Five Tips For Your GRC Risk Scoring System

Enterprises must have meaningful conversations about business risk at all levels and across every department. Risk scoring is a fundamental way of normalizing risk to make sense of complex and disparate data. It enables you to standardize reporting, streamline workflows and communicate risk clearly to stakeholders.

Everyone approaches risk differently so enterprises must develop a risk scoring system that works for all. With the right model you can prioritize risks, remediate incidents, and appropriately allocate resources while performing meaningful vendor comparisons.

Here are Five Concepts Rsam Recommends You Factor into Your Risk Scoring System:

Get Granular

Risks are commonly categorized as Low, Moderate, High and Severe. But a singular, qualitative scale alone isn't good enough. You must get into the nitty gritty to differentiate between assets. Rsam recommends developing a granular numeric scale and converting the value to a risk level. That way you get a deeper understanding of risk while giving end-users something simple to use.

Be Transparent

Your scoring system must be transparent and easily understood. If people don't know how scores are derived, overall credibility will suffer. Complicated algorithms that are difficult to explain will not win fans or adoption. Help users understand the relationship between method and score.

Normalize Scores

Enterprises usually integrate findings from disparate sources, like questionnaires, audits, scanning tools, into their GRC platform. If your organization does this just be sure to normalize scores - like severity ratings from different scanners. That way dashboards and risk-driven workflows will be consistent regardless of the data sources.

Keep it Simple

Even though risk scoring can be quite complex, your job is to keep it simple for stakeholders. Select a scoring system you can easily explain otherwise you won't get traction.

Allow for Flexibility

No one hits the ball out of the park their first time at bat with a risk scoring system. What works for you today, might not continue to work as your program evolves. Make sure your platform allows you to adapt your scoring as your program matures.

Bottom Line

Risk scoring is complicated but your job is to make it easy for the organization to consume. Sacrifice minutia for end-user facing simplicity. Get everyone speaking the same 'risk language' and your program will be more effective.

About Rsam

Rsam is a leader in the field of Governance, Risk, and Compliance (GRC) solutions and is the fastest time-to-value GRC provider. The Rsam platform delivers unparalleled flexibility for companies to leverage out-of-the-box solutions and "Build Your Own" (BYO) applications for a wide range of GRC functional areas, including audit, business continuity management, compliance, enterprise risk, IT risk, incident management, operational risk, policy management, security risk intelligence, vendor risk management, regulatory change management and more. Learn more about Rsam at http://www.rsam.com