DIGITAL AUDIT CHECKLIST

blue wren

1. System Inventory	Yes / No / NA
Have all software systems currently in use been listed?	
Has it been recorded who uses each system and for what purpose?	
Have licence or subscription costs been documented?	
2. Appropriateness of Systems	
Do current tools fully support business processes without forcing workarounds?	
Are any systems outdated or no longer suitable for the company's size or sector?	
Is staff satisfaction with each system reviewed regularly?	
3. Data Management	
Has the location of all critical business information been identified?	
Is key data stored in secure, structured databases rather than flat files?	
Do audit trails exist for edits and updates to records?	
Can reporting be generated consistently and accurately?	
4. Integration and Efficiency	
Has the flow of information between systems been mapped?	
Are there areas where data is still re-entered manually?	
Do systems integrate via APIs or imports/exports?	
Have opportunities to connect systems and reduce duplication been identified?	
5. Security and Compliance	
Is data encrypted at rest and in transit?	
Are access controls (permissions, password policies, MFA) in place and reviewed?	
Are backup processes (frequency, location, restoration testing) in place and tested?	
Is the business compliant with data protection regulations (GDPR, sector standards)?	
6. Cost and Value	
Have current system costs been compared against actual usage and benefits?	
Have unused licences or redundant subscriptions been identified?	
Could costs be reduced through system consolidation?	
Are low-cost tools creating hidden inefficiencies?	
7. Scalability and Future-Proofing	
Can systems handle growth in staff, projects, or clients?	
Can platforms be configured or adapted as processes evolve?	
Do vendors provide regular updates and security enhancements?	
Can data be exported or migrated if systems are changed?	