

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

	Process	Information Technology		
	Quarter	Q2 (2026-27)		
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. To further enhance resilience, BARC India has implemented a cloud-based Disaster Recovery solution for critical applications.
2	Log management	Are all relevant information sources (i.e. alerts, threat, intelligence, remediation/mitigation) being maintained by the company?	Yes	BARC India has implemented a Security Information and Event Management (SIEM) system that facilitates real-time monitoring, detection, and response to security incidents. Furthermore, the company adheres to CERT India guidelines by retaining logs, ensuring compliance.
3	Data Protection	Are there sufficient controls for data protection in the company?	Yes	BARC India has implemented various security measures to protect its data and systems from unauthorized access, data loss, and cyber threats. These measures include Advanced Threat Protection, Data Loss Prevention (DLP), System Encryption, Mobile Device Management (MDM), DNS and Web Security, Virtual Desktop, Endpoint Detection and Response (EDR), and Web Application Firewall (WAF). Additionally, Role-Based Access Control (RBAC) is used to ensure that users have access only to the systems and information required for their roles. BARC India also conducts regular security awareness sessions and Red Team exercises to improve employee awareness and test the effectiveness of its security controls.

Sr no.	Area	Controls	Management Response	Remarks
4	Identity and Access	Does the company have Access Management processes and procedures that are standardized across the organization?	Yes	BARC India manages user access through an Identity and Access Management (IAM) solution. Access is granted based on users' roles and responsibilities using Role-Based Access Control (RBAC). Multi-Factor Authentication (MFA) is implemented to provide an additional layer of security.
5	Incident Management	Does the company have incident response team in place to handle incidents?	Yes	BARC India has established a cross-functional incident response team to effectively manage security incidents. Each function head is responsible for overseeing incident management within their respective areas, ensuring clear ownership and accountability.
6	Operations	Are there sufficient physical/environmental controls over IT assets?	Yes	Visitor activity at BARC India is rigorously logged and monitored to ensure security and safety. This includes a robust badging system, strict escort policies for visitors. All the IT assets are tagged, and physical verification is done by the company as per policy.
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 India enters into Non-Disclosure Agreements with all third parties. The Company has also implemented Mobile Device Management (MDM) protocols to safeguard the information on Mobile devices for information privacy.
8	Policy and Standards	Have IT - related policies and procedures been documented?	Yes	BARC India maintains a comprehensive set of documented IT policies and procedures, regularly reviewing and updating them to address evolving challenges. The Company reviews and enriches these policies to safeguard the interest of Information Technology.
9	Security Monitoring	Is security of data relating to the company being constantly monitored?	Yes	BARC India has a managed Security Operations Center (SOC) that continuously monitors and analyses its assets. The SOC helps identify potential security threats and supports timely response to security incidents.

Sr no.	Area	Controls	Management Response	Remarks
10	Third Party Management/ Procurements	Are there sufficient controls over third party contracts?	Yes	BARC India has a Central Procurement Function, which effectively manages all procurements. Standard Terms and Conditions have been drafted by the Legal Team to avoid conflicts in the terms of agreements.
11	Threat and Vulnerability management	Are vulnerability assessments undertaken to identify in advance any threats to the network?	Yes	Threat management is handled by an Attack Surface Risk Management & Reduction System, and internal vulnerability assessments are conducted quarterly in addition to the external VAPT once a year.
12	Web application Vulnerability Management	Are Web application assessments undertaken to identify in advance any threats to the critical applications?	Yes	Internal Web Application assessments are conducted on quarterly basis, in addition to external Web Application assessments for critical applications, which are carried out by an external agency as and when introduced. In addition, a Managed Web Application Firewall (WAF) is implemented to provide an additional layer of security and protection for web applications.
13	PAM (Privileged Access Management) Management	Are PAM safeguards privileged passwords and credentials, applying a Zero Trust Security to ensure only authorized users gain access to critical systems?	Yes	BARC India has an established PAM solution used to secure, manage, monitor, and control privileged accounts and access to sensitive systems across an organization's IT environment.

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

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 circumstance, without the express prior written permission from BARC India. Further details linked to these reports are bound by client confidentiality agreements and would be provided only on written request made to BARC India.