BROADCAST AUDIENCE RESEARCH COUNCIL
SELF - ASSESSMENT & AUDIT CHECKLIST

	Process	Information Technology		
	Quarter	Q3 (2020-21)		
Sr no.	Area	Controls	Management response	Remarks
1	BCP/DR	Does the company have formal Business continuity policy and procedures?	Yes	Policies and procedures have been defined for Business Continuity.
2	Log management	Are all relevant information sources (i.e. logs, alerts, threat, intelligence, remediation/mitigation, vulnerability scans) being maintained by the company?	Yes	Several third-party audits were conducted, and they have certified that relevant information sources are being maintained by the company.
3	Data Protection	Are there sufficient controls for data protection in the company?	Yes	BARC has implemented security controls for effective data Protections - Advanced threat Protection, Data Leakage Prevention, System Encryption, Mobile Device Management, DNS Web Security, Virtual Desktop, Next generation Antivirus & EDR.
4	Identity and Access	Does the company have Access Management processes and procedures that are standardized across the organization?	Yes	BARC has implemented effective access management procedures by means of Privilege Identity Manager and Continuous access review
5	Incident Management	Does the company have incident response team in place to handle incidents?	Yes	There is a cross-functional incident response team present at BARC. Respective function heads own the responsibility and hierarchy with respect to incident management.
6	Operations	Are there sufficient physical/ environmental controls over IT assets?	Yes	Visitor activity is effectively logged and monitored; including badging, escort policies, and logs for access to sensitive areas
7	Privacy	Are there adequate procedures to ensure privacy of confidential information?	Yes	Data protection policies and procedures are in place to maintain the privacy and confidentiality of information for both internal employees and third-party. Also, BARC enters into Non-Disclosure agreements with all third parties.

Sr no.	Area	Controls	Management response	Remarks
8	Policy and Standards	Have IT - related policies and procedures been documented?	Yes	BARC has documented IT policies and procedures.
9	Security Monitoring	Is security of data relating to the company being constantly monitored?	Yes	A dedicated SOC team at data center is actively functions towards monitoring and maintaining the data security 24*7.
10	Third Party Management/ Procurements	Are there sufficient controls over third party contracts?	Yes	Central procurement function is present at BARC, which manages all procurements. Standard Terms and Conditions have been drafted by our legal team. A standard Contract template is in place
11	Threat and Vulnerability management	Are vulnerability assessments undertaken to identify in advance any threats to the network?	Yes	BARC has operating SOC team to manage and monitor DDOS, IPS, IDS, Web DNS security. Periodic vulnerability assessments are carried out and certified by third parties as well.

Management has represented the existence and operation of the above controls, and the same has been validated by internal audit function of BARC.

Disclaimer: This report is based on confidential material, and may contain proprietary information of BARC India. Neither these reports nor any of the information contained herein may be reproduced in any form under any circumstances without the express prior written permission of BARC India. Further details linked to these reports are bound by client confidentiality agreements, and would be provided on written request made to BARC India.