

90-Day HRM Deployment Playbook

A Tactical Guide to Achieving Measurable Human
Risk Reduction in 90 Days



Living Security helps organizations measure and reduce human cyber risk using AI-native Human Risk Management (HRM). This toolkit is designed to help security leaders build internal alignment, evaluate vendors, and operationalize measurable human risk reduction.

Deployment Overview

This playbook outlines how organizations can deploy Human Risk Management (HRM) within 90 days — without replacing existing infrastructure.

It is designed for:

- Security Operations leaders
- IAM and Identity teams
- Risk & GRC teams
- HRM program owners

This guide focuses on integration sequencing, early wins, automation activation, and exposure reduction milestones.

Deployment Scenarios and Considerations for Organizations Under Contract

In most environments, you can deploy HRM non-disruptively. It operates at the telemetry and orchestration layer, integrating with existing systems rather than replacing them.

Integration with the Security Stack

Mature HRM platforms provide API-driven and prebuilt integrations with:

- Identity providers (Okta, Azure AD, Active Directory)
- Email security platforms (Microsoft 365, Proofpoint, Google)
- Endpoint tools (CrowdStrike, Defender)
- Data Loss Prevention systems
- IAM and GRC platforms
- AI governance tools

This enables:

- Continuous behavioral modeling
- Context-aware intervention triggers
- Exposure duration tracking
- Bi-directional policy influence

Parallel Operation Under Existing SAT Contracts

Many organizations operate under multi-year SAT agreements. HRM platforms can run in parallel, ingesting data from:

- Existing training systems
- Phishing simulation platforms
- Identity providers
- Email security tools
- Endpoint and DLP systems

This enables immediate risk visibility and automation without terminating legacy contracts.

Quantifying Parallel Deployment Benefits

Organizations running HRM in parallel with existing SAT contracts (e.g., KnowBe4, Proofpoint) can expect measurable benefits within the first 90 days:

Timeframe	Benefit Area	Quantified Impact Example
30 days	Enhanced Visibility	Significant increase in detected human risk signals by aggregating identity, endpoint, and behavioral telemetry beyond phishing clicks.
60 days	Automation Efficiency	Meaningful reduction in manual risk scoring and intervention assignment through automated workflows.
90 days	Risk Reduction	Measurable reduction in the population of high-risk users due to targeted, behavior-driven interventions.

PROOF POINT:

“Only about 10% of organizations have adopted progressive HRM capabilities, creating a near-term advantage for teams that operationalize HRM before it becomes table stakes.”

Source: Forrester Wave™ Human Risk Management, Q3 2024 <https://www.livingsecurity.com/forrester-wave-report-2024>

30 / 60 / 90-Day Value Framework

To justify overlapping spend, focus on measurable early outcomes.

First 30 Days: Establish Visibility

- Integrate identity, email, and training telemetry
- Establish baseline human risk scoring
- Identify highest-risk 10% of users
- Quantify exposure duration across workforce

Outcome: Executive-ready visibility into human risk concentration.

60 Days: Activate Risk Reduction

- Deploy dynamic risk scoring
- Launch targeted automated interventions
- Reduce exposure duration for highest-risk cohort
- Deliver first measurable risk movement report

Outcome: Demonstrable reduction in elevated risk states.

90 Days: Demonstrate ROI

- Expand integrations to endpoint and data systems
- Automate intervention workflows
- Present board-level exposure trend reporting
- Quantify reduction in human-driven risk concentration

Outcome: Measured impact before legacy contract renewal decisions.

This parallel model converts overlapping spend into immediate risk reduction and defensible ROI.

Phased Rollout & Proof of Concept

Organizations often begin with:

- High-risk cohorts (privileged users, finance, executives)
- Specific integrations (identity + email first)
- Limited-scope pilots

This validates:

- Risk scoring accuracy
- Exposure duration measurement
- Automation workflows
- Executive reporting value

Before full enterprise deployment.

Change Management & Stakeholder Alignment

HRM initiatives succeed when stakeholders from:

- Security
- IT
- HR
- Compliance
- Procurement
- Business Units

are engaged early.

Position HRM as shared risk accountability, not a training upgrade. When human and AI risk intersect identity, data, and governance, cross-functional alignment becomes a strategic advantage.

Customization & Localization

HRM platforms should support:

- Configurable training paths
- Risk-based workflow automation
- Localization across global regions
- Regulatory alignment
- Cultural reinforcement mechanisms

Flexibility ensures adoption without sacrificing governance.

PROOF POINT:

"Forrester's HRM vendor evaluation criteria emphasize behavioral change metrics, risk-driven policy response, and external-tool behavior identification—reinforcing that HRM value depends on telemetry integration and automated action, not content alone."

Source: Forrester Wave™ Human Risk Management, Q3 2024 <https://www.livingsecurity.com/forrester-wave-report-2024>

Implementation Roadmap

With the right deployment plan, you can achieve measurable visibility in weeks, not years. It is a structured, phased rollout designed to deliver measurable value within the first 30–60 days.

Deployment typically requires configuration and integration, not infrastructure replacement.

Phase 1: Risk Baseline & Stakeholder Alignment (2–4 Weeks)

Objectives: Establish current human risk posture, formalize executive sponsorship, and define measurable success metrics aligned to business risk.

Early Wins:

- Within 2 weeks, identify the top 25 highest-risk users.
- Quantify initial human risk concentration.
- Align cross-functional stakeholders on measurable success criteria.

Outcome: Clear, defensible visibility into current human risk posture.

Phase 2: Integration & Behavioral Visibility (4–6 Weeks)

Objectives: Connect identity providers, endpoint, email, DLP, and SAT telemetry to build unified, dynamic risk profiles.

Early Wins:

- Deliver first executive risk dashboard by Week 4.
- Deliver time-to-first-risk-score in under 30 days.
- Establish measurable exposure duration across the workforce.

Phase 3: Targeted Automation & Scorecards (Begins ~Week 4; Operational by Week 6–8)

Objectives: Deploy automated, risk-based interventions and launch personalized scorecards.

Early Wins:

- Deliver first executive risk dashboard by Week 4.
- Deliver time-to-first-risk-score in under 30 days.
- Establish measurable exposure duration across the workforce.

Phase 4: Continuous Optimization (Ongoing)

Objectives: Mature the program from reactive risk management to predictive governance through AI-driven scoring refinement and expanded telemetry integration.

Milestones:

- Quarterly performance benchmarking.
- Sustained reduction in exposure duration.
- Measurable shrinkage of high-risk user concentration over time.

Time-to-Value Summary

Most organizations achieve:

- **Time to first risk score:** <30 days
- **Time to first executive dashboard:** ~30 days
- **Time to first automated intervention:** 4–6 weeks
- **Time to measurable risk movement:** 60–90 days

This phased model ensures rapid visibility, early wins, and measurable impact, without operational disruption.

PROOF POINT:

"In the Optimized stage of HRM maturity, interventions shift from broad training coverage to data-driven, targeted risk reduction, delivering measurable impact."

Source: Living Security Human Risk Management Maturity Model Ebook <https://www.livingsecurity.com/hrm-maturity-model>

