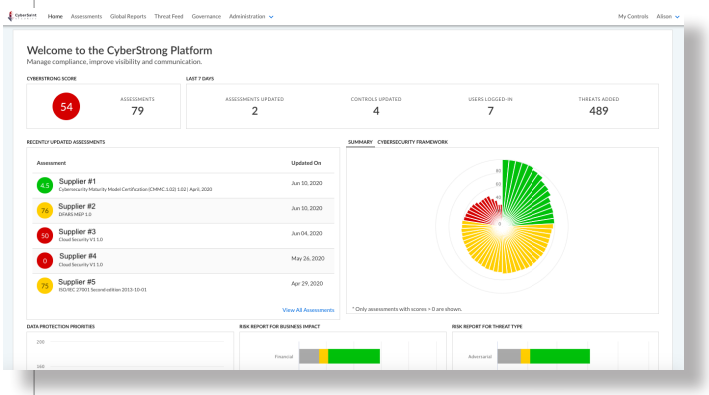
CyberSaint SECURITY

Streamlined Vendor Risk Management

As vendor lists expand and periphery competencies are outsourced, effective vendor risk management is as critical as internal cybersecurity risk management. Enabling vendor risk teams to incorporate their assessment data alongside that of risk, compliance, and audit teams is paramount to a strong security posture. This integrated approach eliminates siloes and miscommunication between internal and external risk management teams and encourages a holistic cybersecurity program strategy. Beyond these benefits, CyberStrong further facilitates greater transparency within vendor-customer relationships that promotes trust and understanding between the goals of organizations and their vendor communities.

Present supply chain risk posture clearly and accurately using visuals that maximize understanding across business leadership.

- Enhance communication of supply chain posture throughout management, and increase cybersecurity program backing from business leaders and the rest of the C-suite.

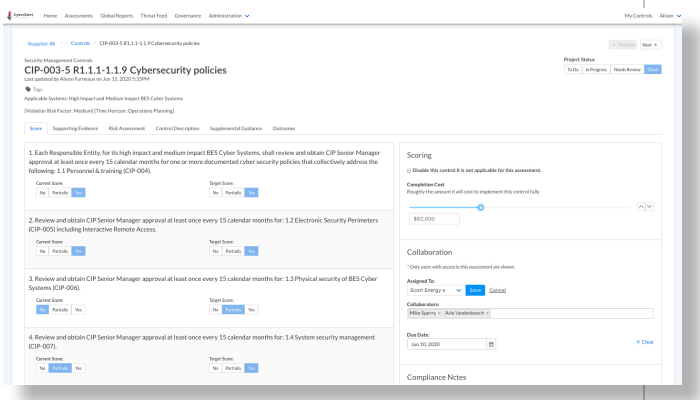


Proactively manage the cybersecurity posture of the supply chain by knowing where your vendors stand.

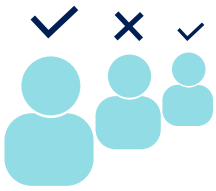
- Know where your supply chain stands on cybersecurity and make sure every vendor knows exactly what is expected of them. Teams increase both the value and also the impact of the security risk and compliance program on the business and increase the value of the investment in human capital already made.

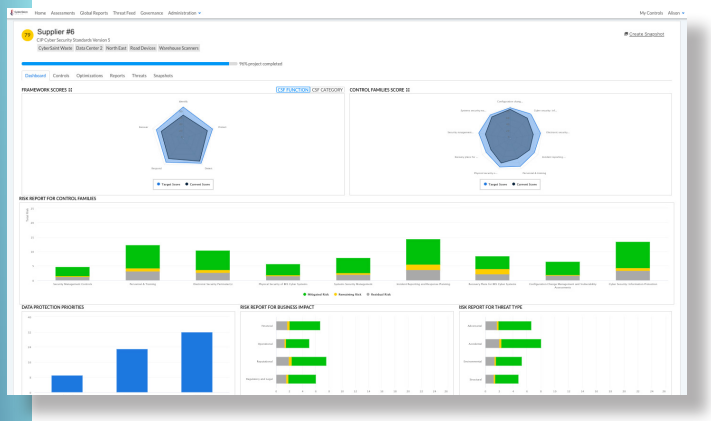
Unify cybersecurity compliance and risk management programs with vendor programs in a single standardized platform.

- Standardization increases awareness of each program function's activity, outputs, and value creation with the ease of reporting on risk and compliance. Increase job satisfaction by eliminating the burden of back-and-forth communication of siloed processes and increasing visibility across the entire program. Team members across the organization are better understood and recognize how their efforts relate to organizational objectives.







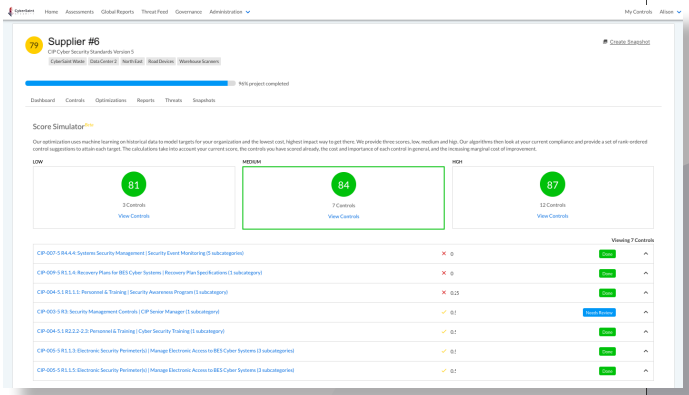



Knowing where vendors stand at all times increases awareness around the program's achievements and showcases its importance.

- When executives ask for a report, security teams and management can deliver those answers almost immediately, delighting their leadership with a fast turn around time and providing eye-catching visuals that present data in a way CISOs are proud of. Answer questions quickly - "What vendors are responsible for the greatest risk in our supply chain?" or "What are our top five vendors by security posture?".

Reveal security program progress in a common language by standardizing measurement across risk, compliance, audit, and vendor programs.

- Leveraging credible measurement is paramount to a proactive security program. Yet, achieving risk quantification with a black-box approach that can confuse their peers and management teams. CyberStrong helps security leaders communicate to leadership in dollars, helping inform better business decisions around what vendors to utilize now and in the future, becoming indispensable to their executive teams for their knowledge and discernment.



> "We looked at other GRC and IRM platforms but they had staggering fees for implementation and integration, were overly complex, and the time-to-value was disappointing...CyberSaint's approach is what CISOs like me have wished for for years."

Chief Information Security Officer
National Healthcare & Hospital Network

Internal team members who own compliance and risk across a segment of vendors are able to:

- Have the oversight to track, report on, and direct vendor risk and compliance activities.
- Collaborate across external vendor teams on questionnaire updates and reports with multi-tenancy.
- Increase efficiencies within internal reporting.
- Inform decision-making processes from which vendors are awarded future contracts to what security responsibilities to require.

CYBERSTRONG FOR VENDOR RISK TEAMS