DOL Cybersecurity Readiness Checklist

Rate your TPA against all 12 EBSA cybersecurity best practices.

SCORING: **YES** = Fully implemented & documented **PARTIAL** = In progress or undocumented **NO** = Not in place

1	**Formal, Documented Cybersecurity Program** Written policy covering your entire TPA, reviewed annually, with defined scope and governance.	☐ Yes	☐ Partial	☐ No
2	**Annual Risk Assessments** Documented evaluation of threats to participant data, systems, and operations — with remediation plans.	☐ Yes	☐ Partial	☐ No
3	**Third-Party Audit of Security Controls** Independent verification via SOC 2 Type II, NIST CSF assessment, or equivalent third-party examination.	☐ Yes	☐ Partial	☐ No
4	**Clearly Defined Security Roles** Named individual(s) responsible for cybersecurity decisions, incident response, and compliance oversight.	☐ Yes	☐ Partial	☐ No
5	**Strong Access Control Procedures** Phishing-resistant MFA on all internet-exposed systems. Least privilege. Quarterly access reviews.	☐ Yes	☐ Partial	☐ No
6	**Third-Party Vendor Security Reviews** Documented due diligence on every vendor touching participant data — recordkeepers, payroll, IT providers.	☐ Yes	☐ Partial	☐ No
7	**Cybersecurity Awareness Training** Regular phishing simulations and security training for all staff. Documented completion rates.	☐ Yes	☐ Partial	☐ No
8	**Secure System Development Life Cycle** Change management procedures for all system modifications. Testing before production deployment.	☐ Yes	☐ Partial	☐ No
9	**Business Resiliency Program** Tested DR & business continuity plans with defined RTO/RPO for critical TPA systems.	☐ Yes	☐ Partial	☐ No
10	**Data Encryption** AES-256 encryption at rest. TLS 1.2+ in transit. Encrypted backups with separate key management.	☐ Yes	☐ Partial	☐ No
11	**Strong Technical Controls (NIST-Aligned)** 24/7 monitoring, EDR/MDR, network segmentation, vulnerability management, patch management.	☐ Yes	☐ Partial	☐ No
12	**Documented Incident Response Procedures** Written IR plan with severity levels, escalation paths, notification timelines. Tested annually.	☐ Yes	☐ Partial	☐ No

Your Score: _____ Yes _____ Partial _____ No **10-12 Yes = Strong** **7-9 Yes = Gaps exist** **<7 Yes = At risk**