Benchmark 2019

Sanlam

Cyber Resilience Benchmark

		SANLAM	ADMINISTRATOR
Governance »	Has your administrator established formal governance policies and processes for Information security, information governance, cyber security, third party management, etc. ?	✓	?
	Does your administrator have cyber insurance to enable financial stability for significant cyber events?	✓	?
Preventative »	Does your current administrator have dedicated information security staff who proactively identify and resolve cyber security vulnerabilities	✓	?
	Is your administrator's information security staff trained to respond to cyber security Incidents?	✓	?
	Does your administrator have processes in place to manage cyber security In terms of: • Prevent data from being stolen from computers (USB port blocking and encrypted hard drives)? • Continuous monitoring of antivirus/anti-malware software to ensure that they are up-to-date?	✓	?
	If there are phishing attempts, is your administrator equipped to identify these events and mitigate the risks?	✓	?
	Does your administrator have processes in place to restrict system accessibllity? (privileged account management and segregation of duties reviews. etc.)	✓	?
Monitoring »	Does your administrator have a dedicated team to actively detect and respond to cyber-attack attempts?	✓	?
Response »	In the event of an Incident, breach or hacking activity. does ~ your administrator have a programme in place to: • Respond to a crisis; • Forensically experts to help investigate; and • The capability to recover data systems after cyber incidents?	✓	?