SYBER GRC

Are You in Compliance?

Securities and Exchange Commission, Title 17 CFR: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure RIN 3235-AM89

Outlined below are some key takeaways from the new SEC rule: RIN 3235-AM89, effective September 5th, 2023; and ways SyberGRC can assist in achieving compliance.

Regulation S–K Item 106(b)—Risk management and strategy

Registrants must describe their processes for the assessment, identification, and management of risks from cybersecurity threats, including if any risks from cybersecurity threats have materially affected or are likely to affect their business strategy, results of operations, or financial condition.

How We Help:
SyberGRC and iDPS can provide the **location of sensitive data across all assets** that your organization manages. This bird's eye view of your data allows you to pinpoint weaknesses that can be addressed and reported on as per the above regulatory requirement.

Form 8–K Item 1.05—Material Cybersecurity Incidents

Registrants must disclose Registrants must disclose any cybersecurity incident they experience that is determined to be material, and describe the material aspects of its nature, scope, timing, and impact - within four business days of determining an incident was material.

How We Help:
iDPS provides a **comprehensive report of your Data Value** based on proprietary metrics. This monetary analysis provides you answers to the impact and scope of any incidents with those specific files involved.

Regulation S–K "Item 106(d)(2)"

Registrants are required to disclose in the next periodic report when, to the extent known to management, a series of previously undisclosed individually immaterial cybersecurity incidents become material in the aggregate, ie: whether any data were stolen or altered in connection with the incidents

How We Help:
iDPS scans classify, identify, and locate all sensitive data across your business using **customized keywords that are critical to your operations and industry**. This mission critical data is what can be assessed and monitored before, during, and after incidents.

Regulation S–K "Item 106(b)"

Requires registrants to provide more consistent and informative disclosure regarding their cybersecurity risk management and strategy, including whether the registrant undertakes activities to prevent, detect, and minimize effects of cybersecurity incidents

How We Help:
iDPS data discovery scans will **identify files that already contain permissions** and can help bifurcate sensitive data that is already encrypted vs. data still requiring protection. This will allow for accurate disclosures and provide a map to begin enhancing data protection efforts .

Form 8–K with periodic reporting on Forms 10–Q and 10–K

Although it has not yet been amended: it could be recommended instead that the materiality trigger be replaced with a quantifiable trigger; for example, an incident implicating a specified percentage of revenue, or the costs of an incident exceeding a specified benchmark, could trigger disclosure.

How We Help:
iDPS uses proprietary, patented technology to **derive the monetary value of each static file it identifies**. This analysis can serve as a benchmark for decision making, in regards to incident disclosure.

Contact Us

https://www.sybergrc.com