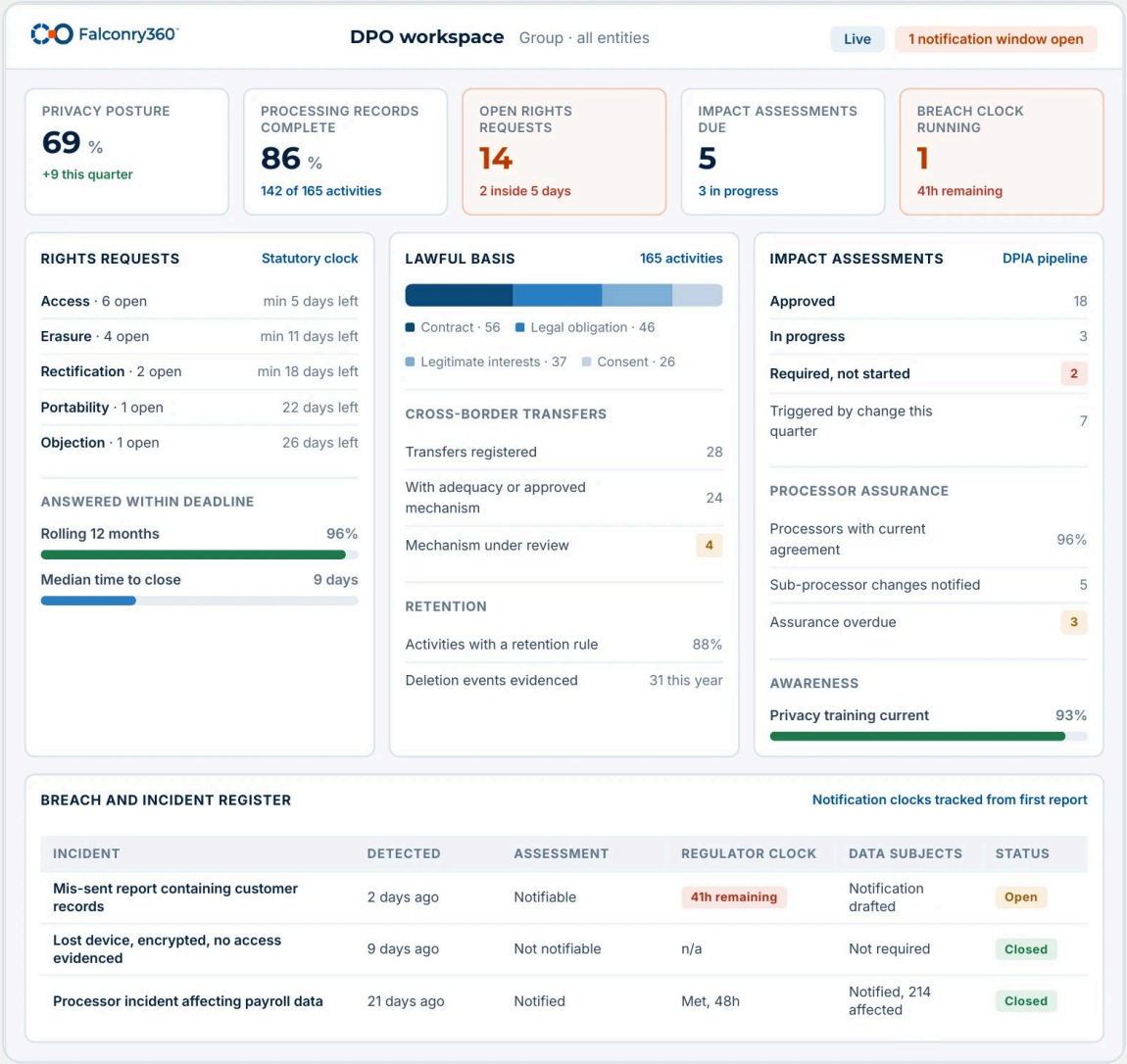
Illustrative Falconry360 view
falconrytrust.com/frameworks.html



# DPO workspace

Privacy posture, records of processing, rights requests, impact assessments and breach clocks.

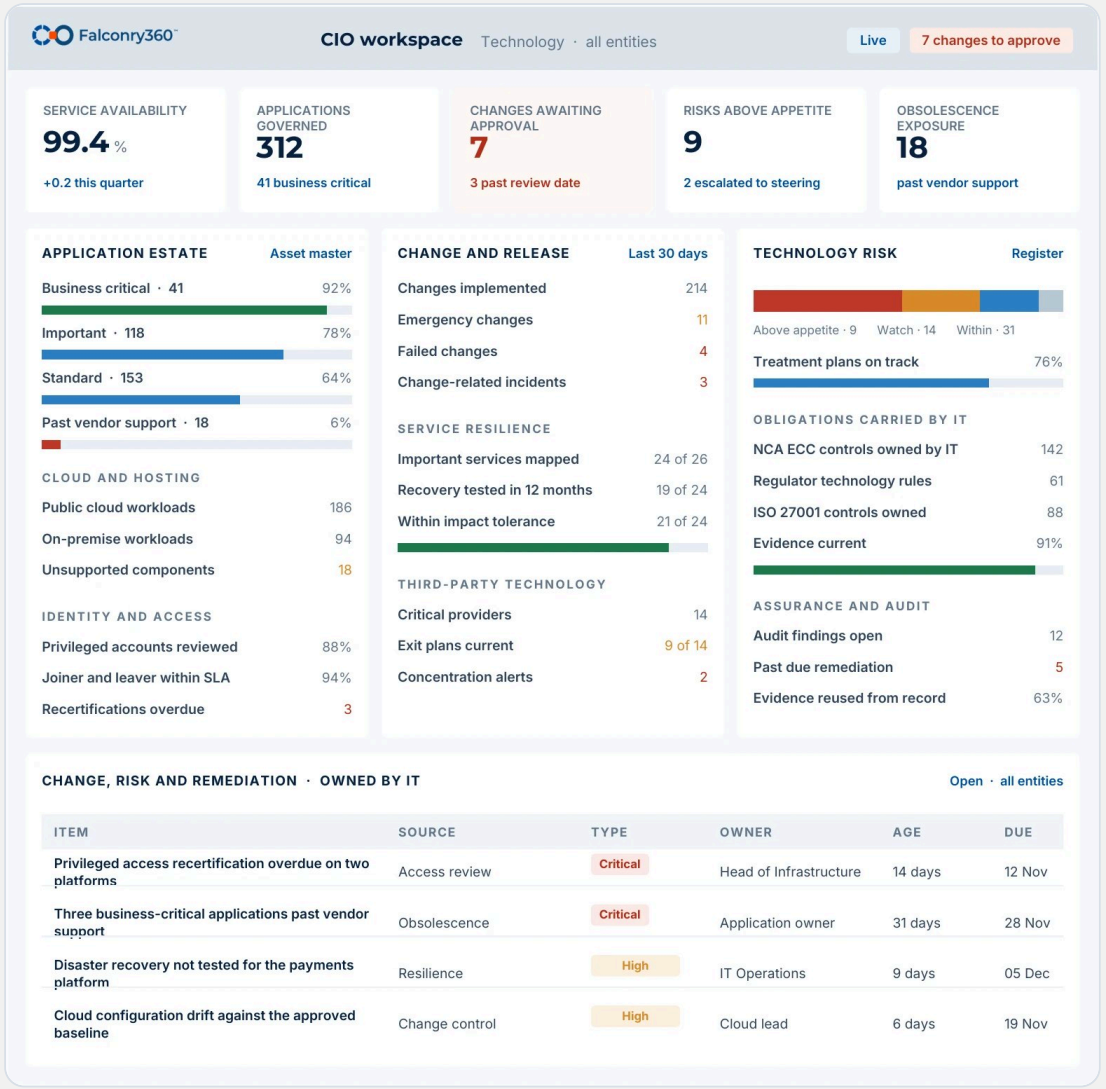
Illustrative Falconry360 view
falconrytrust.com/data-privacy.html



# CIO workspace

Service availability, application estate, change, cloud and the obligations attached to technology.

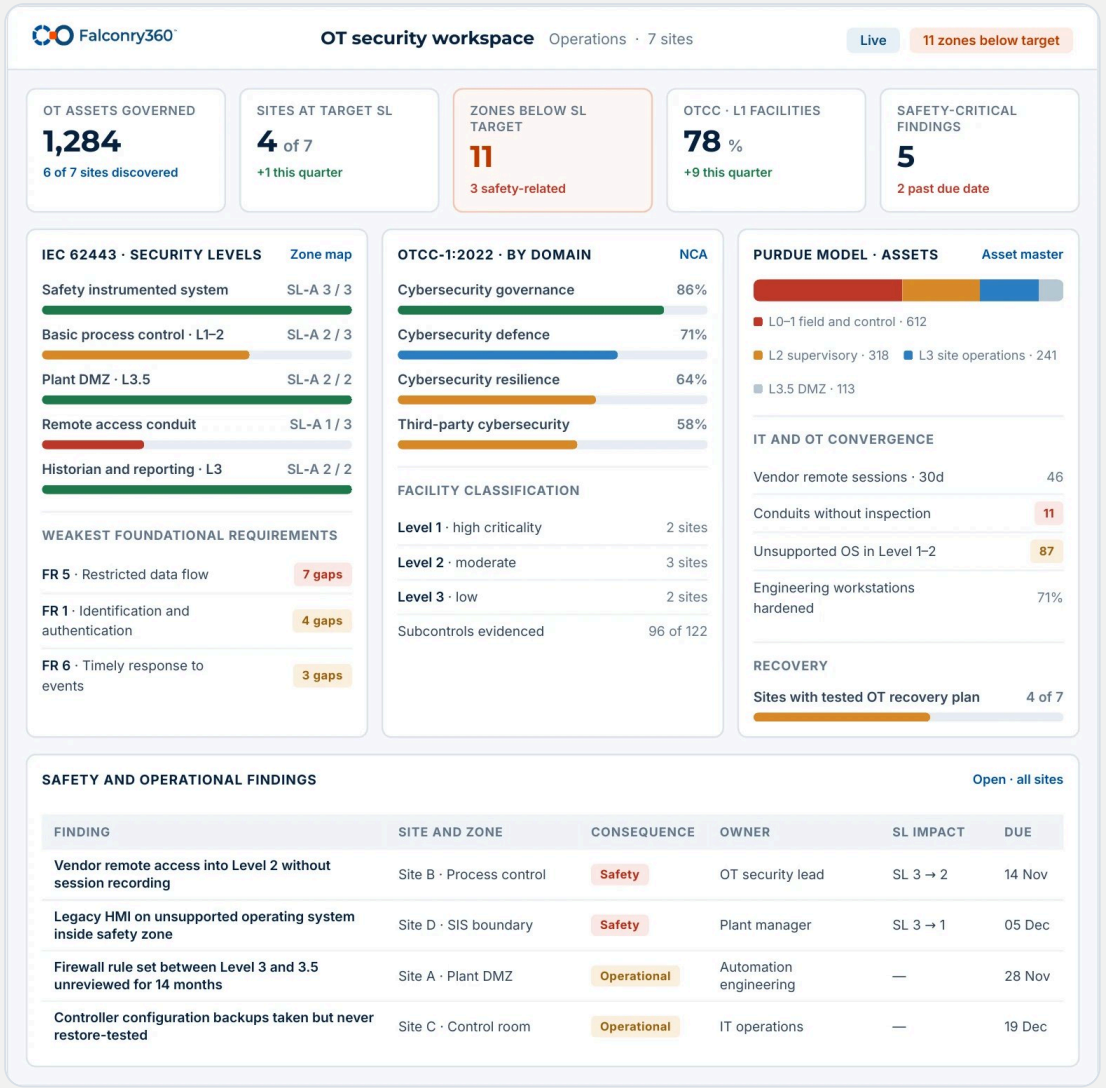
Illustrative Falconry360 view
falconrytrust.com/technology-risk.html



# OT security workspace

IEC 62443 zones, security levels against target, OTCC compliance and plant findings.

Illustrative Falconry360 view
falconrytrust.com/ot-security.html



# Cyber risk quantification

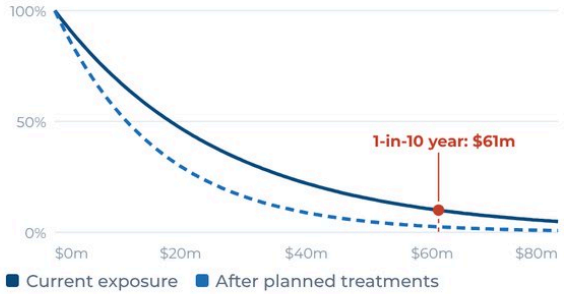
Loss exceedance, exposure by scenario and the treatments that remove the most exposure per dollar.

Illustrative Falconry360 view
falconrytrust.com/risk-quantification.html

Falconry360™ **Cyber risk quantification** Group · 12 scenarios · Open FAIR — Live — 3 above appetite

| MEAN ANNUAL EXPOSURE | 90TH PERCENTILE | ABOVE APPETITE | TREATMENT VALUE | RISK REDUCED PER DOLLAR |
|---|---|---|---|---|
| $24.6m | $61m | 3 | $9.2m | 4.6× |
| 12 loss scenarios | A 1-in-10 year loss | Threshold $4.5m per scenario | For $2.0m of spend | Across three treatments |

**LOSS EXCEEDANCE** — Probability of a loss above




**EXPOSURE BY SCENARIO** — Mean annual

| | |
|---|---|
| Ransomware with exfiltration | $9.8m |
| Cloud region loss | $6.1m |
| Critical supplier outage | $4.7m |
| Insider data theft | $2.9m |
| Eight further scenarios | $1.1m |

**TREATMENT OPTIONS** — Cost and effect

| | |
|---|---|
| Immutable backup and segmentation | −$4.9m · $0.8m |
| Multi-region failover | −$2.8m · $0.9m |
| Tested supplier exit plans | −$1.5m · $0.3m |

**CALIBRATION**

| | |
|---|---|
| Estimates calibrated by owners | 6 |
| Data sources linked to scenarios | 14 |
| Last recalibrated | 28 Oct |

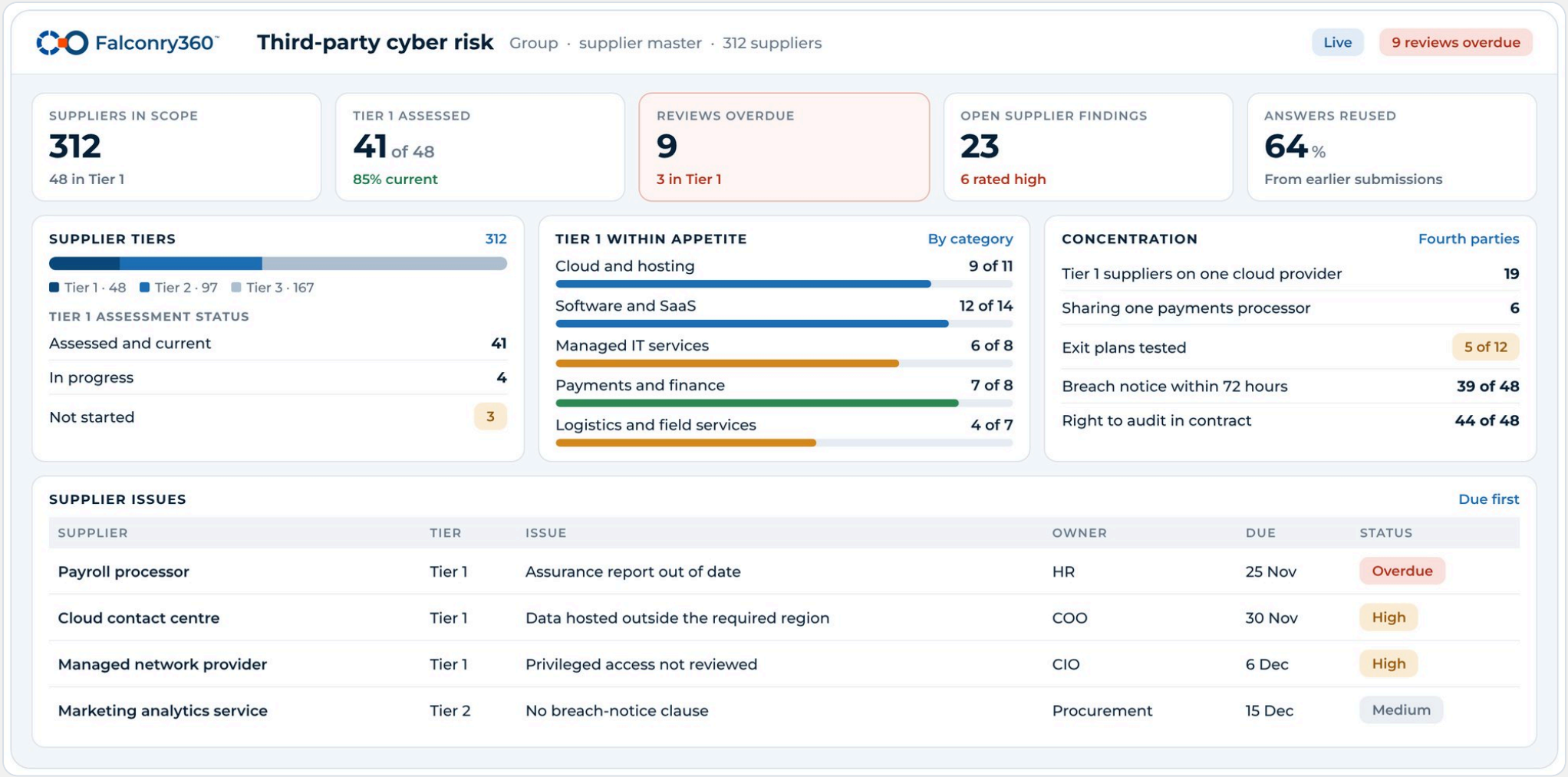
**SCENARIO REGISTER** — Ranked by mean exposure

| SCENARIO | EVENTS PER YEAR | MEAN LOSS PER EVENT | MEAN ANNUAL EXPOSURE | OWNER | APPETITE |
|---|---|---|---|---|---|
| Ransomware with data exfiltration | 0.35 | $28.0m | $9.8m | CISO | Above |
| Loss of the primary cloud region | 0.10 | $61.0m | $6.1m | CIO | Above |
| Outage at a critical supplier | 0.25 | $18.8m | $4.7m | COO | Above |
| Insider theft of customer data | 0.20 | $14.5m | $2.9m | DPO | Within |

# Third-party cyber risk

Supplier tiers, assessments, concentration and the issues due first.

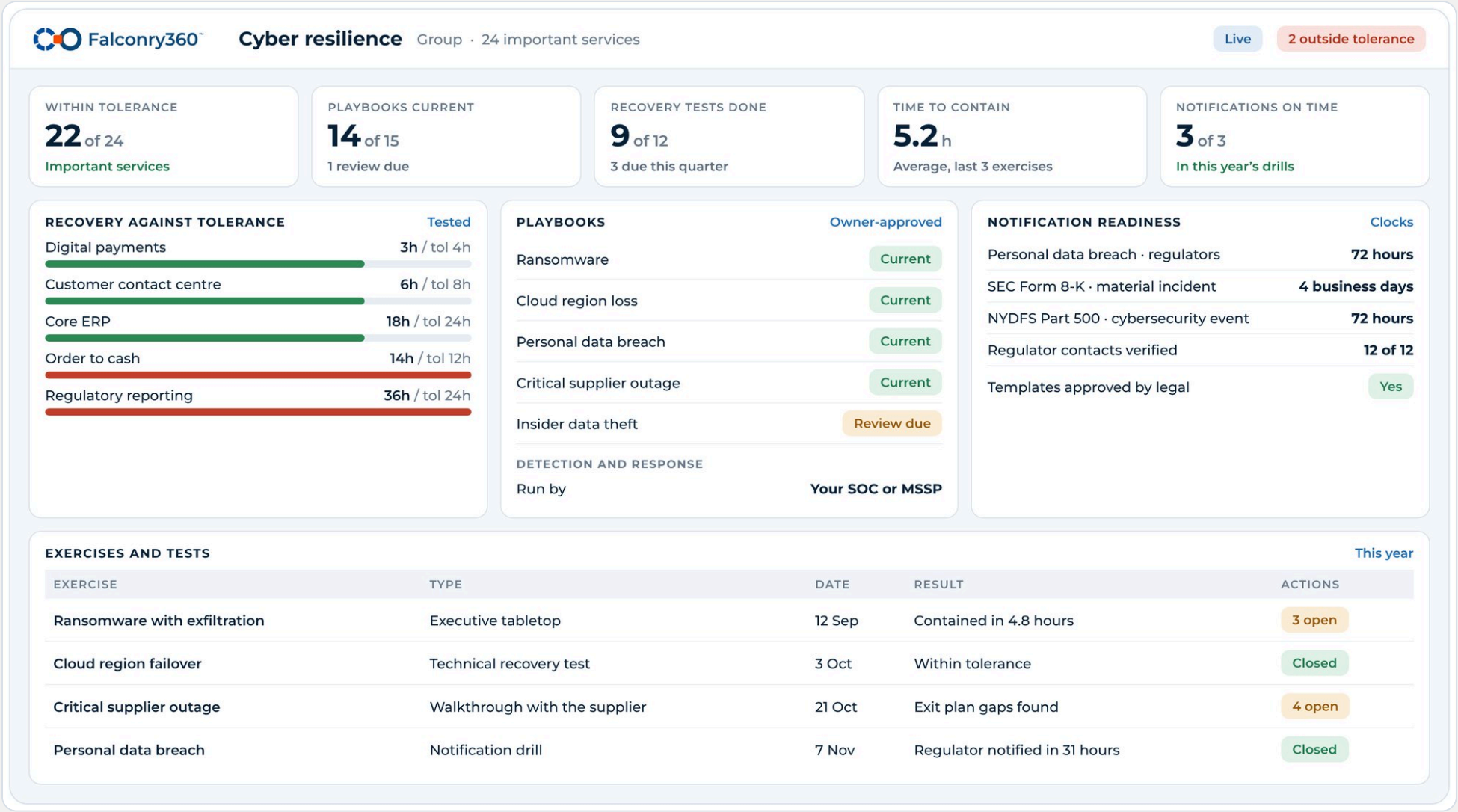
Illustrative Falconry360 view
falconrytrust.com/third-party-risk.html



# Cyber resilience

Recovery against tolerance, playbooks, notification readiness and exercises.

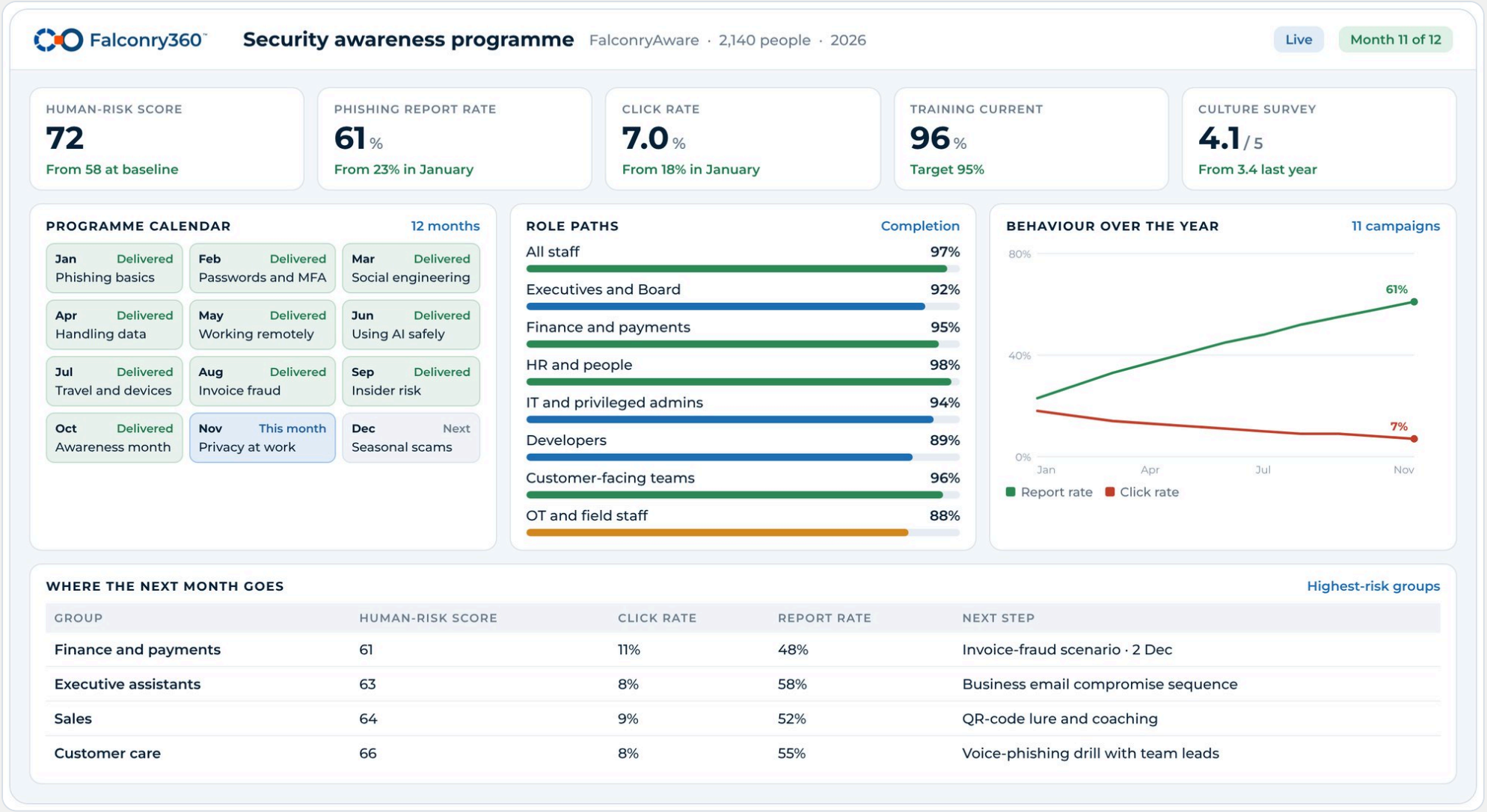
Illustrative Falconry360 view
falconrytrust.com/technology-risk.html



# Security awareness programme

The twelve-month programme, role paths and the behaviour trend across the year.

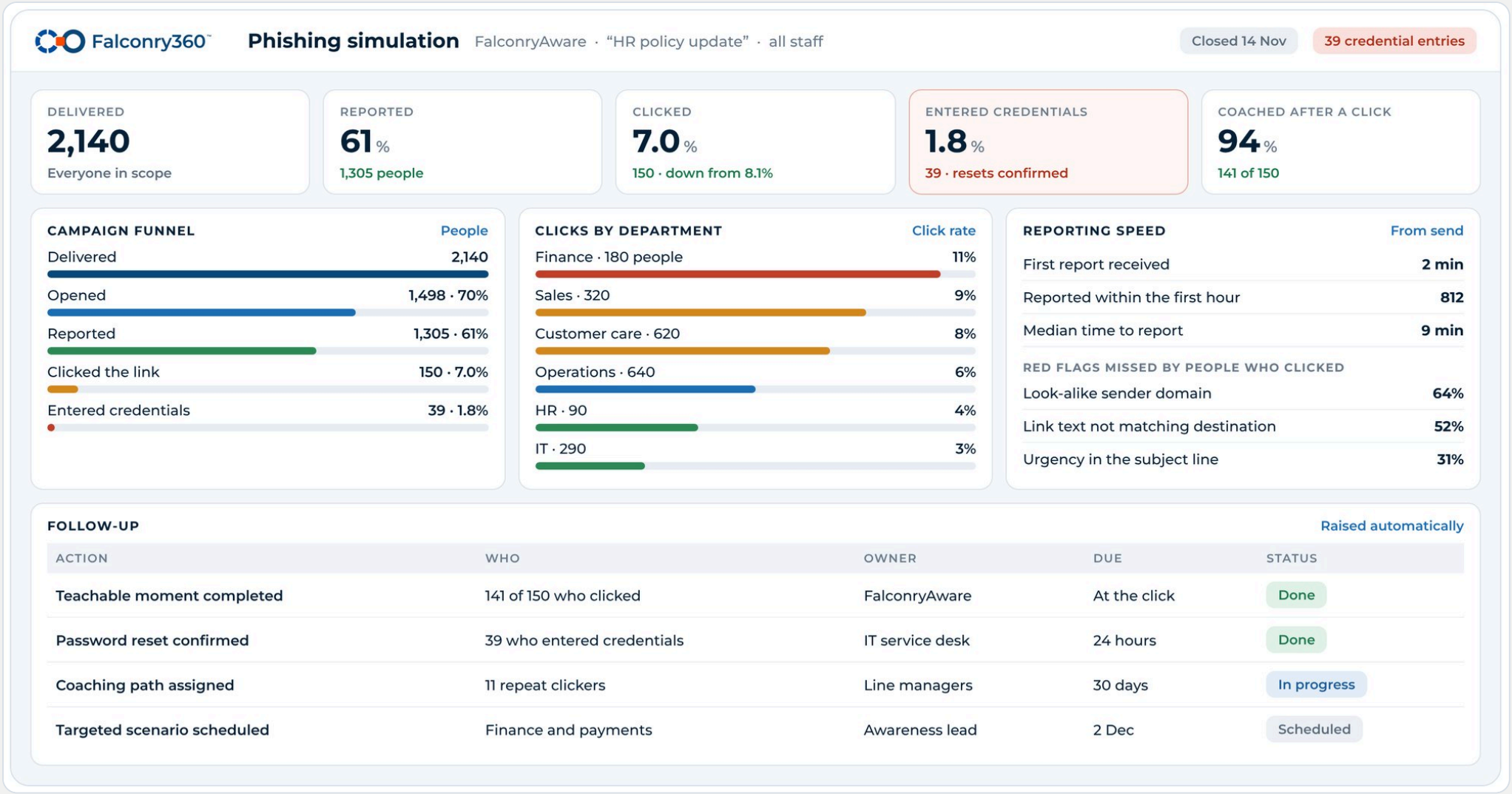
Illustrative Falconry360 view
falconrytrust.com/falconryaware.html



# Phishing simulation

One campaign from delivery to follow-up: funnel, clicks by department and reporting speed.

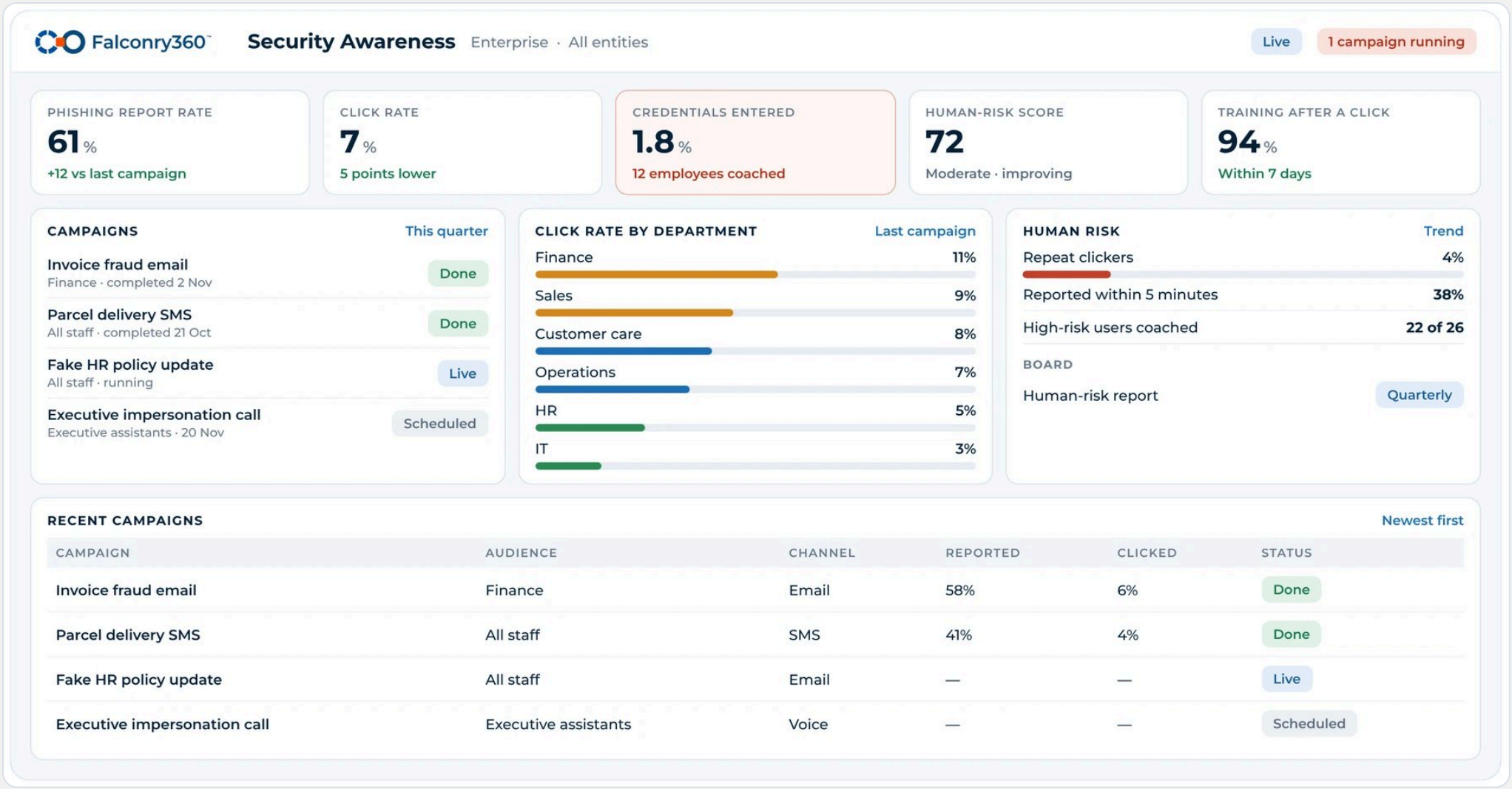
Illustrative Falconry360 view
falconrytrust.com/falconryaware.html



# Security awareness overview

Report rate, click rate, credential entries and the human-risk score in one place.

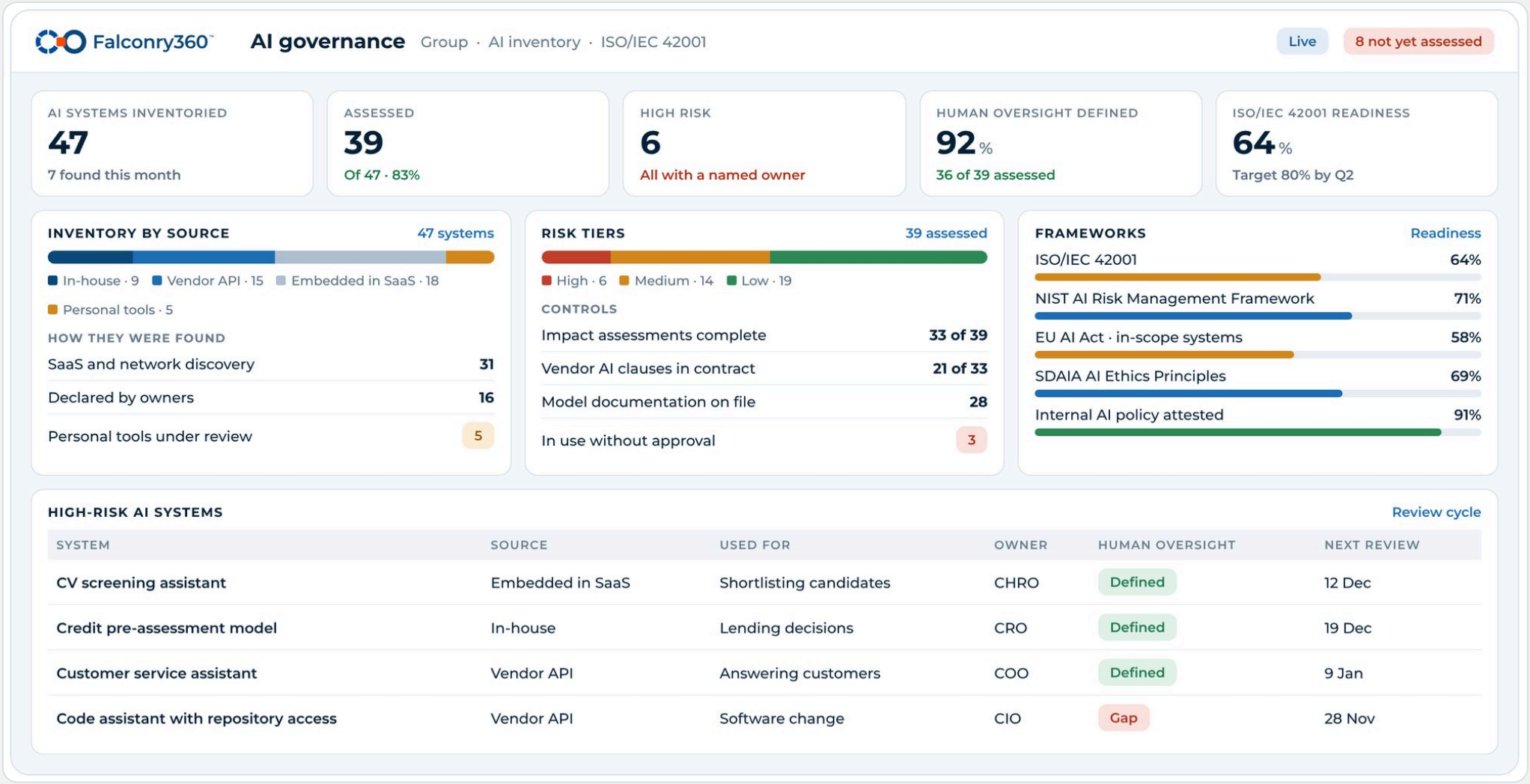
Illustrative Falconry360 view
falconrytrust.com/falconryaware.html



# AI governance

The AI inventory, risk tiers, human oversight and ISO/IEC 42001 readiness.

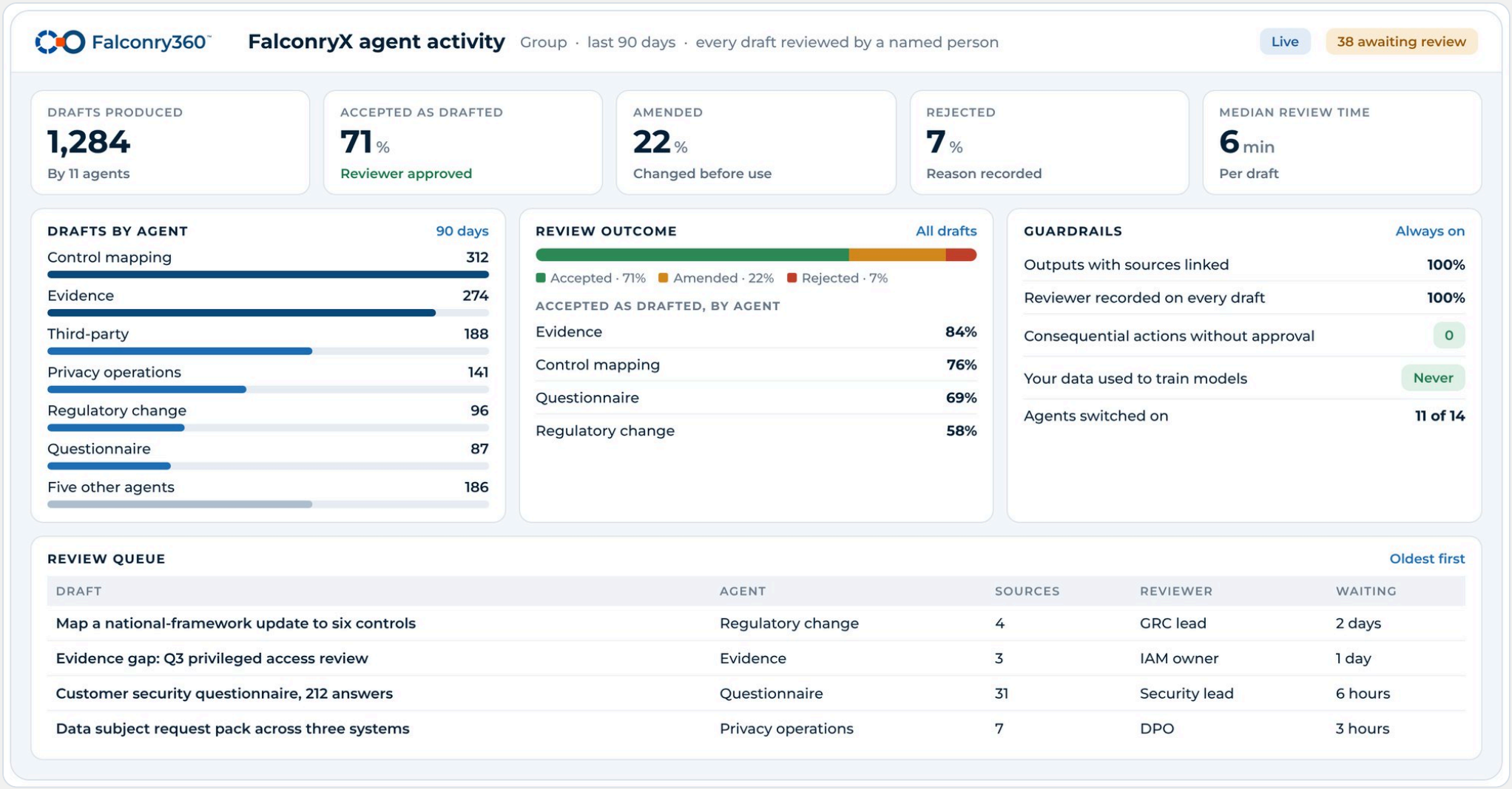
Illustrative Falconry360 view
falconrytrust.com/ai-governance.html



# FalconryX agent activity

What the agents drafted, what reviewers accepted, amended or rejected, and the review queue.

Illustrative Falconry360 view
falconrytrust.com/falconryx.html



# Managed Trust service report

Service levels, what was delivered this month and the decisions waiting on the client.

Illustrative Falconry360 view
falconrytrust.com/managed-services.html

Falconry360™ **Managed Trust service report** October 2026 · vCISO, vDPO and GRC operations — Issued 4 Nov

| SERVICE LEVELS MET | EVIDENCE REQUESTS CLOSED | RISK COMMITTEE PACK | CLIENT ACTIONS OPEN | NAMED TEAM |
|---|---|---|---|---|
| 47 of 48 | 312 | Day 3 | 9 | 4 |
| 98% this month | Median 2 days | After month end | 2 need a decision | vCISO, vDPO, GRC, AI |

**SERVICE LEVELS** — 48 measured

| | |
|---|---|
| Governance reporting | 12 of 12 |
| Control testing and evidence | 16 of 16 |
| Privacy requests answered in time | 11 of 12 |
| Supplier assessments | 8 of 8 |

**THIS MONTH** — Delivered

| | |
|---|---|
| Controls tested | 64 |
| Policies reviewed | 7 |
| Data subject requests closed | 18 |
| Supplier assessments | 8 |
| Phishing campaign | Delivered |

**NEXT MONTH** — Planned

| | |
|---|---|
| Board pack | 18 Dec |
| ISO/IEC 27001 surveillance preparation | Started |
| AI register review | Scheduled |
| Insider threat tabletop | 9 Dec |
| Awareness theme | Seasonal scams |

**DECISIONS AND ESCALATIONS** — For the client

| ITEM | RAISED BY | OWNER | SINCE | STATUS |
|---|---|---|---|---|
| Risk acceptance: legacy file transfer server | vCISO | CIO | 21 Oct | Decision needed |
| Impact assessment sign-off: customer analytics | vDPO | CMO | 28 Oct | Decision needed |
| Privileged access exceptions past expiry | GRC analyst | Head of infrastructure | 2 Oct | Escalated |
| Supplier exit plan for the contact centre | vCISO | COO | 30 Oct | In progress |

NEXT STEP

# Put a working session in the diary.

A thirty-minute session with your team, mapped to the regulators you actually answer to and grounded in your own perimeter.


EMAIL

contact@falconry360.com

WEB

falconrytrust.com



All dashboards and figures are illustrative and do not represent any client. FalconryTrust is the cyber, privacy and digital-trust proposition delivered through Falconry360, the Falconry platform. Falconry LLC is certified to ISO/IEC 27001:2022 for the Falconry360 platform and GRC advisory, training and managed services.