MID SUSSEX
DISTRICT COUNCIL

Oaklands Road
Haywards Heath
West Sussex
RH16 1SS

Switchboard: 01444 458166

DX 300320 Haywards Heath 1
www.midsussex.gov.uk

28 August 2018.

Dear Councillor,

A meeting of the **AUDIT COMMITTEE** will be held in the **COUNCIL CHAMBER** at these offices on **WEDNESDAY, 5 SEPTEMBER 2018 at 7.00 p.m.,** when your attendance is requested.

Yours sincerely,

KATHRYN HALL

Chief Executive

A G E N D A

		Page No.
1.	To note Substitutes in Accordance with Council Procedure Rule 4 – Substitutes at Meetings of Committees etc.	
2.	To receive apologies for absence.	
3.	To receive Declarations of Interest from Members in respect of any matter on the Agenda.	
4.	To confirm the Minutes of the meeting of the Committee held on 24 July 2018.	**3 - 8**
5.	To consider any items that the Chairman agrees to take as urgent business.	
6.	Internal Audit - Monitoring Report 30 June 2018.	**9 - 14**
7.	Committee Work Programme 2018/19	**15 - 16**
8.	Questions pursuant to Council Procedure Rule 10.2 due notice of which has been given.	

To: **Members of Audit Committee** – Councillors J Belsey, Boutrup, de Mierre, Dorey, Andrew Lea, Stockwell and Walker.

Minutes of a Meeting of the Audit Committee held on 24 July 2018 from 7.00 p.m. to 8:02 p.m.

Present: John Belsey (Chairman)
Ruth de Mierre (Vice-Chairman)

Anne Boutrup *	Andrew Lea	Rex Whittaker
Tony Dorey *	Linda Stockwell *	
	Neville Walker	

* Absent.

Also in Attendance: Judy Llewellyn-Burke
(Cabinet Member for Finance and Economic Growth)
Norman Webster (Cabinet Member for Community)
Paul King, Ernst and Young
Tom Wilkins, Ernst and Young
Gillian Edwards, Audit and Risk Manager, Crawley Borough Council
Chris Bowers, Internal Auditor, Crawley Borough Council
Peter Stuart, Head of Corporate Resources and Section 151 Officer
Cathy Craigen, Business Unit Leader for Finance
Tom Clark, Head of Regulatory Services
Alexander Austin, Democratic Services Officer
Alison Hammond, Democratic Services Officer

1. SUBSTITUTES AT MEETINGS OF COMMITTEE – COUNCIL PROCEDURE RULE 4

Councillor Whittaker was in attendance as a substitute for Councillor Stockwell.

2. APOLOGIES FOR ABSENCE

Apologies were received from Councillors Boutrup, Dorey and Stockwell.

3. DECLARATIONS OF INTEREST

Councillor Andrew Lea declared a personal interest as a serving Member of West Sussex County Council.

4. MINUTES

The Minutes of the meeting of the Committee held on 8 March and 9 May 2018 were agreed as correct record and signed by the Chairman.

5. URGENT BUSINESS

None.

6. INTERNAL AUDIT MONITORING REPORT 31 JANUARY 2018

Gillian Edwards, Audit and Risk Manager, introduced the report to update the Committee on the progress of the 2018/19 Internal Audit Plan and to report on progress made in implementing previously agreed recommendations. She highlighted a few key findings:

The monthly reconciliations for payroll 2017/18 had not been completed. This was due to extenuating circumstances with the new payroll system, XCD. However an end of year reconciliation had been completed, a small difference was found and corrected. Monthly reconciliations are required and she will liaise with the Head of Corporate Resources and Section 151 Officer. Therefore the assurance level is recorded as satisfactory.

The NNDR audit, completed by Horsham District Council as part of a shared working program, was given a reasonable assurance. The wording used by Horsham District Council is different but equates to our 'satisfactory' level. A meeting was held today with the relevant Business Unit Leader regarding the two key findings, inspections and procedure notes. These will be resolved as part of the revised structure of the Revenues and Benefits department, an updated report will be received later in the year.

A limited assurance was given for Tech Forge Financial Management System Additional Feeder System 2018/19 given there was only a narrow scope for the audit. The system is still in testing mode and the link between FMS and Tech Forge has not been fully established.

The National Fraud Initiative 2018/19 matches data from the Electoral Roll against claims for Single Persons Discount for Council Tax. There were some inconsistencies with Electoral Roll and Council Tax data entry, 29 queries have been passed to the Business Unit Leader for Revenues and Benefits. An action plan is required to check the remainder of the sample.

There have been some improvements with the Contracts Register and further work is required to show the improvements. There were a few advisory points on Data Migration, the central location of data held and some training issues due to the loss of knowledge as staff have left following the streamlining of the department due to the disaggregation of Census.

A report will be provided in September to include the suggestion of the Council insuring against cyber-attacks. The committee was advised that this is currently a topical issue.

The Chairman thanked Gillian Edwards and her team for the detailed report.

A Member asked for the rankings of assurance level and whether the auditors checked that back-up copies of data were held for data located in the cloud. He wanted assurance that there are back-up copies of data for information held on external servers, since he had a professional interest from an IT perspective. The Internal Auditor explained the rankings were substantial, satisfactory (most controls in place or correctly working), limited and no assurance (this has never been used for this council). They audit fundamental systems only; they do not usually look at the processes to back-up data but do get assurances from the Heads of Service. An audit to test the retrieval of this data can be checked in the next few months and an update report provided.

A Member asked as Tech Forge was still in the testing phase, has a decision been made whether to use it. Peter Stuart, Head of Corporate Resources, replied that it was a long running project that had taken longer than expected and that it was starting to clash with the new FMS project that was to go live on 1 April 2019. There was limited time to check the interface works and if during testing next week the system does not perform correctly it may be shelved for the time being. Invoices would then still be raised through FMS and not Tech Forge.

A Member asked whether the issues with payroll were ongoing, and was there a training need to prevent future occurrences. The Internal Auditor advised that a member of her

team would liaise with the Business Unit Leader to see if it was a system problem or training need. If an end of year reconciliation can be completed monthly reconciliations should be possible, with an update report to follow.

A Member asked for a report in September on how the Council currently deal with cyber-attacks and how it could be prevented, it may be a low risk but is a topical issue. The Internal Auditor confirmed to the committee an update report would be provided to include this issue.

As there were no further questions the Chairman took Members to the recommendation in the report which was unanimously approved.

RESOLVED

The Committee received and noted the report.

7. INTERNAL AUDIT ANNUAL REPORT 2017/18

Gillian Edwards, Audit and Risk Manager, introduced the annual report of the Internal Audit and Risk Manager of Mid Sussex District Council for 2018/19. The report provided the evidence that the auditing team had complied with the relevant regulations, summarised the work that supported the opinion of the auditor and provided the assurance opinions. The Audit and Risk Manager advised that Mid Sussex District Council had an adequate, effective and reliable framework on internal control that provided reasonable assurance regarding the effective and efficient achievement of the Council's objectives.

An update on the recommendations regarding Housing Benefit confirmed all recommendations had been completed, the report having been written on 31 March 2018. There were other items in the progress report that will appear in next year's report, but these do not change the assurance level.

Several Members commented on the comprehensive report and the quality of the work which gives a level of confidence to the Members.

A Member noted that item 2.1 commented on the purchase of the Orchards Shopping Centre. Paul King, from Ernst and Young, informed Members that the purchase was looked at in the 2017/18 audit and they looked at how the lease was obtained. However on a value for money basis it was not qualified as there was no risk.

The Chairman thanked Gillian Edwards and her team for the detailed report.

As there were no further questions the Chairman took Members to the recommendation in the report which was unanimously approved.

RESOLVED

The Committee received and noted the report.

8. AUDIT RESULTS REPORT 2017/18

Tom Wilkins, Manager for Ernst and Young, presented the report which introduced the auditors' "Audit Results Report" and provided some context for Members' consideration. The status of the audit was outlined and most of the work has been completed, and it

was confirmed in response to a Member's question that the statutory deadline of 31 July 2018 would be met. The Manager highlighted two significant differences:

The comparison of the West Sussex Pension Fund's net assets as estimated by the actuary at the year end and the actual net assets showed a difference. The difference was positive, in the favour of the Council. In response to a question by a Member, Paul King advised that it was more a judgemental difference, a timing issue as the initial forecast differed to the actual figure. The second issue related to the all-weather pitches. They had been treated as land and not an asset and had not been depreciated, but this made no significant difference. The report had been complied two months earlier than last year and he thanked the Council's Officers for their assistance.

In reply to a Member question regarding the valuation of some commercial assets, the Manager informed the committee that assets are usually valued every five years but investments properties are usually valued annually. In response to a further question on revaluing only part of the assets each year, Paul King explained that if the assets were broadly similar appropriate adjustments can be made.

A Member thanked the Ernst and Young and the Council finance team for their excellent work.

The Chairman thanked Ernst and Young for providing the detailed report earlier than last year and suggested they report back on suggestions that would assist for next year's report.

As there were no further questions the Chairman took Members to the recommendations in the report which was unanimously approved.

RESOLVED

The Committee received and noted the report.

9. FINANCIAL STATEMENTS 2017/18

The Chairman advised the committee that a number of Members had attended an audit workshop which had been very productive. Members had been encouraged to email in their questions regarding the audit reports before the workshop. The Members were provided with a good level of detail and were reassured.

Peter Stuart, Head of Corporate Resources, thanked his team for producing the report and the attached Statement of Accounts which set out the Council's financial position. He advised that the figures in the statement were unchanged but there were some minor changes in the notes, Cathy Craigen, Business Unit Leader for Finance provided the amendments for pg 69 and 98.

The Chairman advised the Committee that the report could not be signed off as the audit was not yet complete. It was agreed that a delegation would enable the sign off if minor amendments were needed, by the statutory deadline of 31 July 2018.

A Member commented that the Cabinet had received five excellent budget management reports. The year had ended with an under-spend and considering the current pressures on budgets this report was good.

In response to a Member's question the Head of Corporate Resources informed the Committee that the purchase of software is listed as an Intangible Asset. The Council buys major software at a significant cost sometimes and this is capitalised but

increasingly this software is now bought under a 'Software as a Service' platform.

As there were no further questions the Chairman informed the Committee that the Letter of Representation to the Auditors was ready to be signed and asked the Member to receive the report subject to some minor amendments which was unanimously received.

RESOLVED

i) the Financial Statements are approved subject to minor amendments.
ii) the Committee authorises to the Chair and Vice Chair that the Statement of Accounts be signed by them, together with the Head of Corporate Resources, on completion of the audit, subject to any amendments raised and agreed within the Audit Results Report.
iii) the Letter of Representation be approved and the Chairman be authorised to add his signature to that letter.

10. REVIEW OF TREASURY MANAGEMENT ACTIVITY 2017/18 AND AMENDMENTS TO COUNTERPARTIES FOR 2018-19

Peter Stuart, Head of Corporate Resources advised that there had been no breaches of the policy and the Committee were asked to approve the amendments to the specified investments lists as detailed in the report. Approval was sought to add an institution to the specified Money Market Funds list and an amendment was required as the main British banks had split their business into "ring-fenced" and 'non ring-fenced" entities.

A Member asked that in relation to the new CIPFA code, would a report come to the Committee in September or the end of year. In reply the Head of Corporate Resources advised that the report would come before the Committee by the end of the financial year, 31 March 2019.

As there were no further questions the Chairman took Members to the recommendations in the report which were agreed unanimously.

RESOLVED

The Committee noted the contents of the report proposed that Council agree to:

i) approve the addition of the CCLA Public Sector Deposit Fund to the list of specified Money Market Funds.

ii) approve the amendment of the specified investments list to include only the ring-fenced parts of banks which have split their activities.

11. COMMITTEE WORK PROGRAMME 2018/19

The Chairman informed the Committee that the Auditors would have update reports for the next meeting. Members were asked to note the Work Program and the Capital Strategy Report was added to the agenda for 5 November meeting.

RESOLVED

That the Committee Work Programme for 2018/19 be noted accordingly.

12. QUESTIONS PURSUANT TO COUNCIL PROCEDURE RULE 10.2 DUE NOTICE OF WHICH HAS BEEN GIVEN.

None.

Chairman.

6. INTERNAL AUDIT – MONITORING REPORT 30 JUNE 2018

REPORT OF: Audit and Risk Manager
Contact Officer: Gillian Edwards
Email: gillian.edwards@midsussex.gov.uk Tel: 01444 477241

Wards Affected: All MSDC Wards
Key Decision: No
Report to: Audit Committee
5th September 2018

Purpose of Report

1. The purpose of this report is twofold; to update the Committee on the progress of the 2018/2019 Internal Audit Plan and to report on the progress made in implementing previously agreed recommendations.

Recommendation

2. The Committee is asked to receive this report.

Background

3. Work Completed

No audits have been completed since the last report, as at 17th August 2018.

All outstanding work has been scheduled, which mainly relates to the Council's fundamental systems, for completion by 31st March 2019.

4. Work in Progress

The reviews in progress and other work that has been undertaken in the period are shown at Appendix A.

National Fraud Initiative (NFI) Data Matching – Update

Since the last meeting in July, details of outstanding matches have been passed to the Business Unit Leader, Revenues and Benefits who is exploring the possibility of using an external provider to assist in processing and investigating the matches identified in the NFI Data Matching exercise. This is ongoing and more information will be provided at the next Committee meeting in November 2018.

Additionally, a short review is currently being undertaken as part of the NFI Data Matching Exercise, where it appears that there may be more than one person resident at a property where Single Person Discount of 25% is being claimed. The outcome of this work will be reported at the next meeting in November.

5. High priority findings in this period

There were no high priority findings to report in this period.

6. Follow Up Audits:

The follow ups below have been completed since the last Audit Committee.

Income Collection Audit 2017/2018

During this review, it was agreed that the Council would consider insuring against cyber-attacks. The Head of Corporate Resources has considered advice from the Council's insurers and is satisfied that appropriate cover is in place.

Payroll 2017/2018

It was reported at the last meeting that reconciliations between the Payroll system and the Financial Management System (FMS) had not been completed for the period October 2017- January 2018.

It has now been confirmed that these reconciliations are up to date as at 31st July and we are currently reviewing this. We are advised that reconciliations will be prepared on a monthly basis.

Tech Forge

It was reported at the last meeting that a limited assurance was given for Tech Forge Financial Management System as insufficient testing had been undertaken to confirm that information raised on the Tech Forge module correctly interfaced with the Financial Management System. Since then, further testing has been undertaken and the Head of Corporate Resources has confirmed that the system is now working appropriately and will be used.

7. Member Action- Cyber Security

This summary was produced after a request from Councillor Andrew Lea was received at the meeting of the Audit Committee on 24th July 2018 where it was agreed that information would be provided to the Committee about cyber-attacks, what they are and the impact that they can have.

This summary is based largely on information gained from the Chartered Institute of Internal Auditors, which is the Audit and Risk Manager's professional body and the only professional association for internal auditors in the UK and Ireland. It is therefore the foremost authority on internal auditing.

The Oxford English Dictionary defines *cyber* as '**relating to or characteristic of the culture of computers, information technology, and virtual reality'**

The National Cyber Security Centre, which is part of GCHQ provides the following definitions:

Cyber attack

Malicious attempts to damage, disrupt or gain unauthorised access to computer systems, networks or devices, via cyber means.

Cyber incident

A breach of the security rules for a system or service - most commonly:

- Attempts to gain unauthorised access to a system and/or to data.

- Unauthorised use of systems for the processing or storing of data.
- Changes to a systems firmware, software or hardware without the system owners consent.
- Malicious disruption and/or denial of service.

Cyber security

The protection of devices, services and networks — and the information on them — from theft or damage

What are Cyber Attacks?

The National Cyber Security Centre, in its report entitled 'The cyber threat to UK business' published in May 2018 highlighted the major incidents in the year 2017/2018 as follows:

The major incidents in 2017 included:

1. Ransomware and distributed denial of service attacks
2. Massive data breaches
3. Supply chain compromises
4. Fake news and information operations

The first and second are most relevant to the Council at this time.

Ransomware

A global attack using ransomware known as 'WannaCry' was launched on 12 May 2017. payment to allow users access. This was the largest cyber-attack to affect the NHS in England, although individual trusts had been attacked before that date.

The Local Government Association reported that On 5 April 2016, a Council situated in the North of England was hit by a cyber-attack, being a piece of ransomware called TeslaCrypt which managed to get onto the council's network. Whilst virus protection measures were in place, they were bypassed by a member of staff googling the website and going through the

In addition, ransom Distributed Denial of Service (DDoS) attacks - where hackers threaten to conduct DDoS attacks unless a ransom is paid - have increased since mid-2017 when a South Korean web hosting company paid a ransom fee in Bitcoin equivalent to US$ 1 million.

In late 2017, the hacking group Phantom Squad targeted organisations in Europe, Asia and the US. They threatened financial institutions, hosting providers, online gaming services and Software-as-a-Service (SaaS) organisations and demanded a 're-instatement of services' payment in Bitcoin. The anonymity provided by virtual currencies like Bitcoin allow cyber criminals to conduct bold attacks and potentially make a profit.

Massive data breaches

The reported number and scale of data breaches continued to increase in 2017, with Yahoo finally admitting in October that all of its 3 billion customers had been affected by the 2013 breach.

The techniques used in most cases where data breaches have occurred due to cyber-attacks were reported as being not particularly advanced (including exploiting unpatched vulnerabilities and spear-phishing).

There are numerous documented further examples of data breaches caused by cyber-attacks, including a UK-based telecoms company who reported a cyber-attack to Action Fraud, when they discovered that data about individuals due for phone upgrades had been stolen. This case was triaged as a priority by Action Fraud and passed to the National Crime Agency, who liaised with NCSC to ascertain the most appropriate response and analyse the large datasets involved.

Cyber Attacks and Local Government

The National Cyber Security Centre advises that in cyberspace it is often difficult to provide an accurate assessment of the threats that specific organisations face. However, *every* organisation is a potential victim. All organisations have something of value that is worth something to others.

LocalGov, in an article written in February 2018, states that Big Brother Watch found local authorities face 19.5 million cyber-attacks per year and that 29% of councils had experienced at least one security breach between 2013 and 2017. Of the 25 councils who experienced a loss or breach of data due to a cyber-security incident, although 56% failed to report it the report said.

The report also found that three-quarters of local authorities do not provide mandatory cyber security training to staff.

How does the Council protect itself against cyber-attacks

The Head of Digital and Customer Service provided the following summarised description of the measures used by the Council to counter cyber-attacks.

While we experience daily attempts to infect our systems, to date we have prevented them with the measures we have in place.

Last year we experienced an attempt to infect our systems by the first version of the 'WannaCry' software and this was stopped at the infected machine. Data on the machine was restored from backups and further infections prevented.

MSDC has a shared Security Policy with partners on the CenSus network. It aims to provide a basis on which the Council can implement and maintain a secure environment for its information assets across its ICT estate. It encompasses multiple layers of protection including at the systems level, through data governance and through education, awareness and guidance.

The Council's Information Governance Officer and Infrastructure Manager are members of the NCSC and receive regular updates from them, which includes advice on attacks. We are also signed up to NCSC web check, which is part of the overall NCSC active cyber defence. This provides alerts if it notices anything wrong on the website.

Systems Level
The Council approaches network security in a holistic manner ensuring appropriate controls are applied both at boundaries between systems and within the network. The network is segregated from the internet via control barriers as needed with no direct routing between internal systems and external networks.

The Council protects its boundaries to the Internet, in particular from malware attacks. All information supplied to or from Council ICT systems will be scanned for malicious content. At the entry points to our network we are running a device which reads and checks emails for viruses and spam. This uses two different antivirus vendors to ensure coverage. It also has an element, installed late last year following the attempt to infect our systems, which scans for 'active' content that could encrypt a machine and strips this out or disables it. For Councillors on Office 365, there is an additional filter providing another antivirus check.

Each PC is patched regularly and automatically. We also use a current supported version of Windows with the appropriate patches. We are scoping a project to upgrade machines to Windows 10 to ensure that when Windows 7.1 goes out of support that we have a secure environment.

Data Governance

We have recently upgraded our Microsoft licencing to ensure data is classified for use in our new systems, enabling us to implement auto detection of sensitive data and prevent it from being accidentally sent to the wrong people. As we continue to work through our data, checking it against retention schedules we are also ensuring it is classified according to its sensitivity. These processes ensure we apply the appropriate data governance policies to the data according to its risk.

Where sensitive Council data or personal data is being shared with third parties it is encrypted in transit whether the data is being shared via a WAN (e.g. the Internet) or using removable media.

Education, Awareness and Training

The Council ensures that staff are well educated and takes steps to control social media malware attacks, phishing emails and similar attacks. Our current working practices include:

- Full set of Information Security policies
- Subject Access Request procedure
- Breach procedure
- A general privacy notice
- Basic information on what we do with data on forms where we collect personal information
- Online data protection training for staff

Additionally, we review malware protection logs to detect trends and changes in threat profiles and make appropriate adjustments and improvements as needed. For example, providing advice on the Council's intranet if we receive any phishing or spear phishing attacks as well as mailing staff to alert them.

Background Papers

- Internal Audit reports relating to 2018/2019
- Working papers relating to 2018/2019

Appendix A

Internal Audit Plan 2018/2019

Progress Report as at 17th August 2018

Audit	Audit Plan Year	Audit Opinion- Assurance	Number of High Priority Findings	Comments
A. Work Completed in the Current Period				
B. Work In Progress				
NFI Data Matching	2018/19			
Taxi Drivers	2018/19			
Follow Ups				
Payroll	2017/18			

7. COMMITTEE WORK PROGRAMME 2018/19

REPORT OF: Tom Clark, Head of Regulatory Services
Contact Officer: Alison Hammond, Member Services Officer
Email: alison.hammond@midsussex.gov.uk Tel: 01444 477227
Wards Affected: All
Key Decision: No

Purpose of Report

1. For the Audit Committee to note its Work Programme for 2018/19.

Summary

2. Members are asked to note the attached Work Programme. The Work Programme will be reviewed as the final piece of business at each meeting, enabling additional business to be agreed as required.

Recommendations

3. The Committee are recommended to note the Committee's Work Programme as set out at paragraph 5 of this report.

Background

4. It is usual for Committees to agree their Work Programme at the first meeting of a new Council year and review it at each subsequent meeting to allow for the scrutiny of emerging issues during the year.

The Work Programme

5. The Committee's Work Programme for 2018/19 is set out below:

Meeting date	Item
20 November 2018	Review of Treasury Management Strategy Grants Certification Internal Audit – Monitoring Report. Committee Work Programme
March 2019 To Be Advised	Audit Planning Report Treasury Management Strategy Internal Audit Monitoring Report Committee Work Programme

Policy Context

6. The Work Programme should ideally reflect the key priorities of the Council, as defined in the Corporate Plan and Budget.

Financial Implications

7. None.

Risk Management Implications

8. None.

Background Papers

None.