Network Disaster Recovery Audit Checklist

By Paul Kirvan, CISA, FBCI

√	Network DR Audit Controls	Examples of Audit Evidence
	Network DR plan	Documented plan including incident response activities, identification of network DR teams, procedures to take when dealing with a network outage, lists of internal and external contacts
	Network DR program policy	Documented policy that specifies the kinds of disruptions to be addressed and how the organization intends to deal with them
	Network DR program procedures and relevant documentation, forms, etc.	Documented procedures, forms, templates, checklists
	Network operational schedules (e.g., software backups, network rerouting and recovery activities)	Hardcopies or screenshots of schedules
	Network operational elements	Screenshots of network operational controls, e.g., access controls, normal routing methods, emergency alternate routing plans, environment plans, change management, wireless elements
	Network performance reliability metrics	Screenshots of network reliability metrics, e.g., uptime, throughput, MTBF/MTTR*
	Network DR test plans and documented results	Copies of recent network DR test plans, data from actual tests and after-action reports
	Network DR testing and assessment frequency metrics	Screenshots of network DR test and assessment schedules showing frequency metric (e.g., monthly, quarterly) for each activity
	Network DR systems, software, local access facilities, WAN facilities, internet facilities, managed services, cloud-based services	Operational documentation and relevant screenshots for resources used in network DR activities
	Network operational resources -- Local (e.g., data center network devices, local exchange network services)	Operational documentation and relevant screenshots for local network resources
	Network operational resources -- External (e.g., internet service providers, WAN service providers,	Operational documentation and relevant screenshots for external network resources

√	Network DR Audit Controls	Examples of Audit Evidence
	cloud services, wireless providers, managed network services)	
	Network operational security -- this can include perimeter defenses such as firewalls, intrusion detection and prevention systems, internal network security monitoring applications, and physical access into the data center or network operations center	Operational documentation and relevant screenshots for network security measures
	Network DR equipment that can be used in an emergency	Evidence of a supply of network-related devices, e.g., routers, switches, circuit boards, servers, power supplies, wireless components, cabling that are available for use in an emergency

** Mean Time Between Failure (MTBF), Mean Time to Repair (MTTR)*