BROADCAST AUDIENCE RESEARCH COUNCIL
SELF - ASSESSMENT & AUDIT CHECKLIST

	Process	Information Technology		
	Quarter	Q2 (2025-26)		
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 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. Additionally, the organization employs **Role-Based Access Control (RBAC)** to restrict system access based on users' roles.
4	**Identity and Access**	Does the company have Access Management processes and procedures that are standardized across the organization?	Yes	Role-Based Access Control (RBAC) to restrict system access according to the specific roles of individual users within the organization. This is complemented by **Multi-Factor Authentication (MFA)**, adding an extra layer of security to the authentication process.

Sr no.	Area	Controls	Management response	Remarks
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 established a managed Security Operations Center (SOC) to ensure continuous monitoring and analysis of its systems, networks, and data. This proactive setup enables the detection and response to potential security threats and breaches in real time

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.
13	**WAF (Web Application Firewall) Management**	Does WAF protect against online risks by filtering and monitoring HTTP, HTTPS, and custom port traffic between a web application and the internet?	Yes	Managed WAF is in place
14	**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.