

Third Party Security & NYDFS

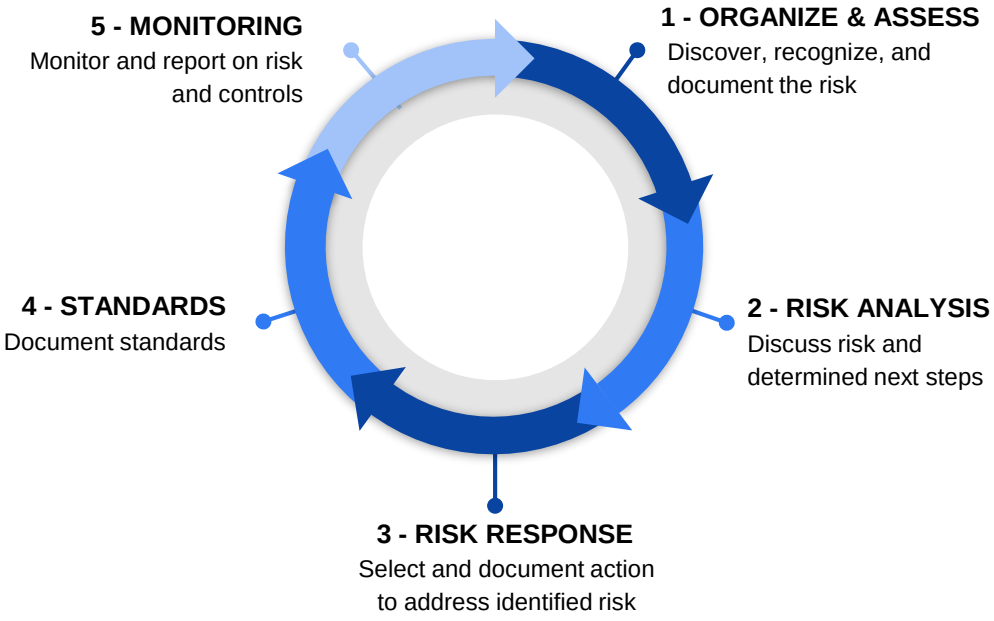
Tony Giannino

October 2020

Public Information

Third Party Cyber Risk Framework

Third party cyber risk management is cyclical, and with any process, the goal is to improve on a daily basis. The diagram below highlights the 5 processes of an effective framework.



Public Information

Organize & Assess

Treat suppliers like assets. Centralize suppliers and organize impact, threat, and control information to determine inherent risk and residual risk.



Capture vendors in a centralized database, triggered by the purchasing contract



Determine impact values through an impact self-assessment



Align threat intelligence to determine likelihood of third party risk scenarios



Collect control effectiveness through a control self-assessment

Public Information

Analysis & Response

After self-assessments and threat intelligence has taken place, risk analysis is the process of creating a space to discuss the risk and determine what to do next.



ACCEPT
Accept residual risk

MITIGATE
Add or improve controls

AVOID
Disqualify supplier

TRANSFER
Get cyber insurance

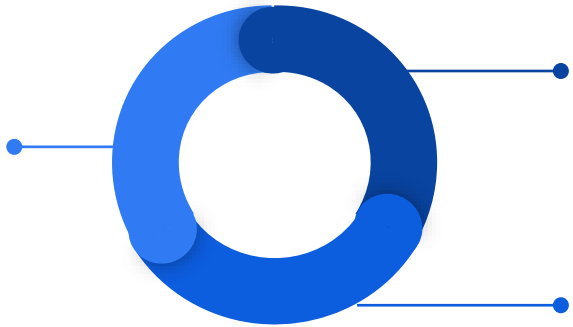
Public Information

Standards & Monitoring

To ensure the enterprise and supplier mutually agree to the controls and processes that are in place, a joint information security standards document should be created. These standards can also be leveraged for control testing and ongoing monitoring.

Regulatory Compliance Controls → Internal Standard Controls → Control Agreement

CONTROL EFFECTIVENESS
Onsite control tests



DATA & ANALYTICS
Control implementation metrics
Control performance metrics

EVENT MONITORING
Event monitoring services
Breach notifications
Threat intelligence

Public Information