Data Center Audit Checklist

No	Audit Questionnaire	Document Available Yes/No?	Comment
1	**Phsyical Security**		
1.1	Do you have a policy that addresses the physical security of the Data Center?		
1.2	Do you maintain a register for entry/exit to the Data Center? Is the purpose of visiting the Data Center recorded?		
1.3	Do you have an electronic access control system (e.g., Swipe Card) for entry/exit to the Data Center?		
1.4	Do you conduct an access control review? If yes, at what frequency?		
1.5	Do you allow temporary access to the Data Center? Is it recorded? Do you remove the temporary access as soon as the work is completed?		
1.6	What process is followed if any new person visits the Data Center? Do you escort the visitor?		
1.7	Do you have control over the door automatic lock? (e.g., audio/visual alarm if the door remains open for more than a specified period or signs indicating the door should be closed and locked, with a contact point to report if found unsecured)		
1.8	Has a security camera been installed to monitor the Data Center? Check for Security Cameras Monitored by whom? Recording period? Recording media? Retention period? Administered by whom?		
2	**Environmental and Electrical Control**		
2.1	Does the Data Center have an adequate and safe fire-suppression system with associated detectors (Heat, Smoke, and Temperature monitoring)?		
2.2	When was the system last tested? Smoke alarms - test report Temperature monitoring system - test report Fire extinguishers - check expiry date, or Inert gas fire suppression system - test report		
2.3	Does the Data Center have redundant cooling systems?		
2.4	Do you have a standard checklist for testing? Is the procedure documented?		
2.5	Do you have a UPS system to back up the Data Center's electricity?		
2.6	Do you have updated details on the current electric load capacity of the Data Center?		
3	**Network Security**		
3.1	Do you have firewalls in place to protect the Data Center's network?		
3.2	Are Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) active and regularly monitored?		
3.3	Is there a process to review network logs? If so, how often is it done?		
3.4	Are all network devices (e.g., routers, switches) regularly updated with the latest firmware?		
3.5	Do you perform regular vulnerability scans on the Data Center's network infrastructure?		
3.6	Are there proper encryption measures in place for data in transit and at rest?		
3.7	Is remote access to the Data Center restricted and secured (e.g., via VPN)?		