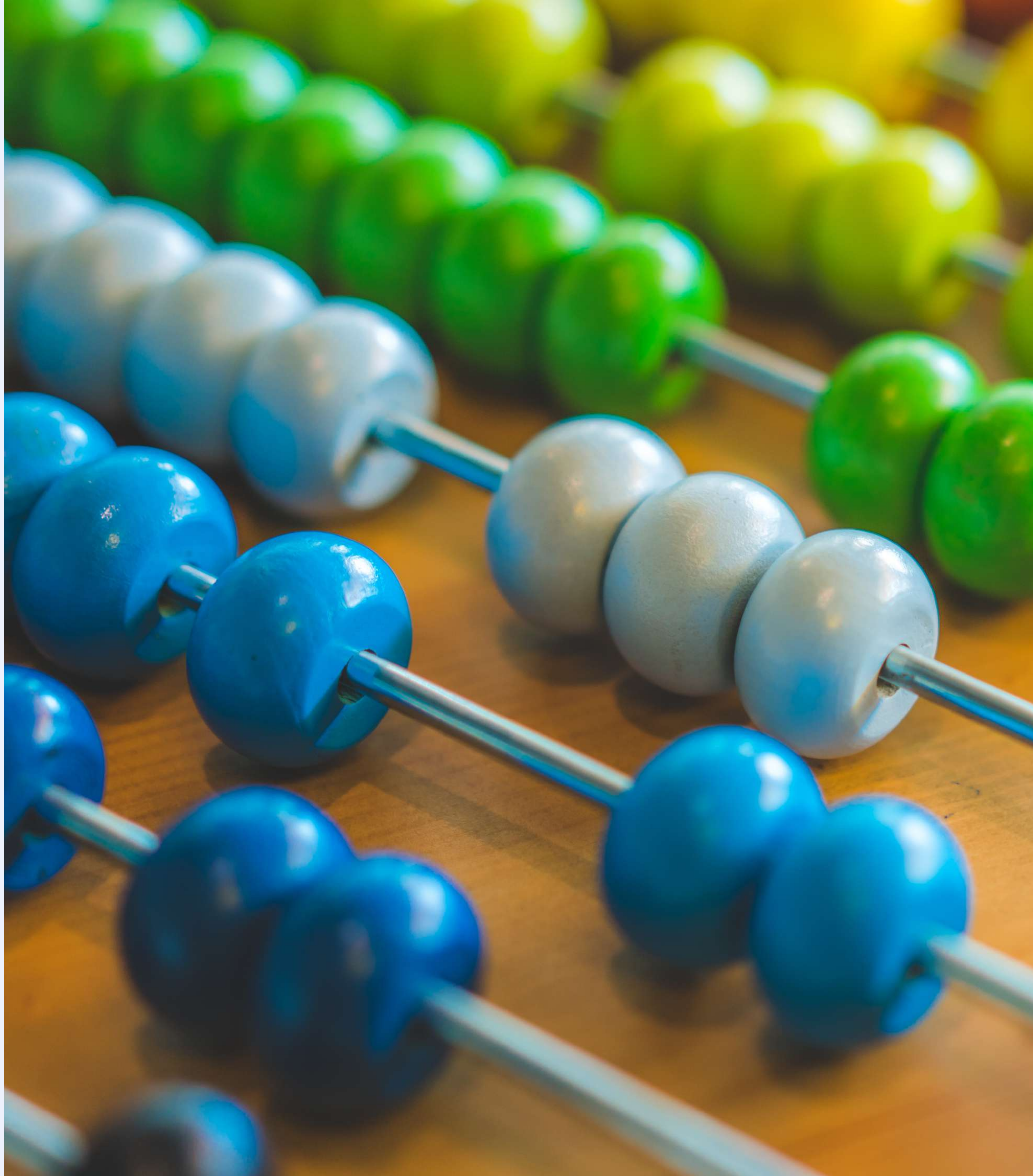
AUDITBOARD

Risk Quantification 101

By Alan Gouevia



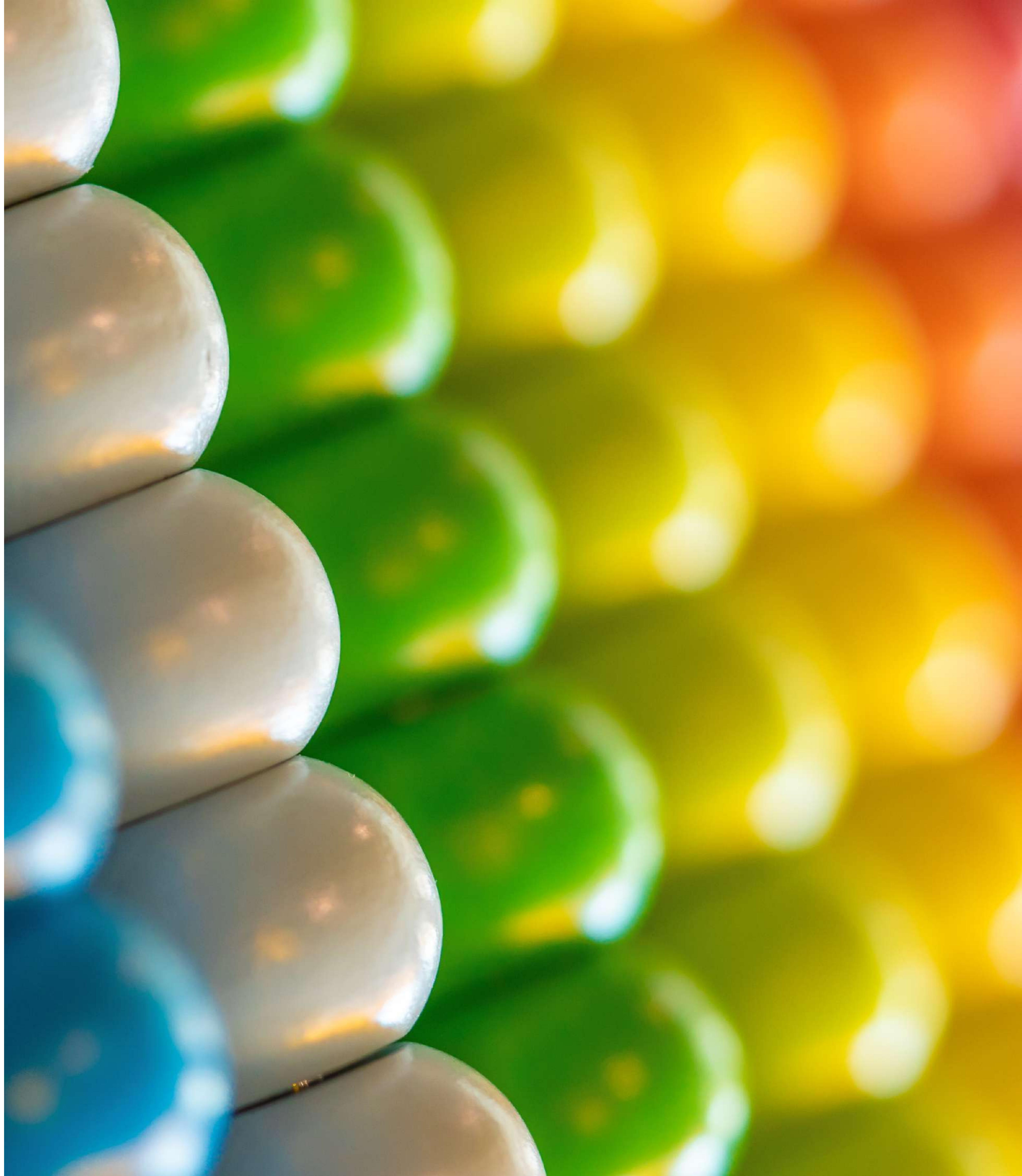
The collective impact of the last two decades of rapid digital transformation across consumer culture and the business world culminated on 5 September 2023 – the day the US Securities and Exchange (SEC) new rules around Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure went into effect. These historic new rules require SEC registrants to disclose their cybersecurity risk management and governance processes, beginning with annual reports for fiscal years ending on or after **15 December 2023**. In addition, Form 8-K Item 1.05 requires all registrants (other than smaller reporting companies) to begin disclosing **material cybersecurity incidents** within four business days starting on **18 December 2023**.

These new rules have forced organizations to transform their IT risk programs from the top down by requiring executive leadership and the board of directors to effectively **identify and assess cybersecurity risk impacts to the business**. As such, registrants that 1) do not have a cybersecurity risk assessment program in place, or 2) are **unable to identify their IT risks** will quickly need to establish these functions and capabilities within their organizations. Private companies are not totally safe writing these new rules off either, as those that are third parties to public companies can potentially be liable for any cyber incidents impacting their public partners.

A recent poll of over 4,000 IT risk professionals, conducted at AuditBoard's IT Risk Now conference, found that **52% of respondents are conducting some form of risk quantification**.

Determining Materiality of Cybersecurity Risks: Why Risk Quantification Matters

In order to determine the **materiality** of a cybersecurity incident or risk, it is necessary for businesses to establish an effective process for quantifying their IT risks. **Risk quantification is the process of defining a risk's impact on the business in terms of a specific value, often in terms of dollars.** For example, take the risk of your business's customer relationship management (CRM) software losing all of its customer data. Categorizing the business impact in terms of dollars — financial loss or loss of new business — is impactful, clear to understand, and helps to set a common context in stakeholder reporting. When set up properly, risk quantification can be an iterative, continuous process that empowers businesses to proactively manage risks, protect valuable assets, and maintain a competitive edge in an ever-evolving landscape of threats and challenges.



Three Tips When Getting Started with Risk Quantification

Understand the myth-based barriers to risk quantification.

Often, the biggest barriers to getting started are narratives based on a poor understanding of risk quantification itself. One of the biggest myths is that the only "right" way to quantify risks is by implementing the Factor Analysis of Information Risk (FAIR) model. While FAIR is a highly useful quantitative risk analysis model that represents an excellent framework goal for businesses to work toward, it is a time-consuming process that can stretch out for a year or more. A poll conducted at AuditBoard's IT Risk Now conference found only **5%** of respondents are utilizing **FAIR**, **24%** are using **NISTRMF**, and **25%** are using other methods to quantify their risks. This helps to illustrate the fact that while most businesses do not have the resources or time for FAIR, they can still take steps to quantify their risks. **The biggest takeaway is that there are many paths to risk quantification.**

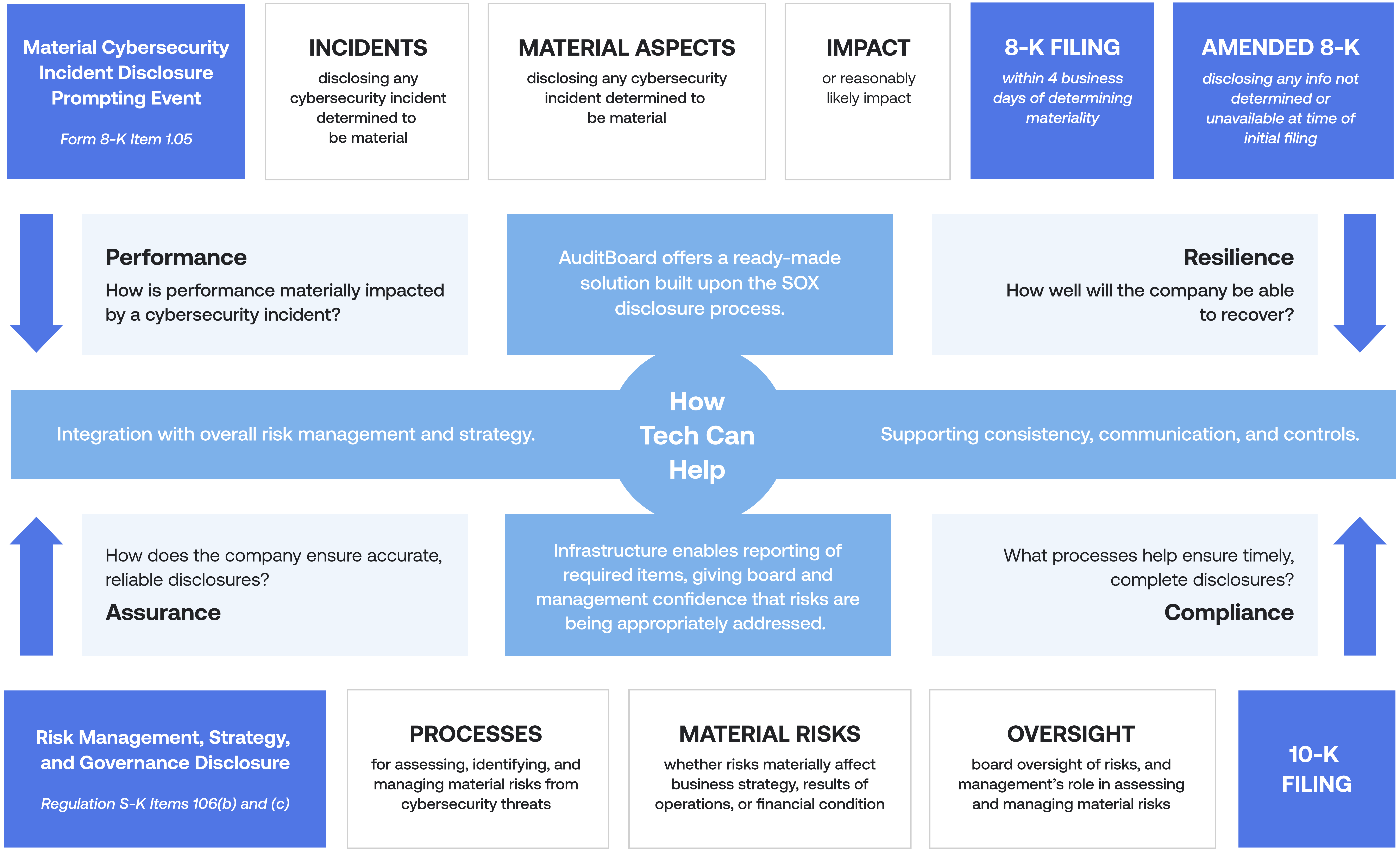
Don't start from scratch — use what you already have.

Risk quantification builds upon any qualitative risk assessment your business currently performs. Rather than starting "from scratch," audit, ITb and InfoSec teams can begin extracting data sources and data streams that can be used for risk quantification from existing risk assessment data collected in the course of complying with IT security requirements and frameworks like ISO, NIST and PCI DSS. **"Building the airplane in mid-air" is a turn of phrase that applies here:** get comfortable with building your cybersecurity risk program while assessing and evaluating your risks. To learn more, see AuditBoard's 7 Steps to Get Started with Asset Data Quantification Checklist.

Technology is a critical resource.

Technology is one of the most important considerations for establishing an effective risk quantification process ahead of the December deadlines, largely because existing risk management resources typically fall short in providing risk teams with accurate and reliable data for their cybersecurity risk efforts. Not only can leveraging IT risk management technology help kick-start your risk quantification efforts, the right solution can enable audit, IT risk and security teams **to organize and streamline their risk quantification processes and automatically connect the dots between their data**. Ideally, the more efficiencies introduced by technology, the more risk quantification work you can perform — and the more efficiently you can improve your feedback.

How Tech Enables IRM and Compliance With SEC Cybersecurity Rules



Material Cybersecurity Incident Disclosure Prompting Event

Form 8-K Item 1.05

INCIDENTS

disclosing any cybersecurity incident determined to be material

MATERIAL ASPECTS

disclosing any cybersecurity incident determined to be material

IMPACT

or reasonably likely impact

8-K FILING

within 4 business days of determining materiality

AMENDED 8-K

disclosing any info not determined or unavailable at time of initial filing

Performance

How is performance materially impacted by a cybersecurity incident?

AuditBoard offers a ready-made solution built upon the SOX disclosure process.

Resilience

How well will the company be able to recover?

Integration with overall risk management and strategy.

How Tech Can Help

Supporting consistency, communication, and controls.

How does the company ensure accurate, reliable disclosures?

Assurance

Infrastructure enables reporting of required items, giving board and management confidence that risks are being appropriately addressed.

What processes help ensure timely, complete disclosures?

Compliance

Risk Management, Strategy, and Governance Disclosure

Regulation S-K Items 106(b) and (c)

PROCESSES

for assessing, identifying, and managing material risks from cybersecurity threats

MATERIAL RISKS

whether risks materially affect business strategy, results of operations, or financial condition

OVERSIGHT

board oversight of risks, and management's role in assessing and managing material risks

10-K FILING

The Most Important Step in Risk Quantification Is Getting Started

By leveraging your organization's existing IT risk data, you can start building the necessary infrastructure for an effective cybersecurity risk management process. Doing so is not only beneficial for compliance with the SEC's new rules but can empower your business to prioritize its IT risk management efforts, better manage its cybersecurity risks and enable leadership to make better, risk-informed decisions. Learn how AuditBoard's ITRM solution helps teams quantify their cybersecurity risks by requesting a tailored demo here.

About the Author

Alan Gouveia is Head of Customer Experience, CrossComply at AuditBoard. Alan has worked in the GRC and cybersecurity space for over 20 years across multiple industries and organizations of different sizes. He specializes in a collaborative approach to GRC and cybersecurity, showing customers how to work across the entire organization to achieve business goals. Connect with Alan on LinkedIn.

About AuditBoard

AuditBoard is the leading cloud-based platform transforming audit, risk, and compliance management. More than 40% of the Fortune 500 leverage AuditBoard to move their businesses forward with greater clarity and agility. AuditBoard is top-rated by customers on G2, Capterra, and Gartner Peer Insights, and was recently ranked for the fifth year in a row as one of the fastest-growing technology companies in North America by Deloitte. To learn more, visit: AuditBoard.com.