Zero Trust Maturity Assessment Checklist for CEOs

Instructions:
Rate each question from **1 (Not Implemented)** to **10 (Fully Implemented and Optimized)**.
Add up the total score to gauge overall Zero Trust maturity.

#	Question	Score (1–10)
1	Are all users, including executives and contractors, required to use multi-factor authentication (MFA) for every access attempt, regardless of location or device?	
2	Is device verification enforced before granting access, ensuring only compliant and managed devices connect to company resources?	
3	Are user permissions based on the principle of least privilege, with regular reviews to remove unnecessary access rights?	
4	Is network segmentation implemented to isolate sensitive systems and limit lateral movement in case of a breach?	
5	Are access requests continuously evaluated based on user behavior, device health, and contextual risk factors?	
6	Is there centralized visibility into all user and device activity across cloud and on-premises environments?	
7	Are privileged accounts protected with additional controls such as just-in-time access and session monitoring?	
8	Is data classified and protected according to sensitivity, with encryption applied both in transit and at rest?	
9	Are third-party vendors and partners subject to the same Zero Trust policies and verification standards as internal users?	
10	Is there a continuous improvement process in place to assess, test, and update Zero Trust policies and technologies?	

Scoring Guide:

- **0–30:** Early Stage – Foundational controls needed.
- **31–60:** Developing – Partial implementation; key gaps remain.
- **61–80:** Mature – Strong controls with room for optimization.
- **81–100:** Advanced – Fully integrated Zero Trust architecture.