Policies:
Policy 1: Access is restricted based on least privilege.
Policy 2: Passwords must be at least 14 characters.
Policy 3: MFA is required for administrative access.
Policy 4: Backups are performed daily and retained 30 days.
Policy 5: Logs are retained for 12 months.
Policy 6: Data at rest is encrypted using AES-256.
Policy 7: Vendors must undergo annual security reviews.
Policy 8: Incident response plans are tested twice yearly.
Policy 9: Patches are applied within 14 days of release.
Policy 10: Access reviews occur quarterly.

Audit Questions:
1. Does the system enforce least-privilege access?
2. Are password length requirements at least 14 characters?
3. Is MFA required for administrative access?
4. Are backups performed daily and retained for 30 days?
5. Are logs retained for 12 months?
6. Is data at rest encrypted with AES-256?
7. Are vendors reviewed annually for security?
8. Are incident response plans tested at least twice per year?
9. Are security patches applied within 14 days?
10. Are access reviews performed quarterly?
11. Is there evidence of exceptions to the least-privilege policy?
12. Are password policies enforced across all systems?
13. Is MFA required for remote administrative access?
14. Are backup failures tracked and remediated?
15. Are logs protected from tampering?
16. Is encryption applied to portable media?
17. Are vendor reviews documented with findings?
18. Are incident response tests documented and reviewed?
19. Are patching timelines tracked for compliance?
20. Are access review results documented and approved?