CHARNWOOD BOROUGH COUNCIL

INTERNAL AUDIT IT PLAN 2019-2022

December 2018

INTRODUCTION

Our role in providing internal audit support on the IT audit programme is to provide independent, objective assurance designed to add value and improve your performance. Our approach, as set out in the Firm's Internal Audit Manual, is to help you accomplish your objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes.

Our approach complies with best professional practice, in particular, CIPFA Internal Audit Standards and Public Sector Internal Audit Standards.

Internal Audit at Charnwood Borough Council

We have been appointed to provide internal audit support on IT audit to Charnwood Borough Council (the 'Council') to provide the Audit and Risk Manager, s151 officer, and the Audit Committee with assurance on the adequacy of internal control arrangements, including risk management and governance, relating to the IT control environment.

Responsibility for these arrangements remains fully with management, who should recognise that internal audit can only provide 'reasonable assurance' and cannot provide any guarantee against material errors, loss or fraud. Our role at the Council will also be aimed at helping management to improve risk management, governance and internal control for IT systems and controls, so reducing the effects of any significant risks facing the organisation.

In producing the IT internal audit operational plan for 2019-20, 2020-21 and 2021-22 strategic plan we have sought to further clarify our initial understanding of the business of the Council together with its risk profile in the context of:

- The overall business strategy and objectives of the Council
- The key areas where management wish to monitor performance and the manner in which performance is measured
- The financial and non-financial measurements and indicators of such performance
- The information required to 'run the business'
- The key challenges facing the Council.

BACKGROUND

Our risk based approach to Internal Audit uses the Council's own risk management process and risk register as a starting point for audit planning as this represents the client's own assessment of the risks to it achieving its strategic objectives.

The extent to which we can rely on management's own perception of risk largely depends on the maturity and effectiveness of the Council's own risk management arrangements. In estimating the amount of audit resource required to address the most significant risks, we have also sought to confirm that senior management's own assessment of risk accurately reflects the Council's current risk profile.

INDIVIDUAL AUDITS

When we scope each review, we will reconsider our estimate for the number of days needed to achieve the objectives established for the work and to complete it to a satisfactory standard in light of the control environment identified within the Council. Where revisions are required we will obtain approval from the Audit and Risk Manager and s151 Officer where appropriate prior to commencing fieldwork and we will report this to the Audit Committee.

In determining the timing of our individual audits we will seek to agree a date which is convenient to the Council and which ensures availability of key management and staff.

VARIATIONS TO THE PLAN

Significant variations to the plan arising from our reviews, changes to the Council's risk profile or due to management requests will be discussed in the first instance with the Audit and Risk Manager and s151 officer as appropriate and approved by the Audit Committee before any variation is confirmed.

APPROACH TO CREATING THE PLAN

The indicative IT Internal Audit programme for 2019-20 is shown in this document. We have not stated which quarter they will be reviewed in because we have been appointed half way through the audit year and therefore once this Plan is approved they all are priority to be completed as soon as Council and BDO resources become available.

1	Agreed approach with Audit and Risk Manager
2	Discussed risks/reviews with IT Service Delivery Manager and Head of Service 12/12/18
3	Issued a survey to the IT Service Delivery Manager and Head of Service asking specific questions around IT risks facing the Council
4	Considered client/sector risks and audit plans across our portfolio
5	Reviewed the Council's Risk Register, Strategic Objectives and prior auditors reports
6	Finalised draft Plan with Audit and Risk Manager, IT leads and s151 officer
7	Presented our Plan to SMT meeting on 16 January 2019 with Plan
7	Presented the Draft Plan to the Audit Committee for consideration and approval in March 2019

STAFFING

The core team that will be delivering the programme to you is shown below:

Name	Role	Telephone	Email
Greg Rubins	Head of Internal Audit	07710 703 441	Greg.Rubins@bdo.co.uk
Gurpreet Dulay	Audit Manager	07870 555 214	Gurpreet.Dulay@bdo.co.uk

The core team will be supported by specialists from our national Risk and Advisory Services Team and wider firm as and when required.

Our indicative staff mix to deliver the programme for 2019-20 is shown below:

Role	Days	Role mix %
Head of Internal Audit	4	10%
Audit Manager	12	30%
Senior Auditor	12	30%
Other (Specialists / Junior Auditor)	12	30%
Total	**40**	

REPORTING TO THE AUDIT COMMITTEE

We will submit the indicative IT Internal Audit Plan for discussion and approval by the Audit Committee in March 2019. We will liaise with the Senior Management Team and other senior officers as appropriate to ensure that internal audit reports summarising the results of our visits are presented to the appropriate Audit Committee meeting.

Following completion of the Internal Audit programme each year we will liaise with the Council’s Audit and Risk Manager as they produce the Internal Audit Annual Report summarising our key findings and evaluating our performance in accordance with agreed service requirements. Please note that should it be felt the number of days in the plan is to be greater than 40 then Internal Audit can accommodate this.

INTERNAL AUDIT PLAN 2019-20, 2020-21, and 2021-22

Review	2019-20	2020-21	2021-22	Description
Strategic Priority - All				
IT Project Management CRR: 1, 3, 44	15			To review the capability of Charnwood to deliver successful IT programmes and projects by reviewing the end-to-end methodology together with a sample of 3 current technology related projects. The following areas will be included within our review: • Reviewing the existing Project Portfolio management methods, tools and governance around how the Council monitor the delivery of its strategic projects • Evaluate the project management standards and methods across the Council and the application of those standards. • Assessing the extent of Project Management resourcing across the Council
IT Strategy CRR: 1-4, 45	12			The absence of a defined IT strategy may result in a misalignment with the Council's strategic objectives. The purpose of this review is to assess the appropriateness of the mechanisms and arrangements to develop the current IT Strategy, its alignment with the wider strategic objectives of the organisation, and the degree of consideration of the current IT environment and future requirements of the organisation.
IT 3rd Party Supplier management CRR: 12, 48	10			The need to assure that services provided by third parties (suppliers, vendors and partners) meet business requirements requires an effective third-party management process. This process is accomplished by clearly defining the roles, responsibilities and expectations in third-party agreements as well as reviewing and monitoring such agreements for effectiveness and compliance. Effective management of third-party services minimises the business risk associated with non-performing suppliers Our review will assess the adequacy of the Councils arrangements to managed IT third parties.
IT Disaster Recovery CRR: 21, 31		13		The core risk associated with this review is that the IT disaster recovery arrangements may not be fit-for-purpose and would not allow IT management to recover their key applications in the timeframe required. The purpose of the review is to provide

				assurance over the design of the disaster recovery planning arrangements, processes and underlying controls that are in operation for promoting resilience within the organisation's IT environment.
Cyber Security CRR: 8 - 25, 36, 37, 42, 43, 51 - 53		16		This is a risk area for all organisations and typical risks are: • Senior management are not aware of the cyber security risks to the Council • The Council does not have adequate policies and procedures related to information security, data protection and IT infrastructure • The Council does not have adequate management arrangements in place for identifying and responding to cyber security threats • The Council is unable to identify and respond to a cyber security attack. • The Council has not identified and risk assessed its critical information assets • Information assets are exposed to a breach through an absence of IT controls
IT Helpdesk / Demand Management CRR: 2, 4, 43	20	8		Understanding key business requirements and being able to provide an effective response to demand management are the key fundamentals to a successful service delivery. Without an appropriate IT Service Delivery framework, there is a risk of poor performance of IT services, which can bring destruction or reduction of value to Charnwood This audit will assess the structure of the Council's IT service and provide assurance that it is aligned to the needs of stakeholders from across the Council.
Application Controls CRR: 1, 11, 13, 14, 18, 22, 37			12	The security of information assets is dependent on the security of the Council's IT applications. For a number of Council applications (to confirm with management), we would review the following: • IT application security standards • IT application identification • User account creation, amendment and removal • User access controls • Report writers • Generic accounts • Interfaces to other applications • Target/destination systems • Database controls • Staging area/testing facility
Change Controls CRR: 10, 11			10	We will assess whether: • all changes, including emergency maintenance and patches, relating to infrastructure and applications

				within the production environment are formally managed in a controlled manner - Changes (including those to procedures, processes, system and service parameters) are logged, assessed and authorised prior to implementation and reviewed against planned outcomes following implementation.
Data Governance and GDPR CRR: 18, 20, 38, 45, 51 - 53			15	As local authorities collect, store and process data with almost every transaction, the risks to an individual in terms of how their data is used and protected is high and there are penalties if standards are not followed. The purpose of this review is to assess the adequacy of Charnwood's arrangements to comply with GDPR requirements. Our review will assess Charnwood's GDPR framework and identify any areas for improvement.
SUB-TOTAL	**37**	**37**	**37**	
Follow Up	3	3	3	This includes all planning, liaison and management of the IT Internal Audit contract
TOTAL DAYS	**40**	**40**	**40**	

FOR MORE INFORMATION:

Gurpreet Dulay

Gurpreet.Dulay@bdo.co.uk

The matters raised in this report are only those which came to our attention during the course of our audit and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. The report has been prepared solely for the management of the organisation and should not be quoted in whole or in part without our prior written consent. BDO LLP neither owes nor accepts any duty to any third party whether in contract or in tort and shall not be liable, in respect of any loss, damage or expense which is caused by their reliance on this report.