



**BROADCAST AUDIENCE RESEARCH COUNCIL
SELF - ASSESSMENT & AUDIT CHECKLIST**

	Process	Information Technology		
	Quarter	Q2 (2019-20)		
Sr no.	Area	Controls	Management response	Remarks
1	Asset Management	Is a centralised repository maintained by the company for IT assets?	Yes	An automated tool has been implemented by BARC which provides a centralised repository of assets.
2	BCP/DR	Does the company have formal Disaster Recovery policy and procedures?	Yes	Policies and procedures have been defined for Disaster Recovery for major applications
3	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 parties are providing their inputs to BARC on a regular basis
4	Data Protection	Are there sufficient controls for data protection in the company?	Yes	BARC has implemented Data Leakage Prevention (DLP) for data protection.
5	Identity and Access	Does the company have Access Management processes and procedures that are standardized across the organization?	Yes	BARC has implemented access management procedures.
6	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. Function heads are responsible for each incident in their team
7	Network Security	Is the wireless network infrastructure provided to employees protected?	Yes	BARC has provided protected wi-fi facility to employees.
8	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
9	Privacy	Are there adequate procedures to ensure privacy of confidential information?	Yes	The third-party agreements have an NDA clause in place.

10	Policy and Standards	Have IT - related policies and procedures been documented?	Yes	BARC has documented IT policies and procedures.
11	Security Monitoring	Is security of data relating to the company being constantly monitored?	Yes	Security monitoring of Data center is carried out by the vendor at all times. SOC (vendor managed) is up and functioning 24*7*365
12	Third Party Management/ Procurements	Are there sufficient controls over third party contracts?	Yes	Central procurement function present at BARC, which manages all procurements. Standard Terms and Conditions have been drafted. A standard Contract template is in place
13	Threat and Vulnerability management	Are vulnerability assessments undertaken to identify in advance any threats to the network?	Yes	BARC undertakes a quarterly VA scan activity and an annual PT exercise

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.