ARAVO

Data Sheet

# Information Security

Ensure your third parties are protecting sensitive information, data, and digital records with Aravo's Information Security due diligence application.

There is nothing that makes businesses more attentive to third-party risks than information security and cyber security. Exposure and the potential loss of physical and digital records, PII data, IP, and other protected information across shared systems cause many organizations to view its security as one of their most critical business imperatives. Controlling access to data and obtaining assurances of best practice security standards, compliance, and processes across your network of third parties is essential and, in some cases, required by compliance legislation.

Businesses may be evaluating hundreds or thousands of third parties. How they capture and assess the information they need to make informed risk-based decisions for whether to work with a third party matters. A centralized system, evaluation criteria, and risk assessment methodology are critical for businesses to best understand the scale, scope, position, and velocity of a risk. Particularly when it comes to information security, a singular and efficient process can deliver the timely and accurate insights a business needs to make the right decisions.

## Taking the Best Approach

The best, most efficient third-party information security evaluation includes a risk assessment that defines the engagement, including the third party's access to and ability to share data, information, systems, and security protocols. And where there is confidential, restricted, private, personal or customer data and records available, further scrutiny, protections, and defensibility assessments and measures should be put in place. Topic and risk-specific surveys should be completed and affirmed by the third party, and when warranted, additional due diligence should be pursued to gain extra confidence and security.

Despite the seriousness of evaluating a third party's information security capabilities and assurances, doing so can be done efficiently and effectively. Heavy, overly detailed, and off-topic 1000-question surveys burden both sides of the engagement, requiring additional resources. As these surveys are no longer acceptable to many businesses, smart alternatives that streamline processes, stay on topic, and reduce the burden are necessary. Surveys and assessments that are accessible, topical, and concise are more likely to be completed, returned, and informative for accurate risk evaluations.

## The Aravo Information Security Application

The Aravo InfoSec Application is designed for businesses to execute efficient and effective third-party information security assessments. The Aravo Information Security Application is designed to improve the assessment experience for both sides of the engagement, reduce resource requirements, streamline processes, and deliver the insights needed to best evaluate the relationship.

With an adaptable, core set of a few dozen questions, Aravo customers can define the specific information security concerns and requirements they have for each third party. Survey scope and scale can be adapted to specific security topics and needs, follow-up questions can be asked where warranted, and responses can be more accurately calculated and scored in Aravo. Ultimately, customers gain more insight into the information security risks each third party represents, are enabled to pursue additional security assurances, or reject the engagement.

## Addressing Your Information Security Requirements

The Aravo Information Security Application places control of your risk-based third-party assessments in your hands. When you can automate and streamline your information security risk assessment workflows and evaluations, you can:

- Gain a more accurate view of your holistic and specific information security risks across your third-party landscape as well as for each third party
- Capture critical assurances of third-party alignment with key information security standards, frameworks, and certifications
- Better understand the specific capabilities, vulnerabilities, and threats third-party access to your records represents and adjust your program to compensate
- Define clear thresholds for acceptable and unacceptable information security practices, require fixes, and reevaluate as necessary to gain assurances or reject the engagement
- Improve survey response rates, accuracy, and due diligence findings throughout your risk assessment processes, enabling the business to focus on alternative strategies

Information security threats and organizational vulnerabilities move at the speed of light. When a business's systems are increasingly central to its methodologies, intellectual property, and strategies, protecting its records, data, and digital supply chain is critical. When you can best assess, evaluate, monitor, and audit a third party's information security practices with Aravo, you can save headaches, resources, time, and effort while gaining insight, accuracy, and security.

**Ready to learn more? Have any questions? Our experts are on hand to help you on your TPRM improvement journey.**

**+1.415.835.7600 [US]** **+44 (0) 203 955 5318 [EMEA]** **info@aravo.com**