**Structure of the questionnaire for the Database - Draft 1:**

|  |  |  |
| --- | --- | --- |
| **Green**   1. Training in the last 3 months 2. Current Cyber Security Strategy 3. Committed & Compliant behaviour 4. Assigned Key Decision Maker 5. Full knowledge of hardware & software 6. Current & updated inventory of IT 7. Clear understanding of user policies 8. Up to date IAM 9. Regular review of Privileged User 10. Up to date Patch Management 11. Appropriate level of competence & resources 12. Comprehensive induction 13. Adequate cyber security budget 14. Strong Password Management System 15. Vetted supply chain 16. Clear and defined Incident Management Team 17. Proactive & Preventative: threat hunting, breach attack simulation (BAS) 18. Strong Information Security Management System (ISMS) | **Amber**   1. Training in the last 6M 2. Outdated CSS 3. Compliant behaviour 4. Unassigned KDM 5. Some knowledge 6. Outdated IT inventory 7. Not fully aware of UP 8. Outdated IAM 9. Outdated PU 10. Outdated PM 11. Inappropriate level 12. Inadequate induction 13. Unspecified CSB 14. Weak PAM 15. Unregulated SC 16. Not defined IMT 17. Reactive 18. Inadequate ISMS | **Red**   1. No training in 12 2. No strategy 3. Non-compliant 4. No KDM 5. No knowledge 6. No IT inventory 7. No UP 8. No IAM 9. No PUA 10. No PM 11. No level of C&R 12. No induction 13. No CSB 14. No PAM 15. Unvetted SC 16. No IMT 17. Oblivious 18. No ISMS |

|  |
| --- |
| 1. When was the last time of education and awareness training? 2. How do you classify your Cyber Security Strategy? 3. What % of the workforce have completed Data Protection, GDPR training? What % of the workforce engage in extra activities? 4. Do you have a dedicated person responsible for cyber security? What is their position? 5. Can you safely account for every hardware and software used within the organisation? 6. Is the IT inventory up to date and documented? 7. Do you have a user policy in place? 8. Do you have an up to date IAM system in place? 9. When was the last review of the Privileged User conducted? 10. When was the last Patch Management conducted? 11. How many IT staff are within the company? What is their level of experience? 12. What is covered during the induction period? 13. What % of your annual turnover is dedicated to cyber security? 14. How often are users prompted to change passwords and what’s the requirement? 15. Who are part of your supply chain. When were they last vetted? 16. Who makes part of your incident management team, and their roles? 17. What proactive measures are in place to prevent data breaches or cyber attacks? 18. Do you have an ISMS in place? |