A 15-Point Checklist: Top Features for Your Cyber Risk Management Solution

The best practices for implementing quantitative cyber risk management must come together in your selected Cyber Risk Management software. You need an application that provides clear visibility into risk across your highly complicated environments, responds dynamically in real-time to changes in the risk landscape, and accurately analyzes risk in a reliable, defensible way. It must produce reporting that's closely targeted to your business decision-makers' needs and communication style. And ultimately, it should lead you to action steps that measurably reduce risk. It's a tall order, but we've got you covered. Here's a 15-point checklist for the must-have features in the Cyber Risk Mnanagement program you plan to invest in.

360-Degree Assessment	❑ Does the solution determine what information is critical for your company based on your geography, industry, and revenue? ❑ Does it integrate with your existing security tools via API? ❑ Does it assess your critical assets, lines of business, and technology stack?
Continuous Assessment	❑ Does it measure your cyber risk in real-time using automated, AI-driven technologies? ❑ Does it allow custom risk scenario creation to estimate the impact of specific events, such as a ransomware attack?
Credibility	❑ Does the solution leverage a transparent and open-source model? ❑ Does it correlate the data with past reports, audits, and settlements? ❑ Does it factor in industry standards such as MITRE ATT&CK and D3FEND while prioritizing risk? ❑ Does it leverage the FAIR™ methodology to translate cyber risk into a business context?
Contextual Reporting	❑ Does the solution report the potential financial impact of cyber risk on your business? ❑ Does it provide macro and micro scores for the security team? ❑ Does it benchmark your risk posture against others in your industry? ❑ Does the report language resonate with regulators, auditors, the Board, and cyber insurers?
Mitigating Risk	❑ Does the solution deliver actionable strategies to accept, mitigate, or transfer risks? ❑ Are the countermeasures and insights prioritized according to your business requirements and threat profile?