NYDFS COMPLIANCE SOLUTION

SAG-PM FEATURES AND CAPABILITIES SUPPORTING THE NYDFS REGULATIONS

PART 500 REQUIREMENT CHECKLIST FOR DFS-REGULATED ENTITIES

- ☑ **File Annual Cybersecurity Compliance Forms** *(by April 15 of each year)*
- ☑ **Review and Approve Written Cybersecurity Policies** *(by April 29 of each year)*
- ☑ **Review and Update Risk Assessment** *(by April 29 of each year)*
- ☑ Perform third-party service provider assessments on the continued adequacy of their cybersecurity practices. (§ 500.11(a)(4))
- ☑ Report cybersecurity incidents and extortion payments and provide required information regarding them. (§ 500.17(a), 500.17(c))
- ☑ Develop and maintain up-to-date asset inventory of information systems beginning November 1, 2025. (§ 500.13(a)(2))

☑ File Annual Cybersecurity Compliance Forms *(by April 15 of each year)*

- BCG provides written documentation describing the methods, practices and processes used to conduct software supply chain risk assessments, including SaaS products used in the cloud
- Continuously update methods and practices in order to ensure that best practices are being implemented to keep up with new tactics, techniques and procedures (TTP) used by cyber criminals
- Describe processes used to automate the rapid detection of cyber risks when a new software vulnerability (CVE) is reported

☑ Review and Approve Written Cybersecurity Policies *(by April 29 of each year)*

- Ensure that BCG policies and practices align with end customer policies and practices
- Ensure alignment of software and cloud supplier policies and practices with customer expectations for secure by design, trustworthy products, based on NIST and CISA Secure by Design best practices

☑ Review and Update Risk Assessment *(by April 29 of each year)*

- BCG is continuously updating its comprehensive software supply chain Software Assurance Guardian™, SAG ™, risk assessment products and services to keep up with cyber criminal innovations
- Provide customers with updated set of risk factors and trust score balancing weights used to calculate a trust score based on the seven categories of risk assessed across the software supply chain, described in the SAG ™ patent, US11374961

☑ Perform third-party service provider assessments on the continued adequacy of their cybersecurity practices. (§ 500.11(a)(4))

- BCG provides two features to support third party assessments on a continuous basis for early detection of cyber risks:
  - Continuous, automated risk monitoring for cyber risks based on newly reported software vulnerabilities (CVE), currently reported at a rate of 130 per day
  - Comprehensive software product and vendor risk assessment across 7 risk categories based on producer provided attestations and corroborating evidence to validate the trustworthiness of these attestations culminating in a Final Risk Assessment Report and SAGScore ™ (trust score)
- Continued involvement with key US Government and State Agencies and the Software, Cybersecurity and Risk Management communities to ensure that SAG™ methods are timely and satisfying regulatory requirements over time

☑ Report cybersecurity incidents and extortion payments and provide required information regarding them. (§ 500.17(a), 500.17(c))

- Maintain evidence produced by each risk assessment
- Produce a “Trust Score”, SAGScore™ Cybersecurity Label indicative of the amount of trust calculated for a product/vendor combination based on most recent information available
- Indicate specific areas of concern within each risk assessment across 7 risk categories within a Final Risk Assessment Report
- Produce a Final Risk Assessment Report in PDF format that can be filed along with incident report materials

☑ Develop and maintain up-to-date asset inventory of information systems beginning November 1, 2025. (§ 500.13(a)(2))

- SAG-PM™ and SAG-CTR ™ maintains a list of software product assets and their suppliers that are regularly reviewed for cyber risk
- SAG-CTR ™ enables the sharing of product “Trust Scores” SAGScore with others in the community in order to provide visibility into the trustworthiness of products and vendors using an anonymous cybersecurity label hiding the identity of the party that submits a “Trust Declaration”
- Adjust a product trust score as needed, SAGScore ™, in SAG-CTR ™ based on any changes impacting the trustworthiness of a product or vendor, similar to a FICO® score, but for software products