proofpoint®

EBOOK

Introducing the Proofpoint Human Risk Management Maturity Model

This guide is designed for CISOs, security awareness managers, and IT security leaders who want to move beyond checkbox compliance and build a measurable, behavior-driven approach to managing human risk.

Whether you're just starting to formalize your security awareness program or looking to mature an existing one, the framework outlined here will help you identify where you are, where you need to go, and how to get there.

The cybersecurity landscape has changed. Not because people suddenly became a risk, but because attackers have become experts at exploiting human behavior. Yet many organizations still rely on compliance-driven training and periodic awareness campaigns that measure success by completion rather than impact. These traditional approaches create the illusion of preparedness while leaving human risk largely unmanaged.

Human Risk Management (HRM) closes this gap. It's a modern, data-driven approach that identifies, prioritizes, and reduces risk caused by human behavior. Rather than assuming awareness leads to safer actions, HRM uses behavioral signals, learning science, and real-world threat data to understand how people actually behave—and to intervene in ways that measurably reduce risk.

HRM is a core pillar of the Proofpoint Human Resilience solution, which combines education, behavioral analytics, and adaptive interventions to protect organizations where attackers most frequently strike. By continuously measuring individual and organizational risk, Proofpoint enables security teams to move beyond one-size-fits-all training and focus resources where they'll have the greatest impact.

To support this vision, we're introducing the Human Risk Management Maturity Model (HRM-MM).

Figure 1. In the HRM-MM, the focus on broad compliance (center) shifts to individualized, behavior-driven interventions (outer ring) as maturity increases.

The HRM-MM defines five progressive levels of maturity, guiding organizations from baseline compliance through awareness and learning, to role-based risk mitigation and adaptive human risk management. As maturity increases, programs become more personalized, targeted, and effective at reducing real-world risk.

This guide walks through each maturity level in detail—what it involves, how it benefits organizations, and where it falls short. Together, these levels provide a practical framework for evolving from training users on key compliance needs to actively managing and reducing human risk.

Table of Contents

Level 1: Obligation

At a Glance

The level establishes a shared security baseline by ensuring all employees complete required training on core policies and regulatory obligations.

Key metric: Completion rates

Typical tools: Learning Management System (LMS), annual or biannual training modules, compliance tracking dashboards

At the core of the HRM-MM is the obligation level, which reflects a required foundation of security knowledge that all employees should have. Organizations that operate at Level 1 typically deliver training once or twice per year in a single, centralized session.

Content focuses on security compliance requirements—including broad security policies, acceptable use, data protection requirements, and regulatory obligations—and is most often delivered through a Learning Management System (LMS). Program success is primarily measured by course completion and acknowledgment, as well as fulfillment of legal, regulatory, and governance requirements.

Research shows that compliance-focused programs alone have limited impact on lasting behavior change (Lain et al., 2022; Ho et al., 2025). They often focus on ticking regulatory boxes rather than on engagement and personalized relevance. The result? Content often feels generic and disconnected from daily tasks, leading employees to rush through training without truly retaining information.

When implemented effectively, compliance training can produce short-term improvements in specific behaviors. For example, anti-phishing training can boost phishing detection by about 20% (Marshall, Sturman, & Auton, 2024, p. 11). However, this change in behavior often lasts only a few weeks at a time (Reinheimer et al., 2020, p. 267). Without reinforcement or behavioral measurement, organizations lack visibility into ongoing human risk and are unable to actively manage it.

Why this level matters

Obligatory training establishes a minimum-security baseline, ensures regulatory coverage, and provides a necessary foundation for more advanced human risk management efforts. However, on its own, it documents training activity rather than reducing risk.

How to progress to Level 2

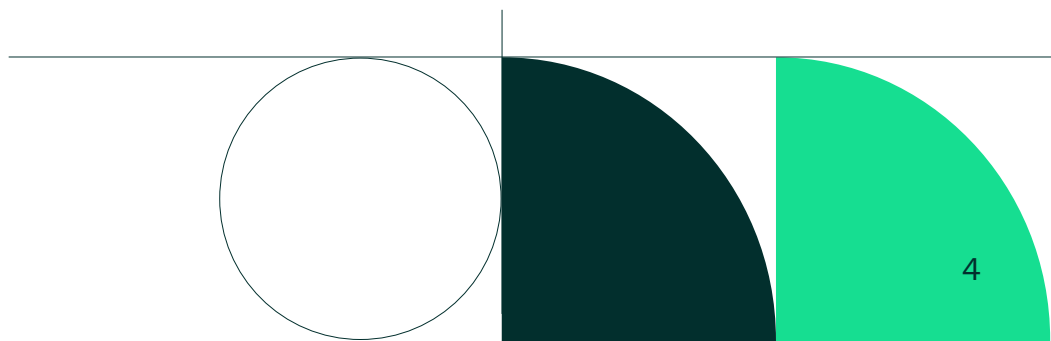
To move beyond this core level, organizations must shift from annual training events to continuous awareness. This includes introducing regular security messaging, reinforcing key behaviors throughout the year, and beginning to measure engagement, not just completion. These steps lay the groundwork for building awareness that supports stronger learning and behavior change.

Self-assessment

Check all that apply:

- ○ We deliver mandatory security training at least annually.
- ○ Training content is primarily policy- or compliance-focused.
- ○ Success is measured by completion rates.
- ○ All users receive the same training.

If most boxes are checked: You are operating at Level 1.



Level 2: Observation

At a Glance

This level extends compliance through continuous, year-round messaging that keeps security top of mind across the organization.

Key metric: Engagement (opens, clicks, participation)

Typical tools: Email campaigns, intranet banners, digital signage, posters, screensavers, looping videos in shared spaces

Level 2 focuses on observation. That means driving awareness through active messaging or passive cues embedded in daily workflows.

Digital awareness assets are especially effective for desk-based employees, enabling security messaging to be delivered in the flow of daily work through email, intranet, collaboration tools, or screensavers. Physical materials, such as posters or looping videos in shared spaces, play a critical role in reaching employees with limited access to computers, including frontline, healthcare, retail, and operational staff.

Awareness initiatives primarily rely on repetition and cueing to enhance recognition and recall (a principle well-established in learning science). By increasing message frequency, organizations can modestly reduce forgetting and improve initial threat recognition. Studies show that awareness campaigns can lead to small but measurable reductions in human risk—typically in the range of 4% to 8%—when compared to compliance-only programs (Reinheimer et al., 2020; Marshall, Sturman, & Auton, 2024).[1]

However, awareness alone has limitations. Exposure does not equate to understanding, and recognition does not reliably translate into behavior change. Because awareness content is broad and broadcast-based, it lacks personalization and does not assess learning, reinforce skills, or measure behavioral outcomes. As a result, improvements tend to plateau quickly, and risky behaviors persist.

Why this level matters

Security awareness extends the impact of compliance training by increasing visibility, recall, and early threat recognition. It creates a necessary bridge between policy education and meaningful learning.

How to progress to Level 3

To achieve lasting impact, organizations must evolve from activities that depend on observation to opportunities for learning reinforcement that test understanding, strengthen memory, and measure improvement over time. This shift enables organizations to move from exposure-based metrics to learning-driven outcomes.

Self-assessment

Check all that apply:

- ◯ We run awareness campaigns throughout the year.
- ◯ We use posters, emails, videos, or newsletters.
- ◯ We track engagement (opens, clicks, participation).
- ◯ Awareness is largely broadcast and not personalized.

If most boxes are checked: You are operating at Level 2.

1. Based on empirical research across cybersecurity, public health, and safety domains, posters and similar awareness materials are associated with modest but measurable risk reduction, typically estimated at 4% to 8%. Cybersecurity-specific evidence is largely indirect. However, VanBruggen (2014) found that 5.61% of participants who received an awareness postcard installed antivirus software, aligning with this estimated range (p. 138).

Level 3: Knowledge Reinforcement

At a Glance

This level builds lasting knowledge through short, frequent lessons and active testing that reinforce concepts before they fade.

Key metric: Knowledge retention over time

Typical tools: Microlearning platforms, phishing simulations, knowledge assessments, spaced repetition systems

Knowledge reinforcement enhances compliance and awareness programs by building security understanding through repeated learning, strengthening retention, and driving lasting behavior change. Instead of a single annual training, organizations at Level 3 use monthly or quarterly training to ensure employees regularly build, test, and refresh their security knowledge.

A core approach at this stage is microlearning, which delivers short, focused lessons that reinforce a single concept or behavior at a time. Learning science shows that people quickly forget information from long, infrequent sessions, while spaced, bite-sized instruction significantly improves retention and recall. Microlearning reinforces key concepts before they fade, making security education continuous and aligned with how adults learn and apply knowledge.

Knowledge reinforcement is most effective when microlearning is paired with active reinforcement methods, such as knowledge assessments and phishing simulations. Quizzes and short assessments validate understanding and reveal knowledge gaps, while simulations allow employees to practice identifying and responding to threats in realistic scenarios. These techniques move reinforcement beyond passive exposure and help translate knowledge into more consistent behavior.

When layered on top of compliance and awareness programs, microlearning and assessments have been shown to increase engagement and knowledge retention by 18% to 22% (Mohammed et al., 2018; Senandheera, et al., 2024). While this represents a meaningful improvement, programs at this stage typically remain generalized, limiting their ability to address role-specific risks or prioritize high-risk behaviors. [2]

Why this level matters

Knowledge reinforcement establishes continuous learning, improves retention, and builds confidence. It creates the foundation needed to influence behavior more consistently over time.

How to progress to Level 4

To move from learning to risk reduction, organizations must align reinforcement to job roles and real-world exposure, using behavioral signals to tailor training and prioritize the highest-risk users and behaviors.

Self-assessment

Check all that apply:

- ◯ We use short, frequent training or microlearning.
- ◯ We assess knowledge using quizzes or simulations.
- ◯ We track improvement over time, not just completion.
- ◯ We identify common knowledge gaps.

If most boxes are checked: You are operating at Level 3.

2. For a detailed description of the effectiveness of microlearning, review our Cybersecurity Education: A Best Practices Guide, which can be found in the ZenGuide Global Library.

Level 4: Risk Mitigation

At a Glance

This level aligns training to specific roles and real threats, so security guidance reflects what employees actually encounter in their jobs.

Key metric: Behavioral change by role

Typical tools: Role-based learning paths, threat-specific simulations, department-level risk reporting, targeted content libraries

As security programs mature, the focus shifts from general learning to reducing real-world risk by aligning training with the threats employees actually face. At Level 4, organizations move beyond one-size-fits-all microlearning and adopt role- and threat-specific reinforcement, ensuring education reflects both job responsibilities and likely attack vectors.

Training becomes more relevant when it's tailored to individuals rather than when it provides the same guidance to everyone. Finance teams receive targeted instruction on business email compromise (BEC), developers engage with secure-coding scenarios, and HR teams focus on protecting sensitive personnel data. By aligning learning with daily tasks and real threat exposure, training feels immediately useful. As a result, engagement is higher, which increases the likelihood that employees apply what they learn when it matters most.

Research consistently shows that personalized training is more effective than one-size-fits-all approaches. Large-scale reviews of digital learning studies have found that tailoring content to learners' roles and needs produces measurable improvements in outcomes, ranging from modest to significant increases (Lin, Lin, Zhang, & Ginns, 2024; Dwivedi, 2024). In practical terms, this translates to an estimated 9% to 15% reduction in risk.[3]

However, despite its advantages, role-based risk mitigation still has limitations. While training is tailored at the group level, individuals within the same role often receive identical content regardless of their personal behaviors, past incidents, or current risk signals. This approach improves relevance but remains static, limiting the ability to respond to changing risk conditions or intervene precisely when an individual is most vulnerable. As a result, opportunities to mitigate risk in real-time remain unrealized.

Why this level matters

Role-based risk mitigation marks the transition from learning to behavior change by focusing effort where threats are most likely to occur. It delivers measurable reductions in risk for high-exposure functions.

How to progress to Level 5

To go beyond role-based mitigation, organizations need to include individual behavioral signals and adapt interventions in real-time for personalized risk management based on actual user behavior.

Self-assessment

Check all that apply:

- ◯ Training is tailored by role or function.
- ◯ We measure risky behavior by department or role.
- ◯ We focus training on relevant threats.
- ◯ We track time-to-report and repeat risky actions.

If most boxes are checked: You are operating at Level 4.

3. We use the Binomial Effect Size Display (BESD) method for converting an effect size (Cohen's *d*) into a percent reduction in risk.

Level 5: Human-Risk Management

At a Glance

This level uses behavioral intelligence to continuously assess individual risk and deliver adaptive interventions at the moment they matter most.

Key metric: Individual risk reduction

Typical tools: Behavioral analytics platforms, dynamic risk scoring, real-time nudges, automated micro-interventions, privacy and governance controls

Level 5 focuses on Human Risk Management. This level represents the most mature stage of security awareness evolution, shifting from training programs to active, behavior-driven risk management. It's here that organizations move beyond role-based learning and use behavioral intelligence—derived from real user actions such as phishing clicks, reporting behavior, password hygiene, and policy violations—to continuously assess and prioritize human risk.

These signals are used to build dynamic risk profiles that reflect how people actually behave. This, in turn, enables targeted nudges, micro-interventions, and just-in-time guidance to be delivered precisely when risky behavior occurs. As a result, learning and correction happen at the moment of risk.

This approach is grounded in behavioral science. The Fogg Behavior Model demonstrates that timely prompts significantly influence decision-making by activating motivation and ability at the right moment (Fogg, 2009). Meta-analyses of behavioral nudges show improvements in safer decision-making ranging from 1.4% to 8.7% (DellaVigna & Linos, 2022). When applied to cybersecurity, aligning interventions to real behavior and risk exposure can reduce human error by up to 22%, making this the most effective stage of the maturity model.[4]

Despite its effectiveness, Human Risk Management introduces new considerations. Implementing behavior-driven programs requires investment in technology, data integration, and analytics, as well as thoughtful governance around privacy, transparency, and ethics. Additionally, adaptive interventions must remain grounded in foundational training and a strong security culture to ensure employees understand why behaviors matter—not just when they are corrected.

Why this level matters

Human Risk Management enables organizations to move from reactive training to proactive risk reduction. It delivers measurable improvements by addressing risk where and when it actually occurs.

Sustaining This Level

Organizations at this stage focus on scaling automation, refining risk models, strengthening privacy controls, and continuously improving interventions to ensure human risk reduction remains adaptive, ethical, and effective.

Self-assessment

Check all that apply:

- ◯ We measure human risk at the individual level.
- ◯ Interventions adapt based on user behavior.
- ◯ We track risk trends over time.
- ◯ Success is defined by reduced risk, not training volume.

If most boxes are checked: You are operating at Level 5.

4. Evaluations of the effectiveness of intelligent tutoring systems, which capture and respond to human behavior, are estimated to be around 22% (VanLehn, 2011).

Conclusion

Human-caused risk is not a secondary concern in cybersecurity. It's one of the primary drivers of incidents. While most organizations recognize this reality, many security awareness programs remain rooted in compliance because compliance defines what must be protected. Far from being irrelevant, compliance establishes the baseline of what matters most to the organization. That's precisely why it serves as the foundation of an effective Human Risk Management program.

The Proofpoint Human Risk Management Maturity Model (HRM-MM), a core component of Proofpoint Human Resilience, is designed to help organizations build on that foundation—layer by layer—rather than move past it. The framework is grounded in an extensive literature review spanning cybersecurity, learning science, behavioral psychology, and risk management. Its core insight is clear: awareness alone is not enough. Lasting risk reduction requires reinforcement, personalization, and interventions that align to how people actually behave.

Each maturity level in the HRM-MM deliberately strengthens the one before it. Progression does not mean abandoning earlier stages; it means integrating and maturing them. As organizations advance, compliance remains intact while measurement evolves from activity-based reporting to behavior- and outcome-driven insights, providing security leaders with a clearer, more actionable understanding of risk.

By strengthening the foundation at every stage of the HRM-MM, organizations can confidently evolve from compliance to behavioral risk management. This ensures they build lasting human resilience that's designed to adapt as threats and organizational priorities change.

HRM Maturity Model at a Glance

Proofpoint Human Resilience enables organizations to transform compliance from a checkbox into a cornerstone, supporting a metrics-driven, risk-based Human Risk Management program.

The following table summarizes each maturity level, its primary activity, estimated risk reduction, key limitation, and the metric that defines success at that stage.

Level	Key activity	Estimated Risk Reduction	Primary limitation	Key metric
Level 1: Obligation	Annual compliance training via LMS	~20% (short-term phishing detection)	Improvements fade within weeks; no ongoing measurement	Completion rates
Level 2: Observation	Year-round awareness messaging (posters, emails, videos)	4% to 8%	Exposure alone does not change behavior; gains plateau quickly	Engagement (opens, clicks)
Level 3: Reinforcement	Microlearning, quizzes, phishing simulations	18% to 22%	Content remains generalized; cannot address role-specific risk	Knowledge retention over time
Level 4: Risk Mitigation	Role- and threat-specific training	9% to 15%	Static at the group level; cannot adapt to individual behavior	Behavioral change by role
Level 5: Human Risk Management	Behavioral intelligence, real-time nudges, adaptive interventions	Up to 22%	Requires investment in technology, analytics, and governance	Individual risk reduction

Next Steps

To support this journey, Proofpoint Human Resilience solution also offers its ZenGuide customers a more detailed Human Risk Management evaluation tool that's designed to assess maturity with greater precision.

This assessment goes beyond high-level categorization by incorporating behavioral signals, measurement practices, and outcome-based metrics, helping organizations identify gaps, prioritize next steps, and track progress over time.

To learn more, contact your Proofpoint representative.

Appendix: Complete Self-Assessment

Use the checklist below to evaluate your organization's security awareness maturity across all five levels. Check every statement that applies, then identify the highest level where most boxes are checked. That's your current maturity level.

Level 1: Obligation

- ○ We deliver mandatory security training at least annually.
- ○ Training content is primarily policy- or compliance-focused.
- ○ Success is measured by completion rates.
- ○ All users receive the same training.

Level 2: Observation

- ○ We run awareness campaigns throughout the year.
- ○ We use posters, emails, videos, or newsletters.
- ○ We track engagement (opens, clicks, participation).
- ○ Awareness is largely broadcast and not personalized.

Level 3: Knowledge Reinforcement

- ○ We use short, frequent training or microlearning.
- ○ We assess knowledge using quizzes or simulations.
- ○ We track improvement over time, not just completion.
- ○ We identify common knowledge gaps.

Level 4: Risk Mitigation

- ○ Training is tailored by role or function.
- ○ We measure risky behavior by department or role.
- ○ We focus training on relevant threats.
- ○ We track time-to-report and repeat risky actions.

Level 5: Human Risk Management

- ○ We measure human risk at the individual level.
- ○ Interventions adapt based on user behavior.
- ○ We track risk trends over time.
- ○ Success is defined by reduced risk, not training volume.

Your highest level where most boxes are checked represents your current maturity stage. Review the corresponding section in this guide for specific recommendations on how to progress to the next level.

DISCOVER THE PROOFPOINT PLATFORM →