Audit and Governance Committee
13 January 2025
Information Governance - Update

For Decision

Cabinet Member and Portfolio:
Cllr N Ireland, Leader of the Council, Climate, Performance and Safeguarding

Executive Director:
J Mair, Director of Legal & Democratic

Report Author: Marc Eyre
Job Title: Service Manager for Assurance
Tel: 01305 224358
Email: marc.eyre@dorsetcouncil.gov.uk

Report Status: Public Choose an item.

Brief Summary: The Annual Information Governance Report was presented to Audit and Governance Committee at the meeting on 22 July 2024. This included the Strategic Information Governance Board's action plan in response to criteria in the Information Commissioner's Accountability Framework for which the Council believes it is not currently fully meeting. It also noted performance across a range of whole authority key performance indicators.

The Committee noted the resource challenges and recognised that this may require further focus. It was agreed that a further report should be presented back to the Committee to present progress.

In addition, SWAP have concluded an internal audit into the Council's business continuity arrangements, which provided a limited assurance and a number of priority actions, including one priority one assessment. Due to the links with the cyber security risk, the Strategic Information Governance Board includes business continuity within its remit. This report also therefore has been extended to provide some context to the audit findings that will be reported in the SWAP paper later on the agenda and sets out an improvement action plan.

Recommendation: To note the progress set out in the report, including the actions identified to respond to the business continuity internal audit.

Reason for Recommendation: To ensure that information governance and business continuity is embedded and effective across Dorset Council

1. Strategic Information Governance Board Action Plan

1.1 The Annual Information Governance report presented to committee on 22 July 2024 included the Strategic Information Governance Board's improvement action plan. This plan is intended to ensure that Dorset Council is meeting the expectations of the Information Commissioners Office (ICO), as set out within the ICO Accountability Framework self assessment.

1.2 The Framework is broken down into the following ten categories:

i) Leadership and oversight;

ii) Policies and Procedures;

iii) Training and Awareness;

iv) Individuals Rights;

v) Transparency;

vi) Records of Processing and Lawful Basis;

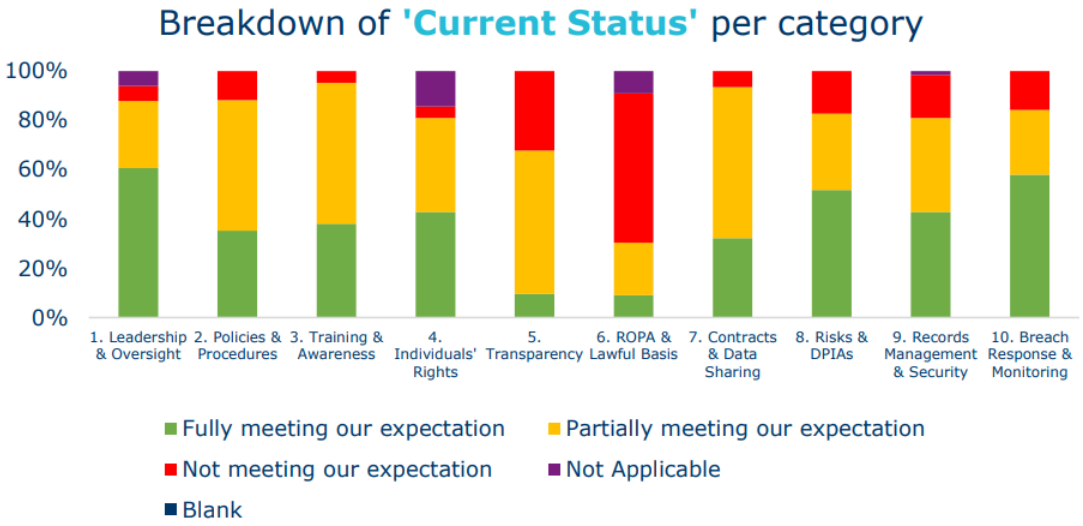
vii) Contracts and Data Sharing;

viii) Risks and Data Protection Impact Assessments;

ix) Records Management and Security; and

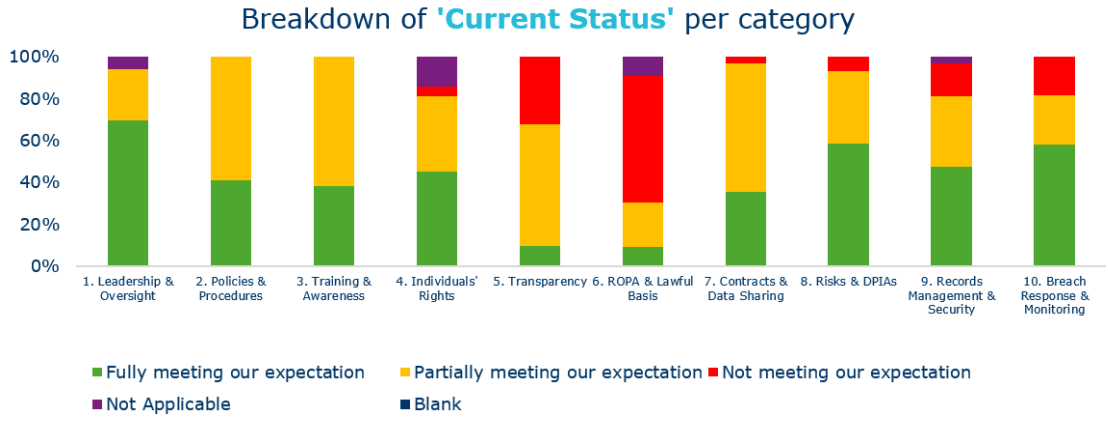
x) Breach Response and Monitoring

1.3 The graphic below summarises the proportion of assessment criteria within the framework where Dorset Council meets ICO expectations, as at the July 2024 report:



1.4 The Operational Information Governance Group has been leading on the majority of the actions, with particular development input from the Service Manager for Assurance; Data Protection Officer; Cyber Security and Service Continuity Lead; and the Data and Information Manager. With the agenda having to meet the dynamic needs of the organisation (particularly the group's role in challenging and making recommendations on Data Protection Impact Assessments related to service change) progress has been slow in some areas. The frequency and duration of Group meetings has been increased to meet this demand. Agreement has been reached to employ a Data Protection Analyst on a 12 month interim basis to support the work required in achieving criteria 1 to 8 and 10. Recruitment will commence shortly.

1.5 The current assessment based on work progressed since the July 2024 report is highlighted below, and shows some positive progress:



1.6 It should be noted that a number of actions are aligned to the roll out of the revised Information Asset Register, and therefore will remain red until that work is complete. This is particularly the case in respect of category 6 – "ROPA and Lawful Basis".

2. Performance

2.1 The annual report provided performance data on a range of key performance indicators including: i) Public (Freedom of Information) and Environmental Information Requests; ii) Requests Relating to Personal Information; and iii) Mandatory Training.

2.2 The Freedom of Information Act 2000 (FOI) and Environmental Information Regulations 2004 (EIR) gives a general right of access to information held by public authorities. The Information Commissioners Office anticipates 90% compliance with the statutory response timescales of 20 working days. The Place and Resources Scrutiny Committee requested a performance report for its meeting on 24 October 2024 (which can be viewed here) and will continue to receive progress reports. The following chart is an extract from this report, but has been extended to include reporting since August 2024. As can be seen, whilst whole authority performance is generally Amber, the % is not too far removed from the 90% target. Work will be initiated with those Directorates that are struggling to meet compliance levels (primarily Childrens). In the meantime, an automated chase up process has been implemented to take administrative pressure off of the Information Compliance Team. A number of other automation possibilities were considered, but were not feasible for implementation, as the case numbers are not high enough to "teach" AI models sufficiently:

	Whole Authority	**Adults & Housing**	**Childrens**	**Corporate**	**Place**
Nov 24	87% (133)	86% (21)	69% (13)	98% (40)	84% (58)
Oct 24	88% (116)	79% (19)	73% (15)	91% (42)	95% (39)
Sep 24	87% (99)	73% (11)	75% (12)	93% (28)	89% (47)
Aug 24	86% (119)	70% (20)	70% (23)	97% (37)	92% (39)
Jul 24	84% (106)	91% (11)	63% (8)	84% (43)	86% (44)

	Whole Authority	Adults & Housing	Childrens	Corporate	Place
Jun 24	82% (114)	55% (11)	65% (20)	84% (44)	95% (37)
May 24	85% (127)	94% (16)	67% (15)	87% (39)	86% (56)
Apr 24	91% (137)	79% (14)	80% (10)	98% (45)	90% (67)
Mar 24	81% (111)	64% (11)	74% (19)	81% (43)	89% (36)
Feb 24	88% (165)	88% (17)	79% (19)	92% (63)	86% (64)
Jan 24	85% (82)	67% (9)	71% (7)	94% (31)	86% (35)
Dec 23	76% (114)	67% (15)	74% (19)	80% (35)	78% (45)
Nov 23	77% (111)	75% (12)	50% (12)	83% (42)	78% (45)
Oct 23	80% (99)	90% (10)	81% (16)	77% (35)	79% (38)
Sep 23	88% (122)	100% (23)	87% (15)	80% (35)	88% (48)
Aug 23	83% (123)	67% (9)	67% (18)	80% (50)	96% (45)
Jul 23	86% (125)	100% (12)	75% (12)	85% (55)	85% (46)
Jun 23	85% (108)	81% (16)	63% (8)	90% (39)	86% (44)
May 23	91% (97)	85% (13)	83% (12)	90% (39)	97% (33)
Apr 23	80% (101)	79% (14)	75% (12)	79% (38)	84% (37)

2.3 Individual Rights allows data subjects to enact certain powers over their personal information that is held. The most common and well known of these rights is the right of access, commonly referred to as subject access or subject access requests (SARs). This gives individuals the right to obtain a copy of their personal data held by an organisation, as set out in the General Data Protection Regulation.

2.4 Historically the Council has struggled to meet compliance with statutory timescales, with regularly reporting as a “Red” performance indicator (below 80% compliance). Significant progress has been made to improve performance since the Children’s SARs team were integrated into the Information Compliance team. Q1 and Q2 of 2024/25 are showing

compliance rates at 95% and 92% respectively, and recorded as Green. This is a significant achievement, as the complexity level of SARs has increased, particularly in terms of care leaver requests. The position has been improved by increasing the headcount in the team by 0.5fte to reduce outsourcing costs.

2.5 Officers and members are required to undertake mandatory data protection training. This is delivered primarily via e-learning, with data protection training completed annually and also incorporated into the elected member induction programme.

2.6 At the time of the July annual report, compliance levels for the mandatory Data Protection training was approx. 84%. As at November 2024 this has increased to 88%, but remains short of the 95% requirement set out in the NHS Data Security and Protection Toolkit, which is key in enabling continued access to health service data. A task and finish sub group has been established to look at improving compliance further, as part of an improvement action plan agreed with NHS, including understanding barriers to completion, identification of focus areas and consideration of consequential actions for non-compliance.

3. Business Continuity

3.1 The Council's Business Continuity Framework contains two main mechanisms:

- The Business Impact Analysis (BIA) – This is a list of Council functions assessed for their criticality in the event of a loss of service. It is a top level schedule that would be utilised by an Incident Management Team, to enable prioritisation for mobilising of services/recovery work and distribution of resources (for instance, repurposing of staff roles from lower criticality functions);

- Business Continuity Action Cards – These provide the detailed response that each Service Manager/Head of Service (action card owners) will take in the event of a business continuity incident

3.2 The Emergency Management and Resilience Team in Assurance facilitates the Council's business continuity framework. However completion and update of both actions cards and the BIA entries rest with individual service areas. Because of the close links to the cyber risk, and in the absence of a better suited corporate working group, business

continuity assurance is built into the remit of the Strategic Information Governance Board, and its associated working groups.

3.3 A 0.5 fte Emergency Management and Resilience Officer leads on business continuity, reporting to the Service Manager for Assurance. However their output is constrained by wider emergency management response and other workstream duties. Emergency Planning activity is reported annually to this Committee.

3.4 On inception of Dorset Council, predecessor Council action cards were adopted pending the restructures that took affect January 2020. As part of the preparations for EU exit, a process of amalgamation and review was undertaken, both of the BIA and action cards. Since then, there have been specific reviews of service criticality, aligned to Covid and, in 2023, the risk of national power outage. This was however light touch and scenario based, and not a full reassessment of business impacts. There has been some Directorate level testing (particularly covering some Place functions) and some whole Council exercises that provided a degree of testing of business continuity (the cyber peer review; Local Resilience Forum national power outage exercise).

3.5 On the 28th May 2024 an Incident Management Team (IMT) was instigated to consider a risk with the microsoft licencing which was thought could have resulted in the Council losing access to microsoft products until licencing could be resolved. The IMT included a prompt for services to ensure that their action cards could be accessed and were up-to-date. There were instances where service level plans had not been developed or reviewed. Following a debrief for the incident, the Service Manager for Assurance commissioned SWAP Internal Audit to carry out a review of business continuity embeddedness. SWAP issued their findings in November 2024, which provided a limited assurance, and 15 management actions, including 1 priority one (Red) and 13 priority two (Amber) actions. A number of these actions are closely linked, and can be packaged together as follows:

a) The BIA is insufficiently risk based (the priority one action) and out of date. The critical systems identified in the BIA are not current. The criticality of services has not been reviewed / signed off by Senior Leadership Team for some time, and there is no process for regular review;

b) The supporting Business Continuity Framework is out of date (last reviewed in April 2022) and is not sufficiently clear on roles and responsibilities. It could be better aligned to national standards;

c) Business continuity action cards are not being regularly reviewed or updated by services;

d) Business continuity action cards have not been regularly tested, either by individual services or on a whole council basis;

e) There is a lack of alignment of methodologies within the Business Impact Analysis and ICT continuity;

f) Whilst the Council is good at undertaking debriefs following incidents, identified actions are not tracked for completion and therefore there is a limited assurance that the issues have been completed;

g) Awareness and training of business continuity could be improved.

3.6 Although priority actions were identified by SWAP, a number of improvements were already underway since the Emergency Management and Resilience Officer lead was established. As recognised in the SWAP report however, corporate resourcing for business continuity within Emergency Management and Resilience Team is sparse, and the framework that we have established is reliant on self-service within Directorates.

3.7 Recent improvements include:

- Transferring of business continuity action cards into an easier to access/use site. This has included a review of action cards with some service areas, including identification of missing plans and updates to contact details;

- Developing a portfolio of mini exercises on a range of scenarios that can be used by service areas to test business continuity plans (power outage; cyber attack; loss of data; fuel);

- Running cyber related business continuity exercises with a range of services across Place Directorate.

3.8 However it is clear from the SWAP outcomes that further action is necessary, and at an increased pace. A draft improvement action plan

has been developed, which will be considered at January 2025's Operational Information Governance Group (OIGG). In summary, it provides the following proposed actions:

Identified Action	**Target Timescale**
Discuss Recovery Time Objectives with ICT (Align BIA to ICT Security criteria)	Jan-25
Finalise BC framework (This is largely already updated, but will require some input from OIGG representatives)	Jan-25
Develop Schedule of Communications and corporate exercises, to include promotion of service level exercises (This is largely complete, but will be agreed with OIGG)	Jan-25
Commence work with each Directorate to review BIA (This is the most resource hungry element and will require dedicated input from each Directorate Management Team)	Feb-25
Challenge output of BIA review via Strategic Information Governance Board, together with sign off of revised framework	Apr-25
Commence KPI reporting of service level action card reviews, for Directorate Management Team intervention as appropriate.	Apr-25
Present proposed BIA/critical services to SLT, as part of annual Emergency Planning report	May-25
Development of a whole authority action tracker, which would include monitoring of lessons learnt from business continuity incidents / exercises	May-25
Whole Council business continuity exercise	Tbc

3.9 It is likely that there will be a national level cyber security exercise during 2025 involving Local Resilience Forums feeding in to MHCLG. This would provide an opportunity to run a Dorset Council "whole authority" business continuity exercise alongside the LRF/national commitment.

3.10 It is proposed to provide a further update to the Committee within the Annual Emergency Planning report circa June 2025, to coincide with the action target dates set out in the audit report.

4. **Financial Implications**

There are no direct financial implications from this report, however information governance and business continuity issues can have an adverse financial impact

5. **Natural Environment, Climate & Ecology Implications**

Good quality and managed data is essential in supporting our climate change agenda

6. **Well-being and Health Implications**

Good quality and managed data is essential in supporting health and wellbeing

7. **Other Implications**

None

8. **Risk Assessment**

8.1 HAVING CONSIDERED: the risks associated with this decision; the level of risk has been identified as:

Current Risk: High
Residual Risk: High

This scoring reflects a number of High risks identified within the Council's risk register.

9. **Equalities Impact Assessment**

Information Governance policies have been subject to Equalities Impact Assessments

10. **Appendices**

None

11. **Background Papers**

Annual Information Governance Report to Audit and Governance Committee 22 July 2024

12. Report Sign Off

11.1 This report has been through the internal report clearance process and has been signed off by the Director for Legal and Democratic (Monitoring Officer), the Executive Director for Corporate Development (Section 151 Officer) and the appropriate Portfolio Holder(s)