APPENDIX 2

PRIVATE AND CONFIDENTIAL

E-tec
Business Services

IT AUDIT NEEDS ASSESSMENT

TAMWORTH BOROUGH COUNCIL

SEPTEMBER 2021

Providing Advice and Assurance
Over Information and Communication Systems

1. INTRODUCTION

1.1 At the request of the Audit Manager we undertook an IT audit needs assessment at Tamworth Borough Council. The purpose of the assessment was to identify the key areas of risk associated with the provision of IT services and to develop a programme of work to provide assurance that these risks are being managed.

1.2 There is no such thing as a risk-free environment and compliance with any number of standards does not create such an environment. Building a strong internal control culture within Information Technology can help to:

- Ensure efficient and effective operations;
- Enhance risk management competencies and prioritisation of initiatives;
- Enhance overall IT governance;
- Enhance the understanding of IT amongst senior management and Executive;
- Optimise operations with an integrated approach to security, availability and processing integrity;
- Contribute to compliance with regulatory requirements in areas such as data security and privacy;
- Align project initiatives with business requirements; and
- Prevent loss of intellectual assets and the possibility of data breaches.

1.3 This report is based upon the high-level work completed at the time of the review and should not be seen as a comprehensive assessment of all IT operations or an evaluation of all areas of IT risk exposure. As such, no specific assurances are provided on the overall IT control framework or the level of risk exposure.

2. METHODOLOGY

2.1 Our approach to completing the IT audit needs assessment was to review the level of risk exposure in five core IT functional areas, as shown in the opposite diagram.

2.2 The level of risk in each area was evaluated and assessed to develop an IT audit plan for the period 2021-22, as detailed in Section 3 of this report. We have also highlighted other areas that may warrant a review in future years at Section 4.

2.3 The risk evaluation was undertaken through discussions with the Head of Technology and Information Services, and:

- A review of the IT risk register;
- Consideration of the IT audit work completed in the last three years and the level of assurance provided by each review;
- Identification of any significant changes made or planned to the IT environment and/or business systems; and
- Our experience and knowledge of issues facing the sector and other similar organisations.

2.4 The IT audit plan should be reviewed annually to reflect any changes to technology, business systems or core IT infrastructure.

3. PROPOSED COMPUTER AUDIT PLAN 2021/22

Area	Audit	Justification	Key Risks	No of Days
Operations	IT Backup and Recovery	• A new IT backup solution is being implemented. • The failure and unavailability of IT systems and services is included on the IT risk register.	• Loss of data, leading to operational disruption due to the unavailability of line of business systems.	10
Compliance	Payment Card Industry Data Security Standard (PCI DSS)	• There is no clear ownership or roadmap for PCI compliance.	• Financial penalties as a result of cardholder data not being secured and safeguarded.	10

4. Forward Plan

4.1 The following are potential areas for future IT audits, subject to an annual review.

Area	Audit	Justification	Key Risks
Cyber Security	Cyber Security	• This remains an area of high risk to all organisations.	• Cyber-attack, leading to a data breach or loss of IT systems and services.
Compliance	GDPR	• This is a high risk on the IT risk register.	• GDPR requirements are not met, leading to financial penalties and reputational damage.
Business Systems	Web Portals	• A number of new web portals are being implemented to enhance online services.	• Poor security configuration, leading to unauthorised access to data.
Cyber Security	IT Disaster Recovery	• This area has not been subject to any recent review.	• IT systems and services cannot be recovered within agreed timescales following a major incident.
Management	IT Strategy	• A new IT Strategy has recently been approved for the period 2020-25.	• The IT Strategy does not have a clear and effectively managed implementation plan to ensure all stated objectives are achieved.