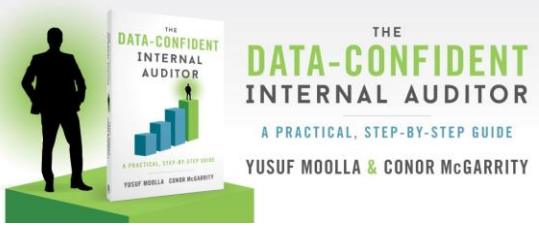

Third Party Compliance Checks

#	Area	Examples of checks to conduct / questions to ask	
1	Governance	1.1	Executive level responsibility for cyber security
		1.2	Data integrity policies, standards and guidelines – e.g., security and access to data, staff onboarding, incident response
2	Assurance	2.1	Independent integrity assurance - nature, frequency, results
		2.2	3rd party security assessment - frequency, results
		2.3	Vulnerability / Penetration testing - frequency, results
		2.4	Provide permission to conduct direct audits (i.e. would the 3rd party allow you to audit them?)
3	Data Protection	3.1	Hosting – which countries, what data centres
		3.2	Encryption of data in transit and data at rest
4	Tech Security	4.1	Patching, antivirus, firewalls, web app firewalls
		4.2	Laptop security, OS Hardening
		4.3	DLP, File integrity monitoring, Intrusion detection, breach identification
		4.4	Secure software development (e.g., OWASP Top 10)
5	User Access	5.1	Multi-factor authentication and account lockout
		5.2	Administrative accounts – how are these controlled?
		5.3	Regular review and timely deletion of user accounts
6	Staff	6.1	Background checks
		6.2	Training
7	Incident Response	7.1	Documented and tested incident response plan, including breach notification and escalation
		7.2	Experienced any incidents?
8	3rd parties	8.1	Expectations of their third parties - same or higher level of control – i.e., how does this 3rd party monitor their 3rd parties?
		8.2	Contracts reviewed, with assurance