Third Party Risk Management Checklist

- [ ] Does the third party have a history of litigation against them or their staff?
- [ ] Are there negative comments/reviews online about the organization?
- [ ] How long has the organization been in business?
- [ ] Do the third party's values align with your organization? Does their mission statement align with your organization's values?
- [ ] Does the third party outsource any of their services?
- [ ] Does the third party have insurance, bonding, and business license documentation?
- [ ] Does the third party contract define their service level agreement with your organization?
- [ ] Does the third party contact define causes for contract/relationship termination?
- [ ] Does the third party operate legally and follow necessary regulatory laws? (HIPAA, PCI, GDPR, CCPA, etc.)
- [ ] Is the third party solvent?
- [ ] How many current clients does the third party have? How many are significant to the third party's operation?
- [ ] How many clients have terminated their relationship with the third party in the last year?
- [ ] Where possible, obtain a list of organizations in the same space that use the third party.
- [ ] Does the third party have policies & procedures for onboarding/off boarding?
- [ ] How does the third party specifically protect customer information?
- [ ] Have they ever experienced a significant cybersecurity incident? Please define and describe it.
- [ ] What types of cybersecurity policies does the third party have in place in your organization today?
- [ ] Does the third party outsource any IT or IT security functions to third-party service providers? If so, who are they, what do they do, and what type of access do they have?
- [ ] How frequently are the third party employees trained on your IT security policies and security awareness training, and do you use automated assessments?

Third Party Risk Management *(continued)*

- ☐ How does the third party inventory authorized and unauthorized devices and software?
- ☐ Has the third party developed secure configurations for hardware and software?
- ☐ What processes does the third party use to monitor the security of your wireless networks?
- ☐ Does the third party have data recovery capabilities?
- ☐ Does the third party have tools that continuously monitor to ensure malicious software is not deployed?
- ☐ What are the processes and tools the third party uses to reduce and control administrative privileges?
- ☐ What processes do you have in place to prevent the exfiltration of sensitive data, particularly sensitive customer data like ours?
- ☐ How do you plan and prepare for a cybersecurity incident? What processes do you have in place to respond to an incident? Do you regularly practice those things?
- ☐ Does the third party conduct regular external and internal tests to identify vulnerabilities and attach vectors? If yes, please describe.
- ☐ How does the third party manage remote access to your corporate network?
- ☐ Does third party have a removable media policy and controls to implement the policy?
- ☐ How do you monitor for unauthorized personnel, connections, devices, and software?
- ☐ Describe the process in place the third party uses to communicate any security incidents affecting your data.
- ☐ Does the third party organization require antivirus on all devices that connect to the network?
- ☐ Does the third party organization have password complexity requirements?
- ☐ Does the third party organization have a patching policy?
- ☐ Does the third party organization have a policy on how to decommission devices?

For more information about third party risk, visit our website at https://www.grfcpa.com/accounting-services/advisory-services/.