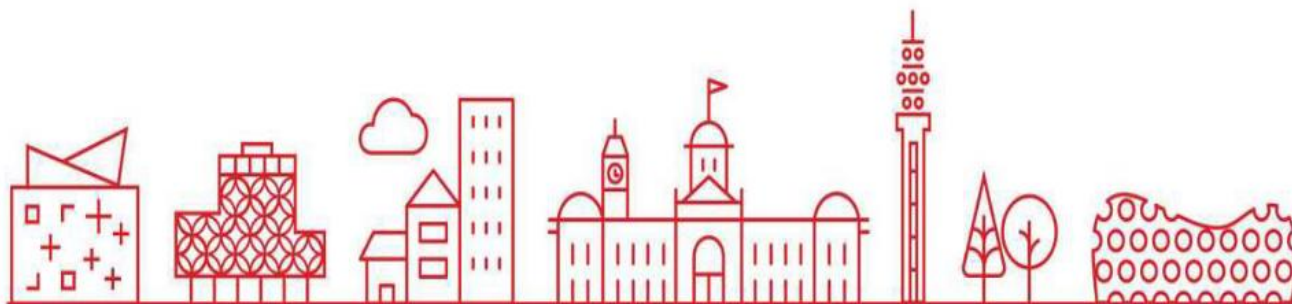


Digital and Customer Services

Audit Review Oct 2021

Peter Bishop

Director, Digital and Customer Services



Areas covered

- Assurance Model for Digital and Customer Services
- Information Assurance Framework
- Information Security
- Complaints Management
- Internal Audit
- Revenue Benefits and Rents
- COVID Business Grants
- External Audit

Assurance Model for Digital and Customer Services

Third Line of Defence

- BSI Audits for ISO 20000 IT Service Management
- Working within ISO27001 Information Security
- DWP returns (RBR)
 - External testing and verifications
- External Accreditation/Certification

Second Line of Defence

- Governance Structures & Processes
 - Internal Audit report
- Directorate Tracking of audit actions being undertaken in a timely manner
- Customer Satisfaction

First Line of Defence

- Directorate Business Plans and strategies
- Directorate Risk register
- Annual Business Unit and Directorate Governance Statements
- Monthly DMT Performance and management board (review of finance and governance)
- Staff training and Induction
- Staff appraisals and 121s

Annual Governance Statement

- No areas of concern raised around Directorate Governance
- Main issues raised were in relation to COVID and the impact on services and demand
- There were no wider Value for Money issues raised.

Information Assurance Framework

It is intended to describe the processes in place to gain confidence that information risk is being adequately identified, mitigated and monitored. It sets out the roles and responsibilities within Birmingham City Council to support Information Assurance with particular emphasis on ensuring appropriate personnel have been assigned responsibilities for the management of information assets within the organisation.

Role of the Senior Information Risk Owner (SIRO)

The Director of Digital and Customer Services undertakes the role of the SIRO for Birmingham City Council. The SIRO is the focus for managing information risk for the entire organisation.

The role of the SIRO is to:

- Lead and foster a culture that values, protects and uses information for the public good
- Own the overall Information Assurance Framework, test its outcome and ensure it is used

Role of the Information Assurance Board (IAB)

The Information Assurance Board will comprise of the following roles:

- Head of Corporate Information Management; (Data Protection Officer)
- Assistant Director, Audit and Risk Management
- CIO & Assistant Director Information, Technology & Digital Services
- City Solicitor
- Caldicott Guardian

The Board will ensure that Birmingham City Council has effective policies and management arrangements covering all aspects of Information Assurance Framework themes

Information Assurance Framework

Themes	Measures
Governance. Established governance structure with defined roles and responsibilities.	SIRO and IAB operate effectively DPO appointed
Policies, standards and guidelines. Policies, procedures and guidelines in place and those policies and procedures are communicated.	Suite of policies, procedures and standards exist, are reviewed regularly and monitored for compliance.
Data inventory. Inventory of databases and systems that collect, process and retain data is in place.	Apps list; data storage volumes; Off site storage of records;
Strategy and risk assessment. Information risk is part of the overall risk management process of the authority.	Audits completed; number of recs; RAG status of recommendations;
Procedures and controls. Procedures are in place for the collection of data and data subjects are aware of how personal data is used.	Records of processing activities; DPIA
Information security. Information security programme is in place and addresses risks around personal data and other sensitive data.	PSN accreditation; N3 connection; Privacy Impact Assessments completed;
Third party management. Established standards and requirements are in place for privacy and security to protect data when working with third parties.	Data sharing agreements in place; Monitoring of compliance of data processors
Regulatory compliance. Ensuring compliance with laws, regulations and good practice to ensure the reliability of data, its quality and accuracy.	Complaints from ICO
Incident management and response. Incident response plans and procedures are in place that manages reported data breaches.	No of data breaches; No of near misses; IT Security incidents;
Training and awareness. Training and awareness programme is in place and delivered.	Training take up

Ensuring our compliance with the GDPR Regulations - developing our Information Assurance Maturity

- We used the HMG Information Assurance Maturity Model and Assessment Framework as a basis for developing our plans to improve our IA maturity and assure our compliance with the Data Protection Act 2018.
- Birmingham Audit conducted an initial assessment and concluded that our maturity was at “0.5-1” on the assessment criteria (Aug 2017).
- Following a report to CLT, approval was given for funding to support the implementation of an IA programme with a view to achieving level 2 on the assessment standard.
- The progress of the programme has been regularly reported to the Information Assurance Board and onto CLT.
- As at May 2021, the Internal Audit assessment of the maturity at the close of the programme was level 2-3.

Information Security - training and awareness

Activity report August 2021:



93% (28/30)

**Information Asset Owners
completed training**



37

Different courses supporting
the "Value Our Information"
behaviour



2223

Employees completed **cyber
security training** as part of
the mandatory bundle
launched April 2021

new

360

Places offered on new **Value
and Protect your
information** virtual workshop
over next 12 months,
including workshops for
members



4 Prompts to complete

IS training within the
Corporate Induction:
Checklist, Virtual workshop,
starter pack and eLearning



**Management behaviour
Framework** reinforces
accountability for the security
of information

new

255 managers enrolled on
Workshops on **accountability
and how to manage and
deal with data breach fall
out** built into FL and F2M
programmes



New Ways of Working
bringing together consistent
message regarding safety and
security of data when **hybrid
working**

CYBER SECURITY METRICS HUMAN FACTOR

CYBER EDUCATION AWARENESS



2223

E-LEARNING
MANDATORY
TRAINING
COMPLETED

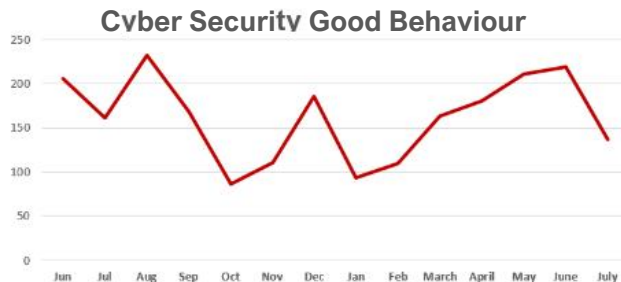


4 Cyber Awareness Sessions
Members and Finance
(MS Teams)

Making a positive difference every day to people's lives

Good Email Behaviour July 2021

140 requests received



6 Monthly Phishing Tests Completed

1099 phishing emails sent

75% Coverage of BCC Workforce

Current overall statistics

63% of staff opened the message

16% of staff clicked on the link



CYBER SECURITY METRICS TECHNOLOGY

MAJOR SECURITY INCIDENTS RANSOMWARE RESILIENCY

0 Successful attempts

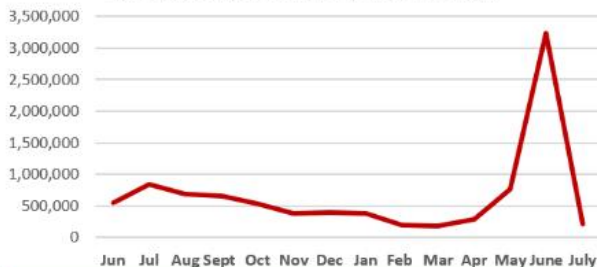


WEBSITE PROTECTION

Birmingham.gov.uk (plus 10 websites)

0 Successful Denial of Service attempts

Cyber Security Website Protection Blocks



5 million

Malicious requests blocked this calendar year 2021
Making a positive difference every day to people's lives

ENTERPRISE VULNERABILITY MANAGEMENT

Daily External Perimeter Scan

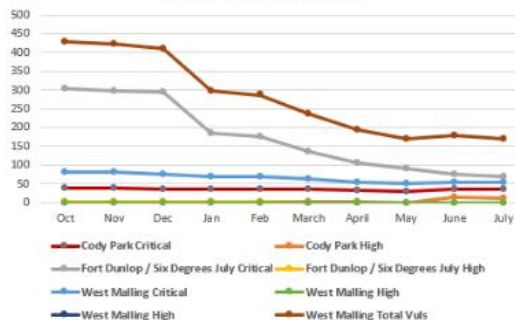
0 Critical and **4** High



Weekly Data Centre Scan

Cody Park	37 CRITICAL VULNERABILITIES	13 HIGH VULNERABILITIES
Fort Dunlop	75 CRITICAL VULNERABILITIES	0 HIGH VULNERABILITIES
West Malling	55 CRITICAL VULNERABILITIES	0 HIGH VULNERABILITIES

Data Centre Scans



APM programme continues to drive the critical numbers down

PENETRATION TESTING HIGHLIGHTS

.GOV.UK website against tech current tech controls
No Critical or High issues found

New Complaints Process – learning the lessons



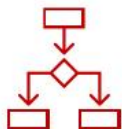
Technology - One System

- One system to be used to track all complaints at every stage
- All data captured in one source
- i-casework configured to enable use across all Directorates
- Ability to track and monitor all complaints
- Other complaint systems decommissioned with data transferred to i-casework



People

- There will be dedicated Complaint Champions embedded and standardised across each Directorate
- New Structure defined and agreed detailing roles and responsibilities
- Recruitment strategy agreed per Directorate
- Consultation (if needed) across impacted staff
- Council-wide communication



Process

- There will be one clear documented process and policy to be used across the council to include all complaint types, Members enquiries and vexatious complaints
- Defined and agreed SLA's
- Clear definitions for complaints/enquiries
- Process implemented to learn from complaints



Members of the Council/MP's

- There will be a consistent approach for all compliments, complaints and members enquiries with enough dedicated resource to maintain quality
- Consultation with Members of the Council/MP's during the development of the process and system
- Communication and training to all Members during the implementation



Citizen

- There will be a clear route to complain and a clear expectation of how the response will be managed
- Both Citizens and Members will have a dedicated Complaint Champion to communicate with
- This will increase the chance of not experiencing the same complaint again in the future



Implementation

- Managed and controlled rollout to all Directorates
- Training of all impacted staff
- Communication to internal and external stakeholder groups
- Post go-live support provided to help resolve any initial issues or enquiries

Breaking the Continuous Failure Cycle



- The failure to resolve Citizen's/ Member's complaints correctly or within the agreed timescales, escalates the complaint and extends the complaint's lifecycle creating further work and additional drain on resources. This is mainly caused by:
 - Managers not having enough time to respond within the required timescales or a lack of resource to investigate and respond to complaints correctly
- Other Citizens or/and Members raise further complaints about the same issue/process due to corrective action not being undertaken to resolve the root cause(s)
- This cycle is increasing the volume of complaints fuelling this current crisis
- To reduce complaint volumes to a manageable level; this continuous failure cycle needs to be broken
- Only when this cycle has been broken consistently across the council, will volumes fall, and costs savings realised (recognising that certain policy decisions will always continue to generate complaints when Citizen's do not agree with them)

Complaint Volumes & Types

Number of Complaints by type

- ASC Statutory complaints not shown on this chart

Complaints 2021



- Number of complaints over the past 3-years

- 2020 volumes were noticeably lower due to Covid-19 measures

Number of complaints received

April to July 2019	7254
April to July 2020	3615
April to July 2021	5928

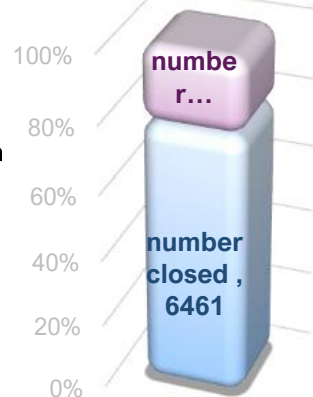
Complaints Analysis

■ Top areas by complaint volume since launch



■ Open and Closed Complaints since launch (26th April)

- Figures will differ from total cases received due to SLA timescales; e.g.: we would closed cases in April that were received in March
- 78.5% closed
- 21.5% open
- Average 461 cases closed per week (14 weeks)



Complaints teams dashboards by Service (Apr-July)

	Customer Services	Adult Social Care	City Housing	City Operations	Education & Skills	Inclusive Growth	CFLT
Total cases	357	164	2913	2834	283	1233	27
Divisions	Contact Centre	Statutory services	Housing options, Housing Management Housing Repairs	Streetscene including Parks and Waste, Regulation and Enforcement, Neighbourhoods Division	SENAR,	Planning, Housing Development, Transportation & Connectivity, Highways, Birmingham Property Service	Finance & Governance HR, CWG, PIP, D&CS (not revs and Bens)

- **Revenues and Benefits total cases - 422** – these teams are currently moving into the complaints process

Audit Reports from April 21

Month	Audit Reports	Risk Rating For Council		Assurance
		Previous	Current	
April	IT Policies	N/A	Low	Level 2
April	Rent Service - Current and Former tenancy arrears	N/A	Medium	Level 2
April	Revenues Payments and Posting Delays	N/A	Medium	Level 2
April	IT Procurement	N/A	Medium	Level 2
May	Information Governance - Data Loss Prevention	N/A	Medium	Level 3
May	IT Applications - Decommissioning Applications	N/A	Low	Level 2
May	IT Projects - Capita Retained Services	N/A	Medium	Level 2
May	IT Projects - Application Platform Modernisation (APM)	N/A	Medium	Level 2
August	Benefit Service - Procedures	N/A	Low	Level 2
August	Housing Benefit Accuracy Awards (DWP)	N/A	Low	Level 1

Revenues, Benefits and Rents - BAU

- Agreed annual plan with audit colleagues, focussing on risk – and in particular any new areas of work (eg Business grants, Social Isolation Payments); these processes were set-up with proactive audit involvement;
- Our £500 million plus benefit grant claim is subject to a further level of external audit/assurance in line with DWP requirements

Restart Grants (the most recent scheme)

- This scheme was announced as part of the Budget on 3 March 2021 and was applicable from 1 April 2021 to qualifying businesses. The primary principle of the Restart Grant scheme was to support businesses offering in-person services
- Strand 1 - to support non-essential retail premises with one-off grants
- Strand 2 – to support hospitality, accommodation, leisure, personal care and gym business premises with one-off grants

Grant Processing

The payment of the Restart Grants has brought to a close all of the grant payments.

The totals paid, for each of the schemes, are provided below

Grant Scheme	Number of payments	Value of payments
Small Business Grants	14,103	£141,030,000
Retail, Hospitality and Leisure Grants	4,098	£77,370,000
Local Restriction Grant Schemes	47,451	£108,923,678
Restart Grants	7,291	£51,682,115
Total	72,943	£379,005,793

Business Grants - Reconciliation, fraud and error

All councils have been required to reconcile the payments made to businesses and provide the Government with assurance reports on how the grant funding has been spent. The Revenues Service has identified a number of payments which have been incorrectly paid, with these being due to error, non-compliance or fraud.

Incorrect payments, were inevitable due to the complexity of some of the schemes. The Government also initially requested that support was paid in 'pace above accuracy'. Guidance has been issued in respect of the recovery of any overpayments. Revenues are now in the process of agreeing the detail of a plan to meet government expectations in attempting to collect the overpayments.

Once the overpayments have been validated and allocated into one of the three categories (error, non-compliance or fraud), invoices are to be issued to the businesses concerned. The Government guidelines state that further action should be taken in the event of non-payment including the issue of Reminder and Final Opportunity letters. The processes for recovery are currently being finalised.

The incorrectly paid figure, of £3.15m, represents less than 1.5% of the total paid which endorses the decision to undertake validations on the eligibility of businesses to receive grants before payments were made.

External audit: SAP IT control deficiencies

External Auditor View

- As a result of these findings, we have extended the substantive testing being undertaken as part of our substantive work in a number of areas.
- Although no issues have been identified that can be attributed to access issues, it is felt that in certain cases, the access control issues present a significant enough weakness in the overall environment that remediation is required.

Management Response

- The Council's approach to prior recommendations around access controls has been to put in place a series of detective controls – monitoring and reviewing for inappropriate system use.
- The more thorough work done by the IT audit team this year has highlighted a number of specific access issues.
- We note that no actual instances of inappropriate use of that access has been identified, but accept that moving to a preventative measure of reducing access to the minimum required as often as possible is a sensible precaution. Accordingly, we will plan to remediate all identified issues, starting with any higher risk ones, in the coming months, and report to Audit committee on our progress.