dohertyassociates

KnowBe4

Security Awareness Training

Manage the ongoing problem of social engineering

www.doherty.co.uk

About **Doherty Associates**

Doherty Associates, experts in managing and securing cloud services, are one of the leading IT Cloud Services and Support companies for London and the South East. Now in its 28th year, Doherty Associates has multi-country presence, a global client base and a team of more than 100 people working round the clock.

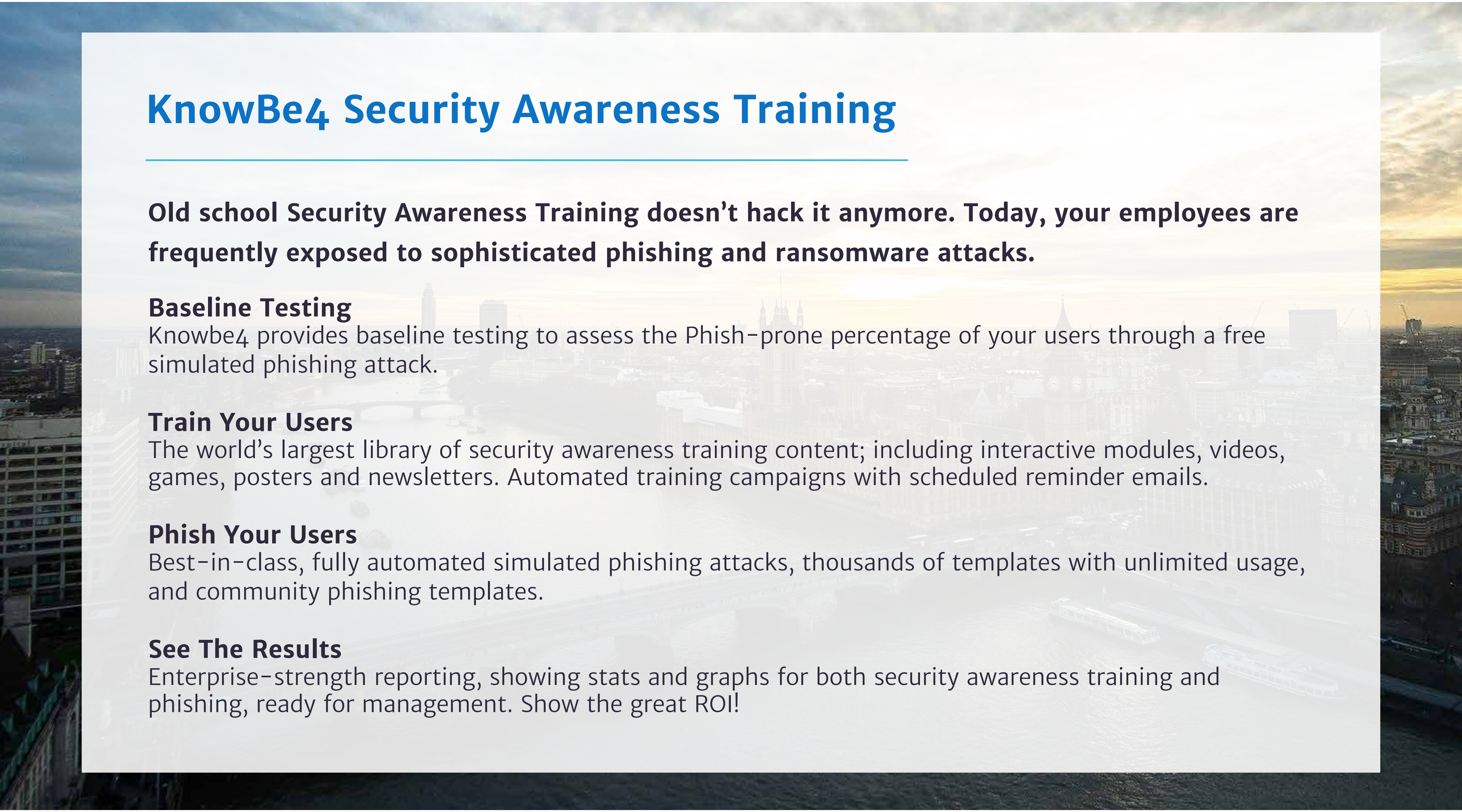
About **KnowBe4**

KnowBe4 is the world's largest security awareness training and simulated phishing platform that helps you manage the ongoing problem of social engineering. It was built to scale for busy IT pros that have 16 other fires to put out. Our goal was to design the most powerful, yet easy-to-use platform available.

Customers of all sizes can get the KnowBe4 platform deployed into production twice as fast as competitor products.

KnowBe4 **Products**

- ◊ Security Awareness Training
- ◊ PhishER
- ◊ KCM GRC Platform



KnowBe4 Security Awareness Training

Old school Security Awareness Training doesn’t hack it anymore. Today, your employees are frequently exposed to sophisticated phishing and ransomware attacks.

Baseline Testing

Knowbe4 provides baseline testing to assess the Phish-prone percentage of your users through a free simulated phishing attack.

Train Your Users

The world’s largest library of security awareness training content; including interactive modules, videos, games, posters and newsletters. Automated training campaigns with scheduled reminder emails.

Phish Your Users

Best-in-class, fully automated simulated phishing attacks, thousands of templates with unlimited usage, and community phishing templates.

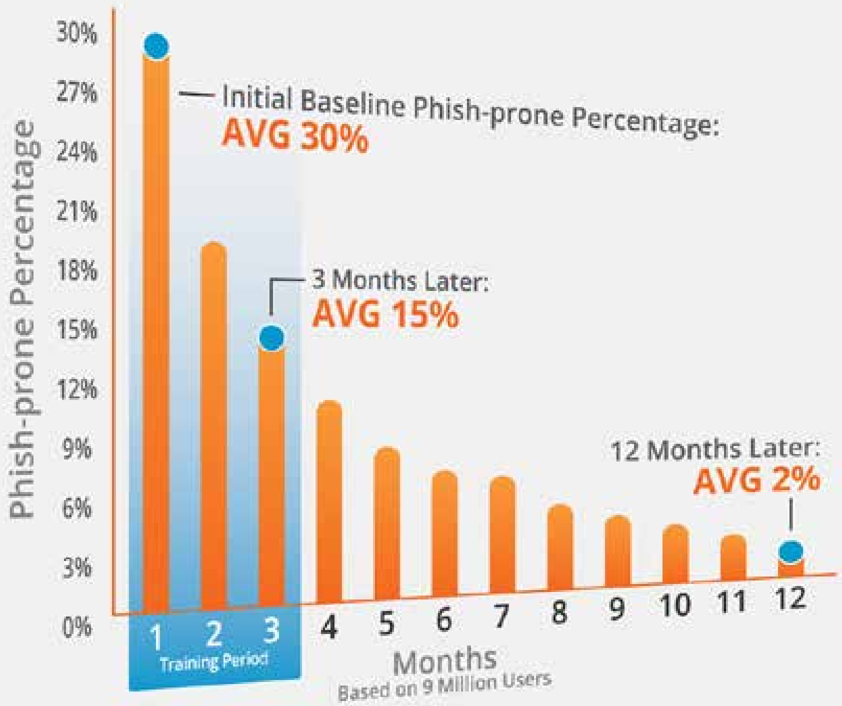
See The Results

Enterprise-strength reporting, showing stats and graphs for both security awareness training and phishing, ready for management. Show the great ROI!

The System Really Works

With KnowBe4's massive database, we analyzed nearly 9 million users over the course of 12 months, and our 2019 research uncovered surprising results.

The overall industry initial Phish-prone percentage benchmark turned out to be a troubling 30%. Fortunately, the data showed that this 30% can be brought down more than half to just 15% in only 90 days by deploying new-school security awareness training. The 365-day results show that by following these best practices, the final Phish-prone percentage can be minimized to 2% on average.



KnowBe4 Security Awareness Training Features

Unlimited Use

We offer three Training Access Levels, giving you access to our content library of 900+ items based on your subscription level. Unlimited access to all phishing features with flexible licensing. No artificial license ceilings and 10% overage allowance. Powerful new features added regularly.

Social Engineering Indicators

Patented technology turns every simulated phishing emailinto a tool IT can use to dynamically train employees by instantly showing them the hidden red flags they missed within that email.

User Management

KnowBe4's Active Directory Integration allows you to easily upload user data and saves you time by eliminating the need to manually manage user changes. You can also leverage the Smart Groups feature to tailor and automate your phishing campaigns, training assignments and remedial learning based on your employees' behavior and user attributes.

Engaging, Interactive Browser-based Training

The interactive training gives your users a fresh new learner experience that makes learning fun and engaging. Currently available in 21 local languages, your users now can choose the language they're most comfortable with for the entire training interface, helping deliver a more immersive training experience. With the optional gamification feature, users can compete against their peers on leaderboards and earn badges while learning how to keep your organization safe from cyber attacks.

Upload Your Own Content

Want to supplement your KnowBe4 security awareness training content with your organization's custom training or other corporate training content? Upload your own SCORM-compliant training and video content and manage it alongside your KnowBe4 ModStore training all in one place - at no extra cost!

Security Roles

Allows you to define unlimited combinations of level access and administrative ability that you'd like specific user groups to have. With delegated permissions you have the ability to limit roles to only display specific data or allow for the phishing, training, and user management of specific groups.

New! Assessments

Find out where your users are in both security knowledge and security culture to help establish baseline security metrics. Use the skills-based assessment and the security culture survey to measure and monitor your users' security knowledge and sentiment to a security aware culture over time.

Advanced Reporting Feature

60+ built-in reports provide holistic views and detailed reporting on your key awareness training indicators over time. Leverage Reporting APIs to pull data from your KnowBe4 console and for multiple accounts, Roll-up Reporting makes it easy to view results in aggregate.

Custom Phishing Templates and Landing Pages

Apart from the thousands of easy-to-use existing templates, you can customize scenarios based on personal information and include simulated attachments to create your own targeted spear phishing campaigns. Each Phishing Email Template can have its own Custom Landing Page, which allows for point-of-failure education.

Phish Alert Button

KnowBe4's Phish Alert add-in button gives your users a safe way to forward email threats to the security team for analysis, and deletes the email from the user’s inbox to prevent future exposure. All with just one click!

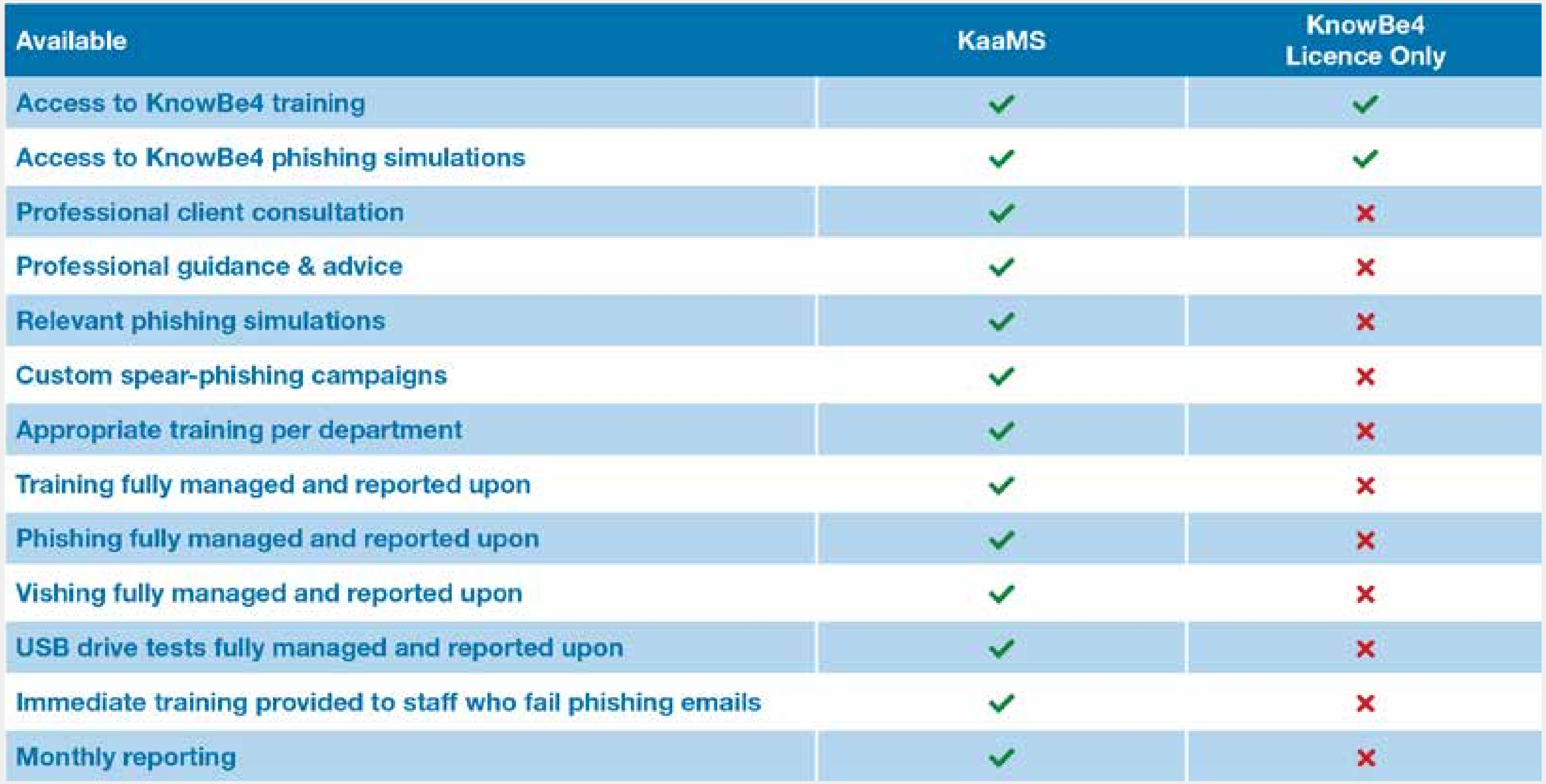
Virtual Risk Officer™

The new innovative Virtual Risk Officer (VRO) functionality helps you identify risk at the user, group and organizational level and enables you to make data-driven decisions when it comes to your security awareness plan. Leverage the User Event API to push custom security-related events from your third-party platforms (like Mimecast or Splunk) to the KnowBe4 Console, influencing your users’ risk scores accordingly.

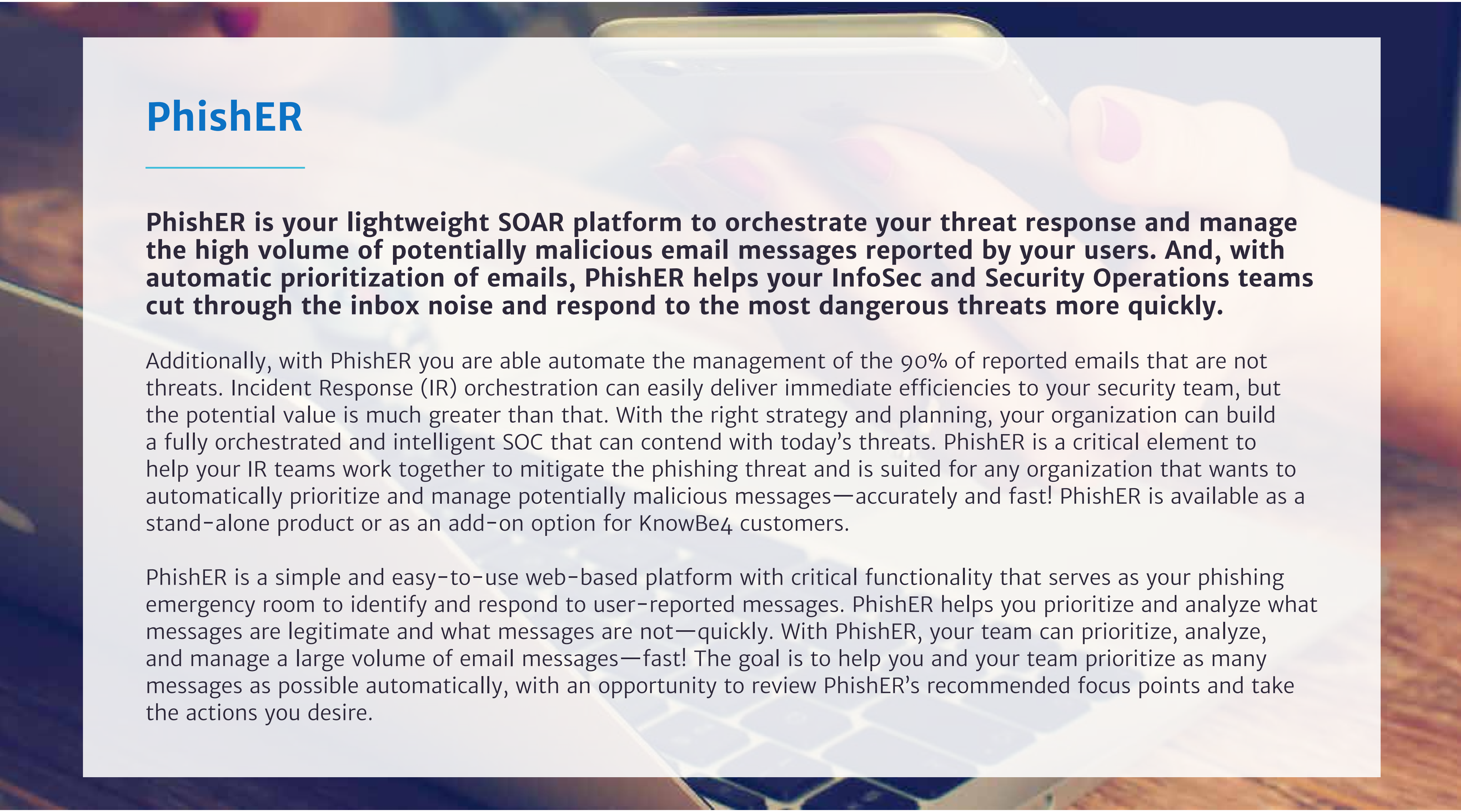
PhishER

As you phish and train your users they will start reporting potentially dangerous emails to your incident response team. The increase of this email traffic... can present a new problem! PhishER, is an optional add-on for managing the high volume of messages reported by your users and helps you identify and respond to email threats faster.

KnowBe4 as a Managed Service (KaaMS)



Available	KaaMS	KnowBe4 Licence Only
Access to KnowBe4 training	✓	✓
Access to KnowBe4 phishing simulations	✓	✓
Professional client consultation	✓	✗
Professional guidance & advice	✓	✗
Relevant phishing simulations	✓	✗
Custom spear-phishing campaigns	✓	✗
Appropriate training per department	✓	✗
Training fully managed and reported upon	✓	✗
Phishing fully managed and reported upon	✓	✗
Vishing fully managed and reported upon	✓	✗
USB drive tests fully managed and reported upon	✓	✗
Immediate training provided to staff who fail phishing emails	✓	✗
Monthly reporting	✓	✗



PhishER

PhishER is your lightweight SOAR platform to orchestrate your threat response and manage the high volume of potentially malicious email messages reported by your users. And, with automatic prioritization of emails, PhishER helps your InfoSec and Security Operations teams cut through the inbox noise and respond to the most dangerous threats more quickly.

Additionally, with PhishER you are able automate the management of the 90% of reported emails that are not threats. Incident Response (IR) orchestration can easily deliver immediate efficiencies to your security team, but the potential value is much greater than that. With the right strategy and planning, your organization can build a fully orchestrated and intelligent SOC that can contend with today's threats. PhishER is a critical element to help your IR teams work together to mitigate the phishing threat and is suited for any organization that wants to automatically prioritize and manage potentially malicious messages—accurately and fast! PhishER is available as a stand-alone product or as an add-on option for KnowBe4 customers.

PhishER is a simple and easy-to-use web-based platform with critical functionality that serves as your phishing emergency room to identify and respond to user-reported messages. PhishER helps you prioritize and analyze what messages are legitimate and what messages are not—quickly. With PhishER, your team can prioritize, analyze, and manage a large volume of email messages—fast! The goal is to help you and your team prioritize as many messages as possible automatically, with an opportunity to review PhishER's recommended focus points and take the actions you desire.

PhishER Key Benefits

- Full integration with KnowBe4's Phish Alert Button allows automatic prioritization of emails that are not threats
- Cut through the IR-inbox noise and respond to the most dangerous threats more quickly and efficiently
- Free up IR resources to identify and manage the 90% of messages that are either spam or legitimate email
- See clusters or groups of messages based on patterns that can help you identify a widespread phishing attack against your organisation
- Meet critical SLAs within your organization to process and prioritize threats and legitimate emails
- Automated email response templates let you quickly communicate back to your employees about the emails they need in order to continue working
- You can create custom workflows for tasks such as prioritization and alerting so that the IR team can focus on the right messages

KnowBe4 Security Awareness Training Features

Automatic Message Prioritization

PhishER will help you prioritize every reported message into one of three categories: Clean, Spam, or Threat. Through rules you set, PhishER helps you develop your process to automatically prioritize as many messages as possible without human
interaction.

With automatic prioritization of emails that are not threats, PhishER helps your team respond to the most dangerous threats more quickly. PhishER easily integrates with KnowBe4's email-add in button, Phish Alert and also works by forwarding to a dedicated mailbox.

Emergency Rooms

PhishER features "Emergency Rooms" to help you identify similar messages reported by your users. Emergency Rooms consist of pre-filtered views of your messages that are unresolved in your PhishER inbox. These messages are dynamically grouped by commonalities and include system pre-filtered views for messages by Top Subject Lines, Top Senders, Top Attachments, and Top URLs.

Each room is interactive, allowing you to drill down into filtered inbox views of the messages and take action across all associated messages at the same time.

PhishML™

PhishML is a PhishER machine-learning module that helps you identify and assess the suspicious messages that are reported by your users, at the beginning of your message prioritization process. PhishML analyzes every message coming into the PhishER platform and gives you the info to make your prioritization process easier, faster, and more accurate.

PhishML is constantly learning based on the messages that are tagged, not only by you but also by other members of the PhishER user community! That means that the learning model is being fed new data to constantly improve its accuracy and more messages can be automatically prioritized based upon PhishER categorization, saving you even more time.

Simple and Advanced Rule Creation

You can create custom rules, use the built-in YARA-based system rules, or edit existing YARA rules. You can use system rules to help simplify your rules requirements or copy and modify to customise rules depending on the proficiency of your incident response team.

Data Enrichment Intelligence

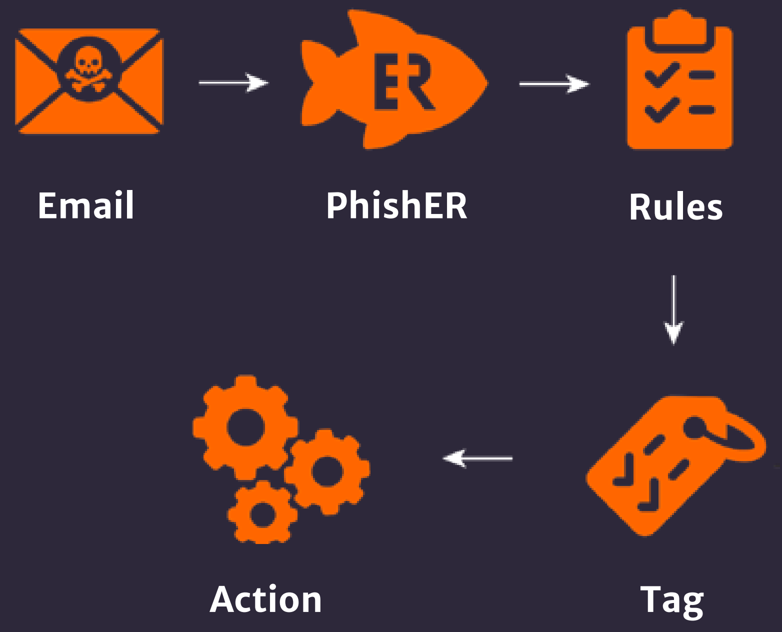
PhishER integrates with external services like VirusTotal to help analyze attachments and malicious domains. Using URL Unwinding, PhishER automatically expands shortened URLs to help see the potential threat level of the final destination.

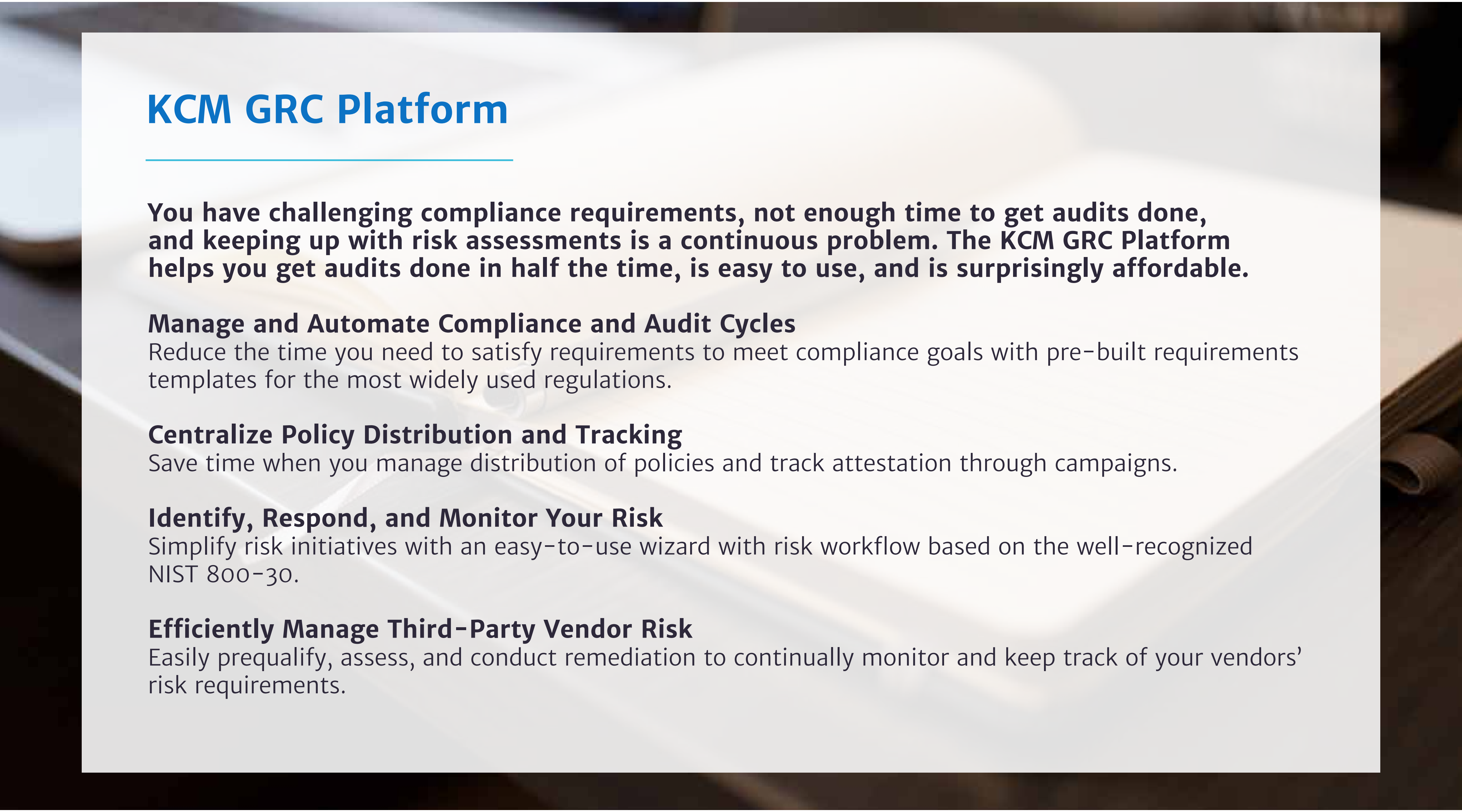
SIEM Integrations

PhishER integrates into your organization by pushing data into popular SIEM platforms such as Splunk and QRadar. With support for multiple syslog destinations available it's also possible to push data into as many other systems as you like.

How PhishER Works

PhishER processes user-reported phishing and other suspicious emails by grouping and categorizing emails based on rules, tags, and actions.





KCM GRC Platform

You have challenging compliance requirements, not enough time to get audits done, and keeping up with risk assessments is a continuous problem. The KCM GRC Platform helps you get audits done in half the time, is easy to use, and is surprisingly affordable.

Manage and Automate Compliance and Audit Cycles
Reduce the time you need to satisfy requirements to meet compliance goals with pre-built requirements templates for the most widely used regulations.

Centralize Policy Distribution and Tracking
Save time when you manage distribution of policies and track attestation through campaigns.

Identify, Respond, and Monitor Your Risk
Simplify risk initiatives with an easy-to-use wizard with risk workflow based on the well-recognized NIST 800-30.

Efficiently Manage Third-Party Vendor Risk
Easily prequalify, assess, and conduct remediation to continually monitor and keep track of your vendors' risk requirements.

An Affordable and Simple GRC Platform

Most organizations leverage spreadsheets, documents and/or collaboration portals, as well as email threads and individual calendars to manage their GRC initiatives. This is inefficient, error prone, costly, and a risk in itself. GRC is primarily a matter of “people and processes” and tools come second.

However, old-school GRC offerings require many months of implementation and high consulting hours to stand up. KCM GRC has a simple, intuitive user interface, easy to understand workflows, a short learning curve, and will be fully functional in a matter of days. KCM GRC was developed to save you the maximum amount of time getting GRC done.

The KCM GRC platform is offered in different packages to meet the needs of all organizations and is available with the following modules to choose from:

- **Compliance Management**
- **Policy Management**
- **Risk Management**
- **Vendor Risk Management**

KCM GRC Platform Features

Compliance Management

Managing Audits and Compliance

Today, most organizations are required to follow some type of regulation or follow industry best practices. Managing compliance for one regulation or framework is time consuming. Having multiple regulations becomes impractical to manage without automation. KCM GRC effectively reduces the time you need to satisfy all requirements necessary to meet compliance goals, leading to significantly less time and money spent dealing with compliance and audits.

Quick Implementation with Compliance Requirements Templates

Using the built-in quick setup capability, KCM GRC can have you on your way to improved compliance quickly. KCM includes pre-built requirements templates for the most widely used regulations. KnowBe4's Experts create new templates as regulations change or are updated... there is no need for you to monitor confusing changes in regulations any more.

Risk Management

Simplified Risk Management Workflow

With an intuitive interface and wizards,getting insight into your organization's risk just became easier. Our risk management workflow is simple: identify the risk, respond to the risk and monitor the risk. The KCM risk workflow is based on the well-recognized NIST 800-30.

Easy Risk Identification

Already working with spreadsheets? Import them into the risk register or manually create unique organizational risks. The risk module integrates with the compliance module by allowing compliance or audit gaps to be escalated to the risk register.

Timely Risk Response

You can link existing controls from the repositories you've created to leverage ongoing risk reduction initiatives. Tie implementation of controls and treatment scores to determine your residual risk and ensure the appropriate personnel are engaged and informed with their task assignments and reminders.

Ongoing Risk Monitoring

Leverage KCM to determine ongoing effectiveness. You can schedule ongoing tasks to ensure controls are being assessed and get insights into risks with the risk dashboard. With KCM, you can simplify and streamline your risk initiatives resulting in better visibility and increased efficiency.

Policy Management

Centralized Policy Distribution and Tracking

KCM allows you to upload a finalized policy, select a targeted list of users, and generate user reports to satisfy compliance requirements. You can set up policy campaigns to help manage policy distribution, reminders, and user acknowledgement.

Automated Policy Management Workflow

Automate your policy management workflow with automated notifications, tasks, and reminders prompted by any event you like, such as an upcoming review date.

Vendor Risk Management

Centralized Vendor Risk Management

KCM's Vendor Risk Management module helps you centralize your process to manage your third-party vendor security risk requirements. With a single pane of glass view, you get continuous visibility into your vendors' controls and evidence libraries and can keep track of their compliance requirements,services they provide, and what data they have access to in one centralized repository.

Vet, Manage, and Monitor Vendor Risk

Prequalify risk, assess your vendors, and conduct remediation to continually monitor risk associated with your vendors. You can also escalate areas of risk to the risk register to increase visibility of vendor risk. Additionally, KCM makes it easy to manage the entire lifecycle of your vendors from onboarding to offboarding to ensure that organizations are compliant and don't retain your data once the relationship has ended.

Automated Workflows for Requirements, Remediation, and Mitigation

Streamline your vendor assessment process with KCM's automated workflow and campaigns. You can easily design an efficient workflow to conduct due-diligence activities and track and monitor tasks assigned to your vendors to ensure accountability. Easily set issue status and priorities based on your organization's security requirements and build repeatable processes to help automate your ongoing vendor assessments.

Managed Vendor Assessment Templates

With no-cost vendor access, your vendors can get started quickly with your assessment process. Ensure standard and consistent vendor assessments with pre-built and customizable questionnaire templates. You have the ability to generate assessments in HTML or CSV, depending on your preferred workflow. You can upload your own custom templates or leverage our managed templates and select from BITS SIG, CSA CAIQ, EDUCAUSE HECVAT and more.

Talk to one of our experts at Doherty Associates today and discover how KnowBe4 can help you achieve all your business goals.

Book a call

Telephone: 020 8987 1150

enquiries@doherty.co.uk

dohertyassociates

KnowBe4

Head Office

3 Water Lane
Richmond
Greater London
TW9 1TJ

Kuala Lumpur Office

D2-3A-5 Solaris Dutamas
No. 1. Jalan Dutamas 1
50480 Kuala Lumpur
Malaysia

Cardiff Office

Cardiff Eagle Lab, First Floor
Brunel House, Fitzalan Road,
Cardiff
CF24 0EB

Telephone: 020 8987 1150
Fax: 020 8987 1151
enquiries@doherty.co.uk

www.doherty.co.uk