System	Cloud Service Availability	**FMEA Number**	1
Subsystem	Infrastructure	**Prepared By**	Adrian Cockcroft
Component		**FMEA Date**	12/5/2018
Design Lead	Adrian Cockcroft	**Revision Date**	11/11/2019
Core Team		**Page**	1 of 1

Potential Failure Modes and Effects

Key Date N/A

											Action Results				
Item / Function	**Potential Failure Mode(s)**	**Potential Effect(s) of Failure**	**Sev**	**Potential Cause(s)/ Mechanism(s) of Failure**	**Prob**	**Current Design Controls**	**Det**	**RPN**	**Recommended Action(s)**	**Responsibility & Target Completion Date**	**Actions Taken**	**ew Se**	**ew Oc**	**ew De**	**New RPN**
Availability Zone Durability	Permanent destruction of zone	Total data loss in zone	8	Fire or flood inside building or destruction of datacenter building	2	Cross zone synchronous replication to over 10Km away	1	**16**	Ensure that system can run on two out of three zones						0
	Temporary loss of zone	Loss of compute capacity and non-durable state in zone	5	Power or cooling outage causes reboot of part or all of a datacenter building	3	Cross zone synchronous replication to over 10Km away	1	**15**	Ensure that system can run on two out of three zones						
								0							0
Region Connectivity	Address un-resolvable	Delay while DNS times out, slow fallback response	5	DNS configuration error, denial of service attack, or provider failure	1			**0**	Dual redundant DNS, fallback to local cache, hardcoded IP addresses. Endpoint monitoring and alerts						0
	Unreachable, request undeliverable	Fast fail, no response	4	Network route down	1			**0**	Failover to secondary region						0
	Request undeliverable	Connect timeout, slow fail, no response	4	Router frozen/not accepting connection	1			**0**	Failover to secondary region						0
	Request delivered, no response - stall	Application request timeout, slow fail, no response	4	Broken router, overloaded network or slow dependencies	1			**0**	Failover to secondary region						0
	Response undeliverable	Application request timeout, slow fail, no response	4	Network return route failure, dropped packets	1			**0**	Failover to secondary region						0
	Response received in time but empty or unintelligible	Fast fail, no response	3	Network response failure	2			**0**	Failover to secondary region						0
	Request delivered, response delayed beyond spec	Degraded response arrives too late, slow fallback response	6	Network overloaded dependent services responding slowly	2			**0**	Failover to secondary region						0
	Request delivered, degraded response delivered in time	Degraded timely response	2	Service overloaded, dependent services responding slowly	2			**0**	Alert operators						0