

## Meet AIDA: The KnowBe4 Approach to Human Risk Management



# Meet AIDA: The KnowBe4 Approach to Human Risk Management

## Table of Contents

<b>Introduction</b> .....	3
Let's Talk About AIDA.....	3
<b>The First Four Agents of AIDA</b> .....	4
Automated Training Agent.....	5
Template Generation Agent.....	6
Knowledge Refresher Agent.....	7
Policy Quiz Agent.....	8
<b>Looking Ahead</b> .....	9
<b>The Upshot</b> .....	9

# Introduction

The rise of AI-powered cyber attacks is making every infosec professional take notice. According to industry research, over 95% of cybersecurity professionals believe AI-generated content makes phishing detection more challenging.

This technological advancement in the hands of bad actors has created a new breed of highly convincing social engineering attacks that generic, one-size-fits-all security awareness training (SAT) struggles to combat.

It's time to fight AI with AI. Meet KnowBe4 AIDA – Artificial Intelligence Defense Agents. AIDA is a suite of AI-powered agents that up-levels your approach to human risk management (HRM) by leveraging multiple AI technologies to create personalized, adaptive and highly effective user training that actually changes behavior.

In this whitepaper, we'll discuss how each of the first four AIDA agents can help improve your HRM strategy and explore use cases.

## Let's Talk About AIDA

AIDA is a comprehensive AI-native suite of agents that revolutionize how organizations approach SAT. By leveraging AI, AIDA delivers hyper-personalized, efficient and adaptive training that reduces organizational risk and drives lasting behavioral change.

Unlike other old-school SAT products, KnowBe4 AIDA continuously learns and adapts to your organization's unique needs, ensuring maximum impact and ROI for your security awareness efforts. One example: by reducing the time it takes your admins to create training content from an average of seven days to mere seconds, AIDA frees up your security team's time dramatically.

We'll go into more detail for each of the first four AIDA features later in this whitepaper, but here is an overview:



**Automated Training Agent:** Uses AI with 316 indicators influencing 37 factors across seven knowledge areas to analyze your users' learning history, job role, risk score, behavior patterns and even languages so AIDA can automatically assign the most relevant and engaging content. This ensures that every one of your users, regardless of position or location, receives training tailored to their specific needs and learning style. This feature helps maximize retention and real-world application of your security best practices.



**Template Generation Agent:** Leveraging generative AI, AIDA creates highly realistic phishing templates that can mirror current attack vectors. Social Engineering Indicators, or red flags, are based upon the [NIST Phish Scale Framework](#).



**Knowledge Refresher Agent:** AIDA delivers bite-sized knowledge refreshers at optimal intervals, ensuring your users actually apply critical security concepts.



**Policy Quiz Agent:** AIDA generates intelligent quizzes based on your organization's specific security and compliance policies. This ensures your users not only acknowledge, but truly understand the guidelines they're expected to follow.

## The Human Risk Management Connection

HRM is now the primary way to address the ongoing need for strong security cultures in organizations of all sizes. The concept focuses on more than just SAT delivered at regular intervals. The goal is a positive security culture through three primary tactics:

- 1 Quantifying human risk through detecting and measuring human behaviors
- 2 Using these measurements to deploy relevant, tailored training content
- 3 Establishing recurring educational knowledge refreshers to ensure users know how to protect themselves against the most prevalent and impactful cyber risk

Generic SAT in the market is no longer effective in your complex work environment. Once-per-year training events don't cut it. Plus, users' schedules are getting busier, so the training that is delivered needs to make the most of their time. Adopting an HRM strategy empowers you to deliver relevant, engaging content that changes user behavior and resonates across different roles, departments and even languages. AIDA is the backbone of this approach.

Next we'll dive into the first four AIDA features that make this all possible, and talk about what's to come.



## The First Four Agents of AIDA

Before we talk about these four agents, let's explore a key KnowBe4 feature that underpins them all: KnowBe4's SmartRisk Agent™. This capability provides actionable data and metrics, called the Risk Score, to help you better understand your organization's security strengths and weaknesses.

[SmartRisk Agent](#) leverages end user behavioral data from across KnowBe4's products to help measure cyber risk in humans. This agent's multidimensional Risk Scores are designed to make it easier for you to see potential problems at the user, group and organizational levels. You'll get more comprehensive insights the more KnowBe4 products you use.

Here's what each of the first four agents can do:



## Automated Training Agent

### What It Does

The Automated Training Agent analyzes multiple data points, including [Risk Scores](#), phishing test results and individual learning preferences, to create a tailored training experience for each user. It excels at identifying knowledge gaps and addressing them with targeted learning modules pulled from [KnowBe4's massive ModStore content library](#).

### How To Use It

Configure the agent to align with your organization's specific needs, such as setting enrollment criteria, completion timeframes, and notification preferences, all from the KnowBe4 console. The agent's Test Mode lets you preview the training recommendations before full deployment, ensuring you're comfortable with the automated assignments.

Need to track training performance? Access tracking metrics such as assignment completion rates and survey results to gauge the effectiveness of your training program.

### Use Cases

***Tackling Phishing Vulnerabilities*** - Take user responses or failure to specific simulated phishing tests and automatically assign training that teaches users about those pinpointed phishing strategies and tactics before they see them in the wild.

***Onboarding New Employees*** - Assess new hire Risk Score and suggest SAT tailored to their existing knowledge base by using targeted Smart Groups.



## Template Generation Agent

### What It Does

The Phishing Template Generator produces highly convincing phishing emails tailored to your organization's specific needs and risk profile using the power of baked-in generative AI. It can craft diverse, multi-lingual phishing scenarios with varying difficulty levels, tones and attack vectors, ensuring that your users are prepared for the full spectrum of potential threats they might encounter in the wild.

### How To Use It

Adjustments including language, locale, tone and desired attack vector are all at your fingertips. Fine-tune simulated phishing email difficulty by selecting specific [Social Engineering Indicators \(SEIs\)](#) or choosing a predefined difficulty level. Once generated, templates can be previewed, edited and saved for future use, saving you valuable time in creating and managing a robust phishing simulation program.

### Use Cases

***Simulating Business Email Compromise (BEC)*** - Take a week per month or once a quarter to craft specific BEC-related emails that appear to come from your CEO or other C-suite executives use the agent's generative AI abilities to mimic the executive's writing style and request a wire transfer or other urgent request.

***Multi-lingual Phishing Tests*** - Quickly draft and deploy phishing emails in multiple languages to support a global workforce. The template generator can even adapt email text to a specific region with local expressions, nuances and cultural styles.

***Rapid Response to Emerging Threats*** - Seeing a brand new, in-the-wild attack? A few minutes with the template generator is all you need to spin up a duplicate simulated phishing attack to prepare your workforce for what's to come.



## Knowledge Refresher Agent

### What It Does

The Knowledge Refresher Agent helps users sharpen their cybersecurity skills and earn badges with short, AI-generated, scenario-based quizzes that are a fun and quick way to revisit key takeaways from their recent training.

### How To Use It

Enable and configure the feature through the AIDA Training tab or when creating a new training campaign. Here you can set parameters such as the time interval between training completion and refresher availability. Once activated, users can access their Knowledge Refreshers in their Learner Experience, streamlining engagement with this ongoing element of their learning process.

### Use Cases

***Reinforcing Phishing Awareness*** - AI-generated, scenario-based knowledge refreshers can be used as part of remedial training delivered after a user has clicked on a simulated phishing email to support the initial training. This continuous reinforcement helps maintain vigilance against evolving phishing tactics.

***Compliance Training Retention*** - By delivering periodic, focused refreshers on key compliance topics, organizations under specific regulatory requirements can demonstrate ongoing due diligence in maintaining a culture of compliance, potentially reducing liability and improving audit outcomes.



## Policy Quiz Agent

### What It Does

This AI-powered Policy Quiz Agent automatically generates quizzes based on your organization's specific policies, ensuring that employees not only read but also comprehend and retain critical information.

### How To Use It

In your KnowBe4 console, you add your organization's policies as a PDF file. After you've added your policy, you can edit and manage quiz questions relating to the policy and then create a training campaign to assign the policy to your users. Once you've assigned the policy to a campaign, you can track your users' progress and acknowledgments.

### Use Cases

***New Employee Onboarding*** - With custom-built policy quizzes, ensure new hires not only review the policies but also demonstrate their understanding. This can provide a measurable benchmark for their initial compliance training and reduce the risk of policy violations due to misunderstanding.

***Annual Policy Review*** - Streamline your annual policy reviewing process by using the Policy Quiz agent to quickly generate updated quizzes that reflect any changes in company guidelines and rules. Policy-based training campaigns will both help ensure knowledge retention and provide administrators with clear metrics on company-wide policy comprehension, helping to identify areas that may require additional training or clarification.

## Looking Ahead

These four agents' capabilities will be significantly enhanced as they work in unison under an AI-powered orchestration model that uses a goal based, always-on approach of achieving the lowest human risk for your organization.

But these are just the beginning. Future additions include:

- **Orchestration Agent:** This AI-powered agent will take on the role of a SAT administrator, managing phishing simulations, delivery and reporting.
- **Goal Driven Agent:** This agent will optimize targeting, attack vectors and training frequency to achieve the lowest possible human risk for your organization.
- **Adaptive Defense Agent:** By considering work schedules and current threats, this agent will schedule training at the least disruptive times and adapt content to address emerging risks.
- **SAT Assessment Agent:** This agent will create custom SAT assessments based on your organization's specific policies and procedures.

## The Upshot

AIDA isn't just the next step in KnowBe4's approach to HRM. It's a quantum leap forward, offering a suite of AI-native agents that transform how you address HRM. AIDA empowers your organization to stay ahead of the curve, using AI to defeat AI threats.

Here's what AIDA brings to you and your organization:

- AIDA's alignment with the [NIST Phish Scale Framework](#) ensures your SAT is consistent with your organization's broader security initiatives
- By reducing the time it takes your admins to create training content from an average of 7 days to mere seconds, AIDA frees up your security team's time dramatically
- Improve relationships between your security team and other departments by ensuring users are aligned with security objectives, fostering your organization's security culture
- By actively managing human risk efficiently, you have flexibility in your security budget to invest in other key initiatives
- Maximize the value of your existing security tech stack with AIDA's seamless integration

KnowBe4 is the only vendor that fully covers awareness, behavior and security culture so that organizations can address the human element of cybersecurity. KnowBe4's focus is helping organizations build a strong security culture, using a data-driven approach to manage human risk.

See AIDA in Action →

## Additional Resources



### Free Phishing Security Test

Find out what percentage of your employees are Phish-prone with your free Phishing Security Test



### Free Automated Security Awareness Program

Create a customized Security Awareness Program for your organization



### Free Phish Alert Button

Your employees now have a safe way to report phishing attacks with one click



### Free Email Exposure Check

Find out which of your users emails are exposed before the bad guys do



### Free Domain Spoof Test

Find out if hackers can spoof an email address of your own domain



## About KnowBe4

KnowBe4 empowers your workforce to make smarter security decisions every day. Tens of thousands of organizations worldwide trust the KnowBe4 platform to strengthen their security culture and reduce human risk. KnowBe4 builds a human layer of defense so organizations can fortify user behavior with new-school security awareness and compliance training.

Deploying KnowBe4 results in users that are alert and care about the damage that phishing, ransomware and other social engineering threats pose. The platform includes a comprehensive suite of awareness and compliance training, real-time user coaching, AI-powered simulated social engineering, and crowdsourced anti-phishing defense.

With content in 35+ languages, KnowBe4 provides the world's largest, always-fresh library of engaging content to strengthen your human firewall.

**For more information, please visit [www.KnowBe4.com](http://www.KnowBe4.com)**

# KnowBe4

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755  
Tel: 855-KNOWBE4 (566-9234) | [www.KnowBe4.com](http://www.KnowBe4.com) | Email: [Sales@KnowBe4.com](mailto:Sales@KnowBe4.com)

© 2025 KnowBe4, Inc. All rights reserved. Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

01F01K01