



## Audit and Governance Committee

**Date:** Monday, 22 July 2024  
**Time:** 6.30 pm  
**Venue:** Council Chamber, County Hall, Dorchester, DT1 1XJ

**Members (Quorum 3)**

Gary Suttle (Chair), Spencer Flower (Vice-Chair), Belinda Bawden, Matt Bell, Neil Eysenck, Jill Haynes, Andrew Parry, Andy Todd, Ben Wilson and Alex Fuhrmann

**Chief Executive:** Matt Prosser, County Hall, Dorchester, Dorset DT1 1XJ

For more information about this agenda please contact Democratic Services Meeting Contact [john.miles@dorsetcouncil.gov.uk](mailto:john.miles@dorsetcouncil.gov.uk)

Members of the public are welcome to attend this meeting, apart from any items listed in the exempt part of this agenda.

For easy access to all the council's committee agendas and minutes download the free public app called Modern.Gov for use on any iPad, Android, and Windows tablet. Once downloaded select Dorset Council.

### Agenda

Item	Pages
<b>1. APOLOGIES</b>	
To receive any apologies for absence.	
<b>2. DECLARATIONS OF INTEREST</b>	
To disclose any pecuniary, other registrable or non-registrable interest as set out in the adopted Code of Conduct. In making their decision councillors are asked to state the agenda item, the nature of the interest and any action they propose to take as part of their declaration.	
If required, further advice should be sought from the Monitoring Officer in advance of the meeting.	

### 3. PUBLIC PARTICIPATION

Representatives of town or parish councils and members of the public who live, work, or represent an organisation within the Dorset Council area are welcome to submit either 1 question or 1 statement for each meeting. You are welcome to attend the meeting in person or via MS Teams to read out your question and to receive the response. If you submit a statement for the committee this will be circulated to all members of the committee in advance of the meeting as a supplement to the agenda and appended to the minutes for the formal record but will not be read out at the meeting. The first 8 questions and the first 8 statements received from members of the public or organisations for each meeting will be accepted on a first come first served basis in accordance with the deadline set out below.

All submissions must be emailed in full to [john.miles@dorsetcouncil.gov.uk](mailto:john.miles@dorsetcouncil.gov.uk) by 8.30 am on Wednesday 17 July.

When submitting your question or statement please note that:

- You can submit 1 question or 1 statement.
- A question may include a short pre-ambule to set the context.
- It must be a single question and any sub-divided questions will not be permitted.
- Each question will consist of no more than 450 words, and you will be given up to 3 minutes to present your question.
- When submitting a question please indicate who the question is for (e.g., the name of the committee or Portfolio Holder)
- Include your name, address, and contact details. Only your name will be published but we may need your other details to contact you about your question or statement in advance of the meeting.
- Questions and statements received in line with the council's rules for public participation will be published as a supplement to the agenda.
- All questions, statements and responses will be published in full within the minutes of the meeting.

- |    |                                                                            |         |
|----|----------------------------------------------------------------------------|---------|
| 4. | <b>ANNUAL EMERGENCY PLANNING REPORT</b>                                    | 5 - 18  |
|    | To receive a report by Marc Eyre, Service Manager for Assurance.           |         |
| 5. | <b>ANNUAL FRAUD AND WHISTLEBLOWING REPORT</b>                              | 19 - 28 |
|    | To receive a report by Marc Eyre, Service Manager for Assurance.           |         |
| 6. | <b>ANNUAL INFORMATION GOVERNANCE REPORT</b>                                | 29 - 54 |
|    | To receive a report by Marc Eyre, Service Manager for Assurance.           |         |
| 7. | <b>QUARTERLY RISK MANAGEMENT UPDATE</b>                                    | 55 - 66 |
|    | To receive a report by Chris Swain, Risk Management and Reporting Officer. |         |

**8. SWAP UPDATE REPORT** 67 - 76

To receive a report by Sally White, Assistant Director for SWAP.

**9. WORK PROGRAMME** 77 - 80

To consider the work programme for the Committee.

**10. URGENT ITEMS**

To consider any items of business which the Chairman has had prior notification and considers to be urgent pursuant to section 100B (4) b) of the Local Government Act 1972. The reason for the urgency shall be recorded in the minutes.

**11. EXEMPT BUSINESS**

To move the exclusion of the press and the public for the following items in view of the likely disclosure of exempt information within meaning of paragraph x of schedule 12 A to the Local Government Act 1972 (as amended).

The public and the press will be asked to leave the meeting whilst the item(s) of business is considered.

**There are no exempt items scheduled for this meeting.**

This page is intentionally left blank

## Audit and Governance Committee

22 July 2024

## Annual Emergency Planning Report – 2023/24

### For Review and Consultation

**Portfolio Holder:** Cllr S Bartlett, Planning and Emergency Planning

**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

**Brief Summary:** This is the first annual report on emergency planning, and follows a request from Audit and Governance Committee to receive a periodic update on activity and learnings from events.

The report provides an overview of workplans, exercising of the plans, a summary of the Council's 'Command and Control' structures and highlights a number of significant events that were responded to during 2023/24. It also sets out priorities for 2024/25.

There is a growing demand for improving overall societal resilience. This paper summarises some of the actions that are being taken to support communities in this respect.

**Recommendation:** To note the annual report and learnings from incidents.

**Reason for Recommendation:** To provide assurance over the Council's ability to respond to significant civil emergencies.

## 1. **Background**

- 1.1 The Civil Contingencies Act (CCA) 2004 establishes a clear set of roles and responsibilities for organisations involved in emergency preparation and response. The Act divides local responders into two categories, imposing a different set of duties on each.
- 1.2 Category 1 Responders are those organisations at the core of the response to most emergencies, which includes local authorities, alongside police, fire, ambulance service, health, coastguard, and the environment agency. Category 1 responders are required to:
- assess the risk of emergencies occurring and use this to inform contingency planning;
  - put in place emergency plans;
  - put in place Business Continuity Management arrangements;
  - put in place arrangements to make information available to the public about civil protection matters and maintain arrangements to warn, inform and advise the public in the event of an emergency;
  - share information with other local responders to enhance co-ordination;
  - co-operate with other local responders to enhance co-ordination and efficiency;
  - provide advice and assistance to businesses and voluntary organisations about business continuity management (local authority responsibility).
- 1.3 Meanwhile Category 2 Responders consist of the Health and Safety Executive, transport, utility companies and the voluntary sector organisations. These organisations are generally less likely to be involved in the heart of planning work but will be heavily involved in incidents that affect their sector.
- 1.4 The CCA requires the establishment of Local Resilience Forums (LRF), usually based on each police area, as a mechanism to discharge the above duties. The Dorset LRF therefore covers both Dorset Council and Bournemouth, Christchurch and Poole Council areas and includes representatives from each of the Category 1 responders. The LRF provides a co-ordinated cross-partner approach to planning, training/exercising, response, recovery and debriefing. The workplan of

the LRF is informed by the [National Risk Register](#), and the localised [Dorset Risk Register](#). The administration and co-ordination of the LRF is facilitated by the Dorset Civil Contingencies Unit (CCU), which is funded by category 1 responders and hosted by Dorset and Wiltshire Fire and Rescue Service (DWFRS).

- 1.5 In the event of a significant emergency requiring multi partner response, the LRF will initiate a Strategic Coordinating Group (SCG), determining the overall strategy for response), and a Tactical Coordinating Group (TCG) that determines how to deliver the strategy. For certain emergencies, and generally once the response to an incident is concluded, a Recovery Co-ordinating Group will be initiated. Recovery is the process of rebuilding, restoring and rehabilitating the community following an emergency. This would most often be led by a local authority.
- 1.6 Emergency Planning at Dorset Council has an identified 'Command and Control' structure set out within the councils' [Emergency Response Plan](#) (internal link), which is reviewed and updated annually. 'Command and Control' is essentially the term used to describe how designated Gold and Silver commanders can effect their authority and direction in an emergency situation, outside of the usual management structures of the organisation. There are 24/7 tours of duty for both Gold (Strategic) officers (Executive and Corporate Directors level), and Silver (Tactical) officers (Heads of Service level).
- 1.7 The Emergency Planning team are part of the Assurance Service, the Legal and Democratic Directorate, and deliver planning, exercising, response and debriefing post incident, as well as facilitating the Council's business continuity arrangements. The team consists of 4.5 fte Emergency Management and Resilience Officers who, together with the Service Manager for Assurance, provide a 24/7 Duty Emergency Planning Officer function for the Council. The Council also hosts the LRF funded Community Resilience Liaison Officer (CRLO), whose main role is to work with and within communities to help improve societal/community resilience.

## 2. **Emergency Planning and Exercising**

- 2.1 Each of the Risk and Resilience Officers lead on a range of workstreams, linked back to the Dorset Risk Register. This incorporates both the Council's response and statutory duties, and in some cases multi-agency plans led by Dorset Council. The key workstreams are set out below:

Humanitarian and Communities	Humanitarian response; Vulnerable people data; National power outage; Large scale evacuations; Community hubs and rest centres; Training and exercising; Summer operations; Health resilience; Voluntary organisations; Utility (water) planning; Low pressure gas; Community resilience; Events Safety Advisory Group (SAG) Football safety advisory groups
Weather and Environmental	Severe weather; Dam and reservoir offsite plans; Stranded motorists; Space weather; Wildfires; Climate change; Rockfalls and landslides; Coastal pollution
External Threats	Cyber attack; Chemical Biological Radiological and Nuclear (CBRN); Counter terrorism
Statutory Workstreams	Radiation (Emergency Preparedness and Public Information) Regulations offsite plans; Radiation monitoring units; Control of Major Accident Hazards (COMAH) offsite plans; Major Accident Hazard pipelines
Miscellaneous (incl internal plans)	Business continuity; Operation Bridges (death of a senior royal); Excess deaths; Mass fatalities; Recovery; Fuel disruption planning; Telecoms; Site clearance;



	Animal health; Technology; Website and external communications
--	----------------------------------------------------------------------

- 2.2 Each workstream also has a nominated deputy, to ensure resilience in the event of absence. Allocation of workstreams is reviewed regularly, and adjusted to ensure a fair caseload across the team. There are also a series of action cards to support responding officers.
- 2.3 In cases of national security, lead on planning and response is provided by central government.
- 2.4 Exercising is a key part of ensuring that the Council (and other LRF partners) are able to effectively respond to incidents. Some exercises are required by law, and hence statutory (for instance, offsite plans for REPPiR and COMAH sites, which are regulated). Other plans are exercised following periodic reviews, or on a risk based schedule.
- 2.5 The risk of a significant loss of power (including a national power outage) remains high on the risk register, due to its significant impacts as well as challenges of responding, at a time when all organisations are so reliant on technology. Dorset LRF participated in a 3 day national exercise at the end of March 2023, and the Council took this opportunity to also test internal planning. An Incident Management Team was role played, and learnings captured to generate and improve plans.
- 2.6 The Emergency Response Plan sets out that all Gold and Silver officers should receive training both before commencing first duties and refresher training every three years. All Gold and Silver officers are provided with an overview of their role by the appropriate emergency planning business partner. In addition to this, multi agency training should be undertaken, together with decision making and inquest/public enquiry training. At present 54% of current Gold officers have received multi agency training within the last three years, and 65% of Silver officers. This is a key priority for the emergency planning team during 2024/25.
- 2.7 Gold and Silver officers are also encouraged (and often required) to participate in exercises, to help boost experiences. The emergency planning team regularly host short workshops to help share knowledge.

### 3. Emergency Response and Debriefing

- 3.1 During 2023/24, the emergency planning team recorded 39 incidents in which they were mobilised, in addition to a range of call outs not associated with response. In the majority of cases, these incidents will be managed within the team (or by the Duty Emergency Planning Officer out of hours), but larger incidents will require input/support from across a number of Dorset Council services, escalation to Gold/Silver and, in some cases, escalation to the multi agency LRF. By their very nature, the most significant events can require ongoing response over a number of days, weeks or even months.
- 3.2 In the event of a significant emergency or business continuity incident, the emergency planning team will liaise with DC Gold/Silver officers to determine the need for calling an Incident Management Team (IMT). This will bring together decision makers from across all impacted services to understand the risks and determine a co-ordinated response. The IMT will help understand and inform Gold/Silver officers of the latest situation, in advance of multi-agency meetings (e.g. SCG and TCG).
- 3.3 Emergency Planning response per calendar months is set out below:

April 2023	Illegal rave; Modern day slavery issue; Pollution incident (x2); Rockfalls (x2); Residential fire
May 2023	Road closure; Illegal rave
June 2023	Security alert (false alarm)
July 2023	Falling trees
August 2023	Potential evacuation; Security alert; Response to unauthorised event
September 2023	Gas leak; Health and safety incident at DC school; Lightning strike; Security alert

October 2023	Gas leak requiring evacuation; Faulty signage; Flooding
November 2023	Storm Ciaran; Storm damage at school; Rockfall; Flooding (x2) Impacts of substation fire Weymouth
December 2023	Rockfall (x2); Mortuary capacity; Police enquiry – serious crime
January 2024	Residential fire with evacuation;
February 2024	Landslide (x3); Prolonged loss of public utility (gas)
March 2024	Bomb disposal; Rockfall; Flooding

3.4 Those incidents requiring Incident Management Teams and/or multi agency co-ordination are set out below. A key emergency planning discipline is to undertake de-briefing, so that plans and response can be enhanced for future incidents. These de-briefs identify i) what went well; ii) what didn't go so well; iii) what could be done better in future. A summary of key learnings is included, where available, below.

### 3.5 **Poole Harbour Oil Spill**

3.5.1 Although occurring on 26 March 2023, and therefore outside the timescale of this annual report, the response continued into 2023/24. This multi-agency environmental response was in relation to a significant leak of crude oil from one of Perenco's well pipes into Poole Harbour - declared a major incident by the LRF. Dorset Council took the lead on the recovery post incident, which continued until 28 February 2024.

3.5.2 The lessons learnt are not yet available, as not yet released by the Local Resilience Forum.

### 3.6 Storm Ciaran

3.6.1 England faced a significant storm when Storm Ciaran hit on 2 November 2023. Although Dorset did not suffer the same levels of disruption as neighbouring counties, it still placed a significant impact on Dorset Councils' resources, with road closures, falling trees and evacuations. Dorset Council instigated an Incident Management Team on 31 October 2023 in preparation and remained stood up throughout the storm.

3.6.2 *What went well?* Proactive contact with vulnerable residents, including proactive use of data; establishing multi agency command point for the Portland Beach Road closure; co-ordinated IMT and response; quick response to evacuation at Freshwater Holiday Park; deployment of flood barriers; good co-ordination of highways; well pitched communications; early stand-up of 4x4 capacity; early mobilisation of rest centre capability.

3.6.3 *What will we do better?* The response was generally deemed to be a success. However there were a number of learnings. We will look to provide a great spread of training for loggists; we will ensure that wellbeing of staff has greater emphasis on IMT agendas, for lengthy responses in adverse weather conditions; we will look to improve how we use mapping in response with prepopulated data.

3.7 The Local Government Association has provided a useful councillors guide setting out [their role in a civil emergency](#). In an emergency councillors are not involved in the operational response which is led by council officers. However, it defines the following areas where councillors can provide good leadership:

- *Political leadership* – Ensuring that the Council is meeting its obligations under the CCA, in terms of preparing for and responding to emergencies. By way of this annual report, Audit and Governance Committee has an opportunity to receive this assurance. Similarly, emergency planning sits within the “Planning and Emergency Planning” portfolio;
- *Civic leadership* – Providing a focal point for the local area during an emergency. This was seen to great effect during the Covid pandemic, and also in response to recent storm events;
- *Community leadership* – Helping to increase community resilience, and supporting communities' emergency responses and through

the period of recovery. This is covered in more detail in section 5 of this report.

#### 4. **Business Continuity**

- 4.1 Whilst Emergency Response focuses on the safety and protection of life, assets, and the environment, business continuity is focused on the continuity of Dorset Council's own critical business operations. All services are ranked for criticality, and this 'business impact assessment' is used to focus critical service maintenance, prioritisation and recovery in an emergency.
- 4.2 All services are required to maintain a business continuity action card, which sets out how it responds to a range of consequences, such as loss of staff, premises, systems or data, and critical third-party supplier failure. The emergency planning team seek to drive engagement to educate and embed BC across Dorset Council. A number of mini exercises have been released, allowing teams to test the adequacy of business continuity plans against a range of scenarios. This has included the response to a significant power outage, a cyber-attack and resultant loss of data. It is intended to hold a whole authority business continuity exercise later in the financial year.
- 4.3 The '[Dorset Prepared](#)' website provides tools and guidance to support businesses and voluntary organisations.

#### 5. **Societal resilience**

- 5.1 There is a growing recognition nationally of the importance of establishing greater resilience within communities, so that they are able to respond to incidents affecting them locally. Societal resilience is about empowering the whole of society, including individuals, families, businesses, sporting and social clubs, cultural groups, educational establishments, institutions and religious groups to become involved in developing how they can become more resilient.
- 5.2 The Dorset LRF's strategy includes:
  - Co-ordinating community resilience across Dorset;
  - Providing the knowledge, expertise and tools to support communities;

- Engaging with communities, groups and networks across Dorset, including parish and town councils, faith groups, voluntary groups and community interest groups;
  - Encouraging effective dialogue between communities and LRF partners;
  - Meet the mandatory requirements and work towards good practice as contained in the National Resilience Standard for Community Resilience
- 5.3 The LRF Community Resilience Group is co-chaired by Dorset and BCP Council officers, and co-ordinates delivery of the strategy. In 2023 the LRF agreed to fund a pan-Dorset Community Resilience Liaison Officer (CRLO) on a fixed term contract. This position is hosted by Dorset Council, but covering both unitary council areas.
- 5.4 The CRLO engages daily with numerous organisations and groups interested in the development of resilience across Dorset and the wider UK. These engagement activities occur in person within communities and online locally and nationally; taking the form of events, festivals, county, and local shows, drop ins, exercises, advisory groups, talks, presentations, assemblies, meetings and webinars. The CRLO visits and engages with local communities and UK organisations within working and outside of normal working hours during evenings and weekends, throughout the year, at the request of the specific group. The CRLO has been engaged in the development of several Community Emergency Response Plans.
- 5.5 The [‘Dorset Prepared’ website](#) has been redeveloped and provides tools and guidance for communities.
6. **Priorities for 2024/25**
- 6.1 Plans relating to a number of workstreams are currently actively being reviewed and updated, notably: coastal pollution; excess deaths; rock falls and landslides; fuel; loss of utilities (water / gas); wildfires; dam and reservoir inundation; vulnerable people data sharing; operation bridges and telecoms.
- 6.2 There remains focus on planning to respond to a national power outage, including resilience communications and establishing community hubs.

- 6.3 The REPPiR and COMAH regulations set out the requirement for statutory exercises for testing offsite plans. In particular, significant planning and exercising is required for the Portland Port submarine berth at least every three years to satisfy the Office for Nuclear Regulation (ONR), and Defence Safety Nuclear Regulator (DNSR). This also allows the MoD to maintain Portland Port as an asset for the Royal Navy's nuclear powered warships. The next REPPiR is due at the end of the financial year, and is the largest multi agency exercise held by the LRF. Whilst not as onerous, COMAH sites are also subject to regular exercising/testing, to satisfy regulators (Health and Safety Executive and the Environment Agency) and maintain the operators' licenses. An exercise is scheduled in September this year for one of the two current COMAH sites. Dorset Council is the lead duty holder authority for both REPPiR and COMAH offsite plans.
- 6.4 The business continuity framework continues to be improved, with the provision of new material to further drive engagement and facilitation of review and update of plans. It is intended to enable a whole authority business continuity exercise later this financial year.
- 6.5 Training and exercising remains a priority, and the emergency planning team will be working with Gold and Silver officers to improve take up. Aside from the statutory exercises, a further two multi agency exercises are scheduled for this financial year, in addition to smaller exercises linked to larger community events.
- 6.6 There will remain a concerted effort to engage with communities and improve societal resilience.

## **7. Financial Implications**

- 7.1 The financial impacts on an organisation of a significant emergency response can be extreme, and an unplanned / unbudgeted expenditure. Some protection is provided via the Bellwin scheme, which is a government financed assistance to reimburse local authorities for costs incurred on, or in connection with, their immediate actions to safeguard life and property or to prevent suffering or severe inconvenience as a result of a disaster or emergency in their area. Where the criteria are met, the grant is normally payable at up to 85% of eligible costs.

## **8. Natural Environment, Climate & Ecology Implications**

8.1 The changing climate informs weather events, and as an example 2023/24 presented a significant number of storm challenges. Emergency response plans need to keep pace with the changing environment.

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

9.1 Protecting life is a key objective for LRFs, containing and mitigating the impacts of an emergency and creating the conditions for a return to normality.

10. **Other Implications**

10.1 None

11. **Risk Assessment**

11.1 HAVING CONSIDERED: the risks associated with this report the level of risk has been identified as:

Current Risk: Low

Residual Risk: Low

11.2 As this is a report setting out activity, the risk has been ranked as low. However it should be noted that a number of high risks are defined within both the Dorset Community Risk Register and Dorset Council's Risk Register. In particular for Dorset Council, the threat of cyber-attack is identified as an extreme risk, and the impacts of a national power outage identified as high risk. In both instances, this recognises that there are significant controls in place, but that both provide high level impacts should they arise.

12. **Equalities Impact Assessment**

12.1 The Emergency Response Plan has been subject of an Equality Impact Assessment.

13. **Appendices**

13.1 None

14. **Background Papers**

14.1 None

15. **Report Sign Off**



15.1 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)

This page is intentionally left blank

## Audit and Governance Committee

22 July 2024

## Annual Fraud and Protected Disclosures Report

### For Review and Consultation

**Portfolio Holder:** Cllr N Ireland, Leader and Cabinet Member for Governance, Performance, Communications, Environment, Climate Change and Safeguarding

**Executive Director:** J Mair, Director of Legal & Democratic

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

**Report Status:** Public

**Brief Summary:** The Audit and Governance Committee receives an annual report on fraud and protected disclosures (often referred to as whistleblowing). This provides an update on the Council's approach to combatting the fraud risk, and a summary of cases reported in the preceding twelve months.

**Recommendation:** The Committee are asked to:

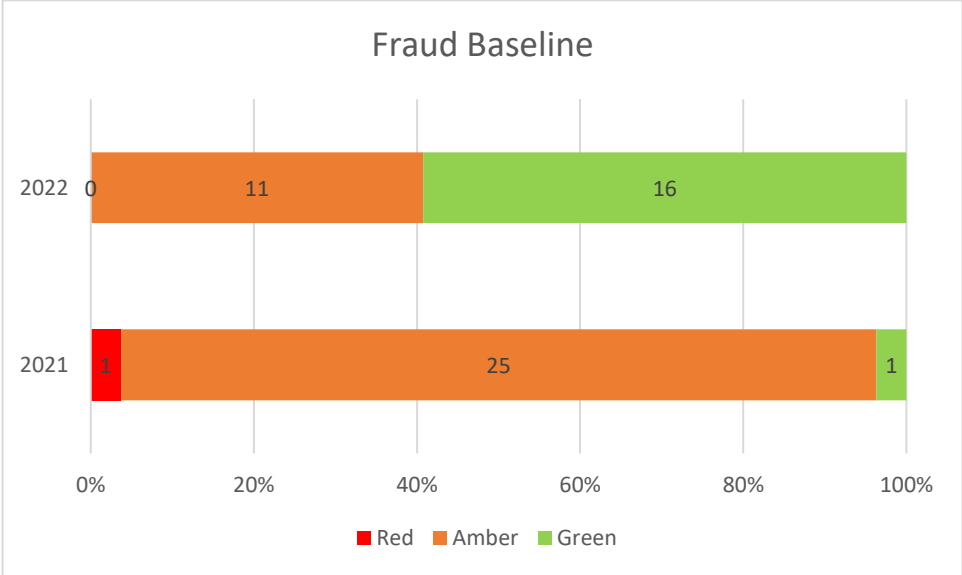
- i) Note the annual update on fraud and protected disclosure activity;
- ii) To reaffirm that the Chair of the Audit and Governance Committee acts as the Council's member fraud prevention champion.

**Reason for Recommendation:** To support the Council's zero tolerance to fraud.

#### 1. Summary of Anti Fraud Initiatives

- 1.1 The 2022/23 annual report highlighted the outcomes of the second SWAP baseline assessment of anti-fraud maturity. This provided a cross-cutting baseline assessment report on the maturity of fraud management across

wider SWAP partners. As shown in the comparison chart below, significant progress was made between the two years.



1.2 The output of the baseline review informs the Council’s fraud action plan to track progress in implementing anti-fraud initiatives. This includes actions to respond to Amber ratings from the baseline review, where appropriate. Ordinarily the annual report provides an update on progress made in the last twelve months (presented last to the [12 June 2023](#)

[committee](#)) but for the benefit of new committee members, a more detailed summary has been provided this year:

Theme	Latest Position	2022 SWAP Rating	24 DC Self Assessment
1) Resources and Communication	<p>The fraud and whistleblowing intranet pages have been reviewed and updated. The Chief Executive issues an annual reminder of our whistleblowing arrangements (issued May 24).</p> <p><b>Outstanding Actions:</b> None</p>	Amber	Green
2) Fraud Risk management	<p>A fraud risk assessment review led by SWAP identified a number of fraud risks that have been embedded into the Council's Service Risk Register framework. These are reviewed and updated by risk owners alongside any other service risks. The SWAP fraud team intend to carry out a further piece of work to determine how embedded processes are within services.</p> <p><b>Outstanding Actions:</b> None</p>	Green	Green
3) Policy framework	<p>The following policies are operative, and due for review by May 2025. They are accessible both internally via the Council's intranet and externally on the internet.</p>	Amber	Amber

Theme	Latest Position	2022 SWAP Rating	24 DC Self Assessment
	<ul style="list-style-type: none"> <li>• <a href="#">Anti Fraud Bribery and Corruption Policy</a>;</li> <li>• <a href="#">Anti Money Laundering Policy</a>;</li> <li>• <a href="#">Whistleblowing Policy</a></li> </ul> <p><b>Outstanding Action:</b> A declaration process for staff is in development for register of interests</p>		
4) Committee Related	<p>The Chair of Audit and Governance Committee is identified as member anti-fraud champion. The Committee receive an annual report on fraud and whistleblowing activity.</p> <p><b>Outstanding Action:</b> Recommend that members of the Audit and Governance Committee undertake the e-learning modules for Fraud and Whistleblowing</p>	Amber	Amber
5) Culture and Awareness	<p>A number of service areas have initiated data matching via <a href="#">Cifas</a> (as part of our internal audit arrangements with SWAP), including insurance and contractor/agency appointment. During 2023/24 Adult Services</p>	Amber	Amber

Theme	Latest Position	2022 SWAP Rating	24 DC Self Assessment
	<p>direct payments, licencing and homelessness applications were added to Cifas checks. Additional service areas are being considered for inclusion, with SWAP currently exploring viability with Adults micro providers, existing Adults high-risk contracts, Financial Agents and Power of Attorneys.</p> <p><b>Outstanding Action:</b> Services identified with highest risk exposure for fraud to be encouraged to undertake fraud and whistleblowing training. SWAP are developing a fraud e-learning module, which will be reviewed for possible adoption.</p>		
6) Reporting, Investigating and Monitoring	<p>Reporting is provided annually to Audit and Governance Committee. Investigations are undertaken either internally or by commissioning the SWAP counter fraud team. A fraud/whistleblowing hotline is operative.</p>	Amber	Green

Theme	Latest Position	2022 SWAP Rating	24 DC Self Assessment
	<p><b>Outstanding Action:</b> Formalise Joint Working Fraud Protocol with SWAP.</p>		

1.3 Last years’ annual report sighted the Committee on a fraud investigation that was ongoing at that time, prompted by whistleblowing. Whilst it is not appropriate to share the full details in a public report, this related to allegations that two employees were undertaking private work using Dorset Council operatives and other resources. SWAP were commissioned to investigate, and following the outcomes of this work one employee resigned and the other was dismissed. The investigations prompted a second report on culture and ethics, which raised some weaknesses in internal controls and following which a number of actions have been incorporated within the ongoing fraud action plan, for wider organisational learning. The service concerned co-operated fully during the investigations and responded swiftly and proactively to recommendations made, with remedial actions implemented to prevent reoccurrence. SWAP can be applauded for the thorough investigation, which resulted in prompt action, halting what was a likely ongoing instance of fraud and the approach reinforced the Council’s zero-tolerance for fraud. It acts as a timely reminder of the effectiveness of whistleblowing. A number of actions have been incorporated into the fraud action plan based on the findings.

1.4 Historically the chair of Audit and Governance Committee has been identified as the elected member fraud prevention champion. The committee are requested to reaffirm this position.

**2. Reporting of Fraud and other Protected Disclosures – 2023/24**

2.1 The Public Interest Disclosure Act 1988 protects any whistleblowing worker from any form of reprisal or mistreatment from their employer after raising a concern, where that concern is in the public interest. The Council’s [whistleblowing policy](#) sets out the Council’s response to this legislation, and applies to all council employees and other workers;



including freelance staff; temporary and agency staff; trainers; volunteers; consultants; and contractors.

- 2.2 Whilst any issues reported via the whistleblowing hotline or directly to either the Monitoring Officer or Section 151 Officer will be recorded centrally, other issues that could constitute fraudulent activity (for instance those related to staff code of conduct) are investigated and reported separately via Human Resources. At this point in time, this report focuses on issues reported to the Monitoring Officer or Section 151 Officer.
- 2.3 The purpose of the whistleblowing policy extends beyond fraud to other perceived cases of malpractice, whether behavioural, procedural or in respect of health and safety failings. Whilst a protected disclosure relates purely to council workers, the spirit and procedures of the policy are also applied if contact is made by a member of the public.
- 2.4 The whistleblowing policy sets out a number of mechanisms for notification of fraud or other perceived malpractice. The table below sets out whistleblowing and fraud activity during 2022/2023, with fourteen cases reported in the twelve month period (April 23 to March 24), up from seven in the previous year. This has likely increased due to an improved promotion of the whistleblowing arrangements, and easier accessibility of the policy from the Council's internet:

Ref	Category (Alleged)	Reported by	Via	Summary
2023/01	Malpractice, negligent, unprofessional or unethical behaviour	Member of the public	Chief Executive	Unethical behaviour. Resignation of employee.
2023/02	Malpractice, negligent, unprofessional or unethical behaviour	Ex-Employee	Monitoring Officer	Ongoing investigations
2023/03	Malpractice, negligent, unprofessional or unethical behaviour	Employee	Monitoring Officer	Alleged faults in process. Minor procedural changes made by service.
2023/04	Malpractice, negligent,	Employee	Line Manager	Alleged unethical use of social media. Awareness

Ref	Category (Alleged)	Reported by	Via	Summary
	unprofessional or unethical behaviour			raised within team on social media use.
2023/05	Malpractice, negligent, unprofessional or unethical behaviour	Member of the Public	Complaints e-form	Allegations about an employee that were investigated but not upheld
2023/06	Malpractice, negligent, unprofessional or unethical behaviour	Member of the Public	Complaints e-form	Allegations about an employee. Managed as an HR issue, outside of whistleblowing policy
2023/07	Fraud, corruption or unauthorised use of public funds	Member of the public	Monitoring Officer	Allegation of fraudulent time keeping. Not upheld
2023/08	Malpractice, negligent, unprofessional or unethical behaviour	Member of the public	Complaints e-form	Allegations about an employee. Not investigated as not related to employee's role.
2023/09	Fraud, corruption or unauthorised use of public funds		Monitoring Officer	Ongoing investigations
2023/10	Malpractice, negligent, unprofessional or unethical behaviour	Ex-employee	Monitoring Officer	Allegations against employees relating to the termination of employment were not upheld
2023/11	Malpractice, negligent, unprofessional or unethical behaviour	Employees	SWAP	Issues addressed within transformation, and therefore file closed
2023/12	Malpractice, negligent, unprofessional or unethical behaviour	Member of the public	Complaints e-form	Allegations against employee not upheld
2023/13	Fraud, corruption or unauthorised	Manager	Monitoring Officer	Polygamous working. Employment terminated.

Ref	Category (Alleged)	Reported by	Via	Summary
	use of public funds			
2023/14	Malpractice, negligent, unprofessional or unethical behaviour	Ex-employee	Service Manager for Assurance	Ongoing investigations

2.5 The following table provides a summary of whistleblowing activity and/or reported fraud across a number of financial years:

Financial Year	2023/24	2022/23	2021/22
Upheld	2 (14%)	1 (14%)	
Partially Upheld	2 (14%)		1 (25%)
Not Upheld	6 (43%)	6 (86%)	3 (75%)
Ongoing	4 (29%)		
<b>Total</b>	<b>14</b>	<b>7</b>	<b>4</b>

### 3. Financial Implications

Fraud presents a financial risk to the Council which needs to be managed to reduce risk down to an acceptable level.

### 4. Climate Implications

None

### 5. Well-being and Health Implications

None

### 6. Other Implications

None

### 7. Risk Assessment

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

Current Risk: Medium  
Residual Risk: Medium

8. **Equalities Impact Assessment**

Fraud policies have been subject to EQIA.

9. **Appendices**

None

10. **Background Papers**

None

11. **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).

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

### For Review and Consultation

**Portfolio Holder:** Cllr N Ireland, Leader and Cabinet Member for Governance, Performance, Communications, Environment, Climate Change 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](mailto:marc.eyre@dorsetcouncil.gov.uk)

**Report Author:** James Fisher  
**Job Title:** Data Protection Officer  
**Tel:** 01305 838125  
**Email:** [james.fisher@dorsetcouncil.gov.uk](mailto:james.fisher@dorsetcouncil.gov.uk)

**Report Status:** Public

**Brief Summary:** This is the second Annual Information Governance Report and sets out the progress made during 2023/24 in further embedding information governance.

**Recommendation:** To note the 2023/24 activity and focus for 2024/25.

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

#### 1 **Information Governance Structures at Dorset Council**

- 1.1 This is the second Annual Information Governance Report, to be presented to both Senior Leadership Team and to the Audit and Governance Committee. The aim of the report is threefold: i) to provide an update on information governance activity; ii) to provide assurance that

- arrangements are fit for purpose; and iii) identify areas of improvement and focus for the forthcoming year.
- 1.2 Information governance at Dorset Council can be broadly split into three main areas: i) information compliance (including data protection, information requests and regulation of investigatory powers); ii) information security (including cyber threats); and iii) information management.
  - 1.3 The report is supported by the Data Protection Officer (DPO). Whilst employed by the Council (and working to the Service Manager for Assurance), the UK General Data Protection Regulations require that the DPO is independent, an expert in data protection, adequately resourced, and reports to the highest management level. This link is provided by the Assurance Service reporting to the Director for Legal and Democratic, who acts as the Senior Information Risk Owner (SIRO) and the conduit with the Senior Leadership Team (SLT).
  - 1.4 The SIRO role is mandatory for public sector organisations and is responsible for implementing and managing information risks within the organisation.
  - 1.5 The role of Caldicott Guardian is now performed by the Corporate Director for Adult Social Care Operations, having previously sat within Childrens Services. This is a statutory role, responsible for protecting the confidentiality of service users' health and care data and making sure that it is used appropriately. Key responsibilities are to act as the 'conscience' of the organisation and champion confidentiality issues with senior management; provide leadership and informed guidance on complex matters involving confidentiality and information sharing; and ensure that the council satisfies the highest practical standards for handling personal information.
  - 1.6 The Council established a Strategic Information Governance Board (SIGB) late 2022, chaired by the SIRO with representatives from all Directorates that sit on their respective management teams. Professional advice is provided to the SIGB by a range of officers (DPO, Caldicott Guardian, information management, cyber security, business intelligence, legal, human resources; and the transformation programme). The SIGB has authority to approve information governance policies, practices and standards developed by the operational groups. The board also has authority to accept risk or enable appropriate controls to bring the risk

- down to an acceptable level, escalating to the SLT at the SIRO's discretion.
- 1.7 The SIGB is supported by a number of operational working groups. These groups will commission separate task and finish groups to undertake particular focussed work as necessary.
  - 1.8 Operational Information Governance Group  
Chaired by the Service Manager for Assurance, as the name suggests this Group has responsibility for operational information governance matters. This includes i) review and development of policies, processes and standards; ii) response to adverse performance; iii) monitoring of service information governance risks; iv) review and challenge of Data Protection Impact Assessments; and v) monitoring the roadmap of legislative change.
  - 1.9 Organisational Compliance and Risk Learning Group  
This is chaired by the Service Manager for Business Intelligence and Performance with a remit for debriefing information related risk events that occur so that learnings can be agreed and cascaded/communicated. The Group also has a lead role in identifying and commissioning audits on information governance activities.
  - 1.10 Cyber Security Technical Group  
Chaired by the Cyber Security and ICT Continuity Lead this group provides the operational capabilities for cyber security and ICT within the Council, in addition to the response and recovery to an incident.
  - 1.11 Digital Applications Governance Group  
This is chaired by a Programme Manager in the Transformation, Innovation and Digital Service. The group monitors the roadmap of Microsoft applications, alongside other system developments. It reviews business requests for accepting applications into the Council's ICT infrastructure, with an analysis of risk (data protection / cyber security / information risk) vs business opportunity.
- 2 Information Governance Activity During 2023/24**
- 2.1 Whilst established towards the end of 2022/23, the SIGB and its supporting working groups have been embedded more fully during 2023/24, to provide a really solid platform for assurance over information governance and challenge/testing of risk acceptance.

- 2.2 The Council's overarching [Information Governance Policy](#) was reviewed and refreshed in January 2024 by the SIGB. This policy outlines the strategic framework of individual responsibilities, accountable roles, governance groups, and cooperation between information-related professionals, to build a culture that values information as an asset.
- 2.3 The [Records Management Policy](#) was also reviewed and updated by the SIGB. This policy sets out Dorset Council's commitment to achieving high standards in records management in order to meet its strategic objectives, legislative and regulatory obligations, mitigate risk and adhere to best practice standards.
- 2.4 **Cyber Security**
- 2.4.1 The Information Commissioners Office released statistics highlighting that cyber attacks on local authority systems have increased by 24% between 2022 and 2023. Because of this inherent risk, the threat of a successful cyber attack is currently identified as an extreme risk in the Council's risk register. Cyber security has made steady progress over the last year. With some changes to technical systems being more of a lateral move initially but with the potential to offer significant improvements mid and long term. This includes replacing the existing Security Incident and Event Management (SIEM) solution with a new product.
- 2.4.2 Vulnerability management procedures have been improved reducing the time the council is exposed to technical flaws in software that can allow a successful cyber attack.
- 2.4.3 The way in which requests for new applications within the council has been improved both for larger line of business applications and for client based smaller applications. This work is not completed although a multi discipline project is underway to review Application Portfolio Management within the council.
- 2.4.4 Cyber security training is mandatory for all officers and councillors, and is delivered via small bitesize modules to ensure that the content remains relevant to the most current threats. At the time of writing this report whole authority compliance is at 73%.
- 2.4.5 A set of business continuity exercises are being distributed to services, to allow them to test their current resilience to both cyber attack and any resultant loss of data.



- 2.4.6 Despite these significant improvements, it is accepted that the impacts of a successful attack can be so significant that the risk level will always remain high. There are measures that the council does not currently have in place which could further reduce both the likelihood and impact of a successful attack. A discussion with senior political and officer leadership regarding our risk appetite would be welcome to ensure we achieve the strongest defensive posture possible within the context of the council's financial position.
- 2.5 The Council's [Data and Business Intelligence Strategy](#) was approved in February 2023. This 5-year strategy sets out to put using data at the heart of the Council's decision-making, and is an integral part of "Our Future Council" transformation. The Data and Business Intelligence programme includes a number of information governance related projects: i) Data Governance, including data policy and sharing; ii) Data Quality; and iii) Records Management.
- 2.6 The Data Quality project recognises that data quality is a key component of the organisations Data and Business Intelligence Strategy. Pilot work for the Data and BI strategy identified that data quality concerns are a barrier to successfully being able to join data sets and hence to derive greater insights. To date the project has focussed on improving the unique identifiers which are captured within our Adults and Childrens services case management systems (NHS numbers; Unique Property Reference Numbers). This work will be expanded to include further systems across the council.
- 2.7 Records Management project**
- 2.7.1 The Simplifying Records Management workstream, which is designing an approach to managing digital records across their lifecycle, produced an initial report in January 2024. This research contributed to the case for improved M365 licences.
- 2.7.2 The Information Asset Register (IAR) and ownership approach was modified following service design research. The IAR is being populated by rolling out a Microsoft Form to service managers, after first meeting with senior managers to gain support. Information Asset Owner live training sessions and self-directed learning content is being developed.
- 2.7.3 Backlog paper records transfers have been physically processed and are available for request from the Records Management Unit (RMU). Project resource is now focused on storage areas not in the control of Records

Management, such as clearing ex-district council records from the G3 warehouse on the Marabout Industrial Estate.

- 2.7.4 The Children's retention schedule was reviewed, expanded and has new owners assigned.
- 2.7.5 For destructions, a new process was established to guide Information Asset Owners to approve disposal at the policy level rather than file-by-file. This is a risk-based approach to resolving the still-large destructions backlog and was endorsed by the SIRO. Currently transfers and destructions data remains on workaround spreadsheets. To improve the Self-Service Portal system tracking paper records, a service designer proposed requirements and this is awaiting ICT resource to implement.
- 2.8 All organisations that have access to NHS patient data and systems must annually complete the NHS Data Security and Protection toolkit to provide assurance that they are practising good data security and that personal information is handled correctly. A failure to meet the requirements of the toolkit could compromise the Council's ability to access NHS data, which is pivotal to service delivery. The toolkit was satisfactorily completed in June 2024, but recognised that the Council was not meeting the mandatory requirements on data protection and cyber security training. As a result, the Council is subject to an action plan to improve compliance rates on mandatory training. The 2024 return was submitted 28 June 2024, noting an improvement in training rates but remaining below the 95% compliance rate. The risks associated with non-compliance with the toolkit are equally applicable to the Public Services Network and other ICT assurance frameworks.
- 2.9 A new "[Use of Covert Surveillance](#)" policy was approved in January 2024, to meet the requirements of Regulation of Investigatory Power Act (RIPA) and associated surveillance legislation. This extended the policy to include those occasions where covert surveillance is necessary, but not meeting the RIPA threshold. The policy sets out that the Audit and Committee will be informed annually on the following covert surveillance activity:
- The number of RIPA authorisations requested and granted – None during 2023/24;
  - The number of RIPA light authorisations requested and granted – One instance in 2023/24, where covert surveillance was adopted for a fraud investigation;

- The number of times social networking sites have been viewed in an investigatory capacity - No RIPA authorisations or RIPA light authorisations were requested or granted for surveillance of social networking sites

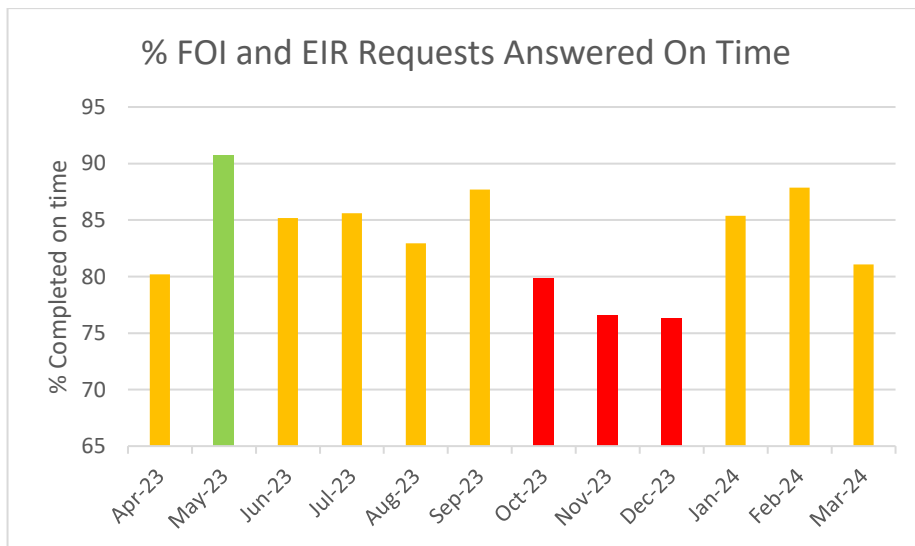
### 3 Performance and Risk

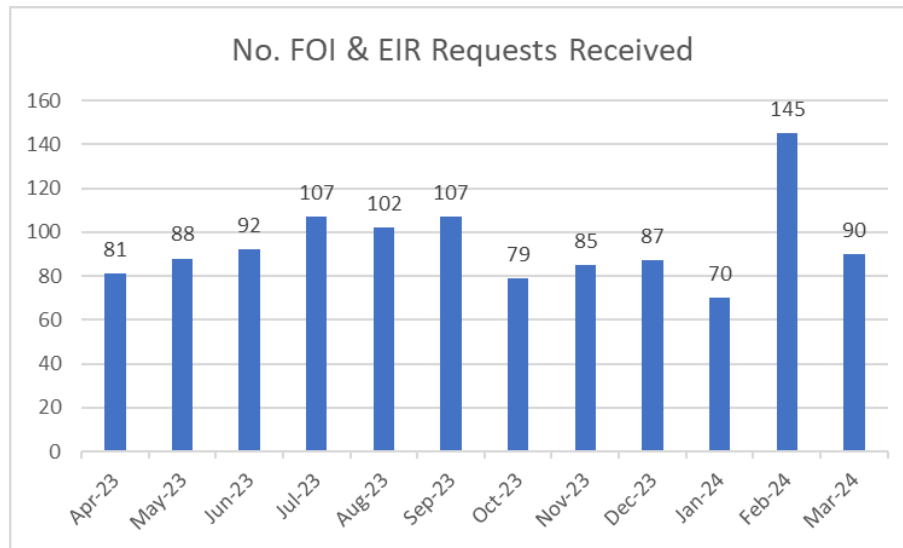
3.1 A range of performance indicators are monitored in respect of the Council’s information compliance arrangements. These are not replicated in full here, but top level “whole Council” figures have been included.

#### 3.2 Public and Environmental Information Requests

3.2.1 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. During 2023/24, the Council received 1,358 requests – approx. 113 per month.

3.2.2 The Information Commissioners Office anticipates 90% compliance with the statutory response timescales of 20 working days. Whilst this was met in only one month during 2023/24, compliance exceeded 85% in six of the twelve months. Compliance dropped below 80% for the three months October to December 2023. With Freedom of Information request numbers on the increase, there is pressure on both the Information Compliance Team and responding services. As part of effort to manage this increase, the Council is currently exploring automation for some elements of the process.





### 3.3 Requests Relating to Personal Information

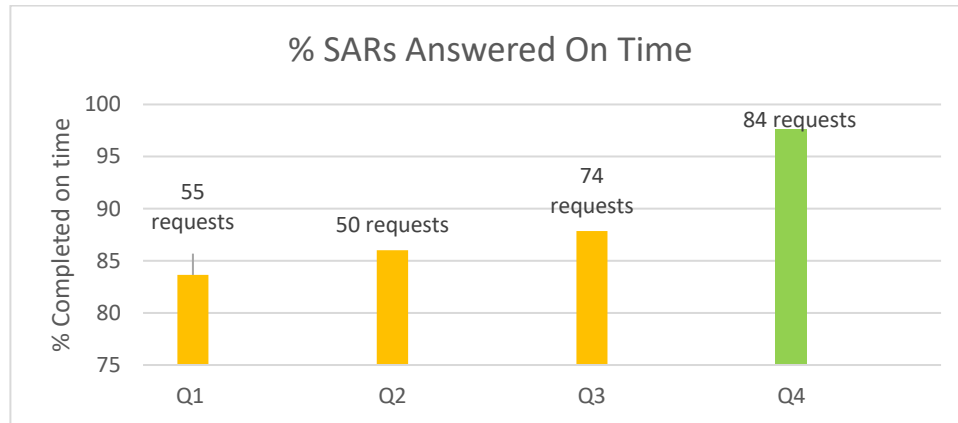
3.3.1 Individual Rights allows data subjects to enact certain powers over their personal information that is held. The most common and well known of these rights is the right of access, commonly referred to as subject access or subject access requests (SARs). This gives individuals the right to obtain a copy of their personal data held by an organisation, as set out in the General Data Protection Regulations. During 2023/24 the Council received 343 SARs. Of these, 266 became active, approx. 22 per month. Of these, 63% related to Childrens Services. Children’s Services requests (and in particular those requested by care leavers) involve highly sensitive and significant case files that require careful review and redaction. Since GDPR legislation became law in 2018, requests have increased at a rate of approximately 24% year on year, but this trend has recently plateaued.

3.3.2 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 SARs team were integrated into the Information Compliance team (tasked with completing all Children’s Services requests). Compliance was above 85% in three of the quarters and achieved 98% in quarter four. This is a significant achievement, as the complexity level of SARs has increased, with approx. 51% of request being deemed as ‘complex’ in nature and an extension being justified.

3.3.3 The improvement in performance has been achieved through an effective and efficient two stage review process, increased knowledge within the SAR team, and outsourcing of redactions where caseloads exceed

capacity. A business case has been approved to increase the internal SAR team by a further 0.5fte, to reduce outsourcing costs, and improve flexibility / resilience. Recruitment is underway for this post.

- 3.3.4 With this being said, requests that are deemed as ‘very complex’ and require the full two-month extension (for example the care leaver requests) are generally onerous to redact, and therefore exceeding 90% compliance for these requests will remain a challenge.



### 3.4 Data Breaches

- 3.4.1 A data breach can be classed as any incident where personal data is incorrectly accessed, disclosed, amended, destroyed or lost. If the breach is likely to result in a risk to the rights and freedoms of individuals, the incident must be reported to the Information Commissioner’s Office (ICO), who will consider the incident, including the adequacy of the council’s response. In response, the ICO may make recommendations to the council aimed at mitigating the breach or preventing further occurrences. In the most serious cases, the ICO may take enforcement action against the council, including issuing a monetary penalty. Where the ICO have historically taken enforcement action against local authorities, they have on occasion levied significant 6-figure sums for personal data breaches, and in the most serious cases they have power to fine a local authority up to £17.5 million.

- 3.4.2 The 2023/24 financial year saw an increase in the number of breaches internally reported by council services. There were 295 incidents reported in 2022, which increased to 376 in 2023. Twenty of these incidents were determined by the Data Protection Officer to meet the criteria for escalation to the ICO. There has been no enforcement action by the ICO, but on a number of occasions recommendations have been made and

actions mandated. The causes of data breaches during 2023/24 are summarised below:

Incident Category	Frequency in 2023/24	% of recorded incidents
Email	271	73%
Post	27	7%
Failure to redact	14	4%
Unauthorised internal access	11	3%
Lost	10	3%
Telephone	9	2%
Other	31	8%

3.4.3 As can be seen from the figures above, 73% of breaches relate to the use of email. 70% of the email breaches relate to an incorrect email address being used; 16% relate to the wrong attachment being included; and 12% relates to inclusion of too many recipients. Email security is already a core part of the council's mandatory data protection and cyber security training for all staff. With recent changes to the Council's licencing arrangement with Microsoft, we plan to explore and introduce additional technological capabilities to help reduce the frequency and severity of email and other technology related data breaches. A working group is determining roll out priorities at this point in time, liaising with the Data Protection Officer as appropriate.

3.4.4 The Organisational Compliance and Risk Learning Group has been operating since the beginning of 2023/24. The role of this group is developing, but it includes cross-Directorate challenge to the more serious breaches, to ensure that appropriate whole council learning can be identified and improved control mechanisms established. This group now reviews all data breach incidents that are reported to the ICO.

### 3.5 **Mandatory Data Protection and Cyber Training**

3.5.1 Officers and members are required to undertake mandatory training for both data protection and cyber. Both are delivered primarily via e-learning, with data protection training completed annually, whereas cyber security training is delivered in bite-size chunks. Training on both areas is incorporated into the elected member induction programme, post elections.

- 3.5.2 Data protection compliance training has improved in the last twelve months, and currently sits at approx. 84%, but is still significantly short of the target 95%. The compliance levels for Cyber Security training are slightly lower, at 73%.
- 3.5.3 The Operational Information Governance Group has initiated a task and finish group to develop both a training matrix for higher risk role training needs and to further improve/refresh content.
- 3.6 The Council's risk register identifies 18 risks with an information governance focus, five of which are identified as "High" or "Very High" as set out in the table below:

<b>Risk</b>	<b>Risk Ranking</b>	<b>Management Response</b>	<b>Risk Owner</b>
213 - Failure to demonstrate evidence to support the NHS Digital Toolkit results in a lack of access to NHS data and systems	High	Satisfactory approval of the NHS toolkit is essential, for continued access to health data sets. The 24/25 return notes that data protection and cyber training is below the 95% compliance rate expected (currently circa 70-85%) and an improvement action plan has been initiated. Improving compliance rates and roll out of the training matrix are priorities for the training task and finish group.	Service Manager for Assurance
286 - Loss of ICT service or data through a cyber-attack	Very High	By very nature, the impacts of cyber risk will always remain high and, despite the significant controls in place, remains possible. A number of local authorities have experienced cyber attacks that have had a severe impact on service delivery.	Head of ICT Operations

Risk	Risk Ranking	Management Response	Risk Owner
		<p>Ongoing focus is on vulnerability management. In simple terms, this is a continuous, proactive process that helps keep computer systems, networks, and enterprise applications safe from cyberattacks and data breaches. It involves identifying, assessing, and addressing potential security weaknesses to prevent attacks and minimise damage. The goal is to reduce overall risk exposure by mitigating as many vulnerabilities as possible. The implementation of vulnerability management technologies has led to an impressive 82% reduction in technical vulnerabilities on devices since introduction. This indicates that these technologies are effective in enhancing security.</p> <p>The council's identity management system, which includes multifactor authentication, conditional access, and account permissions, has undergone a review. With the support of specialist technology, a significant number of vulnerabilities have been removed from the Council's systems.</p>	



Risk	Risk Ranking	Management Response	Risk Owner
348 - There is a business continuity risk from delayed ICT recovery after a disruption such as a power failure.	Very High	An ICT service continuity exercise is currently being scoped. We are moving away from controlled power downs and prioritising core services and recovery testing.	Head of ICT Operations
388 - Insufficient uptake of data protection training and inadequate awareness of statutory obligations	High	The mandatory data protection e-learning module was revised in early 2021. Compliance levels are currently circa 84% for staff. The e-learning has now been rolled out to elected members, to top up the data protection training received by members as part of induction. A training matrix has been established to identify any posts requiring more/less than the "benchmark" e-learning module. A training task and finish group has been established, working to the Operational Information Governance Group, with a focus on gaps in training, compliance and ensuring training fits job role/risk	Service Manager for Assurance
321 - Unable to sustain	High	There are significant pressures on the information compliance team, with an increase in	Service Manager for Assurance

Risk	Risk Ranking	Management Response	Risk Owner
<p>Assurance service due to prolonged pressures (increasing caseloads etc), changing legislative demands and gaps in staff capacity</p>		<p>reported data breach cases and Freedom of Information, increasing complexity of Subject Access Requests and service demands for data protection support.</p> <p>Transformation work is impacting significantly on the demands of the Data Protection Officer. The Information Commissioners Office's Accountability Framework has been completed and identified a number of gaps in DC's arrangements, which will be resource hungry to resolve.</p> <p>A review of caseloads is currently underway, and automation is being explored to assist with rising Freedom of Information requests. Future resource needs are being assessed.</p>	

#### 4 Focus for 2024/25 – The ICO Accountability Framework

- 4.1 The Government has proposed reform changes to the existing data protection legislation. The key focus is around reducing barriers to responsible innovation and mitigating the burdens on organisations whilst continuing to improve outcomes for people. These changes are not envisaged to significantly reduce impacts on public sector organisations, who by very nature of their statutory functions would be deemed to be carrying out high risk processing of personal data.

4.2 The ICO has established an [Accountability Framework](#) toolkit that enables organisations to self assess the extent that current policies and processes meet their expectations. Whilst noting that the changing legislative framework may alter some of the ICO's expectations in the long term, the Operational Information Governance Group is in the process of completing this self assessment. It is envisaged that this will provide a prioritised and risk based work programme for the SIGB and its working groups, and can be monitored alongside other information related compliance frameworks, such as the NHS Data Security and Protection Toolkit. 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

4.3 The self assessment for Dorset Council is summarised within the graph below. Where noted as "blank", this recognises that the self assessment has not yet been completed:

### Breakdown of 'Current status' of all categories



Fig1 – Proportion of assessment criteria where Dorset Council meets ICO expectations

### Breakdown of 'Current Status' per category

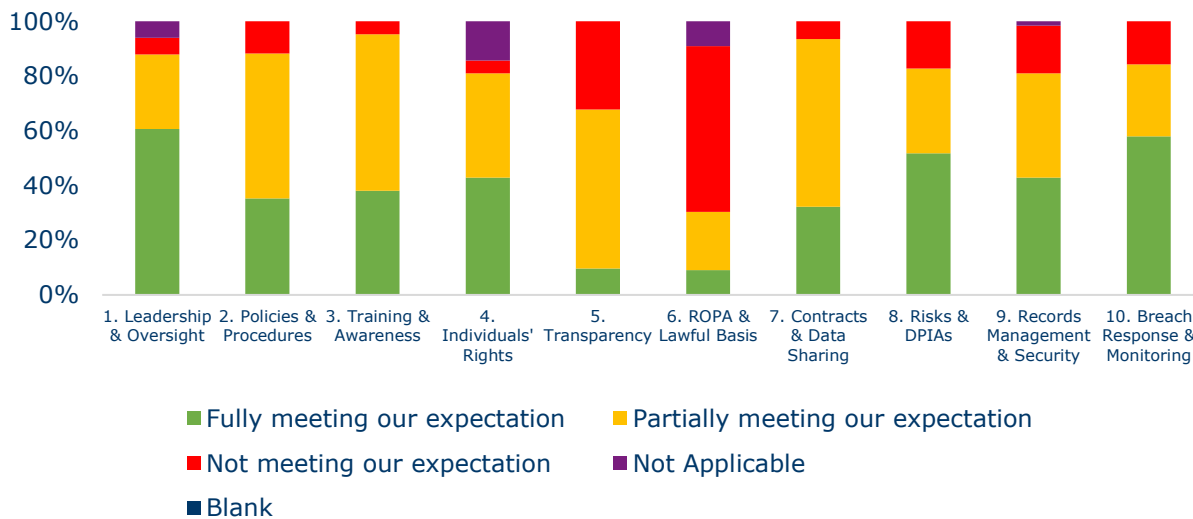


Fig 2 – Proportion of assessment criteria where Dorset Council meets ICO expectations, per category.

4.4 The self assessment identifies that the Council is not fully meeting the ICO's expectations for over 50% of the criteria. In general, the Council scores higher for physical controls, but less well in terms of the application and embeddedness of processes necessary to support strong information governance practices. The Operational Information Governance Group has developed a risk based prioritised action plan for adoption by the SIGB, which is set out in Appendix A. However it is recognised that this is

a challenging agenda, which is likely to determine additional resourcing needs. Delivery is likely to sit with a small number of professional officers, such as that of the Data Protection Officer, the Cyber Security and ICT Continuity Lead, and the Data and Information Manager, which may present resourcing implications to deliver improvement within acceptable timescales. Particular findings are noted below.

- 4.5 **Leadership and Oversight** – The set up of the Strategic Information Governance Board and its associated operational groups provide a positive framework for information governance, with clearly defined roles and escalation to SLT. There are resource shortfalls for what is a challenging agenda to fully meet ICO expectations. **Key actions for 2024/25** – Development of a resourcing plan, for consideration by Strategic Information Governance Board.
- 4.6 **Policies and Procedures** – A set of policies were established for Day One of Dorset Council and a number of these have not yet been reviewed and updated to ensure that they remain fit for purpose. **Key actions for 2024/25** – Development of Data Sharing Agreement and AI policies; develop prioritised workplan for wider policy reviews, including identification of gaps in existing policy framework, as part of the Data Governance project.
- 4.7 **Training and Awareness** – Data protection and cyber security training are mandatory for all staff and councillors. However compliance rates are not currently at the required level. Work is underway to develop a training matrix to determine higher risk staff roles that should be subject to a more “job specific” training. **Key actions for 2024/25** – Finalise and rollout training matrix and update on training modules.
- 4.8 **Individual Rights** - This relates to an individual’s right to access to information about them, the right to rectification, erasure and restriction of processing. Good progress has been made in improving compliance rates for subject access requests.
- 4.9 **Transparency** - This category covers the content and effectiveness of privacy notices – a requirement under UK GDPR setting out how a person’s information is held and used. The combined Information Asset Register and Record of Processing Activities (ROPA) is in the process of rollout, and will be a foundation for information privacy review. **Key actions for 2024/25** – Roll out of Information Asset Register, including

- training programme for Information Asset Owners; enable process for review and update across services.
- 4.10 **Records of Processing and Lawful Basis** – The combined Information Asset Register and ROPA is in the process of rolling out, and a training programme is in place to support Information Asset Owners to submit and manage entries to the register. **Key actions for 2024/25** – Roll out of Information Asset Register, including training programme for Information Asset Owners.
- 4.11 **Contracts and Data Sharing** – A SWAP audit released in April 2023 found that the Council does not currently have a data sharing policy or framework, and that there is limited oversight. Information will be gathered about current data sharing agreements as part of the Data Governance Project and linked to the Information Asset Register. **Key actions for 2024/25** – Identification and logging of data sharing agreements; development of data sharing policy; development of third party supply chain risk management framework.
- 4.12 **Risks and Data Protection Impact Assessments (DPIA)** – “Data protection by design and default” is a key element of ensuring that service delivery change reflects a review of data protection implications. The Council has a process for impact assessments, but is currently being enhanced. The transformation programme incorporates the requirement for DPIAs. DPIAs are reviewed and signed off by the Operational Information Governance Group, but this does put a strain on other key items in the action plan. **Key actions for 2024/25** – Finalise revised DPIA policy.
- 4.13 **Records Management and Security** – This category examines how we manage and secure both paper and digital information. The Simplifying Records Management workstream will design how best to respond to the gaps identified in digital records management. The benefits of good records management are savings in digital storage and greater efficiency for officers' day-to-day work. **Key actions for 2024/25** – Records Management Project: improving our paper records tracking system, identifying uncontrolled paper records and arranging transfer into RMU, taking a resource request to Children's Services to resolve indexing and retention issues, producing user guidance and best practice recommendations on M365 storage and migrating from shared drives; collaborating on processes to maintain and review the IAR; review of the Acceptable Use policy; rollout of cyber business continuity exercises.

- 4.14 **Breach Response and Management** – There are clear processes for managing breaches. The Organisational Compliance and Risk Learning Group is assessing the most significant breaches. **Key actions for 2024/25** – Implement improved lessons learnt process within Directorates, including lines of accountability; develop risk based information governance audit plan.

## 5 **Financial Implications**

There are no direct financial implications from this report. However, the General Data Protection Regulations set out that the Data Protection Officer must be provided with sufficient resources to perform their role. The ongoing work of the Strategic Information Governance Board may identify areas where additional resourcing is required.

## 6 **Natural Environment, Climate & Ecology Implications**

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

## 7 **Well-being and Health Implications**

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

## 8 **Other Implications**

None

## 9 **Risk Assessment**

- 9.1 **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 the five high risks specified in section 3.6 of the report. In particular, there are challenging resourcing demands in implementing the action plan at Appendix A.

## 10 **Equalities Impact Assessment**

Information Governance policies have been subject to Equalities Impact Assessments

11 **Appendices**

None

12 **Background Papers**

None

13 **Report Sign Off**

- 13.1 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).



<b>Appendix A – Information Governance Action Plan</b>							
<b>Ref</b>	<b>Identified action</b>	<b>ICO Framework Category</b>	<b>By Whom / Sub Group</b>	<b>Risk based priority</b>	<b>Resourcing Requirements</b>	<b>Target Timescale</b>	<b>Latest Status</b>
1a	Develop an Information Governance resourcing plan	Leadership and Oversight	Operational	High	SM for Assurance / DPO	Priority 1	
1b	Review intranet guidance and / or develop SharePoint Hub	Leadership and Oversight	Operational	Medium	DPO	Priority 2	
1c	SIGB to review effectiveness of existing operational sub groups	Leadership and Oversight	SIGB	Medium	SIGB and Chairs	Priority 2	
2a	Develop schedule of policies and prioritised review dates, integrating into corporate template	Policies and Procedures	Operational	High	SM for Assurance / DPO / ICT Cyber Security Lead	Priority 1	Schedule completed
2b	Refresh policy framework regarding processing of special category/criminal offence data	Policies and Procedures	Operational	Medium	DPO	Priority 2	
2c	Develop Power BI policy	Policies and Procedures	Operational	High	SM for Business Intelligence	Priority 1	
2d	Review overarching Data Protection policy	Policies and Procedures	Operational	Medium	DPO	Priority 2	
3a	Develop and roll out Information Governance training matrix	Training and Awareness	Operational	Medium	SM for Assurance	Priority 1	Training sub group established and criteria for matrix identified. Rolling out to Directorates for data gathering
3b	Determine mechanisms for delivery of training for high risk roles / service areas (following completion of training matrix)	Training and Awareness	Operational	Medium	DPO / ICT Cyber Security Lead	Priority 3	
3c	Develop communications plan with corporate communications	Training and Awareness	Operational	Medium	SM for Assurance / DPO	Priority 2	

	team, with periodic IG reminders						
3d	Development and delivery of induction training for elected members of data protection / cyber security	Training and Awareness	Operational / Cyber Security	High	DPO / Cyber Security Lead	Priority 1	Built into the May inductions
3e	Review content of existing information governance training modules	Training and Awareness	Operational	Medium	DPO	Priority 3	
3f	Roll out RIPA / Covert Surveillance training	Training and Awareness	Operational	High	SM for Assurance / DPO	Priority 1	The training has not yet been delivered to support the approved Covert Surveillance policy
4a	Strengthen processes to support individual requests for data erasure, with appropriate audit regime, in accordance with article 17	Individuals Rights 4.7.4	Operational	Low	DPO	Priority 4	
4b	Review and update Individuals Rights policy	Individuals Rights	Operational	Low	DPO	Priority 4	
5a	Review public schedule of privacy notices, identifying purposes of the processing and legal basis and ensure process for review and update	Transparency 5.1	Operational	Low	DPO	Priority 4	
5b	Incorporate privacy information into the mandatory data protection training	Transparency 5.5	Operational	Low	DPO	Priority 3	
6a	Roll out of Information Asset Register	ROPA and Lawful Basis	Operational	High	Information Management /	Priority 1	Roll out has begun, but is phased. Due to be completed end 2024.

					DPO; input from all services		
7a	Develop Data Sharing policy, with Information Asset Register providing mechanism for logging agreements and identifying gaps	Contracts and Data Sharing 7.1	Operational	High	DPO	Priority 1	Drafted pending consultation and sign off by Strategic Information Governance Board in Sept 24
7b	Development of third party supply chain risk management framework	Contracts and Data Sharing 7.4	Operational	Medium	DPO	Priority 3	
8a	Reflect information risk into the overarching Data Protection policy, linked to Information Asset Register work	Risks and DPIAs	Operational	Low	DPO / Information Management	Priority 4	
8b	Finalise and roll out revised Data Protection Impact Assessment guidance, with centralised log	Risk and DPIAs	Operational	High	DPO	Priority 2	
8c	Develop DPIA training process	Risk and DPIAs	Operational	Medium	DPO	Priority 3	
8d	Support Our Future Council transformation programme with information governance input	Risk and DPIAs	Operational	High	DPO / OIGG	Priority 1	Ongoing support
9a	Workstream to design digital records' procedures (Simplifying Records Management)	Records management and security	RM Project	High	Information Management / User Adoption	Priority 1	Current RM Project workstream is to design / deliver user guidance and best practice recommendations, and design the approach to migrating data, which is not currently resourced

9b	Improve Self-Service Portal, the paper records tracking system for the Records Management Unit	Records management and security	RM Project	High	ICT / Information Management	Priority 3	Awaiting ICT development resource
9c	Implement a data quality policy and supporting processes	Records management and security	Org Compliance & Risk Learning	Medium	SM for BI	Priority 3	
9d	Revise Acceptable Use policy	Records management and security	Operational	High	ICT Cyber Security Lead	Priority 1	In progress
9e	Revise Access Control policy	Records management and security	Operational	High	ICT Cyber Security Lead	Priority 1	Identified within 2023 SWAP audit on Data Quality and Information Governance
9f	Establish working group to look at the risks associated with WhatsApp and other similar social media messaging facilities	Records management and security	Operational	Medium	SM for Assurance / DPO and working group	Priority 2	
9g	Implement process of clear desk checks	Records management and security	Org Compliance & Risk Learning	Low	SM for BI / DPO	Priority 4	
9h	Refresh of business continuity plans, with transfer of action cards to MS Teams, and focus on data loss	Records management and security	Operational	Medium	SM for Assurance / Emergency Planning	Priority 1	Transfer to MS Teams complete. Gradual engagement across DC services
9i	Roll out of Cyber business continuity exercises	Records management and security	Operational	Medium	Emergency Planning	Priority 1	Exercise developed and rolled out

9j	Develop AI policy	Records management and security	Operational	High	ICT Cyber Security Lead / DPO	Priority 1	
10a	Strengthen data breach recording mechanisms and risk assessment tool	Breach Response and Monitoring	Operational	Medium	DPO / Asst DPO	Priority 1	Process agreed in principle
10b	Strengthen the lessons learnt process and ownership within service areas for low level breaches (ie those not considered by Risk and Learning Group)	Breach Response and Monitoring	Org Compliance & Risk Learning	Medium	DPO	Priority 2	
10c	Develop audit plan for information governance compliance audits and reporting process	Breach Response and Monitoring	Org Compliance & Risk Learning	Medium	SM for BI / DPO	Priority 3	
10d	Review and improve range of Information Governance KPIs	Breach Response and Monitoring	Operational	Medium	SM for Assurance / DPO	Priority 1	Effective wef May 24
10e	Work with ICT colleagues in the roll out of E5 to explore mechanisms to reduce data breaches and cyber exposures	Breach Response and Monitoring	Operational	High	DPO / ICT Cyber Security Lead	Priority 1	Agreed set up of M365 working group. Revised sensitivity labels agreed, subject to sign off
10f	Develop formal process for recording and tracking actions resulting from data / cyber breaches	Breach Response and Monitoring	Org Compliance & Risk Learning	Medium	SM for BI / DPO	Priority 2	
10g	Review and update Data Breach policy	Breach Response and Monitoring	Operational	Medium	DPO	Priority 2	



## Audit and Governance Committee

22 July 2024

## Risk Management Update

### For Review and Consultation

**Cabinet Member and Portfolio:**

Cllr N Ireland, Leader of the Council

**Executive Director:**

A Dunn, Executive Director, Corporate Development

Report Author: Chris Swain

Job Title: Risk Management & Reporting Officer

Tel: 01305 228691

Email: [chris.swain@dorsetcouncil.gov.uk](mailto:chris.swain@dorsetcouncil.gov.uk)

**Report Status:** Public

**Brief Summary:** The continual development and promotion of risk management is integral to strong performance, business continuity, compliance and delivering strong outcomes for the residents of Dorset. Strong risk management with a clear understanding and governance of strategic and operational risks will ensure that Dorset Council remains well placed to demonstrate that objective and informed decisions are being taken. The senior leadership team (SLT) owns strategic risk management, with an agreed risk management framework and policy statement both of which set out the council's commitment. The focus of this report is to provide an overview of the highest-level risks identified within the service risk registers, as well as provide an overview of the processes and work that has been implemented within the last 6 months to drive enhancements in risk management processes.

**Recommendation:** The Audit and Governance Committee note the key risks identified in the risk registers, with escalation to scrutiny committees where appropriate.

**Reason for Recommendation:** To ensure that the council's risk management methodologies remain current, proportionate, and effective in enabling informed decisions based on identified risks to be made.

1. **Report**

1.1 A PowerBI dashboard has been developed by colleagues within the Business Intelligence & Performance team that helps to present risks in a way that is more accessible, with information surrounding risk management across directorates and teams. This dashboard supports the wider governance of risk that is being embedded to capture actions and mitigations from both strategic and operational risks.

1.2 There are ten strategic risk themes informed by operational service level risks owned by heads of service and service managers. These are as follows:

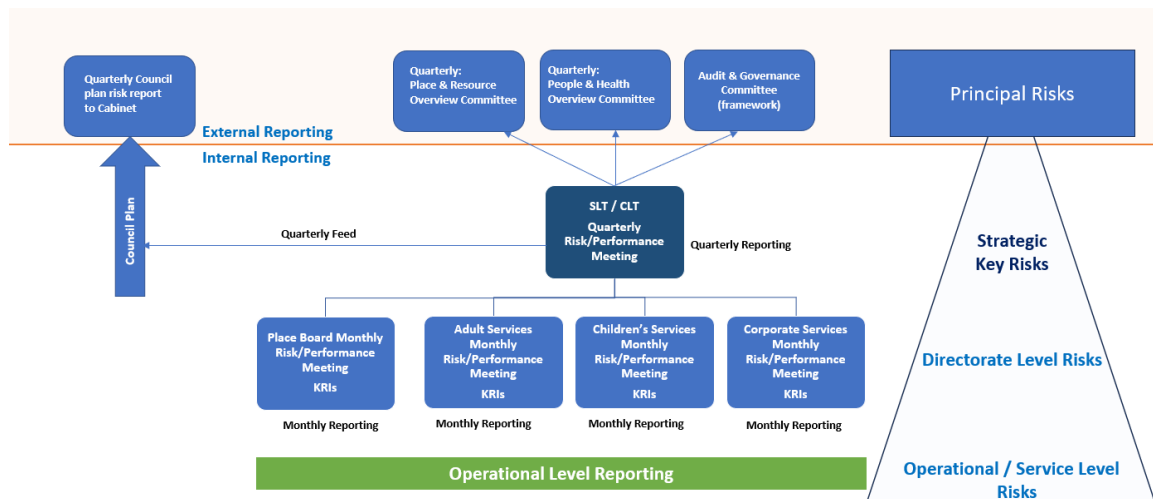
<b>Current Risk Themes</b>	
Communities	Political & Leadership
Compliance	Safeguarding
Digital & Technology	Service Delivery
Finance	Transformation
Health, Safety & Wellbeing	Workforce

1.3 Councillors can view the full schedule of risks by theme from the Risk Register.

1.4 Both the People and Health Scrutiny Committee and Place and Resources Scrutiny Committee consider the detail of individual risks. The role of Audit and Governance Committee is to satisfy itself over the adequacy of the risk management framework.

1.5 The Risk Management & Reporting Officer with assistance from colleagues in Business Intelligence & Performance and The Council Plan Process Working Group are developing a refreshed hierarchy for risk as outlined in the diagram below. Work in this area will be finalised as the new Council Plan is developed.





- 1.6 The service risk register has been improved, with a streamlined approach focussing on controls to manage risks and subsequent actions to be taken in their future management.
- 1.7 Feedback on terminology has resulted in risks previously identified as “Extreme” changing to “Very High”. It is considered that “Very High” is less inflammatory and in greater keeping with the context in which Dorset Council operates. “Very High” risks are the most significant for the authority and the same scoring mechanism is used to arrive at a “Very High” risk rating that was previously used to determine a risk rating of “Extreme”.
- 1.8 The Risk Management & Reporting Officer with support of colleagues in Business Intelligence & Performance and sponsored by the Corporate Director for Place Services, have delivered training to all risk owners in the Place Directorate in pilot format to review all their risks. The objective is to comprehensively review all risks to ensure they are articulated correctly, providing clarity on risk events, their associated controls and future mitigation plans. The intention is to deliver a similar exercise to other directorates in due course once the Place Directorate pilot has drawn to a close.
- 1.9 Following feedback from Simon Roach (Co-Opted Member of the Audit and Governance committee) at the Audit & Governance Committee held on the 15 April 2024, a review of the council’s Very High risks by risk owners has been undertaken out of cycle to ensure the information contained is fit for purpose and in keeping with the new focus on risk controls. A concerted effort has also been made to increase the level of

compliance in those risks with a rating of High, with an enhanced focus on how the processes can have stronger governance and supporting processes.

- 1.10 During the last 6 months improvements have been made to the level of compliance in risk register updates, which currently stands at 92.29% at the time of writing, in comparison to only 41% when presented to this committee on the 15 January 2024. Additionally, there has been significant work across the council on consistency of language, review and where needed rationalisation of risks, and a much stronger demarcation and focus on strategic and operational risks. SLT also have quarterly oversight of Very High and High and worsening risks as part of their wider performance reporting cycle.

**2. Financial Implications**

No budget implications specifically, although unmanaged risks may pose a threat to the council's financial stability. Identified risk improvement measures may also have direct budget implications, each of which need to be subject to a cost/benefit analysis prior to implementation.

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

None specifically, however the risk register itself identifies several climate related risks.

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

Health, safety, and wellbeing is identified as one of our corporate risk themes.

**5. Other Implications**

None.

**6. Risk Assessment**

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

Current Risk: N/A

Residual Risk: N/A

This is a report detailing the risks faced by Dorset Council and therefore does not have a rating to consider relating to a decision. Appendix A

provides an update on those Very High risks which are currently identified within the Council's risk register, which would have a high level of risk impact attached to them including business continuity, reputational and financial.

7. **Equalities Impact Assessment**

None specifically, however the risk register itself identifies several equality related risks.

8. **Appendices**

Appendix A - Summary of Very High Risks

9. **Background Papers**

None.

10. **Report Sign Off**

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)

# Audit and Governance Committee

**22 July 2024**



Risk Management Exception - Quarterly Update Report

**Very High Risks**

As at 27 June 2024

<b>Impact</b>	Catastrophic	5	10	15	20	25
	Major	4	8	12	16	20
	Moderate	3	6	9	12	15
	Slight	2	4	6	8	10
	Limited	1	2	3	4	5
		Very Unlikely	Unlikely	Possible	Likely	Certain
		<b>Likelihood</b>				

<b>Assessing Likelihood</b>		
In assessing likelihood, the following 1 to 5 scoring system is to be followed:		
<b>Likelihood</b>	<b>Certain</b> Score 5	Reasonable to expect that the event <b>WILL</b> happen, reoccur, possibly or frequently.
	<b>Likely</b> Score 4	Event is <b>MORE THAN LIKELY</b> to occur. Will probably happen or reoccur but is not a persisting issue.
	<b>Possible</b> Score 3	<b>LITTLE LIKELIHOOD</b> of event occurring. It might happen or reoccur occasionally.
	<b>Unlikely</b> Score 2	Event <b>NOT EXPECTED</b> . Do not expect it to happen or reoccur, but it is possible that it might do so.
	<b>Very Unlikely</b> Score 1	<b>EXCEPTIONAL EVENT</b> . This will probably never happen or reoccur.

<b>Assessing Impact</b>		
In assessing impact, the following 1 to 5 scoring system is to be followed:		
<b>Impact</b>	<b>Catastrophic</b> Score 5	<b>Multiple deaths</b> of employees or those in the Council's care. <b>Inability to function</b> effectively, Council-wide. Will lead to <b>resignation of Chief Executive</b> and/or Leader. Corporate Manslaughter charges. Service delivery must be <b>taken over by Central Government</b> . <b>Front page news story</b> in National Press. Financial <b>loss over £10m</b> .
	<b>Major</b> Score 4	<b>Suspicious death</b> in Council's care. <b>Major disruption</b> to Council's critical services for more than 48 hours. Noticeable <b>impact achieving strategic objectives</b> . Will lead to <b>resignation of Senior Officers</b> and/or Cabinet Member. <b>Adverse coverage</b> in National press/Front Page news locally. Financial <b>loss £5m-£10m</b> .
	<b>Moderate</b> Score 3	<b>Serious injury</b> to employees or those in the Council's care. <b>Disruption to one critical Council service</b> for more than 48 hours. Will lead to <b>resignation of Head of Service / Project Manager</b> . Adverse Coverage in <b>local press</b> . Financial <b>loss £1m-£5m</b> .
	<b>Slight</b> Score 2	<b>Minor injury</b> to employees or those in the Council's care. <b>Manageable disruption</b> to services. <b>Disciplinary action</b> against employee. Financial <b>loss £100k-£1m</b> .
	<b>Limited</b> Score 1	<b>Day-to-day operational problems</b> . Financial <b>loss less than £100k</b> .

## Overall Risk Summary – 27 June 2024

		Likelihood					Overall Compliance <b>92.29%</b>	Total Risks <b>415</b>
		Very unlikely	Unlikely	Possible	Likely	Certain		
Impact	Catastrophic	1	5	6	3	0	Very High / High Compliance <b>79.66%</b>	Overdue <b>32 (7.71%)</b>
	Major	4	47	16	19	0		
	Moderate	14	60	99	14	1		
	Slight	4	83	24	8	1		
	Limited	2	2	1	1	0		

### Adults and Housing

		Likelihood					Overall Compliance <b>90.70%</b>	Total Risks <b>43</b>
		Very unlikely	Unlikely	Possible	Likely	Certain		
Impact	Catastrophic	0	0	0	0	0	Very High / High Compliance <b>100%</b>	Overdue <b>4 (9.30%)</b>
	Major	0	0	0	2	0		
	Moderate	2	9	13	2	0		
	Slight	1	9	2	3	0		
	Limited	0	0	0	0	0		

**Adults and Housing - Very High: None**

## Childrens Services

	Likelihood					Overall Compliance <b>100%</b>	Total Risks <b>26</b>	
	Very unlikely	Unlikely	Possible	Likely	Certain			
Impact	Catastrophic	0	1	0	1	0	Very High / High Compliance <b>100%</b>	Overdue <b>0</b> <b>(0.00%)</b>
	Major	0	3	5	1	0		
	Moderate	0	2	3	1	0		
	Slight	0	4	2	2	0		
	Limited	0	1	0	0	0		

### Childrens Services - Very High:

1. Instability in the High Needs Block budget may create a increased deficit in the Dedicated Schools Grant (DSG) resulting in a deficit in Dorset Councils financial position.

## Corporate Development

	Likelihood					Overall Compliance <b>96.90%</b>	Total Risks <b>129</b>	
	Very unlikely	Unlikely	Possible	Likely	Certain			
Impact	Catastrophic	1	0	0	2	0	Very High / High Compliance <b>100%</b>	Overdue <b>4</b> <b>(3.10%)</b>
	Major	1	16	7	2	0		
	Moderate	0	12	30	2	0		
	Slight	1	43	8	1	0		
	Limited	2	1	0	0	0		

### Corporate Development - Very High:

1. A successful cyber-attack to IT systems causes loss of service or data.
2. There is a business continuity risk from delayed ICT recovery after a disruption such as a power failure.



## Place

		Likelihood					Overall Compliance <b>86.67%</b>	Total Risks <b>180</b>
		Very unlikely	Unlikely	Possible	Likely	Certain		
Impact	Catastrophic	0	4	6	0	0	Very High / High Compliance <b>55.56%</b>	Overdue <b>24 (13.33%)</b>
	Major	3	24	2	13	0		
	Moderate	10	32	41	5	1		
	Slight	2	25	8	1	1		
	Limited	0	0	1	1	0		

**Place - Very High:** None

## Public Health

		Likelihood					Overall Compliance <b>100%</b>	Total Risks <b>6</b>
		Very unlikely	Unlikely	Possible	Likely	Certain		
Impact	Catastrophic	0	0	0	0	0	Very High / High Compliance <b>100%</b>	Overdue <b>0 (0.00%)</b>
	Major	0	0	0	0	0		
	Moderate	0	0	1	1	0		
	Slight	0	0	3	1	0		
	Limited	0	0	0	0	0		

**Public Health – Very High:** None

This page is intentionally left blank

# Dorset Council

## Report of Internal Audit Activity

### Progress Report 2024/25 – July 2024

Page 67

Agenda Item 8

## Executive Summary

As part of our update reports, we will provide an ongoing opinion to support our end of year annual opinion.

We will also provide details of any significant risks that we have identified in our work, along with the progress of mitigating previously identified significant risks.

The contacts at SWAP in connection with this report are:

**Sally White** Assistant Director  
Tel: 07820312469  
[sally.white@swapaudit.co.uk](mailto:sally.white@swapaudit.co.uk)

**Angie Hooper** Principal Auditor  
Tel: 07536453271  
[angela.hooper@swapaudit.co.uk](mailto:angela.hooper@swapaudit.co.uk)

SWAP is an internal audit partnership covering 24 organisations. Dorset Council is a part-owner of SWAP, and we provide the internal audit service to the Council.

For further details see:  
<https://www.swapaudit.co.uk/>



### Audit Opinion, Significant Risks, and Audit Follow Up Work

#### **Audit Opinion:**

This is our first update report for 2024/25 financial year.

Our live Rolling Plan dashboard available through our audit management system AuditBoard [AuditBoard | Login \(auditboardapp.com\)](#), and specifically the Audit Coverage (*which can be found on the first tab of the dashboard or on page 3 below*), reflects the outcomes of recent reviews completed. Based on these recent reviews, we recognise that generally risks are well managed. We have identified some gaps, weaknesses and areas of non-compliance however, we have reasonable to high levels of confidence that the agreed actions will be implemented and as such are able to offer a **reasonable opinion**.

Since our last progress report in April 2024, we have not issued any **Limited** assurance opinions on the areas and activities we have been auditing.

In order to provide more up to date information, we have introduced an enhancement to the rolling plan dashboard where we will be including links to final one-page reports for Limited and No assurance audits from the Completed tab. We have also developed a SWAP Executive dashboard, available through AuditBoard and accessed in the same way as the Rolling Plan dashboard which provides more information on our audits. The dashboard provides a high level summary of our work that has been concluded. Additionally, it provides a visualisation and status of all priority 1 and 2 actions.

#### **Significant Corporate Risks**

##### **Update on Response to Climate Emergency**

In April, we reported that all actions that were due had been completed. The remaining one priority 1 and one priority 2 actions are not due until 30<sup>th</sup> April 2025, so we will undertake another formal follow up nearer that time to allow the actions to become embedded.

##### **Update on Premises related Health and Safety**

Two of the three remaining outstanding actions have been completed, with a revised due date of 31<sup>st</sup> December 2024 for the last action which is in progress. The Head of Assets and Property has acknowledged that

implementation of all actions has taken significantly longer than was originally anticipated and whilst there is still some progress to be made on implementing the last action, we believe that sufficient action has been taken by the service to mitigate the significant corporate risk. We will continue to monitor the implementation of the remaining action, but we will no longer be formally reporting this to the committee as a Significant Corporate Risk. Members will of course be able to monitor updates to that one remaining action through the Executive dashboard. The detailed follow up report can be found on page 8.

### **Follow Up of Agreed Audit Actions**

The numbers of overdue actions that we report will now include all priority 1's and 2's from all audits, rather than just those from Limited and No assurance opinion audits. We will also report the number of actions with revised due dates, where the original due date has passed and graphs for these can be found on page 5. There are 17 actions that have passed their original due date where a revised date has been agreed and 21 overdue actions where either the original date or the revised date has passed.

It is disappointing to see that the numbers of both overdue actions and those with revised timescales are high, but we are in contact with officers to ensure that actions are implemented in a timely way. Further details on outstanding actions can be found by viewing the Management Actions tab of the SWAP Executive dashboard which is stored in AuditBoard and can be viewed by clicking on this link [AuditBoard | Login \(auditboardapp.com\)](#)

Following the last Committee where a number of questions were raised around outstanding actions and high priority actions with revised due dates, we agreed with the outgoing Chair that we would provide more information around overdue actions, including those that have revised timescales applied to them. Appendix B on page 9 shows all actions where the original agreed deadline is over six months ago.

# Internal Audit Plan Progress 2024/25

Our audit plan coverage assessment is designed to provide an indication of whether we have provided sufficient, independent assurance to monitor the organisation’s risk profile effectively.

For those areas where no audit coverage is planned, assurance should be sought from other sources to provide a holistic picture of assurance against key risks.

Page 70



## SWAP Internal Audit Plan Coverage

The table below, captures our audit coverage, mapped against the Authority’s corporate risk themes since November 2022 when we started using our audit management system, AuditBoard. Furthermore, we have then overlaid the audit assurance outcomes of those risk areas that we have reviewed. As you will see we have provided some level of recent audit work across all of the corporate risk themes. It is possible on the dashboard to also view coverage of our recent audit work mapped by Corporate Priorities, Directorates, SWAP Top 10 Risk Themes, and Core Areas of Recommended Assurance. The audits that make up the coverage can be viewed by right clicking in the coverage cell, select drill through and audit details.

Strategic Risk	Coverage (Completed Audits)	Average Opinion of Completed Audits
DC R01 - Finance	Good	Reasonable
DC R02 - Compliance	Adequate	Reasonable
DC R03 - Health, Safety, Wellbeing	Adequate	Reasonable
DC R04 - Communities	Adequate	Reasonable
DC R05 - Digital & Technology	Some	Reasonable
DC R06 - Safeguarding	Some	Limited
DC R07 - Transformation	Some	Limited
DC R08 - Workforce	Some	Limited
DC R09 - Political & Leadership	Some	Limited
DC R10 - Service Delivery	Adequate	Limited

Coverage	Description
Good	Good audit coverage completed
Adequate	Adequate audit coverage completed
Some	Some aspects of audit coverage completed
In Progress	Some aspects of audit coverage in progress
None	No audit coverage to date

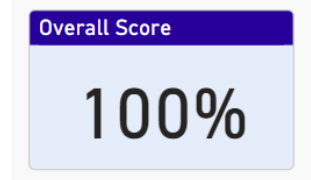
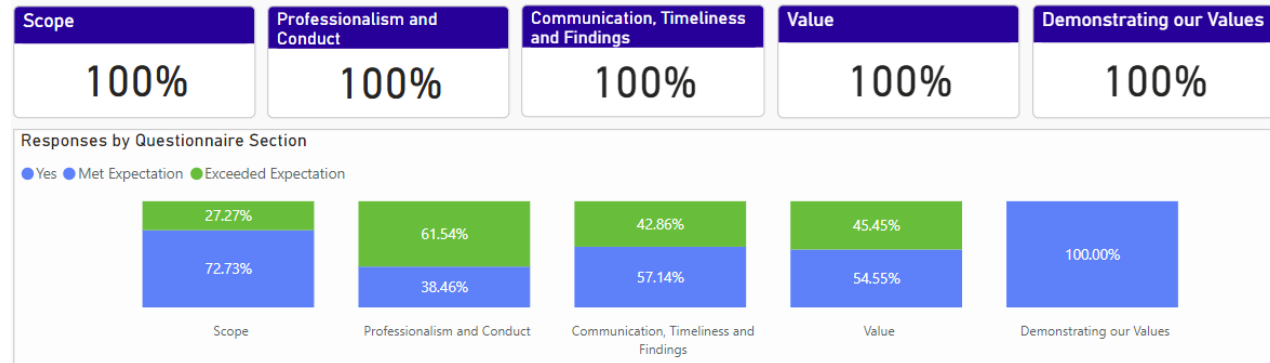
Assurance	Description
Substantial	Sound system of governance, risk management and controls exist
Reasonable	Generally sound system of governance, risk management and control in place
Limited	Significant gaps, weaknesses or non-compliance were identified
No Assurance	Fundamental gaps, weaknesses or non-compliance identified

# Internal Audit Plan Progress 2024/25

We review our performance to ensure that our work meets our clients' expectations and that we are delivering value to the organisation.

## SWAP Performance Measures

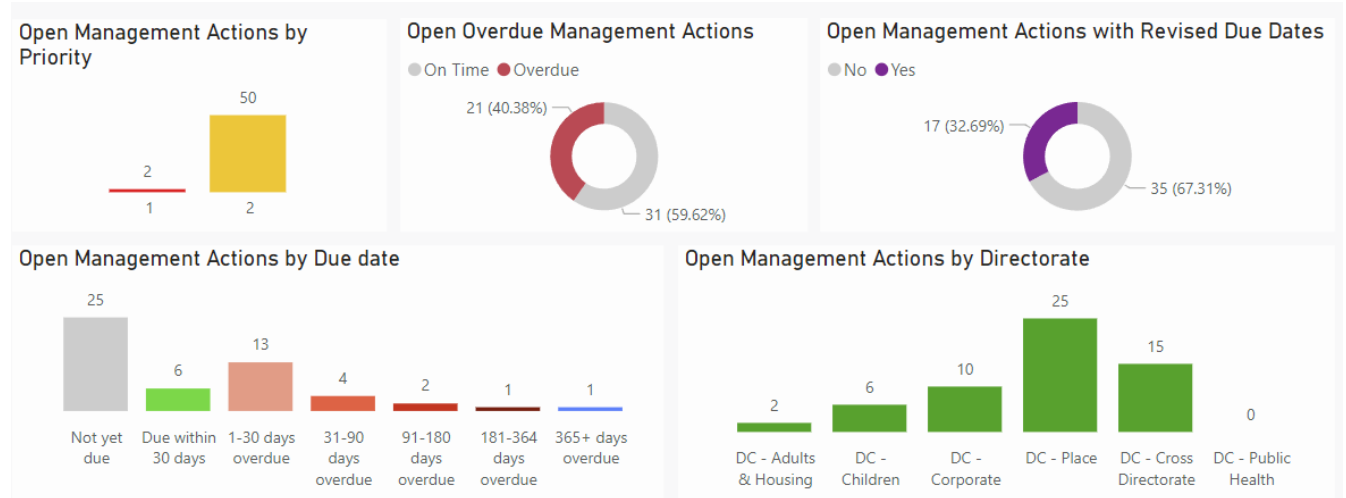
Performance scores from post audit questionnaires:



# Internal Audit Plan Progress 2024/25

We monitor the Council's performance for implementation of agreed actions.

## Outcomes from Follow Up Audit Work



Page 72



## Added Value

**‘Extra feature(s) of an item of interest (product, service, person etc.) that go beyond the standard expectations and provide something more while adding little or nothing to its cost.’**



## Added Value

### Cifas

The use of the Cifas data sharing service continues to bring benefits. Since our last update Financial Agents and Power of Attorneys; and housing register applications are now being run through the database. Potential new areas include checking of senior officers, and re-checks of staff and contractors. ICT Services are also running a project to see if it is possible to use Application Programming Interface (API) between Mosaic and Cifas to upload data directly which would enable a real time search of all Adult Service Users to identify deceased cases. Previously agreed areas continue to be run through the database with matches being identified and action taken where necessary.

### Data Analytics

Data analytics, which has been used to inform audit findings and to provide additional insight has been undertaken for the Delivery of Support for Carers, Establishment Control and Dignity at Work (Place) audits.

### Newsletters and updates

SWAP regularly produces a newsletter and other relevant updates for partners such as fraud bulletins, which provide information on topical issues of interest.

The role of SWAP as the internal auditors for Dorset Council is to provide independent assurance that the Council’s risk management, governance and internal control processes are operating effectively. In order for senior management and members to be able to appreciate the implications of the assurance provided within an audit report, SWAP provide an assurance opinion. The four opinion ratings are defined as follows:

Assurance Definitions	
<b>No Assurance</b>	The review identified fundamental gaps, weaknesses or non-compliance, which require immediate action. The system of governance, risk management and control is inadequate to effectively manage risks to the achievement of objectives in the area audited.
<b>Limited</b>	The review identified significant gaps, weaknesses or non-compliance. The system of governance, risk management and control requires improvement to effectively manage risks to the achievement of objectives in the area audited
<b>Reasonable</b>	The review highlighted a generally sound system of governance, risk management and control in place. We identified some issues, non-compliance or scope for improvement were identified which may put at risk the achievement of objectives in the area audited.
<b>Substantial</b>	The review confirmed a sound system of governance, risk management and control, with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited.

Page 74

In addition to the assurance definitions above we also provide an ‘**assurance dial**’ which indicates on a range of high medium or low where within the range of that assurance a particular audit assurance sits.



As can be seen in this example the assurance provided is low limited as the dial is sitting on the lower end of the limited scale. It could equally have been a medium limited assurance where the dial sits midway or high limited when it is sitting at the upper end close to the reasonable assurance.

The Committee is able to view a record of all internal audit work on the Rolling Plan dashboard held in AuditBoard, including work in progress and all completed work that would have previously been reported to the Committee in a table form. To provide the Committee with additional insight we include our one-page audit report in full for Limited assurance audits.

Premises Health and Safety Further Follow Up Review – Final Report – June 2024



Follow Up Audit Objective

To provide assurance that agreed actions to mitigate against risk exposure identified within the 2022/23 Limited opinion audit of Premises Related Health and Safety report have been implemented.

Follow Up Progress Summary

	Complete	In Progress	Not Started	Summary
Priority 1	2	0	0	2
Priority 2	5	1	0	6
Priority 3	1	0	0	1
<b>Total</b>	<b>8</b>	<b>1</b>	<b>0</b>	<b>9</b>

Follow Up Assessment


The original audit was completed and reported in September 2022 and received a Limited assurance opinion. A follow up was carried out in June 2023 where seven actions remained outstanding. This further follow up audit has found that whilst one action is still in progress the other two have been completed. Key findings have been summarised below.

Follow Up Scope

Testing has been performed in relation to all priority 1 and 2 actions and supporting evidence obtained to support implementation of actions.

Key Findings

The Property Service team have progressed with the agreed actions and as such we have closed off the priority one and one of the priority two actions, the remaining priority two action is still in progress.



There has been significant work completed on the premises health and safety policies. There is now a management action plan which runs alongside the policy which details the council's actions to comply with the policies. There is also a process in place for the policies to be regularly reviewed and updated when necessary. Work has also been completed to ensure tenants conform with the council's expectations concerning health and safety. Through a system called Zetasafe, the tenants are able to upload documents to demonstrate conformance with premises health and safety, they can also record noncompliant things in there which will alert the service to where there is work needed. The service will then program the work when they feel it needs to be addressed and then complete accordingly.

The work the service has completed on the premises health and safety is such that we have concluded that we can lower our risk assessment from High to a medium risk for the council, meaning it is no longer considered a significant corporate risk. Therefore, we will follow up the remaining action through our normal follow up process.

Further Follow Up Required

The outstanding action is due to be implemented by 31<sup>st</sup> December 2024. A summary of the key findings from our review will be presented to the Audit and Governance Committee on 22<sup>nd</sup> July 2024. Going forward, we will follow up the remaining action through our normal follow up process and close off the action once the relevant work has been completed.

Page 75

Audit Title	Priority	Timescale	Revised Date	Original Timescale	Months overdue
Premises Health & Safety	2	31/12/2024	Yes	28/02/2023	16
Data Quality & Information Governance	2	30/06/2023	No	30/06/2023	12
Risk Management	2	31/08/2024	Yes	31/07/2023	11
Risk Management	2	31/08/2024	Yes	31/07/2023	11
Risk Management	2	31/08/2024	Yes	31/07/2023	11
Risk Management	2	31/08/2024	Yes	31/07/2023	11
Effectiveness of Manager Self Service	2	31/03/2024	Yes	30/09/2023	9
Effectiveness of Manager Self Service	2	31/07/2024	Yes	30/09/2023	9
Effectiveness of Manager Self Service	2	31/07/2024	Yes	30/09/2023	9
Effectiveness of Manager Self Service	2	31/07/2024	Yes	30/09/2023	9
Debt Recovery - Access to Data for Collaborative Working	2	30/06/2024	Yes	31/10/2023	8
SEND Transport	2	30/11/2024	Yes	31/10/2023	8
SEND Transport	2	30/11/2024	Yes	30/11/2023	7
Data Quality & Information Governance	2	30/09/2024	Yes	30/11/2023	7

## Audit and Governance Committee Work Programme 2024-25

<b>8 July 2024</b>		
Update on the 2021/22 & 2022/23 Accounts External Audit	Verbal Update	Officer Contact- Sean Cremer and Ian Howse.
Dorset Council Audit Plan Year Ending 31 March 2024	Plan	Officer Contact- Jackson Murray from Grant Thornton
Dorset Pension Fund Audit Plan Year Ending 31 March 2024	Plan	Officer Contact- Jackson Murray from Grant Thornton
Interim Auditor's Annual Report on Dorset Council 2023/24	Report	Officer Contact- Jackson Murray from Grant Thornton Officer Contact – for your information DC Officer is Sean Creamer.
Draft outturn report 2023/24	Report	Officer Contact- Sean Cremer
Update on Effective Property Services (Corporate Landlord Model)	Update	Officer Contact- Tim Hulme and Jessica Maskrey
Councillor Code of Conduct, Complaint Process Review	Review	Officer Contact- Grace Evans
Enhanced DBS Checks for Councillor's	Report	Officer Contact- Jonathan Mair
Planning and Licensing Committees	Report	Officer Contact- Jonathan Mair

<b>22 July 2024</b>		
---------------------	--	--

Annual Emergency Planning Report	Report	Officer Contact- Marc Eyre
Annual Fraud and Whistleblowing Report	Report	Officer Contact- Marc Eyre
Annual Information Governance Report	Report	Officer Contact- Marc Eyre
Quarterly Risk Management Update	Update Report	Officer Contact- David Bonner/ Chris Swain
SWAP Update Report	Update Report	Officer Contact- Sally White/Angie Hooper

<b>23 September 2024</b>		
Quarterly Risk Management Update	Update Report	Officer Contact- David Bonner/ Chris Swain
SWAP Update Report	Update Report	Officer Contact- Sally White/ Angie Hooper
Q1 2024/25 Budget Monitoring Report	Report	Officer Contact- Sean Cremer
ISA260 2021/22 Accounts	Report	Officer Contact- Heather Lappin

<b>11 November 2024</b>		

<b>13 January 2025</b>		
Quarterly Risk Management Update	Update Report	Officer Contact- David Bonner/ Chris

		Swain
SWAP Update Report	Update Report	Officer Contact- Sally White/ Angie Hooper
Q2 2024/25 Budget Monitoring Report	Report	Officer Contact- Sean Cremer

<b>24 February 2025</b>		
Q3 2024/25 Budget Monitoring Report	Report	Officer Contact- Sean Cremer

<b>14 April 2025</b>		
Annual Governance Statement	Statement	Officer Contact- Marc Eyre
Quarterly Risk Management Update	Update Report	Officer Contact- David Bonner/Chris Swain
Planning Paper for 2025-26	Planning Paper	Officer Contact- Sally White/ Angie Hooper
Annual Internal Audit Opinion 2024-25	Opinion Report	Officer Contact- Sally White/Angie Hooper
SWAP Update Report	Update Report	Officer Contact- Sally White/Angie Hooper

**Other items raised by Audit and Governance Committee requiring further consideration.**

<b>Issue</b>	<b>Notes</b>	<b>Date raised</b>
--------------	--------------	--------------------

--	--	--