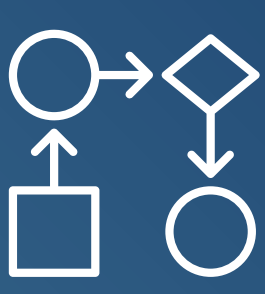
11 must-have functions for your VRM solution

In an ongoing effort to secure their organizations, CISO's are continually challenged with an ever-expanding list of vendors and vendor risk. In fact, 75% of mid-sized companies and enterprises expect their vendor list to grow by 20% or more in the coming years, while only 38% are very confident that they know that number of vendors with privileged access to their systems.

Process and workflow management



A strong VRM solution helps you manage your supply chain risk management program with mapping associated risks to each vendor and the remediation activities necessary. A strong VRM platform such as CyberStrong will provide the flexibility to support any mandate as well as custom control sets and hybrid frameworks.

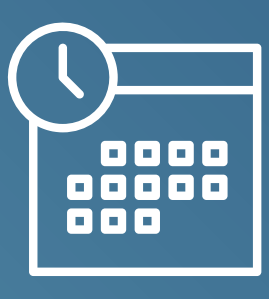
Collaboration

It is critical that any VRM solution you select supports your entire team. Make sure that your solution allows your organization to communicate and share information about vendor risks and remediation. Capable VRM platforms/IRM platforms such as CyberStrong empower team collaboration with control assignment notification, due dates/scheduling, assessment owners, and team access.

Contract management

A VRM solution must support the creation and maintenance of contracts and services associated with a vendor, and the ability to assess the controls and risks associated with each. Ensure that your VRM solution can provide a central location to access these - CyberStrong offers evidence attachment to allow your team easy access.

Control assessment and monitoring



Any VRM solution needs to provide the ability to assess the effectiveness of controls and carry out ongoing monitoring of vendor risks. At a minimum, a solution must support the workflow for the application's other functions, such as exception management and reporting. As you go about implementing your VRM process, ensure that your VRM platform can task out actions with notes and automated reporting to streamline your team.

Exception management

The ability to manage vendor risk exceptions in relation to control requirements, the compensating controls to mitigate risks, and periodic reviews of whether exceptions are still required.

History

The ability to see the IT VRM status of an earlier time, such as a past quarter or year. Make sure you establish early on in a vendor relationship when they will snapshot their status in your VRM solution and that they have the capabilities to do so.

Access and user controls

The ability to provide roles for personalized access to an IT VRM application, and to assign relationships between job roles and individuals, and risks and controls. A strong VRM solution such as CyberStrong will allow you to build teams with Admin, Manager, Collaborator access levels and permissions

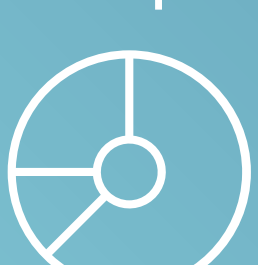
Remediation management

The recording of action plans to identify control failures and other VRM deficiencies, and to track those plans to fulfillment. CyberStrong's graphic representation, benchmarking current scores versus the target offers an "always on" remediation plan they can report against at all times.

Third party content delivery

This includes news feeds, ownership structures, lines, safety violations and financial performance, risk-related alerts, and risk ratings. Foundationally, ensure that your solution allows you to attach documentation as a central storage location for your team.

Vendor performance management

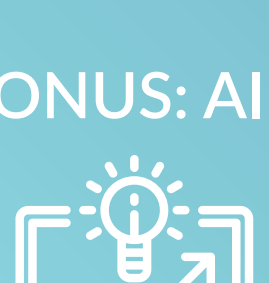


The ability to collect performance data and assess it against expected service levels and deliverables. For example, the CyberStrong platform allows you to benchmark your current control set against a 'Magic Cookie' target. The CyberStrong benchmarking also give you insight into how vendors are improving, allowing you to further optimize your VRM process and program.

Vendor profile management

The ability to import vendor and related contract (engagement) data from other systems, or to input it manually; the ability to collect and organize intelligence about vendors; the ability to manage vendor documentation and other content; and vendor self-service capabilities that enable vendors to maintain and update information themselves. Your VRM solution should allow vendors to access and manage their own profiles to an extent.

BONUS: AI in a VRM solution



With artificial intelligence augmenting security teams more and more, consider exploring VRM solutions that integrate some form of artificial intelligence. The CyberStrong platform uses patented AI and machine learning to provide a live threat feed and remediation suggestions tailored to your organization organized based on impact.

CyberSaint SECURITY