

# Prevalent 3GRC Third-Party Risk Management platform Version 3.11

## New and Updated Features

The Prevalent 3GRC Third-Party Risk Management platform is a unified solution that combines automated vendor assessments, workflow, remediation management, and continuous threat monitoring across the entire vendor life cycle to deliver a 360-degree view of vendor risks. With the platform, customers can:

- Automate the end-to-end process of collecting and analyzing vendor surveys, speeding and simplifying assessments, compliance, and due diligence review.
- Enable categorization of vendors based on risk and organizational importance, prioritizing remediation.
- Deliver clear reporting beyond a score, tying risks to business outcomes and helping to make better risk-based decisions, prove compliance, and prioritize resources.
- Meet industry standards and ensure regulatory compliance targets for cyber risk, InfoSec, and data privacy, keeping pace with the speed and scale of regulatory change.
- Centralize TPRM functions, delivering a single view that provides single repository for effective reporting to satisfy audit and compliance requirements.
- Utilize a consistent, repeatable, proven methodology, enabling a scalable, more mature vendor risk management program.

Version 3.11 of the platform introduces important new capabilities to improve compliance reporting and escalate findings for targeted remediation.

## New Feature Highlights

### Enhanced Regulatory and Control Framework Reporting Provides a Clear Status of Compliance

---

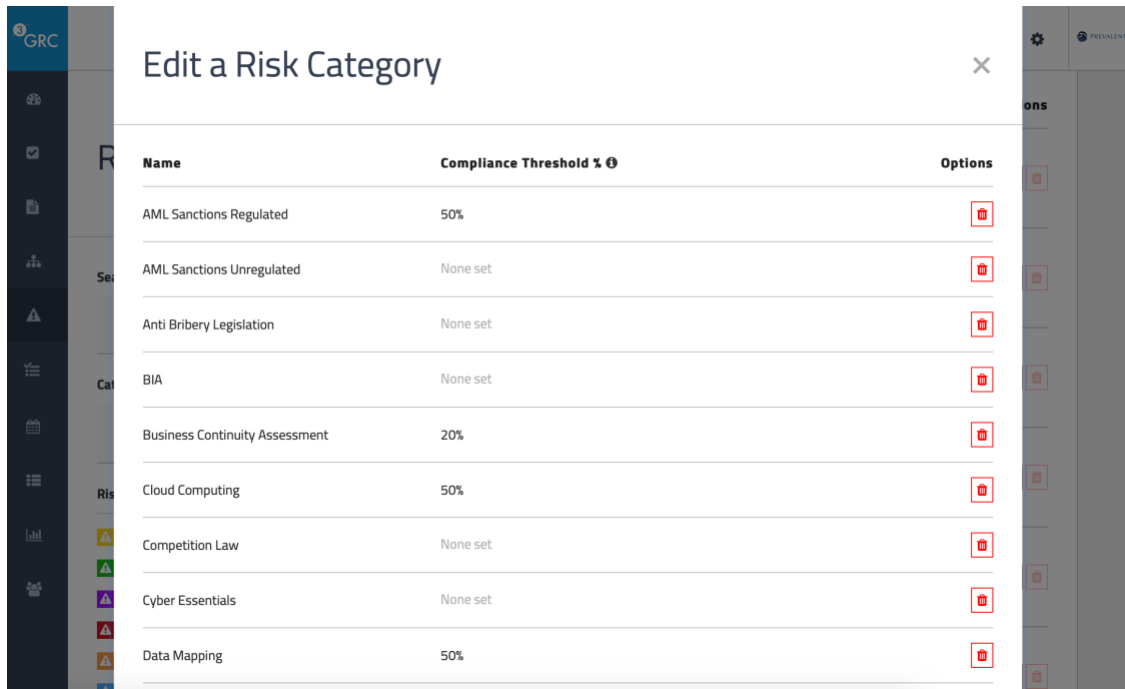
Since third-party risk management is a key control focus in most regulatory regimes and industry frameworks, it's important for organizations to show progress toward achieving compliance with those requirements. However, in many risk management tools specific compliance reporting can be complex and time-consuming.










Prevalent has addressed this need in version 3.11, introducing a new unified framework that maps the information gathered from controls-based assessments to regulatory frameworks including ISO 27001,

NIST, GDPR, CoBiT 5, SSAE 18, SIG, SIG Lite, and NYDFS. Unique to Prevalent is the ability for customers to take the answers and evidence from all submitted questions and map them to multiple frameworks, reducing the time and complexity required for reporting. Ask a question once and map to any framework – existing answers or in the future!

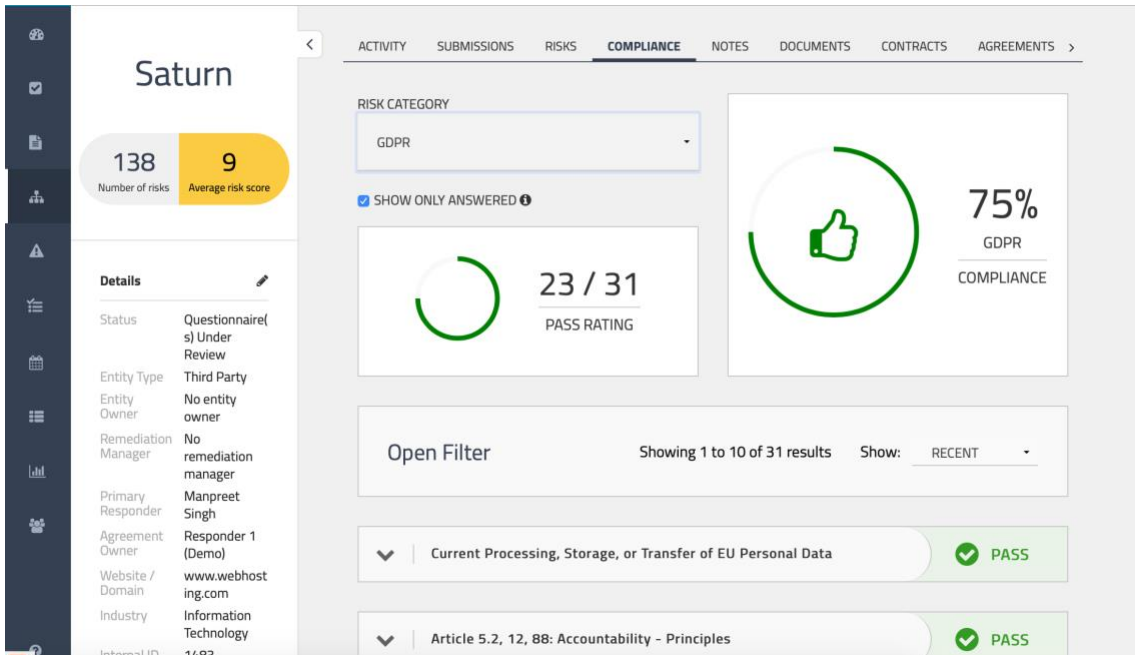
As part of the new compliance reporting capabilities, customers can:

- Establish a compliance “pass” percentage threshold against a risk category, for example X% compliant against a particular framework. This capability provides instant visibility into the compliance status of a vendor and can help customers focus in on problem areas. For a representation of this capability, please see the screenshot below.



| Name                           | Compliance Threshold % | Options   |
|--------------------------------|------------------------|---|
| AML Sanctions Regulated        | 50%                    |    |
| AML Sanctions Unregulated      | None set               |    |
| Anti Bribery Legislation       | None set               |    |
| BIA                            | None set               |  |
| Business Continuity Assessment | 20%                    |  |
| Cloud Computing                | 50%                    |  |
| Competition Law                | None set               |  |
| Cyber Essentials               | None set               |  |
| Data Mapping                   | 50%                    |  |

- Measure compliance against the entire regulation or just the parts that are relevant to the organization by leveraging the “Show Only Answered” feature. This capability will show actual compliance based on the services the vendor provides, instead of the entire regulation. For a representation of this capability, please see the screenshot below.



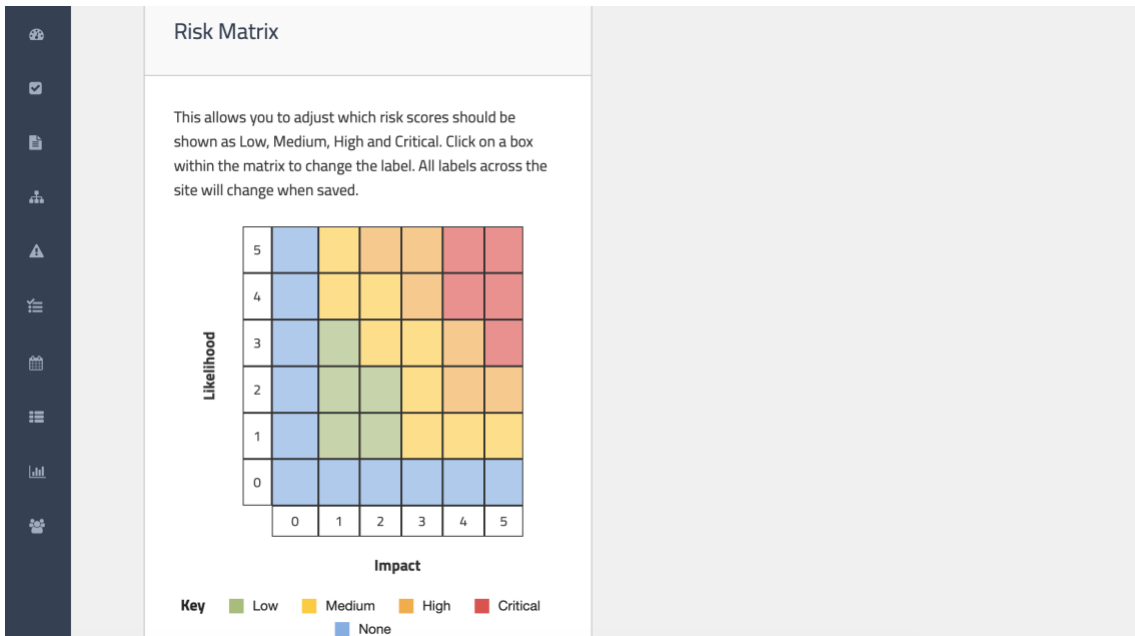
The screenshot shows a compliance dashboard for an entity named 'Saturn'. On the left, a sidebar contains navigation icons. The main header shows 'Saturn' with 138 risks and an average risk score of 9. Below this is a 'Details' section with the following information:

- Status: Questionnaire(s) Under Review
- Entity Type: Third Party
- Entity Owner: No entity owner
- Remediation Manager: No remediation manager
- Primary Responder: Manpreet Singh
- Agreement Owner: Responder 1 (Demo)
- Website / Domain: www.webhosting.com
- Industry: Information Technology
- Internal ID: 1482

The main content area is titled 'COMPLIANCE' and shows a 'RISK CATEGORY' dropdown set to 'GDPR'. A 'SHOW ONLY ANSWERED' checkbox is checked. Two circular progress indicators are displayed: one for '23 / 31 PASS RATING' and another for '75% GDPR COMPLIANCE' with a thumbs-up icon. Below these are filter options and a list of results:

- Open Filter: Showing 1 to 10 of 31 results. Show: RECENT
- Current Processing, Storage, or Transfer of EU Personal Data: PASS
- Article 5.2, 12, 88: Accountability - Principles: PASS

- Customize the 5x5 Risk Matrix by criticality. This heat map then enables customers to drill down into the individual risks in the matrix to quickly prioritize those most impactful to the business. For a representation of this capability, please see the screenshot below.

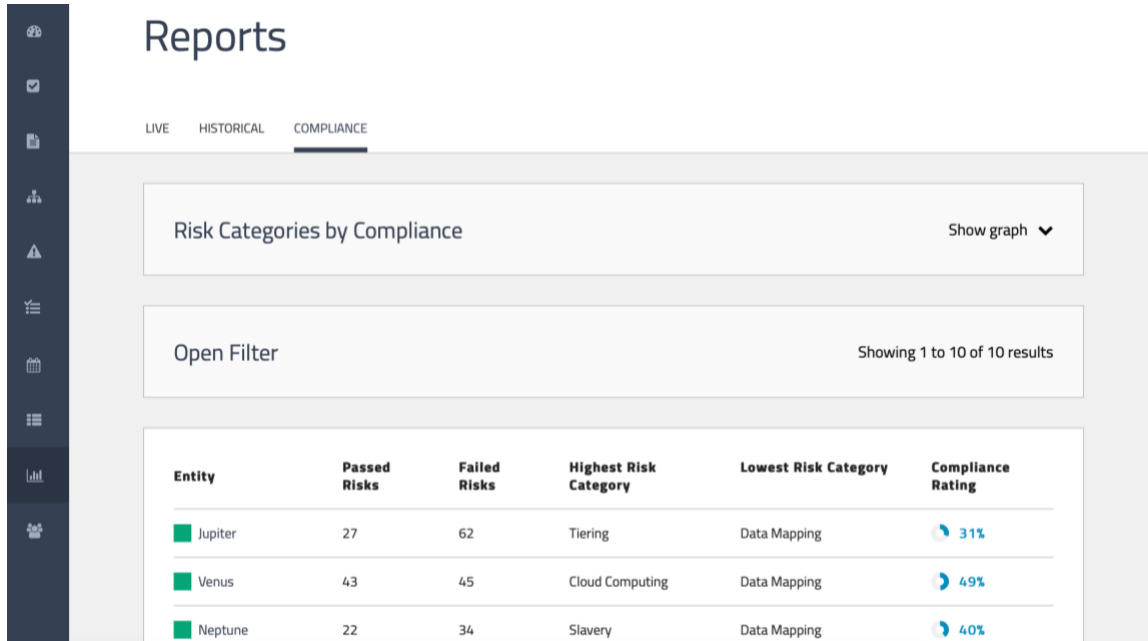


The screenshot shows the 'Risk Matrix' configuration page. It includes a text box explaining that users can adjust risk scores to be shown as Low, Medium, High, and Critical by clicking on boxes in the matrix. Below the text is a 5x5 grid with Likelihood on the y-axis (0-5) and Impact on the x-axis (0-5). A key at the bottom identifies the colors: Low (green), Medium (yellow), High (orange), Critical (red), and None (blue).

| Likelihood | 0    | 1      | 2      | 3      | 4        | 5        |
|------------|------|--------|--------|--------|----------|----------|
| 5          | None | Medium | High   | High   | Critical | Critical |
| 4          | None | Medium | High   | High   | Critical | Critical |
| 3          | None | Low    | Medium | High   | High     | Critical |
| 2          | None | Low    | Low    | Medium | High     | High     |
| 1          | None | Low    | Low    | Medium | Medium   | Medium   |
| 0          | None | None   | None   | None   | None     | None     |

**Key**  
■ Low ■ Medium ■ High ■ Critical  
■ None

- Leverage the new Compliance tab to see reporting for every vendor that has answered a particular question, helping to group particular risks for remediation across all vendors. It is also possible to see compliance by entity. For a representation of this capability, please see the screenshot below.



**Reports**

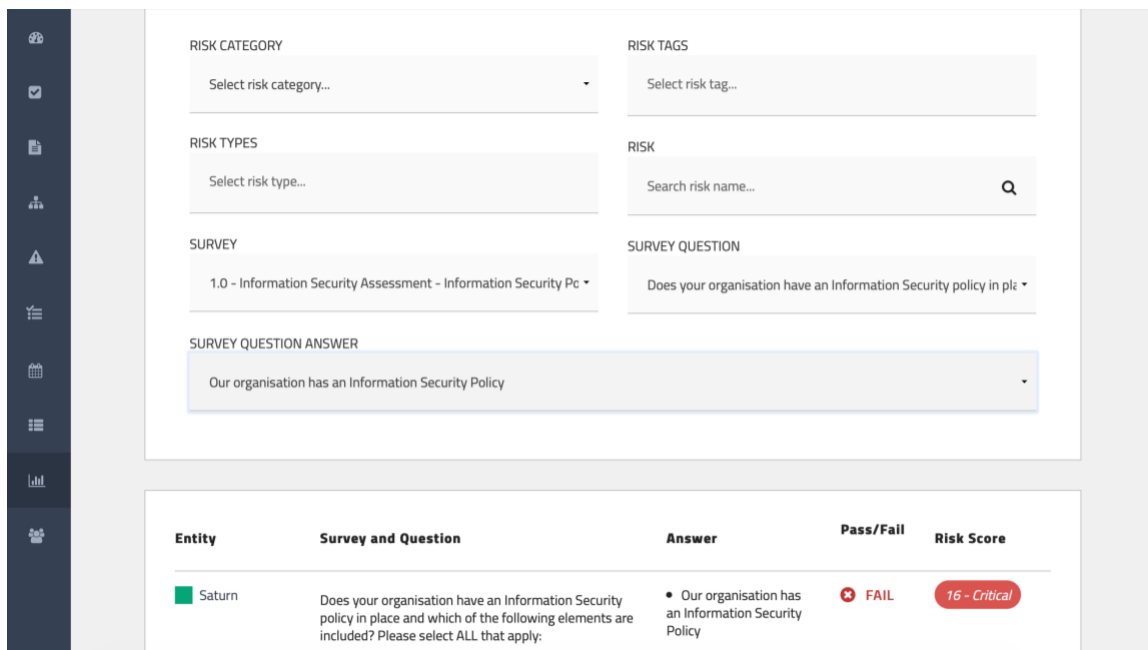
LIVE HISTORICAL **COMPLIANCE**

Risk Categories by Compliance Show graph ▾

Open Filter Showing 1 to 10 of 10 results

| Entity  | Passed Risks | Failed Risks | Highest Risk Category | Lowest Risk Category | Compliance Rating |
|---------|--------------|--------------|-----------------------|----------------------|-------------------|
| Jupiter | 27           | 62           | Tiering               | Data Mapping         | 31%               |
| Venus   | 43           | 45           | Cloud Computing       | Data Mapping         | 49%               |
| Neptune | 22           | 34           | Slavery               | Data Mapping         | 40%               |

- Search entity responses based on filters against specific questions, risks, or surveys, providing increased granularity. For a representation of this capability, please see the screenshot below.



RISK CATEGORY: Select risk category...

RISK TAGS: Select risk tag...

RISK TYPES: Select risk type...

RISK: Search risk name... 🔍

SURVEY: 1.0 - Information Security Assessment - Information Security Pc ▾

SURVEY QUESTION: Does your organisation have an Information Security policy in place? ▾

SURVEY QUESTION ANSWER: Our organisation has an Information Security Policy ▾

| Entity | Survey and Question   | Answer  | Pass/Fail | Risk Score    |
|--------|---|---|-----------|---------------|
| Saturn | Does your organisation have an Information Security policy in place and which of the following elements are included? Please select ALL that apply: | • Our organisation has an Information Security Policy | ✖ FAIL    | 16 - Critical |

With these new compliance reporting capabilities, customers can quickly visualize and address their important compliance requirements.

## Flagging Findings Ensures Thorough Review of Evidence

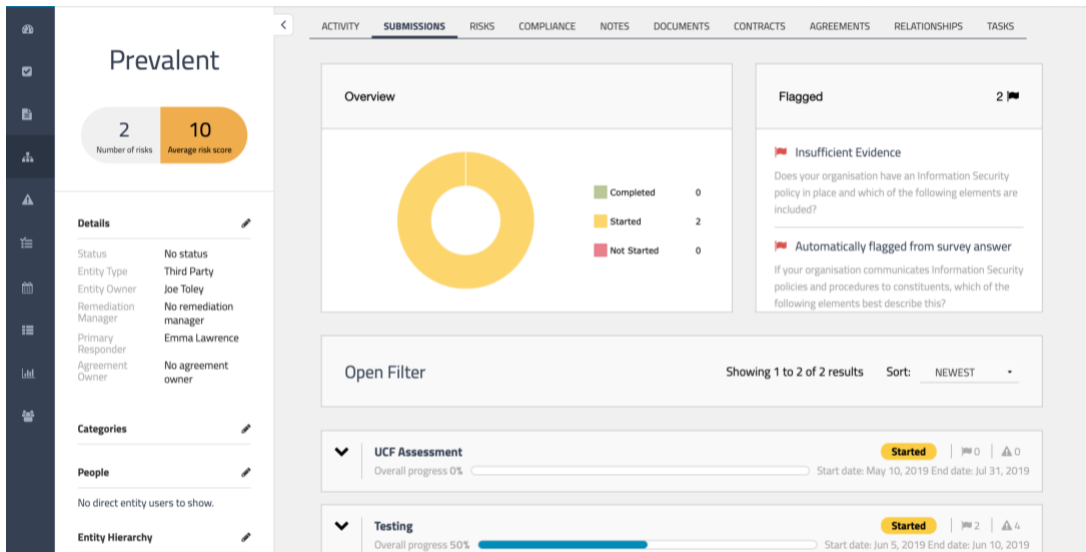
When vendors answer questions in an assessment, the platform automatically creates risks based on how the question was answered. Typically, reviewers or vendor managers will then research the submitted evidence to identify false positives or negatives as part of the submission process.

With version 3.11 the Prevalent platform now provides a workflow mechanism to flag and validate the results beyond the automated risk creation. Flags are points of concern against responses and include a title visible in a summary window. As an example, a vendor may have answered “yes” to an important question but uploaded a document that wasn’t complete or thorough enough to justify a “yes” answer to the question. In this scenario, a flag would be created requiring the attention of the reviewer (a task). The reviewer would validate the evidence and then create the risk if the evidence warranted it.

The new flagging capability helps customers by:

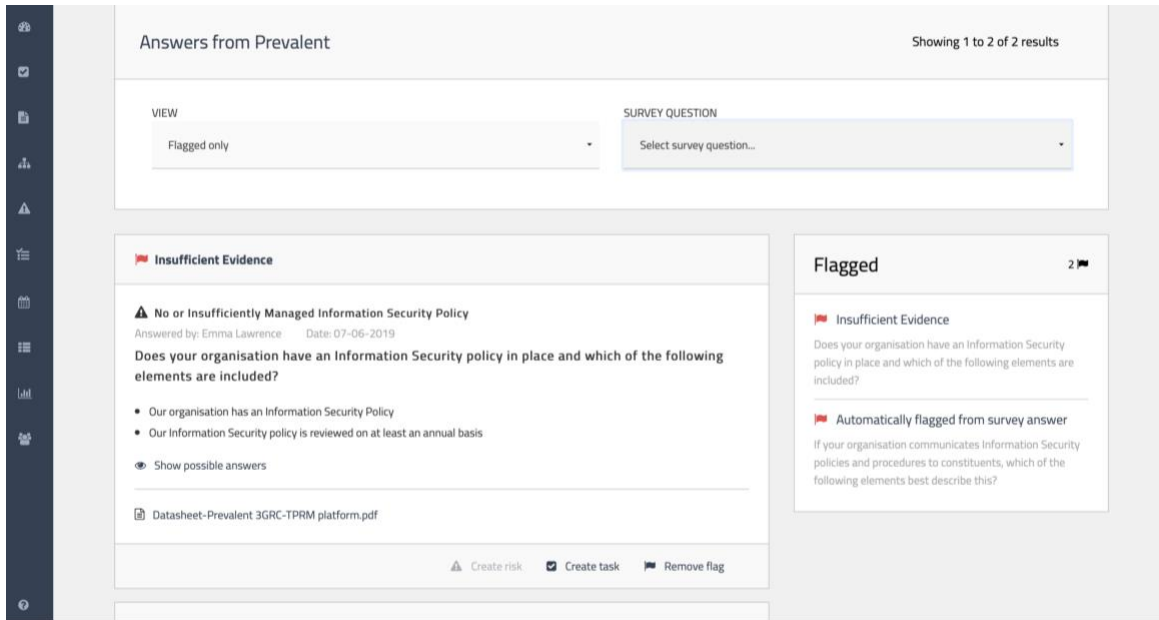
- Creating a flag automatically when an attachment or note has been added.
- Creating a flag automatically when a vendor selects a particular answer. As a validation step, it would be reviewed to determine whether to create a risk.
- Creating a manual flag.

Please see the screenshots below for representations of this new flagging capability.



The screenshot displays the Prevalent platform interface. On the left, a sidebar shows navigation icons and a 'Prevalent' header. Below the header, there are two circular indicators: a grey one with the number '2' labeled 'Number of risks' and an orange one with the number '10' labeled 'Average risk score'. Below these are sections for 'Details', 'Categories', 'People', and 'Entity Hierarchy'. The main content area is titled 'SUBMISSIONS' and features an 'Overview' section with a donut chart showing risk status: Completed (0), Started (2), and Not Started (0). To the right of the chart is a 'Flagged' section with a count of 2. Below the chart is an 'Open Filter' section showing 'Showing 1 to 2 of 2 results' and a 'Sort: NEWEST' dropdown. At the bottom, there are two assessment cards: 'UCF Assessment' with 'Overall progress 0%' and 'Testing' with 'Overall progress 50%'. The 'Testing' card shows a progress bar and a 'Started' status with a count of 2.

*Flags are raised and displayed in the summary window.*



*A clear description of the flag ensures the reviewer has guidance for validation.*

Flagging points of concern in vendor responses ensures that the right risks are investigated, helping to reduce an organization's overall vendor risk profile.

## Additional Enhancements

Please see the Release Notes for a complete list of all enhancements in version 3.11.

## About Prevalent

Prevalent helps enterprises manage risk in third party business relationships. It is the industry's only purpose-built, unified platform that integrates a powerful combination of automated assessments, continuous monitoring, and evidence sharing for collaboration between enterprises and vendors. No other product on the market combines all three components, providing the best solution for a highly-functioning, effective third-party risk program. To learn more, please visit [www.prevalent.net](http://www.prevalent.net).