



# Executive Summary

2021 Edition

## Table of Contents

|   |    |
|---|----|
| <b>Simplifying the Governance, Risk, Compliance, and Audit Management Process</b> | 2  |
| <b>KCM GRC Can Help</b>   | 2  |
| <b>Compliance Management</b>  | 3  |
| View All Compliance Requirements  | 3  |
| View All Compliance Tasks   | 3  |
| View by Scope and Scope Status Report   | 4  |
| Compliance Templates and Control Guidance   | 4  |
| <b>Policy Management</b>  | 5  |
| View Policy Campaign  | 5  |
| Save Time with Policy Templates   | 5  |
| <b>Risk Management</b>  | 6  |
| View Risk Breakdown and Risk Categories   | 6  |
| Easily Add Risks Using the Risk Wizard  | 6  |
| <b>Vendor Risk Management</b>   | 7  |
| Use Pre-built and Customizable Questionnaire Templates                            | 7  |
| View Vendor Details   | 7  |
| Vendor Login  | 8  |
| Vendor Assessment Templates   | 8  |
| <b>Key Features in the KCM GRC Platform</b>                                       | 9  |
| Automated Email Reminders for Task Completion                                     | 9  |
| View Task Details   | 9  |
| Controls Information and Controls Library   | 10 |
| Documents – Uploads and DocuLinks   | 10 |
| Dashboards – Global, by Scope, and User   | 11 |
| Role-Based Access Control   | 11 |
| Generate Custom Reports   | 11 |
| <b>About KnowBe4</b>  | 12 |

# Simplifying the Governance, Risk, Compliance, and Audit Management Process

*The KCM GRC platform simplifies the complexity of achieving compliance and eases the burden of remaining compliant year round; minimizing the busy work commonly associated with audits and risk assessments, while simultaneously allowing your team to remain productive and functioning as usual.*

KCM GRC is a SaaS-based GRC platform that helps you effectively and efficiently manage risk and compliance within your organization and across your third-party security vendors, while gaining insight into gaps within your security program. 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 Can Help

- Manage the complicated area of compliance and audits; clarifying what needs to be done, who is going to do it, when it's due, and where to put the supporting documentation, simplifying and shortening the audit process.
- Centralize your policy distribution and tracking through policy campaigns to help manage policy distribution, reminders, and user acknowledgment.
- Simplify your risk management process with easy risk management workflows that help you identify, respond, and monitor risk.
- Prequalify risk, assess, and conduct remediation to continually monitor risk associated with your third-party vendors. With a single pane of glass view, you get continuous visibility into their controls and evidence libraries.

“We are now free of the stressful and inefficient cycle of playing last minute catch-up each time the next audit period rolls around.”

– KCM Customer in the payment processing industry

# Compliance Management

The KCM Compliance Management module effectively reduces the time you need to satisfy all of the requirements necessary to meet compliance goals, leading to significantly less time and money spent dealing with compliance and audits.

## View All Compliance Requirements

View all your compliance requirements with details, descriptions, status, scope, and controls for each requirement.

Global Dashboard

Compliance

My Dashboard

Requirements

Scope

Policy Management

Risk Management

Vendor Management

Tools

Documents

Metrics

Custom Reporting

View All Requirements

Search...

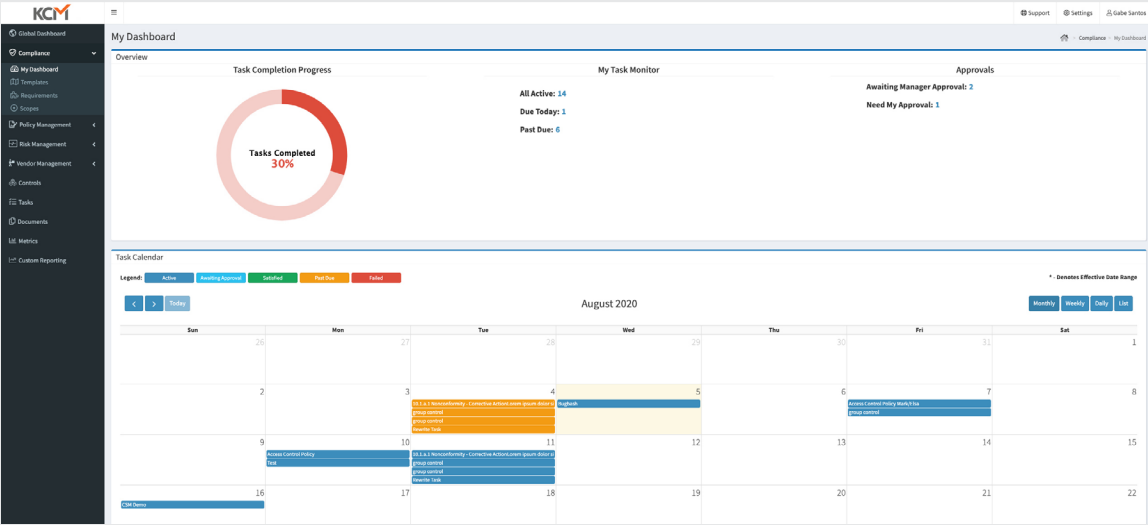
Search...

Search...

| Requirement ID  | Name   | Description   | Templates            | Action |
|-----------------|--|---|----------------------|--------|
| 13402 (A)       | Notification in the Case of Breach - General         | A covered entity that assesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information (as defined in subsection (b)(1)(3)) shall, in the case of a breach of such information that is discovered by the covered entity, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, or disclosed as a result of such breach.   | HITCH 2.0000_CURRENT |        |
| 13402 (B)       | Notification of Covered Entity by Business Associate | A business associate of a covered entity that assesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information shall, following the discovery of a breach of such information, notify the covered entity of such breach. Such notice shall include the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the business associate to have been, accessed, acquired, or disclosed during such breach.  | HITCH 2.0000_CURRENT |        |
| 13402 (C)(1)    | Timeliness of Notification - General                 | Subject to subsection (3), all notifications required under this section shall be made without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach by the covered entity involved (or business associate involved) in the case of a notification required under subsection (B).   | HITCH 2.0000_CURRENT |        |
| 13402 (C)(2)    | Timeliness of Notification - Burden of Proof         | The covered entity involved (or business associate involved) in the case of a notification required under subsection (B), shall have the burden of demonstrating that all notifications were made as required under this part, including evidence demonstrating the necessity of any delay.   | HITCH 2.0000_CURRENT |        |
| 13402 (A)(1)(A) | Methods of Notice - Written                          | Notice required under this section to be provided to an individual, with respect to a breach, shall be provided promptly and in the following form: (A) Written notification by first-class mail to the individual (or the next of kin of the individual if the individual is deceased) at the last known address of the individual or the next of kin, respectively, or, if specified as a preference by the individual, by electronic mail. The notification may be provided in one or more mailings as information is available.   | HITCH 2.0000_CURRENT |        |
| 13402 (A)(1)(B) | Methods of Notice - Outdated Contact Information     | Notice required under this section to be provided to an individual, with respect to a breach, shall be provided promptly and in the following form: (B) In the case in which there is insufficient, or out-of-date contact information (including a phone number, email address, or any other form of appropriate communication) that precludes direct written (or, if specified by the individual under subparagraph (A), electronic) notification to the individual, a substitute form of notice shall be provided, including, in the case that there are 10 or more individuals for which there is insufficient or out-of-date contact information, a comprehensive posting for a period determined by the Secretary on the home page of the Web site of the covered entity involved or notice in major print or broadcast media, including major media in geographic areas where the individuals affected by the breach likely reside. Such a notice in media or web posting will include a toll-free phone number where an individual can learn whether or not the individual's unsecured protected health information is possibly included in the breach. | HITCH 2.0000_CURRENT |        |
| 13402 (A)(1)(C) | Methods of Notice - Individual Notice - Urgency      | Notice required under this section to be provided to an individual, with respect to a breach, shall be provided promptly and in the following form: (C) In any case deemed by the covered entity involved to require urgency because of possible imminent misuse of unsecured protected health information, the covered entity, in addition to notice provided under subparagraph (A), may provide information to individuals by telephone or other means, as appropriate.  | HITCH 2.0000_CURRENT |        |
| 13402 (A)(2)    | Methods of Notice - Media Notice                     | Notice shall be provided to prominent media outlets serving a State or jurisdiction, following the discovery of a breach described in subsection (A), if the unsecured protected health information of more than 500 residents of such State or jurisdiction is, or is reasonably believed to have been, accessed, acquired, or disclosed during such breach.   | HITCH 2.0000_CURRENT |        |
| 13402 (A)(3)    | Methods of Notice - Notice to Secretary              | Notice shall be provided to the Secretary by covered entities of unsecured protected health information that has been acquired or disclosed in a breach. If the breach was with respect to 500 or more individuals than such notice must be provided immediately. If the breach was with respect to less than 500 individuals, the covered entity may maintain a log of any such breach occurring and annually submit such a log to the Secretary documenting such breaches occurring during the year involved.   | HITCH 2.0000_CURRENT |        |
| 13402 (A)(4)    | Methods of Notice - Posting on HHS Public Website    | The Secretary shall make available to the public on the Internet website of the Department of health and human services a list that identifies each covered entity involved in a breach described in subsection (A) in which the unsecured protected health information of more than 500 individuals is acquired or disclosed.  | HITCH 2.0000_CURRENT |        |
| 13402 (I)       | Content of Notifications                             | Regardless of the method by which notice is provided to individuals under this section, notice of a breach shall include, to the extent possible, the following:<br>(1) A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.<br>(2) A description of the types of unsecured protected health information that were involved in the breach such as full name, Social Security number, date of birth, home address, account number, or disability code.<br>(3) The steps individuals should take to protect themselves from potential harm resulting from the breach.<br>(4) A brief description of what the covered entity involved is doing to investigate the breach, to mitigate issues, and to protect against any further breaches.<br>(5) Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.  | HITCH 2.0000_CURRENT |        |

## View All Compliance Tasks

The “My Dashboard” view narrows focus to tasks assigned to an individual end user, allowing your entire organization to work together towards compliance.





Scopes enable you to track multiple projects in one place simultaneously allowing you to provide granular user permissions across each project.



The Compliance Management module comes with over 100 managed compliance templates maintained by KnowBe4. These pre-built templates are available for some of the most common regulations such as PCI, Cloud Security Alliance, Center for Internet Security, NIST, HIPAA, FFIEC, Secure Controls Framework, GDPR, FedRAMP, AICPA SSAE18, and more. You also have the ability to customize existing templates or create your own custom templates to fit the needs of your organization.

Use KCM's control guidance feature to help you create adequate controls to meet your specific scopes and requirements. KCM provides suggestions in-platform with control guidance added for the requirements under many of the managed templates KCM offers. Control guidance is available for the most commonly used frameworks including CMMC, GDPR, HIPAA, NIST, PCI, and more.

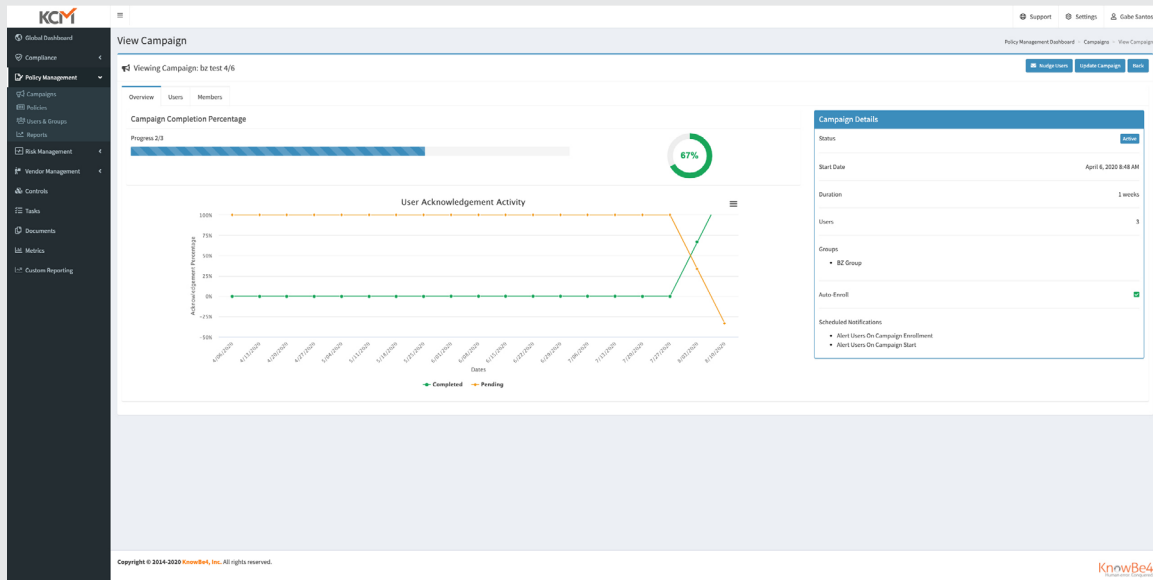


# Policy Management

The KCM Policy Management module helps you centralize policy distribution and tracking. Automate your policy management workflow with automated notifications, tasks, and reminders prompted by any event you like, such as an upcoming review date.

## View Policy Campaign

See all campaign details and easily keep track of your policy campaign completion percentage and user acknowledgments.



## Save Time with Policy Templates

To make it easier to create new policies, you can search KCM's library of available policy templates, customize them for your organization's specific needs, and upload them to the template repository in the Policy Management module.

**Policy Templates**

Download and customize policy templates to establish policies for your organization. You will find a list of the relevant NIST controls within each policy.

In addition to the templates you see here, KnowBe4 has partnered with AlluIT to provide KCM customers with access to over 160 policy templates at a discounted price. To learn more, visit the [AlluIT Policy Collection](#).

Page Size: 100

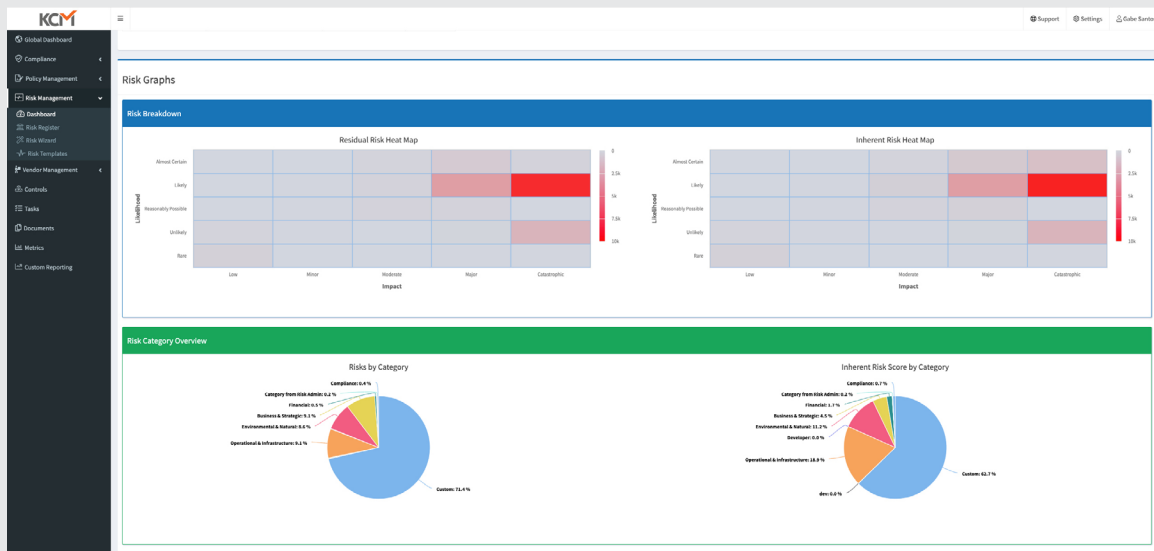
| Name                                     | Created Date | Updated Date | Actions |
|--|--------------|--------------|---------|
| Audit Policy                             | May 12, 2021 | May 12, 2021 |         |
| Contingency Planning Policy              | May 12, 2021 | May 12, 2021 |         |
| Identification and Authentication Policy | May 12, 2021 | May 12, 2021 |         |
| Incident Response Policy                 | May 12, 2021 | May 12, 2021 |         |
| Media Protection Policy                  | May 12, 2021 | May 12, 2021 |         |
| Mobile Device Policy                     | May 12, 2021 | May 12, 2021 |         |
| Personnel Security Policy                | May 12, 2021 | May 12, 2021 |         |
| Physical and Environmental Policy        | May 12, 2021 | May 12, 2021 |         |

# Risk Management

With the KCM Risk Management module you can simplify and streamline your risk initiatives resulting in better visibility and increased efficiency. Ultimately, this leads to a more resilient organization.

## View Risk Breakdown and Risk Categories

The Risk Dashboard gives you high-level details on your risk categories and risk score associated with these categories.



## Easily Add Risks Using the Risk Wizard

The Risk Wizard makes it easy for you to create unique organizational risks or import risks from existing spreadsheets to your risk register.

The screenshot displays the 'Risk Wizard - Manual Selection' screen. The left sidebar is the same as the previous screenshot. The main content area is titled 'Risk Wizard - Manual Selection' and includes three tabs: 'Manual Selection' (selected), 'Import Risks from CSV', and 'Create a Risk'.

**Manual Selection**

The 'Manual Selection' tab is active, showing a 'Search Master Risk List' section with a search bar and a 'Search' button. Below this is a 'Manually Add Risks' section with a 'Import Risks from CSV' button. To the right is a 'Create a Risk' section with a 'Create' button. At the bottom are 'Cancel', 'Back', and 'Next' buttons.

**Import Risks from CSV**

The 'Import Risks from CSV' section includes a description: 'Using the CSV template (click import to view), import your own list of risks your organization has previously identified. Use this feature to bulk import risks.' Below this is an 'Import' button.

**Create a Risk**

The 'Create a Risk' section includes a description: 'Enter new risks that are not part of the master risk repository. This is a manual process useful for entering a small quantity of risks at a time. The CSV import is recommended for longer lists of identified risks. You'll have the ability to customize this immediately after completing the wizard.' Below this is a 'Create' button.

# Vendor Risk Management

The KCM Vendor Risk Management module helps you manage your third-party vendor security risk requirements. Centralize your process, prequalify risk, assess your vendors, and conduct remediation to continually monitor risk associated with your vendors. You can set the frequency of how often your vendors are assessed and easily maintain updated material for all your critical vendors. Easily keep track of your vendors' compliance requirements, services they provide, and what data they have access to in one centralized repository.

## Use Pre-built and Customizable Questionnaire Templates

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.

The screenshot shows the 'Questionnaire Preview' interface in the KCM Vendor Risk Management module. The interface includes a sidebar with navigation options like Global Dashboard, Compliance, Policy Management, Risk Management, and Vendor Management. The main content area displays a questionnaire titled 'Vendor Risk Management' with a 'Details' tab. The questionnaire is a form with multiple-choice questions. The first question is 'Are web server software versions that no longer have security patches released prohibited?'. The second question is 'Are clients allowed to manage access to their own systems and data?'. The third question is 'Are scoped systems or data stored or transferred in cloud-based public file sharing solutions? If yes, please explain in the 'Additional Information' field.' Each question has a 'Correct' answer and a 'Points' value of 10. The interface also includes a 'Vendor' dropdown menu and a 'Support' link.

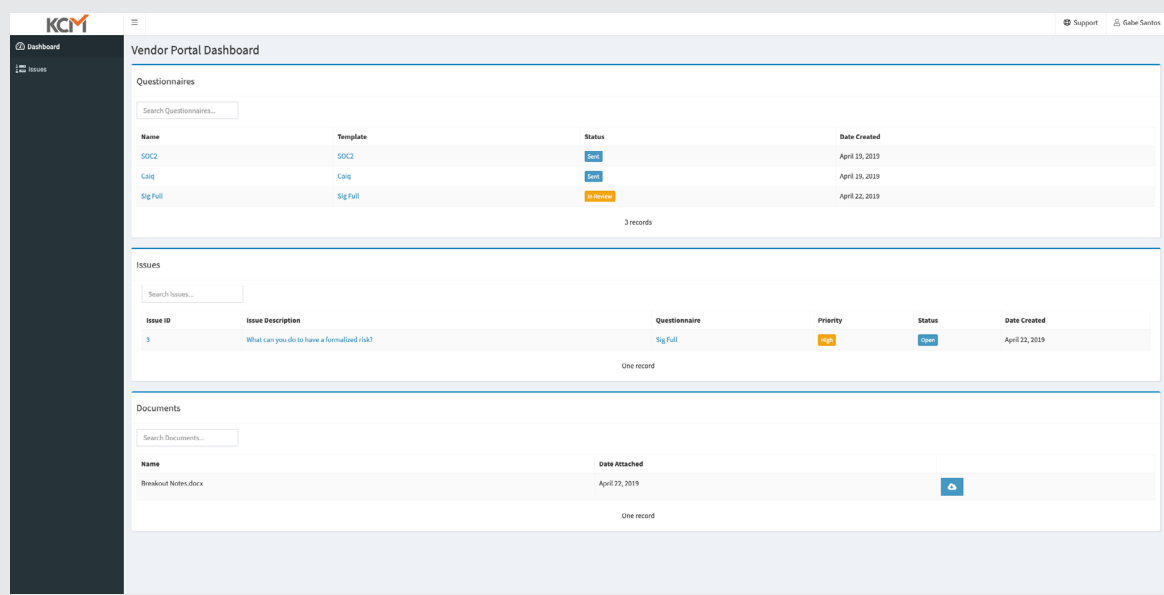
## View Vendor Details

View all your vendor details in one place to assess and monitor compliance and risk requirements for all your third parties.

The screenshot shows the 'Vendor Details - Yachtman' interface in the KCM Vendor Risk Management module. The interface includes a sidebar with navigation options like Global Dashboard, Compliance, Policy Management, Risk Management, and Vendor Management. The main content area displays the vendor details for 'Yachtman'. The details include the vendor's name, contact information, website, and a 'Vendor Score' of 90%. The interface also includes a 'Vendor Score Offset' of 10 and a 'Vendor Score' of 100. The interface includes a 'Vendor' dropdown menu and a 'Support' link. Below the details, there is a table with columns for 'Name', 'Status', and 'Created At'. The table lists several vendors with their status and creation date. The interface also includes a 'Page Size' dropdown menu and a 'Create New Questionnaire' button.

# Vendor Login

Your vendors login to an intuitive portal to upload, import, and complete required questionnaires or to provide their evidence controls.



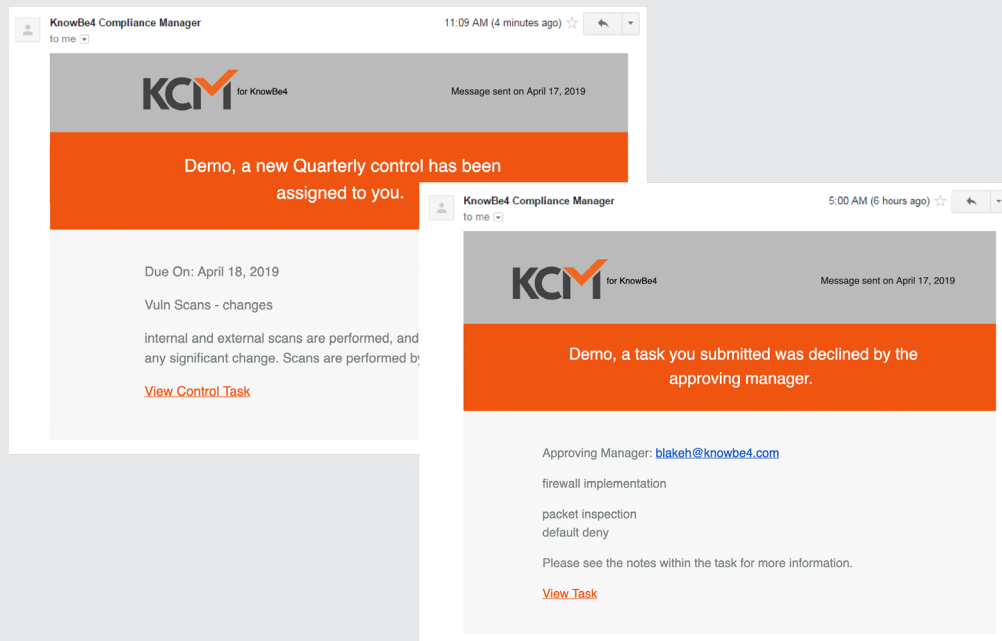
# Vendor Assessment Templates

The KCM Vendor Risk Management module includes some of the common assessment templates. Included are Shared Assessments' SIG questionnaires, Cloud Security Alliance CAIQ, and EDUCAUSE HECVAT. In addition, users can create their own templates or import your own.

# Key Features in the KCM GRC Platform

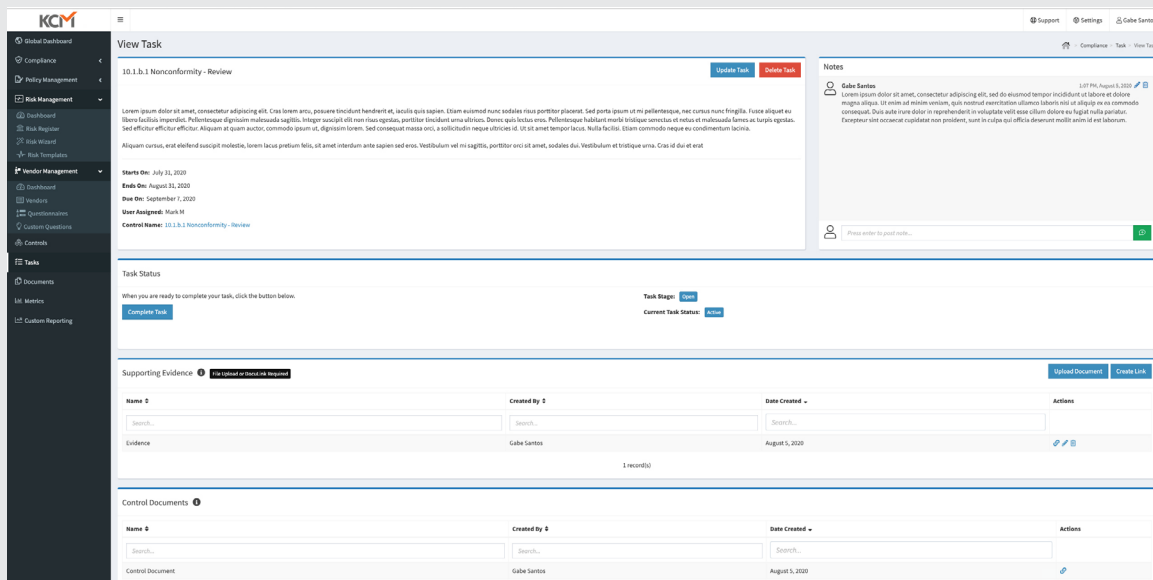
## Automated Email Reminders for Task Completion

Concise reminder emails are automatically sent out to team members based on upcoming due dates on tasks they've been assigned. Streamlining and automating the process of chasing down evidence allowing you to easily remain compliant year round.

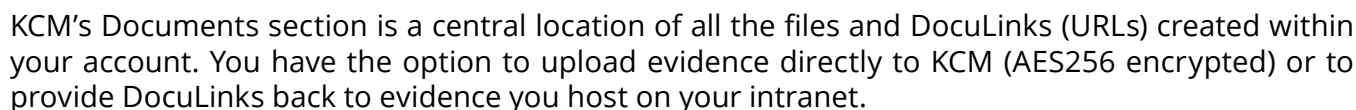
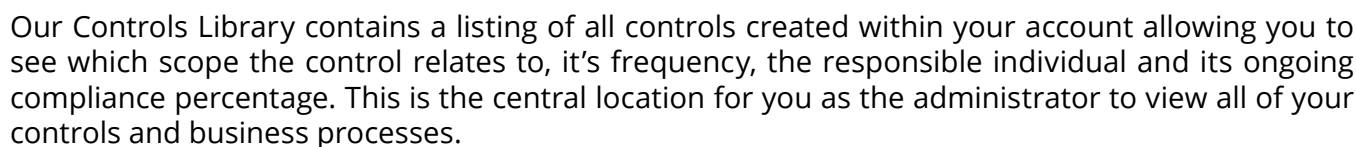


## View Task Details

Our Task view makes providing supporting documentation and notes incredibly simple, giving all departments a painless way to stay on the path to remaining in compliance.

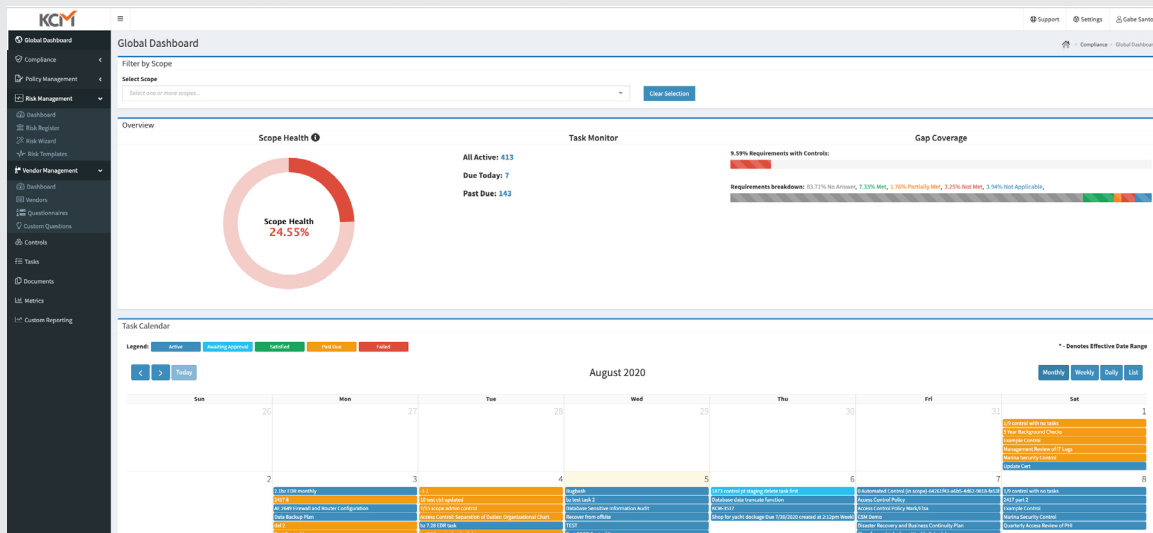


Assign responsibility to individual users, manage testing schedules setting specific dates, and track evidence and requirements in the Controls view.



## Dashboards – Global, by Scope, and User

The global dashboard shows all tasks across the entire organization allowing you to see at-a-glance how your entire organization is doing as you work towards getting compliant and staying compliant. This view can be limited by Scope as well. Each module within KCM has its own dashboard as well.



## Role-Based Access Control

KCM leverages RBAC for user administration. Your users only get access to the information needed based on different role types. Users can have multiple roles, depending on the implemented modules. There are even auditor roles to provide to outside consultants to review evidence and controls.

The screenshot displays the KCM Manage Users interface. The left sidebar contains navigation links for Global Dashboard, Compliance, Policy Management, Risk Management, Dashboard, Risk Register, Risk Mitigation, Vendor Management, Dashboard, Vendors, Questionnaires, Custom Questions, Controls, Tasks, Documents, Metrics, and Custom Reporting. The main content area is titled 'Manage Users' and includes a 'Users' dropdown. The interface shows a list of users with columns for Full Name, Email, User Groups, User Roles, Status, Date Created, Date Updated, Last Login, and Actions. The table lists several users, including Account Admin, philt@knowbet.com, philt@knowbet.com, Anna Sygys, anna@knowbet.com, Ariel Escobar, ariel@knowbet.com, Ben Tygum Admin, ben@knowbet.com, ben@knowbet.com, ben@knowbet.com, ben@knowbet.com, Ben Risk Admin, ben@knowbet.com, Ben Auditor, ben@knowbet.com, Ben Scope Admin, ben@knowbet.com, and Ben Policy Admin, ben@knowbet.com.

## Generate Custom Reports

Effectively report on the status of your compliance and risk management initiatives using KCM's Custom Reporting feature. Easily create and save reports that provide details on task status, user activities, and the rate of completion across your different scopes and control requirements. From within each report, you can filter and sort your data based on the criteria most important to you, and even export your reporting data to third-party BI tools. KCM makes it easy for you to demonstrate overall progress and health of your compliance program to your executive team.





KCM GRC helps you get audits done  
in half the time at half the cost.



## About KnowBe4

KnowBe4 is the world's largest integrated security awareness training and simulated phishing platform. Realizing that the human element of security was being seriously neglected, KnowBe4 was created to help organizations manage the ongoing problem of social engineering through a comprehensive new-school awareness training approach.

Tens of thousands of organizations worldwide use KnowBe4's platform across all industries, including highly regulated fields such as finance, healthcare, energy, government and insurance to mobilize their end users as a last line of defense and enable them to make smarter security decisions.

Many of our customers needed to provide security training to meet regulatory compliance. While working with these customers, KnowBe4 quickly discovered a need for a streamlined system to manage the compliance, risk, and audit process.

KCM GRC is SaaS-based governance, risk, and compliance platform that helps streamline and centralize compliance, risk, and audit processes across your entire organization and across your third-party vendors.

KCM simplifies the complexity of achieving compliance and eases the burden of demonstrating compliance to auditors and stakeholders; minimizing the busy work commonly associated with audits and compliance, eliminating the hassle of evidence collection from multiple departments, while simultaneously allowing your team to remain productive and functioning as usual.

To learn more, visit [ucgtechnologies.com](https://ucgtechnologies.com)



813.513.7402 | [focalpointsg.com](https://focalpointsg.com)



800.211.8798 | [ucgtechnologies.com](https://ucgtechnologies.com)



501.221.0037 | [strategiccompanies.com](https://strategiccompanies.com)

