IT or communication systems and infrastructure Feb-22

Risk Context

Disruption, financial loss or damage to reputation from a failure of information technology systems.
Instability, degradation of performance, or other failure of IT or communication system or infrastructure causing the inability to continue business activities and provide services to the community. This may or may not result in IT Disaster Recovery Plans being invoked.
Examples include failures or disruptions caused by:
-Hardware or software
-Networks
-Failures of IT Vendors
This also includes where poor governance results in the breakdown of IT maintenance such as;
-Configuration management
-Performance monitoring
This does not include new system implementations - refer "Inadequate Project / Change Management".

Potential causes include;

Weather impacts	Non-renewal of licences
Power outage on site or at service provider	Inadequate IT incident, problem management & Disaster Recovery Processes
Out-dated, inefficient or unsupported hardware or software	Lack of process and training
Incompatibility between operating systems	Vulnerability to user error
Cyber crime and viruses	Failure of vendor
Turnover of system administration support	Equipment purchases without input from IT department
Software vulnerability	

Controls Assurance

Key Controls	Type	Date	Rating	Control Owner
Service level agreement with contractor / Vendor	Preventative	Ongoing	***Effective***	DCEO
Performance monitoring by contractor	Preventative	Ongoing	***Effective***	DCEO
Maintenance program	Preventative	Ongoing	***Effective***	DCEO
Formal IT Infrastructure replacement / refresh program	Preventative	Ongoing	***Effective***	DCEO
IT security access protocols and firewalls	Preventative	Ongoing	***Effective***	DCEO
IT Disaster Recovery Plan	**Recovery**		***Inadequate***	DCEO
Multiple data back-up systems	**Recovery**	Ongoing	***Effective***	DCEO
Generator	**Recovery**	Ongoing	***Effective***	DCEO
UPS (20min)	**Recovery**	Ongoing	***Effective***	DCEO
		Overall Control Ratings:	***Effective***	MCSF

Actions	Due Date	Responsibility	Status of Actions
Complete IT Disaster Recovery Plan	Dec-22	DCEO	**Scheduled with IT**

Consequence Category	Risk Ratings	Rating	sk Rating Changed since the la
Service disruption	***Consequence:***	*Major (4)*	***No***
	Likelihood:	*Likely (4)*	***No***
	Overall Risk Ratings:	***High***	**Risk rating trend since last review**

Indicators	Type	Benchmark	Result
Cyber breaches	Lagging	nil	0
Non-availability of network infrastructure during business hours	Lagging	<5	3
System downtime	Lagging	not > than 60 minutes	

Comments

Comments