IT Capability Assessment – Question Review Document

1. Service desk processes for incident, request, and escalation are documented and consistently followed.

2. Incidents are logged, triaged, and resolved using a defined incident management framework.

3. Changes follow a documented change management process including approvals and communication.

4. Knowledge articles are documented, updated, and used to support consistent service delivery.

5. A clear service catalog and self-service portal is available and used effectively.

6. SLAs, KPIs, and service performance metrics are tracked and reviewed regularly.

7. Continuous improvement practices are embedded into service management operations.

8. Multi-factor authentication (MFA) is enforced for all staff and all administrator accounts.

9. Endpoint protection (EDR or next-gen antivirus) is deployed across laptops, workstations, and servers.

10. Patching and vulnerability remediation occur on a regular, enforced schedule.

11. Backups are reliable, secure, and regularly tested for recovery.

12. Admin rights are restricted, monitored, and follow least-privilege principles.

13. Logging, alerting, and monitoring are enabled for critical systems.

14. Cyber controls are aligned with Essential 8, ISO 27001, or SMB1001 requirements.

15. Core business processes are documented and consistently followed.

16. Manual processes have been identified and prioritised for automation.

17. Systems and applications integrate effectively with clear data flows.

18. Approvals and authorisations use automated workflows rather than email-based processes.

19. Process documentation and training materials are current and easily accessible.

20. Operational processes have defined metrics and are monitored regularly.

21. Cross-team workflows are well-defined and minimise handoff delays.

22. Monitoring and alerting are in place for key systems and respond to issues proactively.

23. Standard operating procedures are well-defined and used consistently across operations.

24. Routine tasks (provisioning, checks, updates) are automated where possible.

25. Intelligent tools (AI-assisted or advanced rules-based automation) support operational decision-making and reduce manual workload.

26. Capacity and availability management are monitored and reviewed to prevent outages.

27. Incident patterns and root causes are identified through event correlation.

28. Operational reviews and governance meetings occur regularly with actionable outcomes.

29. Identity and access management is centralised with strong lifecycle processes.

30. Devices are centrally managed with enforced security baselines.

31. Network segmentation and security controls follow modern best practices.

32. Backup and disaster recovery architecture meets defined RTO/RPO requirements.

33. Applications and infrastructure have clear cloud readiness or cloud adoption strategies.

34. Platforms and tooling have clear governance, admin roles, and lifecycle processes.

35. Engineering and platform practices include observability, telemetry, and consistent monitoring.