



Audit and Governance Committee

Date: Monday, 4 August 2025
Time: 6.30 pm
Venue: Council Chamber, County Hall, Dorchester, DT1 1XJ

Members (Quorum: 3)

Gary Suttle (Chair), Spencer Flower (Vice-Chair), Belinda Bawden, Neil Eysenck, Jill Haynes, Andrew Parry, Andy Todd, Beryl Ezzard, Ryan Holloway and Chris Kippax

Co-opted Members: R Ong and S Roach.

Interim Chief Executive: Sam Crowe, County Hall, Dorchester, Dorset DT1 1XJ

For more information about this agenda please contact Democratic Services
Meeting Contact 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. If you would like to attend this meeting and have any specific requirements please contact the Democratic Services Officer named above.

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
1. APOLOGIES	
To receive any apologies for absence.	
2. MINUTES	
To confirm the minutes of the meeting held on 30 th June and 7 th July 2025.	
3. DECLARATIONS OF INTEREST	
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.

4. 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 by 8.30 am on 31st July 2025.

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.

5. MINUTES OF THE AUDIT & GOVERNANCE SUB-COMMITTEE

To note the minutes of the Audit & Governance Hearing Sub-committee (if any meetings have been held).

6. REPORT OF INTERNAL AUDIT ACTIVITY PROGRESS REPORT 2025/26 - JULY 2025

5 - 22

To receive a report by SWAP.

- | | | |
|------------|---|--------------|
| 7. | ANNUAL INFORMATION GOVERNANCE REPORT – 2024/25 | 23 - 50 |
| | To receive a report by Marc Eyre, Service Manager for Assurance. | |
| 8. | ANNUAL FRAUD AND PROTECTED DISCLOSURES REPORT | 51 - 94 |
| | To receive a report by Marc Eyre, Service Manager for Assurance. | |
| 9. | ANNUAL EMERGENCY PLANNING REPORT. | 95 - 112 |
| | To receive a report by Marc Eyre, Service Manager for Assurance. | |
| 10. | RISK MANAGEMENT UPDATE. | 113 -
154 |
| | To receive a report by Chris Swain, Risk Reporting Officer. | |
| 11. | TREASURY MANAGEMENT ANNUAL REPORT 2024/25 | 155 -
176 |
| | To receive a report by David Wilkes, Service Manager Treasury and Investments. | |
| 12. | UPDATE ON OUR FUTURE COUNCIL WORK. | |
| | To receive an update by Sean Cremer, Corporate Director Finance and Commercial. | |
| 13. | GRANT THORNTON - IT AUDIT FINDINGS REPORT. | 177 -
204 |
| | To receive a report by Julie Masci, Grant Thornton. | |
| 14. | WORK PROGRAMME | 205 -
206 |
| | To consider the work programme for the Committee. | |
| 15. | 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. | |
| 16. | EXEMPT BUSINESS | |
| | There is no exempt business. | |

This page is intentionally left blank

Dorset Council

Report of Internal Audit Activity

Progress Report 2025/26 – July 2025

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: 07820 312469
sally.white@swapaudit.co.uk

Sophie Blackburn Principal Auditor
Tel: 07951 245945
sophie.blackburn@swapaudit.co.uk

SWAP is an internal audit partnership covering 27 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 full update report for 2025/26 financial year.

Our live Rolling Plan dashboard available through our audit management system AuditBoard [AuditBoard | Login \(auditboardapp.com\)](#), and specifically the Audit Coverage (*located on the first tab of the dashboard or on page 3 of this report*), reflects the outcomes of recently completed reviews. Based on these reviews, we recognise that, in general, risks are well managed. However, we have identified some gaps, weaknesses and areas of non-compliance. We have a reasonable level of confidence that the agreed actions will be implemented to address these issues.

Since our last report in June 2025, we have not issued any **Limited** assurance opinions on the areas and activities audited. In June, we reported a Limited assurance opinion report to the committee regarding Contract and Expenditure Compliance with Scheme of Delegation and Council Constitution. Our work identified a significant organisational impact, and we are currently conducting follow-up work to review the implementation of agreed actions.

We have also completed a review of the governance framework for the Our Future Council programme. As the programme is still in its early stages and individual projects are yet to be formally initiated, our work was limited to an advisory capacity rather than assurance, due to the restricted testing we were able to undertake. The full advisory report can be found on pages 8 and 9.

Executive Summary

Significant Corporate Risks

Update on Response to Climate Emergency

We originally issued the report on Climate Emergency in April 2023. Due to the complexity of the actions agreed at that time, some implementation has taken up to two years. We can now report that all actions are now fully complete, and the significant risk identified during the audit in 2022/23 has been successfully mitigated. The follow-up report can be found on page 10. Due to the passage of time since that work, we plan to include Climate Emergency or related areas in a future audit cycle for further review.

Update on Effectiveness of Business Continuity Plans

In April, we reported that actions were scheduled for implementation by the end of May 2025. We have undertaken follow-up work that has shown only one action remains in progress, with a revised implementation date of 31st December 2025. The follow-up report can be found on page 11.

Internal Audit Plan Progress 2025/26

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.



SWAP Internal Audit Plan Coverage

Table 1 below presents our audit coverage mapped against the Authority's new **Principal Risks**, introduced in May 2025. For context, we have also included Table 2 which shows our coverage of the **retired Strategic Risk Themes** that are no longer used by the council. This second table captures our coverage from May 2023 to May 2025. Further detail can be found using our audit management system, AuditBoard [AuditBoard | Login \(auditboardapp.com\)](https://auditboardapp.com). As you will see, while we are making progress towards coverage of the new principal risks, we have only been working on this updated framework for two months, and it will take time to achieve full coverage. However, the retired risks table (Table 2) demonstrates that we have delivered some level of recent audit work across all of the corporate risk themes. To view the audits that make up the coverage, log into AuditBoard, right-click on a coverage cell, select "drill through", and then choose "audit details".

Table 1

Principal Risk  Hover over new Principal Risks to see a definition	Coverage	Average Opinion
Commercial	None	
Data and Information Management	None	
Finance	Some	Reasonable
Legal	Some	Limited
Operations	Some	Reasonable
People	None	
Project / programme	In Progress	
Property	None	
Reputation	Some	Reasonable
Security	In Progress	
Technology	In Progress	

Internal Audit Plan Progress 2025/26

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

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

Table 2

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

Internal Audit Plan Progress 2025/26

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

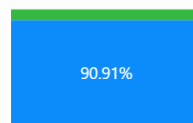
SWAP Performance Measures

Performance scores from post audit questionnaires:

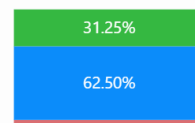
Scope	Professionalism and Conduct	Communication, Timeliness and Findings	Value	Demonstrating our Values
100%	95%	100%	91%	100%

Responses by Questionnaire Section

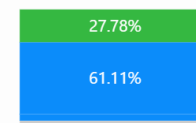
● Not Applicable ● Fell Below Expectation ● Yes ● Met Expectation ● Exceeded Expectation



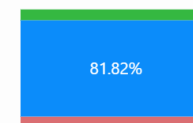
Scope



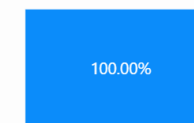
Professionalism and Conduct



Communication, Timeliness and Findings



Value



Demonstrating our Values

Overall Score

98%

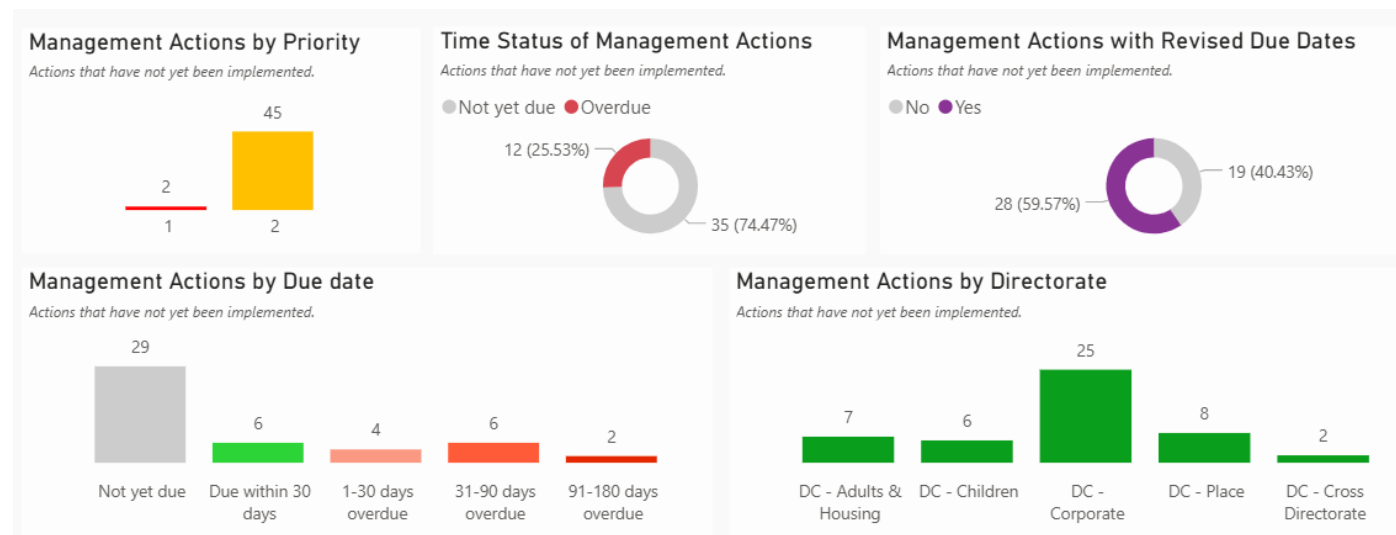
Internal Audit Plan Progress 2025/26

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

Outcomes from Follow-Up Audit Work

The graphic below provides an analysis of overdue priority 1 and 2 actions. There are currently 12 overdue actions - seven have passed their original due dates, and five have passed at least one revised due date.

Both the number of overdue actions and those not due but with revised timescales remain high. To support this, we have included a table in Appendix B (pages 12-15), which lists both overdue actions and those with one or more revised implementation dates. Additional information is available in the Management Actions tab of the SWAP Executive dashboard, which can be accessed via this link: [AuditBoard | Login \(auditboardapp.com\)](https://auditboardapp.com)



Internal Audit Plan Progress 2025/26

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 deliver benefits in the prevention and detection of fraud. Previously agreed areas are still being routinely checked against the databased, with matches identified and appropriate action taken where necessary.

Whistleblowing Investigations

SWAP's Counter Fraud team has recently completed an investigation arising from a whistleblowing referral.

Benchmarking

Benchmarking exercises have been undertaken to provide comparative insights in the following areas:

- Capital Governance
- Spend around the High Needs Block
- Management of Subject Access Requests by other Local Authorities.

Newsletters and updates

SWAP regularly produces a newsletter and other relevant updates for partners, including fraud bulletins. These communications highlight topical issues and provide useful information to support awareness and risk mitigation.

Our Future Council Governance Structure – Final Position Statement – July 2025



Audit Objective

To review the governance and reporting framework for the Our Future Council programme.

Executive Summary

Advisory

Background

Dorset Council's future Target Operating Model (TOM) is a strategic blueprint that outlines how the organisation can be structured and operate in the future to deliver its strategic objectives, serving as a guide for transforming current operations. This focusses on four functions (programmes) that are currently being delivered by most teams across the Council – Customer, Commissioning & Procurement, Business Support and Strategic & Enabling Services.

The TOM is Phase 1 of a broader 3-year programme which includes the redesign of ways of working, embedding digital and automation solutions, and reducing duplication.

Audit Scope

Our Future Council programme is in its initial stages and therefore our work has reviewed the frameworks and mechanisms in place and focused on the readiness of these in terms of delivering future benefits to the Council as follows; -

- The governance and reporting framework, including how decisions are and will be made.
- The risk management framework and how risks are and will be managed through the life of the programme.
- The deliverables, milestones and outcomes/savings framework and the mechanisms in place to monitor these and report any slippage.

Key Conclusion Summary

The implementation of the new Target Operating Model (TOM) under the Our Future Council (OFC) transformation programme is in its early stages, with Phase 1 staff consultations scheduled to begin in July 2025. A comprehensive governance framework is in place, providing oversight at both the programme and project levels. The dual membership of senior leaders on the Programme Board and Transformation Board has strengthened alignment and decision making, though it introduces some risks related to role clarity and independent scrutiny. Nonetheless, this structure is currently viewed as necessary to support effective delivery.

We have reviewed the overarching governance arrangements and can confirm they are operational, with risks being actively managed. However, due to the early stage of the programme, we have not yet been able to assess the governance of individual project groups. A framework for monitoring project level outcomes and savings exists, but these elements are still under development.

The OFC business case, approved in January 2025, originally proposed £10 million in savings. The current estimated savings to date are £1.7m, which are from vacancies.

Audit access to the Council's Project Portfolio management tool *Project for the Web* was limited; however, the system feeds into the Transformation and OFC Dashboard, which provided visibility into risks and benefits. A more detailed review of selected projects is planned for the next audit phase.

Please see below for a detailed summary of our observations.

Other Relevant Information

We have agreed that there will be further pieces of audit work to review the outcomes and savings achieved and benefits delivered. We have also added a review in the plan for Transformation where the scope will be wider than Our Future Council and this will be undertaken once the new Transformation Office has been established.

Our Future Council Governance Structure – Final Position Statement – July 2025

**Observations**

Timeline - In 2023 and early 2024 the council's change team established "Our Future Council," a cross-directorate portfolio. During summer 2024 an enhanced version of the council's target operating model (TOM) was developed. In September and October 2024, the change team established infrastructure to support the whole council transformation, drafting service reduction proposals and setting up workstreams with Programme Managers. Approval was sought from Cabinet in November 2024 to continue engagement with PwC to leverage their expertise and ensure the successful delivery of the transformation programme. CLT leads and task groups were appointed for each TOM layer and the council portfolio was re-prioritised deciding which activities to stop, start, or continue. Some projects remain within the Directorates, but those 'in scope' for OFC were moved into the OFC programme. The OFC business case was developed and approved by Cabinet in January 2025. The original timeline has slipped slightly with staff consultations now starting on 21st July and not the 1st of July. A decision has also been made not to deliver all four programmes together in July, but to stagger them across July to November 2025. The Programme Board have made 17 recent key decisions, with ten still to be made and it is understood that dependencies will be revisited once all decisions have been made.

Governance Structure - The Transformation Governance Framework document clearly sets out the Governance groups and boards in place. The dual membership of Senior Leadership on both the Programme Board and the Transformation Board offers benefits, including improved alignment, faster decision making, and executive knowledge. However, it also introduces challenges such as potential role confusion, and reduced scrutiny. Despite these concerns, within the current context, this dual membership is considered essential for effective decision making and the application of organisational knowledge.

The document also sets out expectations of how the projects should be run, managed and reported including the completion of a summary assessment with a proposed score to be put forward for each evaluation criterion to enable the projects to be prioritised. The project team have confirmed that these have not yet been completed for all of the proposed projects. In addition to this, the benefits realisation plans and decisions on governance gateways for the new projects have not been formulated made.

All projects are governed by a 'workstream', during this period of development activity, all workstream decisions are escalated to the programme board. Decisions taken in workstreams will be mobilised as part of transition to go-live plans due to begin in July. Some of the existing projects brought across to OFC have overdue timelines (2 -4 months) and when questioned it was confirmed that the project staff have been working on the mapping for the new operating model, which is due for completion by 21st July. The latest update, 30th June 2025, reports a total of 272/545 processes mapped and signed off. For the first programme of Customer Experience, 128/204 (63%), have been mapped and signed off.

Project managers compile monthly updates for the individual projects which go through the Programme Board and then onto the Transformation Board monthly. On Project for the Web, not all current projects contain a recent highlight report, which we understand is due to some projects being paused in order to deliver the pre consultation activities. There is a weekly OFC update which serves as an agenda for the weekly Programme Board meetings and weekly CLT leads stand ups.

Audit attended the Members Steering Group where a concern was raised around the timings of making staff redundant in comparison to the automation of processes. A question was also raised around adequacy of ICT staff remaining to implement the technology changes that are required to deliver the savings. Colleagues agreed to bring a roadmap and timeline to the next meeting.

Savings - A total of £10m of savings were proposed in the business case. These have been amended several times, particularly since the decision to introduce voluntary redundancies. The total remains the same but changes have been made, OFC Consolidation has been lowered from £5.8m to £1m, Third Party Spend has been raised from £1m to £1.8m, Removal of vacancies has been raised from £2m to £4.2m, voluntary redundancies newly added at £3m and realigning transitional structures according to organisational design principles has been removed (was £1.2m). The current estimated savings to date are £1.7m which are from vacancies.

Audit Access - To ensure consistency across the whole Council a Project Portfolio management tool 'Project for the Web' (PFTW) is used. Audit has access to this system, but permissions did not allow us to see all of the detail. However, the data from PFTW feeds the Transformation dashboard and we were able to drill down and see examples of activities such as risks and benefits. In our next review we will select a sample of projects and gain full access for the review of these specific projects.

Response to Climate Emergency Follow Up 3 – Final Report – July 2025



Follow Up Audit Objective

To provide assurance that agreed actions to mitigate against risk exposure identified within the 2022/23 Limited opinion audit of the Response to Climate Emergency report have been implemented.

Follow Up Progress Summary

Priority	Complete	In Progress	Not Started	Summary
Priority 1	2	0	0	2
Priority 2	6	0	0	6
Priority 3	0	0	0	0
Total	8	0	0	8

Follow Up Assessment

The original audit was completed and reported in January 2023 and received a Limited assurance opinion. Follow up audits were undertaken in June 2023 and March 2024 which closed off six actions. This follow up audit has found that the remaining two actions are now complete.

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 Council are working with other public sector partners developing an approach to sustainable procurement. The procurement scope 3 emissions toolkit has been developed and will continually evolve. Work is being undertaken on a roadmap which sets out the Council's expectations as a public sector buying group where suppliers will be required to publish their carbon footprint and sign up to reducing it. All of this will support colleagues to improve the ability to measure, monitor and score against carbon emissions.

There has also been increased engagement with Children's and Adults on different projects that feed into the Council's carbon footprint, along with input from the team into new strategies across different services.

Further Follow-Up Required/Next Steps

A summary of the key findings from our review will be presented to the Audit and Governance Committee on 4th August 2025. As the original audit work was completed in January 2023, we are in talks with the Corporate Director to arrange a further audit before the end of the financial year.

Effectiveness of Business Continuity Plans Follow Up – Final Report – July 2025



Follow Up Audit Objective

To provide assurance that agreed actions to mitigate against risk exposure identified within the 2024/25 Limited opinion audit of the Effectiveness of Business Continuity Plans report have been implemented.

Follow Up Progress Summary

Priority	Complete	In Progress	Not Started	Summary
Priority 1	1	0	0	1
Priority 2	12	1	0	13
Priority 3	1	0	0	1
Total	14	1	0	15

Follow Up Assessment

The original audit was completed and reported in November 2024 and received a Limited assurance opinion. Follow up work has been undertaken by audit over the past few months with actions being closed off. This follow up audit has found that there is just one action remaining in progress. There is a revised implementation date of 31st December 2025 for this remaining action. 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



There has been significant work undertaken by the service to implement all of the actions, with one remaining. This is for the services to identify their critical systems, which has been partially completed, with Children's outstanding. The revised Business Continuity Framework was approved at the Strategic Information Governance Board on 28 April 2025. The Annual Emergency Planning report and revised Business Impact Analysis has been reported to the Senior Leadership Team.

Further Follow Up Required

A second follow up will be undertaken to enable the service to demonstrate implementation of the one action which is due to be implemented by 31st December 2025.

A summary of the key findings from our review will be presented to the Audit and Governance Committee on 4th August 2025. Progress of the one remaining action will be reported to Audit and Governance Committee in 2026.

Overdue Actions with Number of Times the Implementation Date has been Amended as at 14.7.2025

Audit Title	Officer Responsible	Directorate	Action	Priority	Original Date	Current Revised Date	No. of Revisions	Current Revised Date v Original Date in Days
Use of Consultants and Temporary Staff	Chris Matthews – Head of People and Workforce	Corporate Services	Procurement will work with the BI & Performance Team and develop a dashboard to report performance metrics on consultants and temporary staff.	2	30/4/24	30/4/25	3	365
Data Quality & Information Governance	Marc Eyre – Service Manager for Assurance	Corporate Services	Taking a risk-based approach, the Strategic Information Governance board will review the data sharing arrangements for the cohort of c.800 employees and consider which of them require a Microsoft licence.	2	30/6/23	30/4/25	3	670
Temporary Accommodation	Andrew Billany – Corporate Director for Housing	Adults and Housing	The Housing service will design and roll out a thorough staff training program for effective use of the internal software system (Huume).	2	30/4/25	30/6/25	1	61
Temporary Accommodation	Andrew Billany - Corporate Director for Housing	Adults and Housing	The housing service will in conjunction with assets and property formalise a comprehensive asset register to track all accommodation assets. This includes recording property location, ownership, acquisition date, value, and related agreements which will be regularly updated to maintain accuracy and compliance with policies and regulations.	2	31/3/25	30/6/25	1	91
MCA Best Interest Assessment - Independent Assessor Investigation	Julie Ingram - Corporate Director for ASC	Adults and Housing	Appropriate recovery steps will be taken regarding two duplicate invoices for work. The payments for BIA work which appear to be Form 4s will also be considered for recovery. Finance will be instructed to write to these individuals where there is overpayment for work with a view to recovering this money.	2	31/3/25	n/a	0	0
MCA Best Interest Assessment -	Julie Ingram - Corporate	Adults and Housing	Flexi balances and long working days will be monitored more effectively in line with the corporate expectations	2	31/3/25	n/a	0	0

Audit Title	Officer Responsible	Directorate	Action	Priority	Original Date	Current Revised Date	No. of Revisions	Current Revised Date v Original Date in Days
Independent Assessor Investigation	Director for ASC		and consideration given to working time directives. Work has started in this area with the Service Manager and the Head of Service. This action will be picked up as part of the wider service enhancement review.					
Children's Service Direct Payments	Pru Caldwell-McGee - Service Manager, B2SA	Children's	The Direct Payments Policy will be reviewed to ensure alignment with current practices and regulations. A standardised case review process will be established based on policy criteria and provide training to staff and regular monitoring and quality assurance checks for ongoing compliance will be conducted.	2	30/4/25	n/a	0	0
Children's Service Direct Payments	Pru Caldwell-McGee - Service Manager, B2SA	Children's	A process will be implemented to ensure all direct payment bank accounts are reviewed on a regular basis. This will check the surplus of money in the account and ensure the money is spent on agreed resources.	2	30/4/25	n/a	0	0
DC Dignity at Work (Place)	Jan Britton – Executive Director	Place	The Place directorate will look at introducing ways of empowering employees to speak up. Examples of this could be: - Sharing anonymised cases studies from other services in the directorate and using these as a basis of a lessons learned exercise. - Introducing a working group which covers all services and employees at all different levels where learning across services can be covered and brought back to the services. - Introducing a positive role model within the services. They would encourage all employees to speak up when they experience unacceptable behaviour in the workplace.	2	31/5/25	n/a	0	0

Audit Title	Officer Responsible	Directorate	Action	Priority	Original Date	Current Revised Date	No. of Revisions	Current Revised Date v Original Date in Days
DC Dignity at Work (Place)	Jan Britton – Executive Director	Place	The directorate will try to identify ways the process after reporting an incident is more transparent for the victim.	2	31/5/25	n/a	0	0

Actions not yet due with multiple revision dates as at 14.7.2025

Audit Title	Officer Responsible	Directorate	Action	Priority	Original Date	Current Revised Date	No. of Revisions	Current Revised Date v Original Date in Days
Joint Funding Arrangements	Beth Whittaker - Corporate Director for Education & Learning	Children's	The work being carried out for the automation of decisions made by the MARP will include a mechanism for recording, tracking and monitoring cases. This will include upwards reporting to the appropriate committee/ directorate leadership group.	2	30/4/24	30/9/25	2	518
RMMSCW Framework	Jess Maskrey – Head of Assets and Property	Place	Guidance will be written for the procurement of a contractor when a lot becomes available. This will be communicated to all staff and included within the new framework.	2	30/6/24	30/9/25	2	457
RMMSCW Framework	Jess Maskrey – Head of Assets and Property	Place	A system will be established for the approval of works above the limit set for Lots within the current RMMSCW Framework. This should also be duplicated within the new proposed framework.	2	30/6/24	30/9/25	2	457
RMMSCW Framework	Jess Maskrey – Head of Assets and Property	Place	Assets and Property will work with Housing to establish a formal process for requesting work and signing off invoices.	2	30/9/24	30/9/25	2	365
RMMSCW Framework	Jess Maskrey – Head of Assets and Property	Place	Consideration will be given to including audit actions contained within this report with the tender process for the new framework, for example the requirement to	2	30/6/24	30/9/25	2	457

Audit Title	Officer Responsible	Directorate	Action	Priority	Original Date	Current Revised Date	No. of Revisions	Current Revised Date v Original Date in Days
			seek an exemption when the estimate is over the schedule of rates prior to the award of the work.					
Temporary Accommodation	Andrew Billany – Corporate Director for Housing	Adults and Housing	The Housing Service will ensure that temporary accommodation rents will be set at the level recommended in the Housing Revenue Accounts guidance.	2	31/3/25	30/6/26	1	456
Effectiveness of Business Continuity Plans	Marc Eyre – Service Manager for Assurance	Corporate Services	Services will be required to identify their critical systems within the review of the Business Impact Analysis (BIA). Additionally, a review will be conducted to remove any outdated systems from the list.	2	31/5/25	31/12/25	4	214
Estates Income and Debt Management	Jess Maskrey – Head of Assets and Property	Place	Investigate the options and feasibility for having SAP interface with TF Cloud, and decide on the most appropriate next steps.	2	30/11/24	30/9/25	1	304
Estates Income and Debt Management	Jess Maskrey – Head of Assets and Property	Place	Once TF Cloud has been implemented and had time to embed, Estates will undertake a benefits realisation exercise to establish the value added by the new system and understand how it is allowing the service to meet its objectives. Any gaps identified by the work will be investigated further.	2	31/1/25	30/9/25	1	242
Adults Block Booked Beds Contracts	Elaine Stratman - Brokerage & Market Service Manager	Adults and Housing	A standardised reconciliation process will be implemented to compare provider invoices against both void rates and fixed rates to ensure accurate and consistent billing. This process should be conducted regularly to identify and address any discrepancies.	2	31/3/25	30/7/25	3	121

The Global Internal Audit Standards were published by the Institute of Internal Audit (IIA) in January 2024. In late 2024, the UK's Public Sector—acting on recommendation of the Internal Audit Standards Advisory Board (IASAB) – advised the Standards would become mandatory in the UK from 1 April 2025. A full guide to the Standards aimed at Audit Committee members is here. In the UK Public Sector, the Standards are made more exacting by auditors also needing to comply with the UK Public Sector Application Note and the CIPFA Code of Practice for the Governance of Internal Audit in UK Local Government. At SWAP, we received an External Quality Assessment (EQA) in January 2025 confirming that we “Generally Conform” with the old standards. We must commission an assessment under the new Standards by 2030.	➡	Focus on Risk
		What do the Standards Say? The Standards emphasise Internal Audit’s role as an independent and objective source of assurance, advice insight and foresight. However, Principles 9 and 13 focus that assurance on being a risk-based exercise. What will the Committee see? Auditors should be able to explain what they do (and what they don’t do) in terms of risk to the authority’s strategic objectives. Audit findings, too, will be drawn direct from what matters to the authority.
	➡	Focus on Quality
		What do the Standards Say? Principle 12 emphasises the value of a challenging and stretching quality assurance process. Seeking continuous improvement for our partners begins with the internal audit service owning that ambition itself. What will the Committee see? Throughout 2025 we will be reviewing our quality assurance processes to form a clear programme with milestones to track our improvements. You should see reporting against those milestones later this year.
	➡	Focus on the Role of the Audit Committee
		What do the Standards Say? Domain III of the Standards recognise that to be truly effective internal audit must exist in an organisation that supports its mission, seeks improvement and is open to constructive challenge from critical friends. What will the Committee see? We have revised our Internal Audit Charter and other key documents to set out how internal audit and the Committee mutually support one another to pursue good governance at the authority. You saw and approved the new version of the charter in April this year. This document sets out the relationships and responsibilities needed to fulfil our objectives.



Global Internal Audit Standards

Five Domains, 15 Principles



I. Purpose of Internal Auditing

II. Ethics and Professionalism

1. Demonstrate Integrity 2. Maintain Objectivity 3. Demonstrate Competency 4. Exercise Due Professional Care 5. Maintain Confidentiality

III. Governing the Internal Audit Function

- 6. Authorized by the Board
- 7. Positioned Independently
- 8. Overseen by the Board

IV. Managing the Internal Audit Function

- 9. Plans Strategically
- 10. Manages Resources
- 11. Communicates Effectively
- 12. Enhances Quality

V. Performing Internal Audit Services

- 13. Plan Engagements Effectively
- 14. Conduct Engagement Work
- 15. Communicate Engagement Conclusions and Monitor Action Plans

Audit and Governance Committee

4 August 2025

Annual Information Governance Report – 2024/25

For Review and Consultation

Cabinet Member:

Cllr N Ireland, Leader of the Council, Climate, Performance and Safeguarding

Local Councillor(s): N/A

Executive Director:

J Mair, Director of Legal & Democratic

Report author and job title: Marc Eyre, Service Manager for Assurance
Email: marc.eyre@dorsetcouncil.gov.uk

Statutory Authority:

Report status: Public Choose an item.

1. Executive summary

- 1.1 This is the third 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 Appendix A to this report sets out background information on the Council's information governance structures. This should provide some context to new members of the committee.
- 1.3 Key Developments in 2024/25 included:
 - **Policy Updates:** New policies were introduced for Use of AI and data sharing, while existing ones like records management were refreshed. Email encryption and Data Loss Prevention tools were implemented to reduce data breach risks.
 - **AI Governance:** Microsoft Co-Pilot was approved for internal AI needs, while third-party AI tools were blacklisted unless demonstrated by a clear business need.

- **Cyber Security and ICT Continuity:** Cyber threats remain a “very high” risk. Investments were made in Microsoft E5 capabilities and cyber monitoring. Training and phishing simulations are conducted. A successful ICT continuity exercise during Easter reduced the strategic risk level for ICT continuity.
- **Records Management:** A simplification project was launched to migrate content from shared drives to Microsoft 365. Training for Information Asset Owners was delivered, and improvements were made to paper records tracking.
- **Subject Access Requests (SARs):** SARs rose by 39% to 478, with 78% related to Children’s Services. Despite the increase, compliance exceeded 90% in all quarters due to improved processes and team integration.
- **Freedom of Information (FOI):** 1,445 FOI/EIR requests were received. While the 90% response target was met in only two months, compliance stayed above 80% throughout the year. Transparency initiatives are underway to manage rising volumes.
- **Data Breaches:** 382 breaches were reported (up from 376), with 14 reported to the Information Commissioner. Email misuse accounted for 71% of incidents. No enforcement actions were taken. New sensitivity labels and breach monitoring tools were introduced.
- **Training Compliance:** Data protection training compliance ranged from 80–89%, below the 95% target. Cyber training compliance dropped to 65%. Senior Leadership Team have approved introducing system access restrictions for non-compliance.

1.4 Looking Ahead to 2025/26, priorities include:

- Developing a Power BI policy
- Ongoing roll out of the Information Asset Register
- Enhancing breach response mechanisms
- Enabling improved compliance on information governance training
- Supporting the “Our Future Council” transformation programme

1.5 The upcoming Data (Use and Access) Bill introduces a mandatory internal complaints process before escalation to the ICO. Dorset is preparing by establishing a dedicated complaints database, which will be supported by a policy document.

2. Recommendation(s)

2.1 To note the 2024/25 activity and focus for 2025/26.

3. Reason for the recommendation(s)

3.1 To ensure that information governance is embedded and effective across Dorset Council.

4. Information Governance Activity During 2024/25

4.1 A number of policies have been updated via the Operational Information Governance Group (OIGG) and signed off by the Strategic Information Governance Board (SIGB) during 2024/25:

- [Use of AI Automation Algorithmic Data Processing](#) (New policy)
- [Data Sharing](#) (New policy)
- [Records Management](#) (Refresh)
- Acceptable Use (Refresh)
- Business Continuity Framework (Refresh)

4.2 Data Loss Prevention and Email encryption have been enabled, both linked to the use of sensitivity labels. Data Loss Prevention is a capability within Microsoft Purview that includes prompts to users where certain risk data is included within an email, to reduce the risk of information being incorrectly shared. Additional controls have also been implemented to assist the identification of out of date membership of shared inboxes (for instance where staff move roles internally), to ensure that data isn't unnecessarily shared.

4.3 The OIGG has received, challenged and approved 12 Data Protection Impact Assessments (DPIA) during 2024/25. This has included:

- AI Communications Mining tool;
- Booking Solutions;
- Care Dorset
- Citizens Space
- Digitisation of Mental Health Act Assessments;
- Drug related deaths;
- E-signatures;
- Parent Assess;
- Right Care at Home;
- Sharing of Equality Data;
- Urgent and Emergency Care Transformation;
- Use of Microsoft Co-pilot;
- Whole Family Working

- 4.4 An improved workflow for DPIAs is in development. It is recognised that the Our Future Council programme will be looking to deliver efficiency through technology use. This will impact on the work programme for the OIGG, as it is anticipated that there will be a significant increase in DPIAs.
- 4.5 The OIGG is linked in closely with the developing AI agenda, in line with the [Use of AI, Automation and Algorithmic Data Processing policy](#). An assessment was undertaken of the number of different AI tools that have been accessed by staff. There are risks associated with this use, particularly where sensitive information is included, and without appropriate governance sensitive information could be retained and incorporated into the AI tools models. The decision was taken to blacklist the use of third party AI tools, as the functionality is provided by Microsoft Co-Pilot. As a Microsoft customer, the use of this application ensures that our data remains within our domain. There is a process to whitelist where there is an identified business need. An Acceptable Use of AI policy has recently been approved.
- 4.6 **Cyber Security**
- 4.6.1 During 2024/25 a number of local authorities suffered high profile attacks and/or continue to recover from the consequences of the incident. Because of this inherent risk, the threat of a successful cyber attack is currently identified as a “very high” risk in the Council’s risk register.
- 4.6.2 Cyber security has made steady progress over the last year. The council is working to build on Microsoft E5 licence baseline capabilities to increase the organisation’s ability to detect and respond to threats within our infrastructure. The intention is to invest further in employing a small team of cyber risk specialists, to significantly improve our ability to use the cyber monitoring data to identify actions to strengthen our technical defences. Third party monitoring would also be funded by these additional funds to provide a managed service providing out of hours monitoring service and response to cyber threats. This is subject to consideration as part of transformation proposals.
- 4.6.3 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. Performance is covered within 3.5 of this report. Training is supported by phishing simulations to test the extent of understanding.
- 4.6.4 Over the Easter Bank Holiday period, an ICT service continuity exercise was undertaken, to co-incide with planned maintenance. This provided positive assurance, to the extent that the strategic risk relating to ICT service continuity has reduced from “very high” to “high”. By very nature of the

consequences, the inherent risk will always remain at quite a high level. There were a number of lessons learnt, and an action plan is in development.

4.6.5 Directorates are reviewing their Business Impact Assessments and supporting business continuity action cards, which include resilience against the cyber risk. A set of business continuity exercises are available to services, to allow them to test their current resilience to both cyber attack and any resultant loss of data. This initiative was recognised by ALARM – the Public Sector Risk Management Association, who shortlisted it as a finalist within their annual awards, under the “resilience” category.

4.7 The Council's [Data and Business Intelligence Strategy](#) which was approved in February 2023 will be superseded by a Data and Technology Strategy later this year. This will include a focus on automating key processes to safeguard data quality, improve the self-service offerings, and address pain points in the customer experience.

4.8 **Information Management**

4.8.1 The Records Management Policy has been refreshed to more clearly define the role of Information Asset Owners in managing the risks to their service's information.

4.8.2 Work on the Simplifying Records Management workstream has resulted in a proposal focusing on migrating necessary content from shared drives and improving use of Microsoft 365. This is an important foundation for Our Future Council, supporting services to work efficiently with their information organised and in one place. Internal funding was sought from Senior Leadership Team for this business case, but it was not supported. However there remains a commitment for services to deliver migration within existing resources. An updated plan will be presented to SLT in October 2025.

4.8.3 An introductory training session was provided for all Information Asset Owners in February 2025, covering the responsibilities of their role and some of the tools available to them. Self-directed learning content is now being developed to assist managers with contributing to the Information Asset Register.

4.8.4 New Sensitivity labels for emails and Microsoft Office tools, and supporting information handling guidance, have been made available to all employees. Site container labels have also been updated - both informed by Government good practice.

4.8.5 Improvements have been made to the in-house system for tracking paper files held at the Records Management Unit. These changes will enable Information Asset Owners to manage their paper files more easily, and customers to track progress of their paper records transfers.

- 4.8.6 A new 2-year project has started to improve the management of paper and digital children's records. This will involve increasing the retention period for all records belonging to care-experienced and adopted children, restarting file disposals after a long-term nationwide hold, consolidating paper records into one storage location and supporting Children's Services managers to contribute to the Information Asset Register.
- 4.9 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 completed in June 2025, but recognised that the Council was still not meeting the mandatory requirements on data protection and cyber security training. As a result, the Council remains subject to an action plan to improve compliance rates on mandatory training. The risks associated with non-compliance with the toolkit are equally applicable to the Public Services Network and other ICT assurance frameworks.
- 4.10 The Council operates a "[Use of Covert Surveillance](#)" policy 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 2024/25;
 - The number of RIPA light authorisations requested and granted – None during 2024/25;
 - 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

5. Performance and Risk

- 5.1 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.
- 5.2 **Public and Environmental Information Requests**

- 5.2.1 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 2024/25, the Council received 1,445 requests (approx. 120 per month).
- 5.2.2 The Information Commissioners Office anticipates 90% compliance with the statutory response timescales of 20 working days. Whilst this was met in only two months during 2024/25, compliance exceeded 85% in nine of the twelve months, and at no point dropped below 80%. With Freedom of Information request numbers on the increase (6% from 2023/24), there is pressure on both the Information Compliance Team and responding services. As part of effort to manage this increase, the Council implemented a degree of automation, to carry out the reminder element of the process. It had been hoped to provide further automation, but this was restricted as there is insufficient data from request numbers to train an AI model. Work is underway to understand the most regular requests and determine if more can be done with signposting and information transparency to reduce requests. The Information Commissioner's Publication Scheme, which sets out documents that authorities should look to publish, has also been reviewed, and the Information Compliance team are liaising with services where there are gaps.

	Whole Authority	Adults & Housing	Childrens	Corporate	Place
Mar 25	86% (129)	60% (10)	86% (22)	88% (41)	89% (56)
Feb 25	88% (140)	67% (15)	91% (22)	90% (40)	90% (62)
Jan 25	91% (107)	90% (20)	92% (13)	96% (25)	88% (48)
Dec 24	83% (128)	64% (14)	67% (15)	84% (51)	91% (47)
Nov 24	87% (133)	86% (21)	69% (13)	98% (40)	84% (58)
Oct 24	88% (116)	79% (19)	73% (15)	91% (42)	95% (39)
Sep 24	87% (99)	73% (11)	75% (12)	93% (28)	89% (47)
Aug 24	86% (119)	70% (20)	70% (23)	97% (37)	92% (39)
Jul 24	84% (106)	91% (11)	63% (8)	84% (43)	86% (44)
Jun 24	82% (114)	55% (11)	65% (20)	84% (44)	95% (37)
May 24	85% (127)	94% (16)	67% (15)	87% (39)	86% (56)
Apr 24	91% (137)	79% (14)	80% (10)	98% (45)	90% (67)

- 5.2.3 For clarification, Corporate includes the following services: Legal; Democratic and Elections; Assurance; Finance; ICT; Human Resources; Strategy Performance and Sustainability; Transformation Customer and Cultural Services.
- 5.2.4 Place includes the following: Highways; Waste; Planning; Transport; Assets and Regeneration; Community and Public Protection; Environment and Wellbeing.
- 5.2.5 The following chart shows the number of FOIs overdue by more than 20 days (ie over 40 days from receipt). We have started to collect this information with effect from December 2024, and what it demonstrates is that even where we are not meeting the 90% target, it is rare for FOIs to exceed the target by much:

	Whole Authority	Adults & Housing	Childrens	Corporate	Place
Mar 25	3	3	0	0	0
Feb 25	3	2	1	0	0
Jan 25	3	3	0	0	0
Dec 24	1	1	0	0	0

- 5.2.6 Within Adults and Housing there is a process established for Corporate Director sign off to provide assurance over the information being released. This has caused some delay, rather than the collection of data which is generally collected within timescale. FOIs are becoming more complex in their ask for information, which can impact on the timeliness of the information as it is often a response requiring input from a number of officers.

5.3 **Requests Relating to Personal Information**

- 5.3.1 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 2024/25 the Council received 478 SARs, up from 343 in the previous financial year. Of these, 317 became active (up from 266), approx. 27 per month (up from 22). Of these, 78% related to Childrens Services (up from 63%). 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.

- 5.3.2 Since GDPR legislation became law in 2018, requests had increased at a rate of approximately 24% year on year, although this trend appeared to plateau in the 2023/24 financial year. This year, there has been an increase of 39% on requests and 19% on active requests.
- 5.3.3 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) in early 2022. Compliance was above the 90% target set by the Information Commissioner in all four quarters, which is a significant achievement, given the increased number of requests and their complexity.
- 5.3.4 The improvement in performance has been achieved through an effective and efficient two stage review process, and dedicated professional knowledge within the SAR team enhanced by training. The need reported in the last two years to outsource requests above capacity has been significantly reduced, but will continue to be utilised where demand exceeds capacity.

	Whole Authority	Adults & Housing	Childrens	Corporate	Place
Q4	98% (66)	100% (8)	98% (53)	100% (2)	100% (3)
Q3	95% (84)	83% (6)	98% (64)	60% (5)	100% (9)
Q2	92% (86)	89% (9)	94% (66)	77% (6)	100% (5)
Q1	95% (81)	94% (16)	100% (51)	73% (11)	100% (3)

- 5.3.5 The chart above highlights red performance within corporate services. It should be noted that request numbers are low. Equally the compiling, reviewing and redaction will be undertaken by the service holding the information, rather than the corporate team (who manage the whole process for Childrens requests), and therefore not benefitting from the dedicated knowledge and skillsets that that central team provides.
- 5.3.6 Outside of the 2024/25 timescales within scope for this report, there has been a significant data breach relating to the SARs process and sensitive childrens services data. This prompted the Service Manager for Assurance to initiate an internal audit on the SARs process, in addition to personally carrying out a review of the incident. Whilst the breach was regrettable, and a matter of human error, the committee can be assured that the internal audit process has presented a reasonable level of assurance. The auditor acknowledged

that the childrens services SARs process alone would have presented a substantial assurance, and there is some good practice that could be extended to other directorate requests.

5.4 Data Breaches

- 5.4.1 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.
- 5.4.2 The 2024/25 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. This has continued an upward trajectory to 382 breaches reported for 2024/25. 14 of these incidents were determined by the Data Protection Officer to meet the criteria for escalation to the ICO. A further 2 were reported to the ICO by an external individual or organisation. There has been no enforcement action by the ICO, but on several occasions recommendations have been made and actions mandated. The causes of data breaches during 2024/25 are summarised below:

Incident Category	Frequency in 2024/25	% of recorded incidents
Email	271	71%
Fax	1	0%
Post	20	5%
Unauthorised online access	33	9%
Unauthorised internal access	19	5%
Lost	11	3%
Telephone	10	3%
Other (including AI bots)	17	4%

- 5.4.3 As can be seen from the figures above, 71% of breaches relate to the use of email. Email security is already a core part of the council's mandatory data protection and cyber security training for all staff. As reported earlier in the report, technology is being used to help reduce the data breach risk, through improved email encryption and use of Data Loss Prevention tools. Similarly the introduction of sensitivity labelling provides the ability to revoke access. These mechanisms are in their infancy, and further work is underway to embed and enhance, and will be monitored. Over time it is hoped that this will reduce breaches, but there is acceptance that in the short term we may see an increase due to a higher awareness of what constitutes a breach and needs reporting (as it is likely there is currently under reporting).
- 5.4.4 Where a data breach has occurred appropriate management action is considered on a case-by-case basis, dependent upon the severity of the breach and level of culpability. In the last year formal action has been taken in several cases.
- 5.4.5 The Organisational Compliance and Risk Learning Group has been operating since the beginning of 2023/24. The role of this 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 aims to review all data breach incidents that are reported to the ICO. Change of officers has impacted on this group meeting over the last six months, and it is recognised that this group is a key function of the Council's information governance arrangements.

5.5 Mandatory Data Protection and Cyber Training

- 5.5.1 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 also incorporated into the elected member induction programme.
- 5.5.2 The mandatory data protection compliance training remains stubbornly between 80% and 89% across the last six months, but is still short of the target 95%. At the time of writing this report cyber training compliance is at approximately 65%, which has reduced from the 73% reported last year. As highlighted earlier in the report, this presents a continuing risk to compliance with the NHS Data Security and Protection toolkit.
- 5.5.3 There remain regular reminders, and managers have access to dashboards to identify where staff are not completing either training module. The Operational Information Governance Group has supported introducing removal of systems access to those that have not carried out the training within a reasonable period of time. This was supported by the Senior

Leadership Team in June 2025, and work is now underway to determine how this can be enabled. Where the removal of access to IT systems can directly impact on an employee's ability to undertake their role, appropriate management action can be taken.

- 5.6 The Council's risk register identifies 42 risks in the Data and Information Management risk category, five of which are identified as “High” or “Very High” as set out in the table below:

Risk	Risk Ranking	Management Response	Risk Owner
107 - Inadequate evidence base (including Partnership data) to determine service need for children's care and protection	High	We have undertaken significant work to further strengthen practice and services through our Strengthening Services for Children and Families Programme. The developments in Business Intelligence are supporting us to understand and model service need and we continue to develop this approach.	Corporate Director – Care and Protection
286 - A successful cyber-attack to IT systems causes loss of service or data	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. The council's identity management (multifactor, conditional access and account permission) has been reviewed with the support of specialist technology. Baseline Microsoft licence E5 capabilities have been implemented.	Head of ICT Operations

Risk	Risk Ranking	Management Response	Risk Owner
		Continuous monitoring and improvement of over 60 individual elements of cyber security through increased controls. All areas are either planned, investigated or implemented to continuously improve the Councils cyber security posture.	
348 - There is a business continuity risk from delayed ICT recovery after a disruption such as a power failure.	High	Resilience for critical services hosted by the Council, including duplicated services operating from multiple data centres. Service continuity and exercise response processes are managed by an experienced team and this will be reviewed as part of a set of new exercises to provide assurance on its outcomes. Limited testing on key applications took place easter 2025, this is the foundation for twice yearly regular testing to maintain and improve the Councils posture.	Head of ICT Operations
612 - Loss of the ability to find, open, work with, understand or trust Dorset Council's digital information causes disruption to	High	The Simplifying workstream is designing how to implement better protections and retention on digital information stored in Microsoft 365 and our legacy information on shared drives – ensuring it is managed through its lifecycle from creation to disposal or transfer to Dorset History Centre. This work plans to review 'orphaned' information and propose ownership by the most relevant Information Asset Owner.	Service Manager for Archives and Records

Risk	Risk Ranking	Management Response	Risk Owner
business operations		Records management requirements are now included in general requirements used when procuring new ICT systems. There is still much to be done in upgrading the retention capabilities of current line-of-business systems (e.g. Mosaic, ModGov) and putting in place differentiated controls according to the value and longevity of the information concerned. Simplifying has now reached a point where it will be shortly presented to senior officers for consideration and potential funding. A business case is due to go before the Design Authority in April 2025. If agreed, this project will address the question of the shared drives and the 94 million documents stored there - prior to switchoff in 2027 and migration of selected content to Sharepoint.	
809 - Contraction of the ICT function to contribute to meeting financial pressures results in insufficient ICT capacity and capabilities to deliver the	High	Proactively engaging in benchmarking activity with SWAP to benchmark resourcing of ICT functions across councils. Proactively engaging in the Our Future Council programme Strategic & Enabling workstream to make the case for change to the ICT establishment as part of forming the wider new 'strategic core' of the council, balancing financial pressures with the need to adopt new technologies, and deploy technologies more widely to support new ways of working	Head of ICT Operations

Risk	Risk Ranking	Management Response	Risk Owner
technology platforms that enable future ways of working and whole-council performance			

6. Focus for 2025/26 – The ICO Accountability Framework

- 6.1 The Government has proposed reform changes to the existing data protection legislation with the “Data (Use and Access)” Bill. 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. One change worth highlighting however is the introduction of a data protection complaints process.
- 6.2 Whereas historically individuals could complain directly to the Information Commissioner, the Bill proposes that they must first submit complaints directly to the organisation. They would then be escalated to the Information Commissioner if not handled properly by the organisation (which in many ways mirrors the complaints escalation route via the ombudsman). The aim of this is to give organisations the opportunity to resolve issues without escalation, and ensure that the Information Commissioner’s capacity is focussed on the most significant complaints. The Information Compliance Team are actively working on establishing the data protection complaint process, in readiness.
- 6.3 As reported in the 2024/25 report, the ICO has established an [Accountability Framework](#) toolkit that enables organisations to self assess the extent that current policies and processes meet their expectations. This has been completed and built on to provide a prioritised and risk based work programme for the SIGB and its working groups, and is 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

6.4 The action plan is included as Appendix B to this report. Progress has been slower than hoped, as the OIGG are owners of the majority of actions, and have had a challenging agenda due to the level of business change (in particular the need to review Data Protection Impact Assessments). Similarly there have been pressures on the supporting teams with delivery sitting 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. The recruitment of a temporary Data Protection Analyst has been completed (subject to successful references), and it is hoped that during their 12 month tenure there will be an improved movement on outstanding actions. The Priority One actions are noted below:

- 02c: Develop a Power BI Policy
- 02e: Develop Data Protection Complaints process
- 03a: Develop and roll out information governance training matrix
- 03f: Roll out RIPA / covert surveillance training
- 06a: Roll out of Information Asset Register
- 08d: Support Our Future Council transformation programme with information governance input
- 09a: Workstream to design digital records procedures (“simplifying records management”)
- 09e: Revise access control policy

- 10a: Strengthening data breach recording mechanisms and risk assessment tool

7. Alternative options considered

7.1 None

8. Legal considerations

8.1 Ensure that the Council is meeting the obligations of the forthcoming “Data (Use and Access)” Bill, alongside the General Data Protection Regulations.

9. Financial implications

9.1 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.

10. Natural environment, climate & ecology implications

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

11. Well-being and health implications

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

12. Other implications

12.1 None

13. Risk implications

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

Current Risk: High

Residual Risk: High

- 13.2 This scoring reflects the four high risks specified in section 5.6 of the report. There are also challenging resourcing demands in implementing the action plan at Appendix B.

14. Equalities

- 14.1 None

15. Appendices

Appendix A – Background information – Information Governance Structures

Appendix B – Information Governance Action Plan

16. Background papers

None

17. Report sign-off

- 17.1 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)

Appendix A

Information Governance Structures at Dorset Council

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. This is set out in more detail in the [Information Governance Policy](#).

The Assurance Team includes a statutory 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).

The SIRO role is mandatory for public sector organisations and is responsible for implementing and managing information risks within the organisation.

The role of Caldicott Guardian is performed by the Corporate Director for Adult Social Care Operations. 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.

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. Recognising that loss of data is a key component of the fraud risk, the board's remit has been extended to provide an overview of fraud management arrangements.

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.

Operational Information Governance Group (OIGG)

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. The OIGG is identified as a consultee within the Our Future Council transformation programme.

Organisational Compliance and Risk Learning Group

This is chaired by the Strategic Performance Intelligence and Risk Officer 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.

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.

Digital Applications Governance Group

This was previously chaired by a Programme Manager in the Transformation, Innovation and Digital Service, but has been decommissioned and replaced by the Internal Technical Design Authority as part of the Our Future Council programme. Its former role had been to monitor the roadmap of Microsoft applications, alongside other system developments, and 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. An action has been identified to look at whether the decommissioning results in gaps that need to be picked up by the other task and finish groups.

Appendix B – Information Governance Action Plan						
Ref	Identified action	ICO Framework Category	By Whom / Sub Group	Risk based priority	Resourcing Requirements	Latest Status
01a	Develop an Information Governance resourcing plan	1) Leadership & Oversight	Operational	Priority 1	SM for Assurance / DPO	Completed
01b	Review intranet guidance and / or develop SharePoint Hub	1) Leadership & Oversight	Operational	Priority 2	DPO	
01c	SIGB to review effectiveness of existing operational sub groups	1) Leadership & Oversight	Strategic Information Governance Board	Priority 2	SIGB and Chairs	Operational Information Governance Group has carried out a review.
02a	Develop schedule of policies and prioritised review dates, integrating into corporate template	2) Policies & Procedures	Operational	Priority 1	SM for Assurance / DPO / ICT Cyber Security Lead	Completed
02b	Refresh policy framework regarding processing of special category/criminal offence data	2) Policies & Procedures	Operational	Priority 2	DPO	
02c	Develop Power BI policy	2) Policies & Procedures	Operational	Priority 1	Head of Strategy	This has been drafted, pending sign off.

Ref	Identified action	ICO Framework Category	By Whom / Sub Group	Risk based priority	Resourcing Requirements	Latest Status
02d	Review overarching Data Protection policy	2) Policies & Procedures	Operational	Priority 2	DPO	
02e (New)	Develop data protection complaints policy and supporting process	2) Policies & Procedures	Operational	Priority 1	DPO	
03a	Develop and roll out Information Governance training matrix	3) Training & Awareness	Operational	Priority 1	SM for Assurance	Training sub group established and criteria for matrix identified. Rolling out to Directorates for data gathering
03b	Determine mechanisms for delivery of training for high risk roles / service areas (following completion of training matrix)	3) Training & Awareness	Operational	Priority 3	DPO / ICT Cyber Security Lead	
03c	Develop communications plan with corporate communications team, with periodic IG reminders	3) Training & Awareness	Operational	Priority 2	SM for Assurance / DPO	Completed. Periodic items have now been agreed within the training calendar
03d	Development and delivery of induction training for elected members of data	3) Training & Awareness	Cyber Security;#Operational	Priority 1	DPO / Cyber Security Lead	Completed

Ref	Identified action	ICO Framework Category	By Whom / Sub Group	Risk based priority	Resourcing Requirements	Latest Status
	protection / cyber security					
03e	Review content of existing information governance training modules	3) Training & Awareness	Operational	Priority 3	DPO	This will be undertaken by the training sub group
03f	Roll out RIPA / Covert Surveillance training	3) Training & Awareness	Operational	Priority 1	SM for Assurance / DPO	The training has not yet been delivered to support the approved Covert Surveillance policy
04a	Strengthen processes to support individual requests for data erasure, with appropriate audit regime, in accordance with article 17	4) Individuals Rights	Operational	Priority 4	DPO	
04b	Review and update Individuals Rights policy	4) Individuals Rights	Operational	Priority 4	DPO	
05a	Review public schedule of privacy notices, identifying purposes of the processing and legal basis and ensure	5) Transparency	Operational	Priority 4	DPO	

Ref	Identified action	ICO Framework Category	By Whom / Sub Group	Risk based priority	Resourcing Requirements	Latest Status
	process for review and update					
05b	Incorporate privacy information into the mandatory data protection training	5) Transparency	Operational	Priority 3	DPO	
06a	Roll out of Information Asset Register	6) ROPA & Lawful Basis	Operational	Priority 1	Information Management / DPO; input from all services	Partially complete. External introductory IAO training delivered in Feb 2025. In-house training content now being developed by RM and OD, including e-learning modules. This will facilitate launching a self-directed approach for managers to contribute to the IAR.
07a	Develop Data Sharing policy, with Information Asset Register providing mechanism for logging agreements and identifying gaps	7) Contracts & Data Sharing	Operational	Priority 1	DPO	Completed
07b	Development of third party supply chain risk management framework	7) Contracts & Data Sharing	Operational	Priority 3	DPO	Audit questionnaire being developed via OIGG

Ref	Identified action	ICO Framework Category	By Whom / Sub Group	Risk based priority	Resourcing Requirements	Latest Status
08a	Reflect information risk into the overarching Data Protection policy, linked to Information Asset Register work	8) Risks & DPIAs	Operational	Priority 4	DPO / Information Management	
08b	Finalise and roll out revised Data Protection Impact Assessment guidance, with centralised log	8) Risks & DPIAs	Operational	Priority 2	DPO	Good progress, and “show and share” for staff is imminent
08c	Develop DPIA training process	8) Risks & DPIAs	Operational	Priority 3	DPO	
08d	Support Our Future Council transformation programme with information governance input	8) Risks & DPIAs	Operational	Priority 1	DPO / OIGG	Governance arrangements established, and OIGG included as a consultee
09a	Workstream to design digital records' procedures (Simplifying Records Management)	9) Records Management & Security	Records Management Project	Priority 1	Information Management / User Adoption	Business case drafted to focus on migrating necessary information from shared drives, resource request to be taken to Senior Leadership Team in June 2025

Ref	Identified action	ICO Framework Category	By Whom / Sub Group	Risk based priority	Resourcing Requirements	Latest Status
09b	Improve Self-Service Portal, the paper records tracking system for the Records Management Unit	9) Records Management & Security	Records Management Project	Priority 3	ICT / Information Management	Completed
09c	Implement Data and Technology Strategy	9) Records Management & Security	Organisational Compliance & Risk Learning Group	Priority 3	Head of Strategy	
09d	Revise Acceptable Use policy	9) Records Management & Security	Operational	Priority 1	ICT Cyber Security Lead	Completed
09e	Revise Access Control policy	9) Records Management & Security	Operational	Priority 1	ICT Cyber Security Lead	Identified within 2023 SWAP audit on Data Quality and Information Governance
09f	Establish working group to look at the risks associated with WhatsApp and other similar social media messaging facilities	9) Records Management & Security	Operational	Priority 2	SM for Assurance / DPO and working group	
09g	Implement process of clear desk checks	9) Records Management & Security	Organisational Compliance & Risk Learning Group	Priority 4	DPO	

Ref	Identified action	ICO Framework Category	By Whom / Sub Group	Risk based priority	Resourcing Requirements	Latest Status
09h	Refresh of business continuity plans, with transfer of action cards to MS Teams, and focus on data loss	9) Records Management & Security	Operational	Priority 1	SM for Assurance / Emergency Planning	Completed
09i	Roll out of Cyber business continuity exercises	9) Records Management & Security	Operational	Priority 1	Emergency Planning	Completed
09j	Develop AI policy	9) Records Management & Security	Operational	Priority 1	ICT Cyber Security Lead / DPO	Completed
09k	Develop Account Activity Policy	9) Records Management & Security	Operational	Priority 2	ICT Cyber Security Lead	Completed
10a	Strengthen data breach recording mechanisms and risk assessment tool	10) Breach Response & Monitoring	Operational	Priority 1	DPO / Asst DPO	
10b	Strengthen the lessons learnt process and ownership within service areas for low level breaches (ie those not considered by Risk and Learning Group	10) Breach Response & Monitoring	Organisational Compliance & Risk Learning Group	Priority 2	DPO	

Ref	Identified action	ICO Framework Category	By Whom / Sub Group	Risk based priority	Resourcing Requirements	Latest Status
10c	Develop audit plan for information governance compliance audits and reporting process	10) Breach Response & Monitoring	Organisational Compliance & Risk Learning Group	Priority 3	Head of Strategy / DPO	
10d	Review and improve range of Information Governance KPIs	10) Breach Response & Monitoring	Operational	Priority 1	SM for Assurance / DPO	Completed
10e	Work with ICT colleagues in the roll out of E5 to explore mechanisms to reduce data breaches and cyber exposures	10) Breach Response & Monitoring	Operational	Priority 1	DPO / ICT Cyber Security Lead	Completed
10f	Develop formal process for recording and tracking actions resulting from data / cyber breaches	10) Breach Response & Monitoring	Organisational Compliance & Risk Learning Group	Priority 2	Head of Strategy/ DPO	
10g	Review and update Data Breach policy	10) Breach Response & Monitoring	Operational	Priority 2	DPO	

Audit and Governance Committee

4 August 2025

Annual Fraud and Protected Disclosures Report For Decision

Cabinet Member:

Cllr N Ireland, Leader of the Council, Climate, Performance and Safeguarding

Local Councillor(s): N/A

Executive Director:

J Mair, Director of Legal & Democratic

Report author and job title: Marc Eyre, Service Manager for Assurance
Email: marc.eyre@dorsetcouncil.gov.uk

Statutory Authority:

Report status: Public Choose an item.

1. Executive summary

- 1.1 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 Councils approach to combatting the fraud risk, and a summary of cases reported in the preceding twelve months.
- 1.2 The Committee is also responsible for signing off counter fraud related policy documents. These are now due for review, and have been reworked. The whistleblowing policy has been renamed “Protected Disclosure (Whistleblowing) Policy” and has been updated to reflect a number of minor “priority three” SWAP audit requirements.
- 1.3 A new “Counter Fraud and Financial Crime” policy has been developed, superseding and combining the previous “Anti Fraud, Bribery and Corruption” and “Anti-Money Laundering” policies, in addition to incorporating anti tax evasion and recognising a compliance regime in respect of the new offence of “Failure to Prevent Fraud” as per the Economic Crime and Corporate Transparency Act 2023.

2. Recommendation(s)

2.1 The Committee are asked to:

- i) Note the annual update on fraud and protected disclosure activity;
- ii) approve the revised “Protected Disclosure (Whistleblowing) Policy”;
- iii) approve the new “Counter Fraud and Financial Crime Policy”; and
- iv) note the compliance matrix

3. Reason for the recommendation(s)

3.1 To support the Council’s zero tolerance to fraud and other financial crimes.

4. Summary of Anti Fraud Initiatives

4.1 Previous annual reports have noted the SWAP internal audit baseline assessment of anti-fraud maturity, which provided a cross-cutting baseline assessment report on the maturity of fraud management across wider SWAP partners. This was last completed in 2022 but provided a good tool for the development of a counter fraud compliance matrix.

4.2 The Economic Crime and Corporate Transparency Act (ECCTA) 2023 received Royal Assent on 26 October 2023. Whilst the most direct impacts of this act fall on companies (including local authority-owned ones), all local authorities have a role to play in ensuring compliance, especially in procurement, partnerships, and fraud prevention. This act introduces a new “failure to prevent fraud” offence, which could be found against local authorities if they:

- Fail to put in place reasonable fraud prevention procedures
- Are involved in economic activities where fraud risks are present

4.3 There are also implications in relation to commissioning and procurement arrangements, in particular:

- To meet diligence obligations under the Act
- The need to verify the legitimacy and transparency of corporate partners
- Potential liability if they engage with entities involved in economic crime

4.4 The compliance matrix included at Appendix A incorporates the key requirements set out in the ECCTA, ie:

- Implement procedures proportionate to the fraud risks faced by the authority;
- Assess the nature and extent of exposure to fraud risks;
- Foster a culture of integrity and anti-fraud commitment from senior leadership;
- Apply due diligence to associated persons (e.g. contractors, suppliers);
- Ensure staff and associates are aware of fraud risks and prevention procedures;
- Monitor and review fraud prevention procedures regularly

4.5 There are a number of areas noted as Green in the matrix where we are refreshing actions (for instance, the review of the policy framework) or where we believe we are already demonstrating commitment to fraud risk reduction but are looking at enhancing existing controls.

4.6 The main gap when measuring current controls against the expected commitment within the new legislation is the training regime. Whilst there is an e-learning module, take up is low. The development of a training matrix for higher risk areas and a review of the module will be undertaken as priority actions.

4.7 The SWAP Internal Audit Annual Opinion Report 2024/25 presented to the committee on 2 June 2025 provided the following update on the CiFAS data matching service:

SWAP has paid an annual subscription of £17,215 for 2024/25 to enable Dorset Council to be part of CIFAS. This data matching service will help the Council to both detect and prevent fraud. SWAP, working with both CIFAS and the council have facilitated data matching work in the following areas across the Council:

- *Potential new contractors – all company directors are being searched for potential new contracts.*
- *Insurance – all liability cases are being searched.*
- *Adult Service Users – at the point of a direct payment being agreed a search is undertaken. This includes Powers of Attorney and Finance Agents. Whilst the provision of care cannot be refused the Council can keep a closer watch on cases if a fraud has previously been committed.*
- *Adults Homelessness – applications are being searched, and this can include facial matching where identity documents are*

searched to see if they have previously been used within a fraud.

- *Adults Housing Register - applications are being searched and this can include facial matching.*
- *Licensing – applications for taxi licenses are being searched and this can include facial matching.*
- *All new permanent staff are being searched and if a match is returned this is shared with the hiring manager for a risk assessment to be undertaken.*
- *All new agency staff are being searched and if a match is returned this is shared with the hiring manager for a risk assessment to be undertaken.*
- *Shared Lives Carers – all existing and new applications are searched. New for 2024/25*
- *Senior Officers (Executive Directors, Monitoring Officer and Chief Executive) were searched, and this will be an annual check.*

Data matching has had a positive impact with some matches being identified resulting in an agency worker not being employed, and where insurance claims are being refused where Cifas information has confirmed this is the correct decision. Matches have also been returned within Procurement and Licensing but risk assessments have deemed that the Council proceed with the engagements.

5. Reporting of Fraud and other Protected Disclosures – 2024/25

- 5.1 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](#) (to be superseded by the Protected Disclosure policy included with this report) 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.
- 5.2 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, the Section 151 Officer or via the whistleblowing hotline.
- 5.3 The purpose of the 'Protected Disclosure' 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 contractor or a member of the public.

- 5.4 The table below sets out whistleblowing and fraud activity during 2024/2025, with ten cases reported in the twelve month period (April 24 to March 25), down from fourteen in the previous year:

Ref	Category (Alleged)	Reported by	Via	Summary	Directorate	Status
2024/01	Malpractice, negligent, unprofessional or unethical behaviour	Employee	SWAP	Alleged breach of code of conduct – private work	Place	Not Upheld
2024/02	Malpractice, negligent, unprofessional or unethical behaviour	Employee	Whistleblow hotline	Management Practices	Adults & Housing	Not Upheld
2024/03	Safeguarding and financial irregularities	Member of Public	Whistleblow hotline	Alleged safeguarding issue and potential fraud	Childrens	Not Upheld
2024/04	Financial irregularities (fraud, corruption or unauthorised use of public funds)	External	SWAP	Alleged fraudulent grant claim	Childrens	Not Upheld
2024/05	Malpractice, negligent, unprofessional or unethical behaviour / Financial irregularities (fraud, corruption or unauthorised use of public funds)	Employee	Whistleblow hotline	Circumventing contract procedural rules / bullying	Place	Upheld
2024/06	Health and safety	Member of the Public	Whistleblow hotline	Allegations about health & safety at a commissioned service	Childrens	Not Upheld
2024/07	Malpractice, negligent, unprofessional or unethical behaviour	Member of the public	Complaints e-form	Allegation of polygamous working	Adults & Housing	Not Upheld

Ref	Category (Alleged)	Reported by	Via	Summary	Directorate	Status
2024/08	Malpractice, negligent, unprofessional or unethical behaviour	Member of the public	Complaints e-form	Allegations about an employee.	Place	Not Upheld
2024/09	Financial irregularities (fraud, corruption or unauthorised use of public funds)	Service	Monitoring Officer	Ongoing investigations re commissioned service	Childrens	Open
2024/10	Malpractice, negligent, unprofessional or unethical behaviour	Ex-employee	Monitoring Officer	Ongoing investigations	Adults & Housing	Open

5.5 The case 2024/05 that is marked as upheld was a whistleblow that prompted the investigations by SWAP that have been subject to discussion at this committee on 2 June and 7 July 2025.

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

Financial Year	2024/25	2023/24	2022/23	2021/22
Upheld	1 (10%)	2 (14%)	1 (14%)	
Partially Upheld		3 (21%)		1 (25%)
Not Upheld	7 (70%)	9 (65%)	6 (86%)	3 (75%)
Ongoing	2 (20%)			
Total	10	14	7	4

6. **Policy Framework**

6.1 The portfolio of fraud related policies are reviewed every three years, or more frequently where required. Previously the Council operated a number of separate policies –

- Anti Fraud, Corruption and Bribery Policy;
- Anti Money Laundering Policy
- Whistleblowing Policy

- 6.2 The opportunity has been taken to merge the anti-fraud, corruption and bribery and anti money laundering policy into a single document, to reduce duplication. During this rewrite, the opportunity was also taken to incorporate the risk of tax evasion, which had been identified as a gap in the policy framework. Recognising the new “failure to prevent fraud” offence, the policy also more clearly sets out the Council’s commitment and establishes a compliance matrix to supersede the previous action plan, which forms Appendix A of this report.
- 6.3 As whistleblowing has a wider reach than financial wrong-doing, this has been retained as a separate policy, but clearly linked. The title has however been amended to “Protected Disclosure (Whistleblowing)” policy. Aside from the name change, the policy reinforces more strongly the need for training and awareness.
- 6.4 The Committee are requested to review and endorse these revised policies.

7. **Alternative options considered**

- 7.1 To retain separate policies for Anti Fraud, Bribery and Corruption and Anti Money Laundering and introduce a new Anti Tax Evasion policy. This was discounted however as there was a lot of duplication across policies, and instead this brings all financial crime related processes under a single umbrella.
- 7.2 Consideration was also given to incorporating the Protected Disclosure policy within the new Counter Fraud and Financial Crime policy, but this was discounted because whistleblowing extends beyond financial matters to incorporate wider perceived management practice issues.

8. **Legal considerations**

- 8.1 The revised policy framework considers the Economic Crime and Corporate Transparency Act (ECCTA) 2023, and in particular the corporate offence of “failure to prevent fraud”.

9. **Financial implications**

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

10. **Natural environment, climate & ecology implications**

- 10.1 None

11. **Well-being and health implications**

- 11.1 None

12. **Other implications**

12.1 None

13. **Risk implications**

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

Current Risk: Medium

Residual Risk: Medium

14. **Equalities**

14.1 None

15. **Appendices**

Appendix A – Compliance Matrix

Appendix B – Draft Protected Disclosure (Whistleblowing) Policy

Appendix C – Draft Counter Fraud and Financial Crime Policy

16. **Background papers**

16.1 None

17. **Report sign-off**

17.1 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)

Fraud and Protected Disclosures Compliance Matrix

Appendix A

Theme	Requirement Assessment	2022 SWAP RAG		Further Actions/Status	By Whom	By When	SMA Assess- ment
1) Resources and Communication	1a) The organisation has internal audit and external audit planning aligned to fraud risks. Fraud resources are assessed proportionately to the risk the local authority faces and are adequately resourced	A	* SWAP Internal Audit planning and liaison with External Audit is aligned to fraud risks; * Fraud risks identified and embedded into risk management process, monitored by risk owners alongside other service risks				G
	1b) There is a programme of counter fraud work to ensure a strong counter fraud culture across all departments and delivery agents led by counter fraud experts. There is an annual fraud plan which is agreed by Audit & Governance committee and reflects resources mapped to risks and arrangements for reporting outcomes.	G	* Policy framework for whistleblowing and counter fraud and financial crime; * Annual reporting to Audit and Governance Committee; * Action plan included with annual report, and updated to respond to the new offence of "failure to prevent fraud"; * Outcomes of whistleblowing and fraud investigations included in annual report, with separate investigation reports shared with Audit and Governance Committee as appropriate	Revised policy framework to be reviewed and signed off by Audit and Governance Committee in August 2025	SM for Assurance	Aug-25	G
Page 59	1c) The local authority has put in place arrangements to prevent and detect fraud and corruption and a mechanism for ensuring that this is effective and is reported to committee.	G	* Close working with SWAP's Internal Audit Counter Fraud Team; * CIFAS subscription via SWAP fee; * Sharing of NAFN fraud alerts with relevant services; * Services (such as licencing, revenues, trading standards) work closely with enforcement agencies; * Annual reporting to Audit and Governance Committee				G
	1d) The counter fraud team works jointly with other enforcement agencies and encourages a corporate approach and co-location of enforcement activity	A	* Close working with SWAP's Internal Audit Counter Fraud Team; * CIFAS subscription via SWAP fee; * Sharing of NAFN fraud alerts with relevant services; * Services (such as licencing, revenues, trading standards) work closely with enforcement agencies; * Annual reporting to Audit and Governance Committee * Fraud risk assessment undertaken and embedded within service risk register				G
	1e) The organisation has access to a trained counter fraud resource.	G	* Access to a trained counter fraud resources through the SWAP Internal Audit Services Counter Fraud Team				G
Risk Management	2a) The risks of fraud and corruption are specifically considered in the local authority's overall risk management process.	G	* Fraud risk assessment undertaken and embedded within service risk register, including identification of service specific controls and improvement actions * The Council's Risk Management Strategy has considered fraud risk				G

Fraud and Protected Disclosures Compliance Matrix

Appendix A

Theme	Requirement Assessment	2022 SWAP RAG		Further Actions/Status	By Whom	By When	SMA Assess- ment
	2b) The local authority has made a proper assessment of its fraud and corruption risks, has an action plan to deal with them and regularly reports to its senior Board and its members. Horizon scanning is completed to look for future fraud and corruption risks.	G	* Fraud risk assessment undertaken and embedded within service risk register * Risk is reported quarterly to Audit and Governance Committee, with the risk register also informing the agenda of the scrutiny committees where appropriate * NAFN fraud alerts shared with relevant services				G
Policy Related	3a) The local authority has put in place arrangements for monitoring compliance with standards of conduct across the local authority covering: Codes of conduct including behaviour for counter fraud, anti-bribery, and corruption; Register of interests; Register of gifts and hospitality; and Members and staff are aware of the need to make appropriate disclosures of gifts, hospitality, and business. This is checked independently.	A	* Codes of Conduct for Officers and Members, including declaration of interest and reference to fraud; * Councillor e-form for declarations of interest; * Revision to Home and Hybrid working principles and associated communications re-inforced employee declarations of interest (June 25)	A declaration process for staff is in development	Monitoring Officer	tbc	A
	3b) There are employee and member Code of Conducts in place, which include reference to fraud.	G	* Codes of Conduct for Officers and Members, including declaration of interest and reference to fraud;				G
	3c) The organisation has an appropriate and approved Anti-Fraud and Corruption Policy available to stakeholders.	G	* Policy framework for whistleblowing and counter fraud and financial crime;				G
	3d) There is a counter fraud and corruption strategy applying to all aspects of the local authority's business which has been communicated throughout the local authority and acknowledged by those charged with governance. There is a zero-tolerance approach.	G	* Policy framework for whistleblowing and counter fraud and financial crime; * Clear statement of zero tolerance to fraud				G
	3e) The organisation has an appropriate and approved money laundering policy available to stakeholders	G	* Policy framework for whistleblowing and counter fraud and financial crime, which incorporates money-laundering				G

Fraud and Protected Disclosures Compliance Matrix

Appendix A

Theme	Requirement Assessment	2022 SWAP RAG		Further Actions/Status	By Whom	By When	SMA Assess- ment
	3f) There is an independent and up-to-date whistleblowing policy which is monitored for take up and can show that suspicion	G	* Policy framework for whistleblowing and counter fraud and financial crime; * Reporting of whistleblowing numbers is included in the Annual Report				G
	3g) Counter fraud staff are consulted to fraudproof new policies, strategies, and initiatives across departments and this is reported upon to committee.	G	* Policy framework is reviewed and updated by Service Manager for Assurance; * Policy framework considered and approved via Audit and Governance Committee; * Policies are subject to clearance process, ensuring review with Monitoring Officer and S151				G
Page 61	3h) Contractors and third parties sign up to the whistleblowing policy and there is evidence of this. There should be no discrimination against whistle-blowers.	G	* Policies are clear in that they apply to contractors and third parties, and can be accessed via the external website; * Legal Services have included reference to the policy in the terms and conditions of the contracts and reference to it is in the Procurement Document / Invitation to Tender; * There is a link to the policy on Selling to Dorset Council on the Dorset Council website; * Whistleblowing policy and supporting comms reinforces the safeguards contained in the Public Disclosure Act				G
Committee Related	4a) Audit Committees and Portfolio Lead roles in relation to fraud management are agreed and understood, including: Awareness and support counter fraud activity (including proactive and reactive) and receive training to support them; Receiving of regular reports on the work of those leading on fraud; Supporting counter fraud work and challenges the level of activity to ensure it is appropriate in terms of fraud risk and resources.	A	* An annual fraud and protected disclosure report is presented to Audit and Governance Committee; * The Chair of the Audit and Governance Committee is identified as the member anti-fraud champion; * Fraud and whistleblowing training is available via e-learning module, but is not mandatory.	Develop training matrix to identify officer/councillor roles that are higher risk and should be subject to formal training	SM for Assurance	Sep-25	A

Fraud and Protected Disclosures Compliance Matrix

Appendix A

Theme	Requirement Assessment	2022 SWAP RAG		Further Actions/Status	By Whom	By When	SMA Assess- ment
Culture & Awareness	5a) The organisation educates and trains employees regarding the importance of ethics and anti-fraud programs and senior management exhibit and encourage ethical behaviour.	A	* Fraud and whistleblowing training is available via e-learning module, but is not mandatory; * Awareness training from periodic intranet communications	Develop training matrix to identify officer/councillor roles that are higher risk and should be subject to formal training Inclusion of awareness on whistleblowing within induction programme Review of e-learning module content	SM for Assurance	Oct-25	A
Page 62	5b) The local authority has arrangements in place that are designed to promote and ensure probity and propriety in the conduct of its business.	G	* Whistleblowing and Fraud policy portfolio; * Code of conduct, including declarations of interest and reference to fraud; * Annual Governance Statement; * Annual reporting to Audit and Governance Committee on Fraud and Whistleblowing; * Financial Procedural Rules; * Contract Procedural Rules; * Guidance on the intranet, supported by periodic promotion	Consider implementation of a Governance Group, to support revised CIPFA/Solace guidance on Annual Governance Statement wef 25/26 financial year reporting; Respond to findings from SWAP investigations	SM for Assurance SLT	Sep-25	G
	5c) Relevant staff and members are up to date with latest anti-fraud practice and trends in fraud.	A	* SWAP and NAFN Fraud Alerts shared as appropriate to relevant services; * Member of CiFAS				G
	5d) The organisation routinely publicises successful cases of proven fraud and corruption to raise awareness; this is endorsed by the communications/ media team	A	* Upheld cases considered for promotion on a case by case basis				G
	5e) The local authority undertakes recruitment vetting of staff prior to employment by risk assessing posts and undertaking the relevant checks.	A	* CiFAS data matching for agency staff / new employees; * CiFAS checkin annually for SLT	Consider whether more frequent checks should be undertaken on staff (post recruitment), as suggested by best practice	SLT	tbc	G

Fraud and Protected Disclosures Compliance Matrix

Theme	Requirement Assessment	2022 SWAP RAG		Further Actions/Status	By Whom	By When	SMA Assess- ment
	5f) *New* The local authority fosters a culture of integrity and anti-fraud commitment from senior leadership		* Fraud has recently been incorporated within the remit of the Strategic Information Governance Board, with escalation to SLT via the Chair/Monitoring Officer; * Internal controls around fraud are identified within the Annual Governance Statement and supporting Local Code of Corporate Governance	Consider implementation of a Governance Group, to support revised CIPFA/Solace guidance on Annual Governance Statement wef 25/26 financial year reporting, including the interface with Audit and Governance Committee and Portfolio Holder;	SM for Assurance	Sep-25	A
Reporting, Investigating & Monitoring	6a) Statistics are kept and reported which cover all areas of activity and outcomes. Are number of investigations and outcomes recorded.	G	* Annual fraud and whistleblowing report is submitted to Audit and Governance Committee, including stats; * Database maintained by the Service Manager of Assurance				G
Page 63	6b) All allegations of fraud and corruption are risk assessed.	G	* The concept of risk assessing allegations was considered together with the Portfolio lead and Audit and Governance Committee (pre May 24 elections and change of administration). It was determined as being counterproductive to demonstrating a zero tolerance to fraud. * Service Manager for Assurance and the Monitoring Officer review the seriousness of the allegations before calibrating the appropriate resources, making sure the investigations teams have the right expertise				G
	6c) Prevention measures and projects are undertaken using data analytics where possible and sharing of data across internal departments and between other enforcement agencies.	A	* The Council takes part in the bi-annual NFI data matching exercise; * Dorset Council are members of CiFAS, via the SWAP internal audit partnership. This facilitates data sharing in relation to Fraud across a number of service areas.				G
	6d) The organisation provides an anonymous way to report suspected violations of the ethics and anti-fraud programs.	A	* Fraud/Whistleblowing hotline and email in place and monitored by the Service Manager for Assurance; * Monitoring by Data Protection Officer and Complaints Manager (in absence of Service Manager)				G
	6e) Fraud incidents are promptly and thoroughly investigated by a designated and qualified resource, with unfettered access to premises and documents for the purposes of counter fraud investigation.	A	* Investigation process clearly set out in the policy framework; * Commissioning of SWAP specialist fraud team for higher risk investigations	Formalise a lessons learnt process, to be embedded into the workings of the Organisational Compliance and Risk Learning Group	SM for Assurance	Sep-25	G

Fraud and Protected Disclosures Compliance Matrix

Theme	Requirement Assessment	2022 SWAP RAG		Further Actions/Status	By Whom	By When	SMA Assess- ment
	6f) There is a fraud and corruption response plan which covers all areas of counter fraud work: – prevention – detection – investigation – sanctions – redress	G	* Covered within policy framework				G

Protected Disclosures (Whistleblowing) Policy



Contents

Contents

1. Introduction	2
2. Raising a Concern	4
3. What Action Will the Council Take?	6
4. Support to Whistleblowers.....	7
5. External Disclosures	8
6. Key Roles and Responsibilities	9



1. Introduction

- 1.1 Dorset Council is committed to achieving high standards of integrity and accountability and expects the same commitment from all of its employees and others working for and with the council.
- 1.2 We aim to provide an open environment so that employees and those working for the Council can raise issues that they believe to be in the public interest, with the confidence that they will be acted upon appropriately. The Council is committed to a culture in which individuals with serious concerns can feel confident that in raising those concerns they will be protected from any detrimental treatment, such as victimisation and/or harassment.
- 1.3 The Protected Disclosure (Whistleblowing) Policy describes the Council's commitment to supporting and protecting whistleblowers; the steps that you should take if you wish to blow the whistle on serious wrong-doing in the workplace (known as making a "protected disclosure"); and how the Council will respond. It is also important for potential whistleblowers to understand that their employment will be protected by the Council on the strict assumption that any disclosures or allegations are not malicious in nature.
- 1.4 This procedure complies with the Public Interest Disclosure Act 1998 and the Enterprise and Regulatory Reform Act 2013.
- 1.5 Concerns raised under this policy can include:
 - Failure to observe health and safety regulations, or actions which involve risks to the public or other employees;
 - Financial irregularities - including fraud, corruption or unauthorised use of public funds;
 - Conduct which is unlawful;
 - Action causing major harm to the environment;
 - Employees claiming benefits to which they are not entitled;
 - Sexual, racial, physical or other abuse of service users;
 - Other causes of malpractice, negligent, unprofessional or unethical behaviour;
 - Concealment of any of the above.



- 1.6 The Council will support and protect whistleblowers who raise a concern under this policy, in accordance with the safeguards contained in the Public Interest Disclosure Act.
- 1.7 Allegations should only be made where the whistleblower reasonably believes that the disclosure is in the public interest.
- 1.8 All reported wrong-doings will be treated in absolute confidence, with every effort made by the Council not to reveal a whistleblower's identity if they so wish. However, it may be necessary for a whistleblower to become an identified witness at an appropriate time, particularly if it has not been possible to substantiate the allegations by other means. The implications of this, together with the appropriate support/protection arrangement, will be discussed with the whistleblower.
- 1.9 Whistleblowers are encouraged to put their name to allegations. Anonymous allegations will be investigated but are much less powerful and are more difficult for the Council to act upon.
- 1.10 If the Council finds that allegations have been made maliciously or for personal advantage, action will be taken against an employee making the allegation in accordance with the Council's disciplinary policies.
- 1.11 This policy is not a substitute for the council's other policies and procedures on matters such as personal grievances, bullying and harassment, health and safety, safeguarding issues (children and/or adults) or complaints. It should also not be used to raise matters relating to an employee's own terms and conditions of service.
- 1.12 This policy and procedure applies to all council employees and other workers (regardless as to whether they remain employed by the Council at the time that the whistleblow is made); including freelance staff; temporary and agency staff; trainers; volunteers; consultants; and contractors. It will be published to ensure that it is available and easily accessible to all such groups.
- 1.13 The spirit of this policy and the procedure will also be applied to all employees in organisations who work in partnership with the Council or who supply goods and services to the Council, recognising though that these are not employees of the Council (and therefore not a 'protected disclosure').
- 1.14 It will also be applied in spirit to elected members of the Council, recognising though that they have separate and distinct roles as the elected



representatives of their communities who operate within a political environment. Elected members to whom the whistle is blown should in the first place contact the Monitoring Officer.

- 1.15 Members of the public may also have serious concerns about which they wish to “blow the whistle”. As they are not employees, members of the public cannot suffer detriment in their employment as a result of whistleblowing. Again though, it is important the spirit of this policy and procedure is applied so that service users are not discouraged from coming forward and raising serious concerns for fear that they will receive a lower level of service in the future.
- 1.16 For the sake of clarity this policy is not to be used by members of the public to pursue complaints about individual service delivery. Instead, these should be referred to and dealt with through the council’s complaints procedure

2. Raising a Concern

- 2.1 There is an obligation on every one of us to raise serious issues of concern so that they can be addressed. This procedure describes how you should do this if you wish your concerns to be treated as a “protected disclosure”.
- 2.2 The Council’s Code of Conduct for employees makes it clear that employees who have serious concerns about aspects of work, or practices which affect the integrity of the Council, or safety of its employees or the general public, must come forward and voice these concerns.
- 2.3 When you raise an issue, you must do this in writing. You can write anonymously but the Protected Disclosure (Whistleblowing) Policy is intended to give you the confidence to put your name to your concerns.
- 2.4 It is important to make it clear that the issue is being raised under the Protected Disclosure (Whistleblowing) Policy. Concerns such as complaints or safeguarding (children or adults) issues should be raised under those specific policies.
- 2.5 In the first instance you should normally raise issues and concerns with your line manager. There may though be instances where the seriousness of your concerns, or the involvement of your line manager, mean that you need to go



straight to your Service Manager, Head of Service or Corporate Director. In the most serious cases or where you do not feel able to raise concerns within your own directorate then you can also make a direct disclosure to:

- Confidential reporting line: 01305 225009 (this includes an out of hours messaging service) – whistleblowingdc@dorsetcouncil.gov.uk
- The 'Monitoring Officer' (Director for Legal and Democratic)
- The 'Chief Financial Officer' / Section 151 Officer (Executive Director for Corporate Development)
- The Chief Executive

Contact details for the Monitoring Officer; Chief Financial Officer; and Chief Executive are held on the [internal intranet](#).

- 2.6 Managers who receive whistleblowing complaints or allegations must ensure that they are referred immediately to the Monitoring Officer.
- 2.7 It is important for managers to understand that a complaint or allegation may fall within the scope of this policy and procedure even though the employee might not actually write that they are “whistleblowing” or making a “protected disclosure”. Managers must recognise the nature of the complaint and if it is within the scope of this policy and procedure then it must be referred to the Monitoring Officer.
- 2.8 The Monitoring Officer will then ensure that any appropriate subsequent notifications are made to others. For example, in the case of a financial irregularity (e.g. fraud, corruption or unauthorised use of public funds), the Council’s Section 151 Officer (Chief Financial Officer) must also be informed.
- 2.9 In some situations, you may wish to take advice from and/or involve a colleague or Trade Union representative. The Council welcomes this involvement as it can help to give you the confidence to raise concerns that you might not otherwise feel able to disclose to senior management.
- 2.10 Employees raising concerns under this policy and managers to whom allegations are disclosed must maintain confidentiality in all areas, including among service users and other employees.



3. What Action Will the Council Take?

- 3.1 Depending on the nature of the alleged wrong doing, the Council will arrange for the matter to be:
- Investigated internally by directorate management, or a senior manager from another directorate, or by another independent professional;
 - Referred to audit (internal or external) to be investigated; and/or
 - Referred to the appropriate external enforcement agency (e.g. Police, Health and Safety Executive, Environmental Agency, or the appropriate Government Department).
- 3.2 The Monitoring Officer (or the Service Manager of Assurance on their behalf) will write to you (the whistleblower) within 10 working days of the concern being raised to acknowledge receipt of the issue and to indicate how the Council proposes to deal with the matter.
- 3.3 Investigations will be planned and controlled to ensure a thorough and speedy conclusion. The Monitoring Officer (or the Service Manager of Assurance on their behalf) will oversee the process to ensure that this is achieved.
- 3.4 When the issue raised is about another employee's conduct, following an initial investigation under the Protected Disclosure (Whistleblowing) Policy, the matter may then be dealt with by management as part of an appropriate HR procedure (e.g. Fairness and Dignity at Work, Disciplinary or Capability Procedure etc.)



- 3.5 When considering anonymous allegations, the Council will take the following factors into account:
- The seriousness of the matter raised.
 - The credibility of the allegation.
 - The likelihood of obtaining information which could confirm the allegation.
- 3.6 In some situations, urgent action may need to be taken prior to any investigation process (e.g. to protect the safety of individuals, or if immediate action is needed to secure relevant information etc.).
- 3.7 The investigating officer will provide you with initial feedback on the actions being taken and the likely timescales within 20 working days of the complaint being made. Thereafter, feedback will be provided on an agreed regular basis.
- 3.8 Subject to any legal constraints, the Council will inform you of the outcome of the investigation although clearly it will not be possible to do this if the whistleblower is determined to remain anonymous. In most cases, this will be to inform you if the allegations have been upheld, partly upheld, or not upheld.
- 3.9 If when you are informed of the response to the allegation you have raised you are dissatisfied, you should put your concerns in writing to the Chief Executive within 20 working days of receipt of the correspondence, who will arrange for these to be reviewed.

4. Support to Whistleblowers

- 4.1 The Council will identify an individual to provide support and advice to you throughout the investigation process.
- 4.2 Similarly, a contact/liaison officer will be provided to an employee under investigation as part of a whistle-blowing complaint.



- 4.3 If you feel victimised or harassed or believe that you have suffered any other detriment as a result of raising a concern in accordance with this procedure, then you should advise the person identified in 4.1 and/or the Monitoring Officer. You are actively encouraged to raise concerns directly with these individuals if you feel dissatisfied with the application of this policy.
- 4.4 A free, personal and confidential counselling service is available to all council employees.

5. External Disclosures

- 5.1 If you are dissatisfied with the Council's response through its internal procedures, then you should consider contacting an external organisation. These could include:
- External Auditor
 - Health and Safety Executive
 - Ofsted
 - Care Quality Commission (CQC)
 - Environmental Agency
 - Her Majesty's Revenue & Customs (HMRC)
 - Public Concern at Work
- 5.2 Advice should be taken before making an external disclosure and, under normal circumstances, the internal procedure should have been followed first.
- 5.3 The Council has established this policy and procedure as a means of enabling its employees to raise serious concerns in a way that protects them from any detriment. In doing so the clear expectation is that you follow the Whistleblowing Policy and Procedure and must not make disclosures through the media (e.g. the press and/or internet, social media etc.)
- 5.4 The Public Interest Disclosure Act 1998 provides some employment protection rights to individuals who 'blow the whistle' outside their organisation. However, the types of information and the situations in which concerns are disclosed externally are tightly defined in the legislation. The Act only protects those making disclosures which are considered to be in the public interest. As such, the Council reserves the right to take action against any employee where an inappropriate external disclosure is made. This would include, for example, cases when an allegation has made maliciously



or for personal advantage or direct to the media without any attempt to address issues through the whistle-blowing policy and procedure.

6. Key Roles and Responsibilities

6.1 Employees / Councillors –

- Will ensure that they raise serious concerns about any aspects of work and/or practices which affect the integrity of the council and/or the safety of employees or the public.

6.2 All Managers –

- Will ensure that their members of staff (including agency staff, consultants, contractors, volunteers etc) are aware of and follow approved council procedures (e.g. financial regulations; health and safety etc.);
- Will register any whistle-blowing cases brought to their attention immediately with the Monitoring Officer;
- Will respond to whistle-blowing submissions positively within the timescales set out within this policy;
- Will ensure that they are appraised of the Council's whistleblowing arrangements. Managers are encouraged to undertake the whistleblowing training available via the learning hub.

6.3 Monitoring Officer –

- Will take overall responsibility for overseeing the appropriate application and ensure adherence to the requirements of the Whistleblowing policy and procedures;
- Will maintain a record of all whistle-blowing allegations
- Will respond to the whistle-blower within 10 working days of receiving an allegation;
- Will provide proactive support and advice to managers as required; including attendance at meetings as necessary;
- Will ensure that this policy is subject to formal review on a regular basis.

6.4 Strategic Information Governance Board –

- Have an overview of whistleblowing activity, at least once annually, ahead of reporting to Audit and Governance Committee;
- Will ensure that an appropriate training regime is available;



- Will ensure that appropriate mechanisms are in place to raise awareness to employees, councillors and managers of the Council's whistleblowing arrangements.

Policy Owner - Marc Eyre, Service Manager for Assurance

Date Approved: Audit & Governance Committee [[Presentation to Audit & Governance Committee 04.08.25](#)]

Review Date: August 2028



This page is intentionally left blank

Counter Fraud and Financial Crime Policy

Annual Fraud and Protected Disclosures Report

Incorporating: anti-fraud; corruption; bribery;
anti-money laundering; anti-tax evasion



Dorset
Council

Contents

1. Introduction	2
2. Reporting.....	6
3. Investigation Process.....	8
4. Anti-Fraud, Corruption and Bribery	9
5. Anti Money Laundering.....	9
6. Corporate Criminal Offence / Anti-Tax Evasion Policy	11
7. Key Roles & Responsibilities.....	14



1. Introduction

- 1.1 The purpose of this policy is for the Council to set out clearly for Councillors, employees, contractors, the Council's partners and the public:
- Its commitment to tackling fraud and other financial crimes;
 - The actions it promotes to prevent any such acts;
 - The responsibilities of Members and employees in minimising the risk of fraud and other financial crimes and reporting any suspicions they may have.
- 1.2 This unified policy consolidates Dorset Council's approach to preventing and responding to fraud, bribery, corruption, money laundering, and tax evasion. It reflects the Council's zero-tolerance stance and commitment to compliance with relevant legislation including the Fraud Act 2006, Bribery Act 2010, Proceeds of Crime Act 2002, Criminal Finances Act 2017, and the Economic Crime and Corporate Transparency Act 2023.
- 1.3 The Fraud Act 2006 created a general criminal offence of fraud and identifies three specific ways in which it can be committed, carrying a maximum penalty of 10 years of imprisonment:
- Fraud by false representation
 - Fraud by failing to disclose information
 - Fraud by abuse of position
- 1.4 The Act also created four related criminal offences of:
- Possession of articles for use in frauds
 - Making or supplying articles for use in frauds
 - Participating in fraudulent business
 - Obtaining services dishonestly
- 1.5 The Theft Act 1968 and the Forgery and Counterfeit Act 1981 define offences of:
- Theft
 - False Accounting
 - Forgery



- 1.6 The Bribery Act 2010 defines bribery as “giving someone a financial or other advantage to encourage that person to perform their functions or activities improperly or to reward that person for having already done so.” There are four key offences under the Act:
- Bribery of another person
 - Accepting a bribe
 - Bribing a foreign public official
 - A corporate offence of failing to prevent bribery
- 1.7 The Proceeds of Crime Act 2002 and the Terrorism Act 2000 place obligations on the Council and its employees with respect to suspected money laundering and makes it a criminal offence to help a criminal ‘launder’ the proceeds of crime. Money laundering is the disguising of the source of money, either in cash, paper or electronic form to conceal that the money has originated from crime, or that is to be used in the pursuit of future crime.
- 1.8 The Economic Crime and Corporate Transparency Act 2023 creates a new corporate offence of failure to prevent fraud, enhances transparency of company ownership, tightens regulations on limited partnerships, and expands powers for law enforcement and regulators to tackle illicit finance.
- 1.9 Fraud, alongside wider financial crimes, is a serious matter that affects both the council and the local area. It can have a direct impact on the level of council tax, the level of resources available to share amongst our community and local services such as housing, social care and education. Dorset Council is committed to achieving high standards of integrity and accountability and expects the same commitment from employees and others working for and dealing with the council. Proper accountability, achieved through probity, internal control and honest administration is therefore an essential aspect of public service.
- 1.10 The Council operates a zero-tolerance culture to fraud and other financial crimes and is committed to minimising the risks to an acceptable level and will deal with any cases robustly. This policy sets the clearest message to the Council’s stakeholders the importance that the Council places on its responsibility for the effective stewardship and safeguarding of public funds.
- 1.11 We all have a special responsibility for dealing with public funds and assets. The Council takes very seriously its important stewardship role and, as such, is committed to meeting the high expectations and scrutiny to which the affairs of the Council are quite rightly subject.



- 1.12 This policy and supporting procedures apply to all Councillors, council employees (including school based staff), volunteers, agency workers and any other stakeholders working on behalf of the Council.
- 1.13 It supersedes the following separate policies:
- Anti-fraud, corruption and bribery strategy 2022 to 2025; and
 - Anti-money laundering policy 2022 to 2025
- 1.14 Thankfully acts of dishonesty associated with Dorset Council is rare and our zero-tolerance approach provides our clear and continuing commitment to dealing with any acts robustly. Widely recognised national guidance in terms of an effective fraud strategy provides three key themes to help focus the public sector approach to eliminating fraud. The Council is fully committed to each of these:
- Acknowledge – Establishing a clear recognition that fraud happens and have an understanding of fraud risks.
 - Prevent – The active prevention and detection of fraudulent activity.
 - Pursue – Being stronger in seeking to punish fraudulent activity and recovering losses.
- 1.15 The Council's key principles in respect of fraud and other financial crime can be summarised as follows:
- Take a zero-tolerance approach to any such matters;
 - Introduce appropriate measures designed to minimise the risk;
 - Operate a procedure to enable genuine concerns to be reported and to protect those who do so;
 - Adopt formal procedures to investigate situations when it is suspected;
 - Aim to reduce losses to an absolute minimum;
 - Work closely with the Police (and other appropriate agencies) to combat fraud and seek appropriate redress through legal proceedings;
 - Use powers to work with others and share information to identify potential areas of concern;
 - Deter people from making malicious or unfounded accusations;



- The Council also expects that any individual, associated or outside organisations;
 - including suppliers, contractors and claimants, will act honestly in their dealings with the Council;
 - Where concern exists that this is not the case, the Council actively encourages any such matters to be reported.
- 1.16 This policy is supplemented by Our Values and our Code of Conduct for Employees. Our Values are an integral part of the recruitment and selection process for all employees of Dorset Council, and can be found [on the intranet](#). The code of conduct is also [on the intranet](#), and compulsory reading for all employees of Dorset Council.
- 1.17 The Council also has procedures in place for segregation of duties where appropriate to counter fraud and ensure there are no situations of unfettered power. Members and senior officers provide the high-level commitment to such risk-based prevention procedures with are supported by service directors. The S151 officer promotes the “no Tolerance” stance through work undertaken by Internal Audit who have a role to promote compliance with counter fraud arrangements and raise awareness amongst staff.
- 1.18 In recognising the new corporate offence of “failure to prevent fraud” within the Economic Crime and Corporate Transparency Act 2023, the Council is committed to the following:
- To maintain and demonstrate a zero tolerance approach and a robust response to fraud and other financial crimes;
 - To regularly review and update procedures to reflect changes in risk and legislation, every three years and more regularly where required;
 - To undertake regular risk assessments to identify areas where the risk of fraud is highest, particularly in relation to third-party relationships, procurement, and financial transactions. These assessments will inform the design and implementation of proportionate prevention procedures;
 - Ensure that all employees, contractors, and associated persons are aware of their responsibilities through training and communication;
 - Provide targeted training to staff in high-risk roles;
 - Enable an appropriate identification and monitoring regime, via internal reporting requirements (including whistleblowing); use of proportionate fraud identification processes (including consideration of any technology



to improve detection); and proportionate risk based coverage within the internal audit plan;

- To collaborate and data share with other agencies, where appropriate;
- Include anti-fraud clauses in contracts with suppliers and service providers; and
- Conduct due diligence on third parties, including verification of beneficial ownership and financial standing.

1.19 A fraud and financial crimes compliance matrix will be maintained and reported annually to the Senior Leadership Team and Audit and Governance Committee. This will include an improvement action plan. Any gaps in compliance will be reported within the Annual Governance Statement.

1.20 Where fraud or other financial crimes are identified, the Council will:

- Take immediate action when detection occurs;
- Maintain a capability and capacity to investigate;
- Make effective use of legislation and civil redress to ensure recovery;
- Effectively collaborate with all other public sector organisations;
- Publicise successful prosecutions.

2. Reporting

2.1 Although prevention is the most efficient and effective way to address fraud and other financial crimes, it is acknowledged that despite best efforts, the Council may not always be successful in achieving this. Therefore, if anyone has a reasonable concern or suspicion that any such acts may be occurring, they must report them.

2.2 We aim to provide an open environment so that anyone can raise issues that they believe to be in the public interest, with the confidence that they will be acted upon appropriately. Therefore, those raising any such concerns are actively encouraged to do so and can have confidence that they will be protected from any detrimental treatment, such as victimisation and/or harassment. This is known as making a protected disclosure, or whistleblowing.

2.3 This policy should therefore be read in conjunction with the Council's Whistleblowing and Protected Disclosure policy and procedures which set out how those working on behalf of the Council can make a protected disclosure on fraud and other financial crimes, alongside wider management failings. It includes contact details for officers, and a mechanism for issues to be raised



in confidence, and anonymously if appropriate. Details will not be shared wider than the officer reported to, without consent. **[LINK TO PROTECTED DISCLOSURE POLICY ONCE PUBLISHED]**

- 2.4 The Council's Financial Regulations specifically require that cases of suspected financial irregularity are reported to the Chief Financial Officer. Concerns should be reported, without delay, to a line manager or more senior directorate manager. In the first instance you should normally raise concerns with your line manager, who will report to the Chief Financial Officer. There may though be instances where the seriousness of your concerns, or the suspected involvement of your line manager, means you need to go straight to your service manager, head of service or director. In the most serious of cases, or where you do not feel able to raise concerns within your own directorate, then you can also make a direct disclosure to:

- **Chief Financial Officer**
- **Monitoring Officer**
- **Chief Executive**

Contact details for the Monitoring Officer; Chief Financial Officer; and Chief Executive are held on the [internal intranet](#).

- 2.5 In the event that you suspect money laundering activity, this must be reported promptly to the Chief Financial Officer, as the nominated Money Laundering Reporting Officer (MLRO). If you would prefer, you can discuss your suspicions with the MLRO first.

- 2.6 Reporting should be subject to 'official sensitive' labelling and should include:

- Your name, post title, service / directorate, contact number and email address;
- Name(s) and address(es) of persons suspected of the offence (if a company / public body please include details of the nature of business);
- The nature, value and timing of the suspected activity (please include full details of the contact with the council - what; where; when; how; and who)

- 2.7 Employees must follow any direction and/or guidance given by the Monitoring Officer, Chief Financial Officer (or their appointed representatives) and must not themselves make any further enquiries into the matter. They must not take any further steps in any related transaction without authorisation.

- 2.8 Although people are actively encouraged to report their concerns through the internal procedures and can be confident that they can do so with appropriate protection, in rare cases where this is not considered to be possible, then concerns can be raised through the following channels:



- The Council's Confidential 'Fraud Hotline' – 01305 225009 / whistleblowingdc@dorsetcouncil.gov.uk
 - External Audit
 - SWAP Internal Audit
- 2.9 When cases are reported, the Council is committed to objectively considering the concerns raised and, where appropriate, investigating and/or referring the matter to the appropriate authorities.
- 2.10 The employee must not disclose or otherwise indicate their suspicions to the person suspected of the fraud or financial crime. They must not discuss the matter with others or note on the file that a report has been escalated in case this results in the suspect becoming aware of the situation.

3. Investigation Process

- 3.1 The investigation of fraud and other financial crimes is a complex and specialist area. It is important that any potential evidence that may be associated with the concerns is collected in a way that complies with the relevant legislation and does not compromise actions to be taken if fraud is established. It, therefore, usually requires the involvement of specially trained staff to either advise, or to consider the requirement for, and/or to conduct, any subsequent investigations. Certain staff have various rights accorded to them under the 'Accounts and Audit Regulations', to access all necessary documents, records and information and to seek explanations from any member of staff.
- 3.2 Appendix A sets out the Fraud and Financial Crimes Response Plan that will be adopted as the investigation process.
- 3.3 Any decision to refer an investigation to the Police will be taken by the Council's Section 151 Officer / Chief Financial Officer, in consultation with the Chief Executive. Officers will be subject to appropriate action, in accordance with the Council's disciplinary procedures, if there is evidence that they have been involved in any such activities in addition to any appropriate criminal proceedings, dependent upon the circumstances and the advice of the Police.
- 3.4 The Council's Communications Team will also need to be consulted and used to help manage any publicity associated with any proven cases. This will include where any financial loss has occurred, and actions taken to seek recovery and/or redress. Any such publications will be discussed with the Council's Section 151 / Chief Financial Officer and approved prior to their release.



4. Anti-Fraud, Corruption and Bribery

4.1 Fraud can be defined as any intentional false representation, including a failure to declare information or abuse of position that is carried out to make a gain, cause loss or expose another to the risk of loss. It can be used to describe many acts such as:

- **Deception:** Causing someone to accept as true or valid what is false or invalid;
- **Bribery:** Offering someone money or something valuable in order to persuade them to do something for you
- **Forgery:** Copying a document, signature etc in order to deceive
- **Extortion:** Using violence, threats, intimidation, or pressure from one's authority to force someone to hand over money or something valuable
- **Corruption:** Offering, giving or accepting an inducement or reward which would influence the actions taken
- **Conspiracy:** A plan or agreement formulated by two or more persons to commit an unlawful, harmful, or treacherous act
- **Embezzlement:** Theft or misappropriation of funds placed in one's trust or belonging to one's employer
- **Misappropriation:** The wrongful, fraudulent or corrupt use of other's funds in one's care
- **False representation:** An untrue or incorrect representation regarding a material fact that is made with knowledge or belief of its inaccuracy
- **Concealment of material facts:** The act of hiding or not putting forward any relevant fact that should to be revealed
- **Collusion:** The act of doing something secret or illegal with another person, company, etc. in order to deceive people

4.2 The Council can be exposed to fraud and corruption through a variety of internal and external sources. It can involve anyone that is employed by or on behalf of the Council or anyone or group that has a relationship with the Council either as a supplier, contractor, customer, or service user. This means that fraud could be committed by any one of the thousands of people that the Council deals with on a daily basis.

4.3 Should staff or associates be concerned that another employee or associate is committing fraud, or engaged in corruption or bribery, this should be reported as per reporting arrangements set out in Section 2 of this policy.

5. Anti Money Laundering

5.1 Money laundering is the term used for a number of offences involving the proceeds of crime or terrorism funds. The following acts constitute the act of



money laundering:

- Concealing, disguising, converting, transferring criminal property or removing it from the UK (section 327 of the Proceeds of Crime Act 2002);
- Entering into or becoming concerned in an arrangement which you know, or suspect facilitates the acquisition, retention, use or control of criminal property by or on behalf of another person (section 328); or
- Acquiring, using or possessing criminal property (section 329).

These are the primary money laundering offences and are thus prohibited acts under the legislation.

5.2 There are also two secondary offences:

- Failure to disclose any of the three primary offences; and
- Tipping off - This is where someone informs a person or people who are, or are suspected of being involved in money laundering, in such a way as to reduce the likelihood of them being investigated or prejudicing an investigation.

5.3 Any member of staff could potentially be caught by the money laundering provisions, if they suspect money laundering and either become involved with it in some way and/or do nothing to raise their concerns about it. Should staff or associates become aware of potential money laundering this should be reported as per reporting arrangements set out in Section 2 of this policy.

5.4 While the risk to the Council of contravening the legislation is low, it is important that all employees are familiar with their responsibilities as serious criminal sanctions may be imposed for breaches of the legislation. The key requirement on employees is to promptly report any suspected money laundering activity to the Council's appointed Money Laundering Reporting Officer (MLRO).

5.5 When cases are reported, the MLRO is committed to objectively considering the concerns raised on behalf of the Council and, where appropriate, investigating and/or referring the matter to the appropriate authorities. The MLRO will commit a criminal offence if they know or suspect, or have reasonable grounds to do so, through a disclosure being made to them, that another person is engaged in money laundering and they do not disclose this as soon as practicable to the appropriate external authorities.

5.6 No payment to the Council will be accepted in cash if it exceeds £5,000. (NB: Cash is defined as including notes, coins or travellers' cheques in any currency).



- 5.7 The Client Identification Procedure must be followed as set out below before any business is undertaken for that client where the Council is carrying out 'relevant business' and, as part of this:
- forms an ongoing business relationship with a client; or
 - undertakes a one-off transaction involving payment by or to the client of 15,000 Euros (or the equivalent in Sterling) or more; or
 - undertakes a series of linked one-off transactions involving total payment by or to the client(s) of 15,000 Euros (or the equivalent in Sterling) or more; or
 - it is known or suspected that a one-off transaction (or series of them) involves money laundering;
- 5.8 'Relevant Business' is defined as the provision 'by way of business' of: advice about tax affairs; accounting services; audit services; legal services; services involving the formation, operation or arrangement of a company or trust; or dealing in goods wherever a transaction involves a cash payment of 15,000 Euros or more.)
- 5.9 Where the 'relevant business' is being provided to another public-sector body, then you must ensure that you have signed, written instructions on the body's headed paper before any business is undertaken.
- 5.10 Where the 'relevant business' is not a public-sector body, then you should seek additional evidence of identity, for example:
- Checking with the organisation's website to confirm their business address;
 - Conducting an on-line search via Companies House;
 - Seeking evidence from the key contact of their personal identity and position within the organisation.
- 5.11 Where 'relevant business' is carried out then the client identification evidence and details of the relevant transactions(s) for that client must be retained for at least five years.

6. Corporate Criminal Offence / Anti-Tax Evasion Policy

- 6.1 Dorset Council conducts its financial affairs in a law-abiding manner and does not tolerate tax evasion in any form. The Criminal Finances Act 2017 (hereafter referred to as "the Act") was implemented by HMRC to foster co-



operative monitoring and self-reporting of criminal activity related to facilitating tax evasion. Under the Act, if Dorset Council is found to be facilitating tax evasion, it could face an unlimited fine and damage to its reputation. The Council will be guilty of the offence where a third party commits tax evasion, aided by a Dorset Council member of staff (or a contractual associate) unless the Council can establish a defence. This policy is one part of that defence.

- 6.2 To prevent tax evasion, Council staff (and contracted associates) should follow Council policies, procedures and the code of conduct; report to management if there is suspected criminal activity; attend any appropriate training offered. Specifically, staff and associates must not knowingly do anything that helps someone else evade tax.
- 6.3 Tax evasion is the illegal non-payment or under-payment of taxes, usually as the result of making a false declaration (or no declaration) of taxes due to the relevant tax authorities, which results in legal penalties if the perpetrator is caught.
- 6.4 Tax avoidance, by contrast, is seeking to minimise the payment of taxes without deliberate deception. This is legitimate and covers a whole range of activities from simply choosing more tax efficient options, up to careful tax planning within the word of the law.
- 6.5 Part 3 of the Act entered into force on 30 September 2017 and created the corporate criminal offence of failure to prevent the facilitation of tax evasion. Importantly the corporate criminal offence of facilitation only applies to tax evasion. The third party must be found guilty of tax evasion before the Council can be found to have facilitated it.
- 6.6 It is a defence to the corporate criminal offence of facilitating tax evasion if the Council can prove that it has in place such prevention procedures as it is reasonable to expect in the circumstances.
- 6.7 Should staff or associates be concerned that another employee or associate is facilitating a third party's tax evasion, this should be reported as per reporting arrangements set out in Section 2 of this policy.
- 6.8 Reasonable care and caution is exercised when processing all financial transactions, particularly high value/high risk payments. Regular monitoring takes place and particular caution is exercised when making payments to new suppliers. Controls and limits are maintained in relation to payments being processed through the Source to Pay Hub. This work is kept separate to Accounts Payable who undertake checks on vendors prior to payments.
- 6.9 The Accounts Payable Team conduct regular vendor cleansing exercises, where vendors which have remained unused for 14 months or more are closed. Should future requests be received which require use of the closed



vendor, the AP team will independently reconfirm the vendor's bank details.

- 6.10 Changes to vendor bank details require that the vendor confirm the existing bank details which we hold on file. Where the detail change request was made via email, AP will attempt to independently find an email address to contact that company rather than replying directly to minimise the risk of spoof emails.

All contractors are assessed by AP for CIS deduction requirements, and HMRC advice for classification is stored for future payments. Any amendments to CIS classification is communicated to us directly by HMRC.

- 6.11 There are very few foreign transactions at Dorset Council. We do not typically trade with anyone overseas. This means the potential for missing trader or carousel fraud between Dorset Council and a directly connected third party is practically impossible. As a result, the risk of foreign transactions is low, and the rest of the VAT risk assessment is based on domestic transactions.

- 6.12 Trade payments are commissioned by a shopper, who request a purchase order number from and then S2P create this. S2P have a limit of £50,000 before the request needs to go to the budget holder for approval. This means that there are either 3 or 4 separate people involved in the process when it runs as planned. Making a bogus trade payment would require collusion between an AP team member and an S2P team member.

- 6.13 Any spend over £1000 is sent to the Budget Holder if payment is processed through DES. AP cannot edit the cost centre field so they cannot submit this way without another person to input the Cost Centre. SAP has no comparative authorisation limit, and in theory it would be possible for someone to send an invoice of unlimited value.



7. Key Roles & Responsibilities

7.1 Employees /Councillors will:

- Ensure that any genuine concerns associated with the activities of the Council in respect of any fraud or other financial crime are reported.

7.2 All Managers will:

- Ensure that their members of staff (including agency staff, consultants, contractors, volunteers etc) are aware of and follow approved Council procedures;
- Ensure any concerns are raised with relevant officers.

7.3 Directors / Chief Executive / Monitoring Officer will:

- Respond to concerns positively and ensure that relevant notifications are reported and acted upon. The Monitoring Officer has a particular responsibility for the Whistle-Blowing Policy and Procedure.

7.4 Chief Financial Officer (and designated Money Laundering Reporting Officer) will:

- Take overall responsibility for overseeing the appropriate application and adherence to the requirements of this policy and maintain a record of all such notifications;
- Provide proactive support and advice to managers as required; including attendance at meetings as necessary;
- Ensure that fraud and financial risks have been identified and are subject to regular review, in line with the Council's risk management strategy;
- Ensure that this strategy is subject to formal review on a regular basis.

7.5 Strategic Information Governance Board will:

- Have an overview of fraud and financial crime, at least once annually, ahead of reporting to Audit and Governance Committee within the Annual Fraud and Whistleblowing report;
- Ensure that an appropriate training regime is available;



- Ensure that appropriate awareness raising mechanisms are in place for employees, councillors and managers.

Policy Owner: Marc Eyre, Service Manager for Assurance

Date Approved: Audit & Governance Committee [**Presentation to Audit & Governance Committee 04.08.25**]

Review Date: August 2028



Appendix A – Fraud and Financial Crimes Response Plan

The following fraud response approach should be used for incidents involving employees:

Step 1 – Commencing an Investigation: Decisions to proceed with an investigation will be made by the Senior Manager, in conjunction with the Chief Financial Officer, Monitoring Officer and Human Resources. A decision will also need to be made at this point as to whether the circumstances require the employee to be suspended from duty.

Step 2 – Appointment of Investigating Officers: For each investigation, the first action will be to appoint an Investigating Officer (further guidance is included in the Council's Disciplinary Procedures)

Step 3 – Planning the Investigation: The Investigating Officer will need to engage and liaise with appropriate professional support (e.g. Internal Audit, HR) to ensure that a clear plan of action is drawn up to guide the investigation process. This will ensure that, as a matter of priority, any relevant and necessary documentary evidence pertaining to the investigation is immediately secured.

Step 4 – Referral to the Police (or other Agencies): If the investigation relates to a suspected criminal offence, a decision will need to be made from the outset whether to inform the Police. This decision will be made in conjunction with the Chief Financial Officer and the Monitoring Officer.

Step 5 – Gathering Evidence: The Investigating Officer will ensure, in conjunction with their professional support colleagues working on the case, that all evidence of fraud or corruption relating to the case are gathered swiftly, systematically, objectively and in a well-documented manner. The approach will follow requirements as set down in discussion with the Police, including statements and exhibits etc. The Investigating Officer will seek to ensure that they are kept closely informed of progress and key developments of any Police investigations.

Step 6 – Progress Reviews: During the course of the investigation, interim reports will be produced by any professional support colleagues working on the case to provide regular updates on progress and findings. These can be either written or verbal as required. These will help to ensure a close and focused attention to progress.

Step 7 – Conclude Investigation: A final report, setting out the findings and conclusions from the investigation, will be produced that may be used by management as a basis for disciplinary action in conjunction with HR.

Step 8 – Recommendation to Improve System Controls: The final report will also include any requirements and/or opportunities that have been identified during the investigation process to reduce risk and improve system and controls. Responsible managers will be expected to take the necessary actions to implement these recommendations in a timely



manner.

Step 9 – Recovering Losses: The Investigating Officer will ensure that all available opportunities are followed to obtain compensation for any losses to the Council, including insurance, voluntary restitution or by compensation claims.

Step 10 – Communication and/or Press Release: The decision to issue communications about fraud or corruption cases that have been investigated and proven by the Council will be made in discussions with the Investigating Officer, Chief Financial Officer, Monitoring Officer and Chief Executive. In doing so they will give due consideration, on a case by case basis, to any sensitive and legal issues involved and the need for confidentiality.

Any information concerning suspected fraud and corruption involving elected councillors must be referred to the Chief Executive, who will refer the matter to the Monitoring Officer. The Monitoring Officer will decide upon the most appropriate method of investigation.



Audit and Governance Committee

4 August 2025

Annual Emergency Management and Resilience Report 2024/25

For Review and Consultation

Cabinet Member:

Cllr S Bartlett, Planning and Emergency Planning

Local Councillor(s): N/A

Executive Director:

J Mair, Director of Legal & Democratic

Report author and job title: Marc Eyre, Service Manager for Assurance
Email: marc.eyre@dorsetcouncil.gov.uk

Statutory Authority: Civil Contingencies Act 2004

Report status: Public [Choose an item.](#)

1. Executive summary

- 1.1 This is the second annual report on emergency management and resilience and follows a request from Audit and Governance Committee to receive a periodic update on activity and learnings from events. It provides a comprehensive overview of Dorset Council's preparedness, response, and recovery efforts in managing civil emergencies. It reflects on key incidents, evaluates performance, and outlines strategic priorities for 2025/26.
- 1.2 Appendix A to this report sets out background information on the Civil Contingencies Act (CCA) legislation; Dorset Council's command and control structure; arrangements for business continuity and community resilience; and the role of councillors. This should provide some context to those members of the committee with limited knowledge of the Council's emergency management arrangements.
- 1.3 Over the reporting period, the Emergency Management and Resilience team responded to 49 incidents, ranging from severe weather events and fires to ICT disruptions and pollution threats. Notable incidents included Storm Bert, the Gainsborough Care Home evacuation, and the Gorge Café fire. These events tested the Council's command and control structures, which were refined in 2024 to streamline Gold and Silver officer roles and improve training

compliance—now at 94%.

- 1.4 The Council's Incident Management Teams (IMTs) played a pivotal role in coordinating multi-agency responses. Lessons learned from debriefs have led to improvements in communication, resource deployment, and integration of humanitarian support, particularly through the proposed Humanitarian Assistance Lead Officer (HALO) role.
- 1.5 Exercising remains a cornerstone of resilience. Dorset Council participated in statutory and multi-agency exercises, including "Operation Shortbill" and "Exercise Eleos," to test readiness for nuclear, coastal flooding, and recovery scenarios. Planning is underway for national exercises on i) communicable disease, pandemic and public health emergencies; and ii) counter-terrorism.
- 1.6 Business continuity has been a focus following a critical ICT incident and a limited assurance audit. A revised framework, updated action cards, and a training plan have been implemented, with 69% of services reviewing their continuity plans in the past year. Automation is being explored to support ongoing updates.
- 1.7 Community resilience efforts faced challenges due to the expiration of funding for the Community Resilience Liaison Officer. However, integration with the "Our Future Council" programme and continued engagement through the Dorset Prepared website aim to sustain momentum.
- 1.8 National developments, including the governments' recently published UK Resilience Action Plan and Strategic Defence Review, alongside findings from a number of national public inquiries, are shaping local strategies. The Council is aligning with these to enhance preparedness, particularly for high-risk scenarios like national power outages and cyber-attacks.
- 1.9 Priorities for 2025/26 include:
 - Strengthening business continuity and humanitarian planning.
 - Enhancing societal resilience through community engagement.
 - Delivery and participating in national and local exercises.
 - Responding to evolving risks, including climate-related events and technological threats.
- 1.10 This report provides assurance of Dorset Council's capability to manage emergencies and highlights its commitment to continuous improvement in resilience planning and response.

2. Recommendation(s)

- 2.1 To note the annual report and learnings from incidents.

3. Reason for the recommendation(s)

- 3.1 To provide assurance over the Council's ability to respond to significant civil emergencies, in meeting its obligations as a Category One Responder under the Civil Contingencies Act and associated legislation.

4. Incidents During 2024/25

- 4.1 During 2024/25, the Emergency Management and Resilience team recorded 49 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 Management and Resilience 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.
- 4.2 In the event of a significant emergency or business continuity incident, the Emergency Management and Resilience 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. Strategic Coordinating Groups and Tactical Coordination Groups).
- 4.3 Emergency Management and Resilience response per calendar months is set out below:

April 2024	Fatality at an event; Blue light response to health and safety incident
May 2024	Mutual aid support to evacuation; ICT business continuity incident; Support to Dorset Police for criminal investigation
June 2024	Body found on boat in Weymouth Marina Animal carcass on beach

July 2024	Beached vessel Swanage Out of hours alleged data breach Power outages Bridport
August 2024	Multiple right wing Protests; ICT business continuity incident
September 2024	Sunk uninsured vessel and salvage in Swanage waters Dorset Council website failure; Vehicle in river; Potential pollution incident with sunken vessel; Severe weather; Explosive items in car park
October 2024	Potential pollution incident with sunken vessel; Fire requiring evacuation; Deaths at care home
November 2024	Snow event; Lorry fire incident Fire at residential property with possible evacuation; HGV carrying fireworks Severe weather - Snow event and flooding Landslip
December 2024	Severe weather; Fire requiring evacuation; Fire requiring possible evacuation; Gas leak and evacuation
January 2025	Unknown chemical; Road traffic collision involving DC vehicle; Fire requiring possible evacuation; Fire at care home requiring evacuation Severe weather – multiple Pollution reports
February 2025	Severe weather; RTC and road closure Diesel spill on highway; Stranded cetacean Dangerous structure

March 2025	Security incident requiring evacuation; Multiple wildfires within close vicinity; Wildfire; Dangerous structure; Unexploded device; Loss of Dorset Council phone lines; Chemicals on public bus; Safeguarding issue
------------	--

2.1 Those incidents requiring Incident Management Teams and/or multi agency co-ordination are set out below. A key Emergency Management and Resilience 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.

2.2 **ICT Business Continuity Incident**

2.2.1 On the 28th May 2024 an Incident Management Team was instigated to consider a risk with licencing which was thought could have resulted in the Council losing access to critical ICT products until licencing could be resolved, which presented significant business continuity implications.

2.2.2 This incident prompted the Service Manager for Assurance to commission a SWAP Internal Audit on business continuity, which is discussed elsewhere in this report and led to a review of the framework, business impact analysis and introduction of action card review monitoring.

2.3 **Storm Bert and Snow Event**

2.3.1 The county was subjected to a severe weather event through the period 21 to 24 November 2024, which started with a snow event and continued in the following days with a named Storm (Storm Bert).

2.3.2 Debriefing identified that some elements of the response may have operated more smoothly if a precautionary incident management team had been held (weather warnings had not met the thresholds); 4 x4 provision should be considered for stand up as a precaution; improvements to out of hours warning and informing for live traffic updates etc.

2.4 **Gainsborough Care Home**

2.4.1 On 23 October 2024 the Council received notification from South Western Ambulance Service that a care home operated by a provider - Gainsborough Care Home in Swanage - had reported three deceased residents overnight. The cause of the incident had not been determined, and residents

were evacuated to a rest centre. Whilst investigations were ongoing it was necessary to establish alternative provision for residents at speed. The Police have now concluded their investigation, no further action will be taken.

- 2.4.2 Learnings included improving the interface between the command and control/emergency response processes, Adults Social Care and health processes; earlier deployment of additional local authority liaison officers as resourcing was stretched; early determination of when the Council needs to take control of processes being followed under the provider business continuity arrangements; earlier and more co-ordinated communication with councillors and staff; embedding the humanitarian assistance role with associated training for designated officers.

2.5 Gorge Café Fire, Dorchester

- 2.5.1 On 8 December, whilst officers were in response to a concurrent storm event, a fire broke out at the Gorge Café in Dorchester resulting in a partial collapse of the building. This required temporary closure of South Street, an impact of local businesses and an immediate need to rehouse some residents.
- 2.5.2 The local debrief has not yet been signed off, but there was a feeling expressed from services that we could improve inter-departmental communications for a prolonged incident involving multiple service areas. Future Incident Management Team close downs will include a consideration of whether a recovery group (whether full or light touch) would be of assistance to provide more joined up work.

3. Changes to the Command and Control Structure

- 3.1 In 2024 the decision was reached to reduce the number of Gold and Silver officers to ensure that those fulfilling the roles build up a greater level of experience and makes it easier to maintain training levels. Therefore, Gold is now performed by six members of the Senior Leadership Team (supplemented by Corporate Directors if necessary). Silver is performed by volunteer officers across a range of Corporate Directors, Heads of Service and Service Managers.
- 3.2 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 Management and Resilience business partner ahead of the first duty. In addition to this, multi-agency training should be undertaken, together with decision making and inquest/public enquiry training. At present 94% of current Gold and Silver officers have received or booked on multi agency training (refreshed every within the last three years). This is an improvement from 67% and 65% respectively last financial year.

- 3.3 Gold and Silver officers are also encouraged (and often required) to participate in exercises, to help boost experience. The Emergency Management and Resilience team periodically host short workshops to help share knowledge.
4. **Exercising**
- 4.1 The REPPIR (Radiation Emergency Preparedness and Public Information Regulations) and COMAH (Control of Major Accident Hazards) regulations set out the requirement for statutory exercises for demonstrating offsite plans. In particular, significant planning and exercising is statutorily required for the Portland Port MoD submarine operational 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. Operation Shortbill is the largest multi-agency exercise held by the LRF and was successfully completed under regulator observation in February 2025. 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.
- 4.2 The Council planned and participated in a two day multi agency exercise in October 2024 called "Exercise Eleos". Day one was a response to a widespread coastal flooding and high wind incident. Day two looked at the recovery from that incident and there were a number of in person workshops looking at the humanitarian response, communities, health and infrastructure. Dorset Council played fully throughout both days.
- 4.3 The Covid-19 module one findings highlighted a need for stronger national led exercises. Planning has commenced across the Local Resilience Forum for two significant exercises, relating to i) communicable disease, pandemic and public health emergencies; and ii) counter terrorism. The Council will participate in both the planning and delivery, in terms of national requirements and reporting; Local Resilience Forum level exercising, but also as an opportunity to test internal planning arrangements.
- 4.4 Exercises involve a whole range of Dorset Council services, depending on the scenario, in addition to providing hands on experience to Gold and Silver officers.
5. **Community Resilience**
- 5.1 In 2023 the LRF agreed to fund a pan-Dorset Community Resilience Liaison Officer (CRLO) on a fixed term contract, however this contract expired and future funding is currently unclear. This limits the amount of proactive engagement that the team are able to have with Parish and Town Councils and community groups. A bid for future funding from the LRF has been

agreed in principle, subject to LRF Executive sign off. However, spend has to be achieved within the financial year, which limits the recruitment capabilities. A range of options for delivery are being explored, including additional hours within the team and potential zero hour contract work.

- 5.2 An approach has been made to the Our Future Council programme to seek embedding of community resilience principles within the community partnership project.

6. **National Learnings**

- 6.1 Alongside learnings from Dorset specific incidents, the Council will also review findings from significant national incidents, particularly where subject to a public inquiry. The Chancellor of the Duchy of Lancaster committed to undertaking a review of UK national resilience in his statement to the House of Commons on 19 July, in response to the Covid-19 Inquiry's Module 1 report, and reflecting on other significant civil emergencies such as Grenfell and the Manchester Arena bombings. The [UK Government Resilience Action Plan](#) was released in July 2025. Whilst at this stage a number of the points within the action plan are aspirations, the likely implications for local authorities and other category one responders includes:

- Local authorities are expected to take a more proactive role in resilience, recognising that government alone cannot manage all risks. Resilience is now framed as a whole-of-society responsibility;
- Local responders must align their risk assessments with the National Security Risk Assessment (NSRA) and National Resilience Planning Assumptions, applying them to local contexts;
- Local authorities are expected to participate in more frequent and realistic training and exercising, including multi-agency simulations, to improve preparedness and response capabilities;
- Local responders must work with infrastructure operators to ensure local critical services (e.g. utilities, transport, health) are resilient to disruptions, including cyber threats and power outages;
- Local authorities are encouraged to strengthen ties with voluntary, community, and faith groups to enhance community-level preparedness and response. This may become a legislative requirement (subject currently to consultation);
- Councils are expected to improve public awareness and preparedness through better communication strategies, including encouraging households to take basic preparedness actions;

- There is an emphasis on improving data sharing between national and local levels to support better situational awareness and decision-making during emergencies;
 - Local authorities are urged to embed resilience considerations into spatial planning, housing, and infrastructure development to reduce long-term vulnerabilities;
 - Local responders will be subject to more structured assurance processes to evaluate their resilience capabilities and identify areas for improvement.
- 6.2 The Government also recently issued its [Strategic Defence Review for 2025](#), which includes within section 6 of the paper a focus on the whole of society approach to home defence and resilience. Whilst the primary focus is on the military, there are aspirations for wider resilience which is likely to impact on the local authority and other Local Resilience Forum partners.
- 6.3 The previous government initiated a public inquiry into the handling of the Covid pandemic. The inquiry is ongoing, but the findings from Module One, which covered resilience structures and preparedness across at both a national and local level have been released. The Cabinet Office released a response to the findings, which can be viewed [here](#). Although largely targeted at a national level, there were some learnings that have been localised, such as improved data provision (through business intelligence attendance at Incident Management Teams) and a review of the command and control structure to ensure that training and experience can be more easily achieved. As mentioned elsewhere in this report, there is also an increased expectation in relation to exercising.
- 6.4 The Grenfell Inquiry highlighted the need for local authorities to have effective plans in place for providing humanitarian assistance, with those plans to be supported by a humanitarian assistance lead officer (HALO). The Dorset LRF Humanitarian Assistance Capability Group has proposed that the HALO role is taken forward by both local authorities. Senior officers in Adults and Housing, Children's and Public Health would be best placed to fulfil that role. The HALO is responsible for ensuring the delivery of effective, person-centered humanitarian care to meet the needs of people affected by major incidents or emergencies. Although not formalised, dedicated officers did perform the key aspects of this HALO role during the Gainsborough and Gorge Café incidents. The Emergency Management and Resilience Team will be working with three Directorates to formalise arrangements.
7. **Business Continuity**
- 7.1 Following some concerns around embeddedness of business continuity plans following an incident in 2025, the Service Manager for Assurance commissioned SWAP Internal Audit Partnership to carry out a review. This

identified a number of weaknesses and presented a limited assurance opinion. The majority of actions in response to the findings have now been completed, including signoff of the revised Business Continuity framework; a review of the business impact analysis by Directorate Management Teams with sign-off by Senior Leadership Team in June 2025; and a training and exercising plan.

- 7.2 All services operate an action card identifying how they respond to a business continuity incident. As at May 2025, 69% of action cards had been reviewed and updated by owners (generally Service Managers or Heads of Service) in the last year. Since this annual key performance indicator has been calculated, an ICT related business continuity incident related to an attempted cyber attack has prompted a further influx of requests to access and review action cards.
- 7.3 A proposal is in development to look at whether elements of the business continuity requirements on action card owners can be supported by automation, but this will be subject to review vs conflicting automation priorities.
- 7.4 The work of the Emergency Management and Resilience team in developing a range of simple “self service” exercises that can be adopted by services to test their resilience against a range of risks was shortlisted for the national ALARM (Public Sector Risk Management) awards, held in June 2025. Although not winning the category, the national recognition of this initiative was positive.

8. Priorities for 2025/26

- 8.1 The Local Resilience Forum workplan is very challenging, with a wide range of plans subject to review, and an increase in national led exercises requiring local level planning. Plans relating to a number of workstreams are currently actively being reviewed and updated, notably: coastal pollution; mass fatalities; rock falls and landslides; animal disease; fuel; loss of utilities (water / gas); wildfires; dam and reservoir inundation; vulnerable people data sharing; recovery, telecoms, community resilience, humanitarian assistance, National Power Outage, communicable disease, pandemic and public health emergencies, major accident hazard pipelines (MAHP) and Radiation Monitoring Units.
- 8.2 The key priority is to respond to incidents effectively and efficiently, and ensure that any subsequent learnings are incorporated into future planning and response. As noted elsewhere in the report, we are experiencing an increase in incidents, for instance through the changing weather patterns and technology risks.

- 8.3 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. There remains focus on planning to respond to a national power outage, including resilient communications and establishing community hubs.
- 8.4 Embeddedness of business continuity action cards remains a priority, to ensure that all critical services have reviewed and tested their plans. The action cards will need to be updated to reflect any structural changes following the move to a new operating model as part of the Our Future Council programme. We are looking at whether automation can be used to ease some of the pressure on managers in updating both the action cards and business impact assessment.
- 8.5 Dorset LRF has highlighted several large gaps around the planning for humanitarian assistance. This work has progressed over the last year, with some smaller plans being developed that sit under the umbrella of human aspects planning. Within Dorset Council, Emergency Management and Resilience have already developed excellent working relationships with Adults and Housing, especially in an incident and from the learnings of the Gainsborough Care Home Evacuation. Developing the adults on call manager role in an incident was a key feature. Once agreed, implementation of the HALO role and the processes will be worked on and will become embedded into the Local Resilience Forum.
- 8.6 A number of national led exercises will commence this year, including communicable disease, pandemic and public health emergencies and counter terrorism. The Council will participate in the planning and delivery, in terms of national requirements and reporting; Local Resilience Forum level exercising, but also as an opportunity to test internal planning arrangements.
- 8.7 There will remain a concerted effort to engage with communities and improve societal resilience. The Council is exploring funding opportunities to support this work, alongside any work integrated into the Community Partnerships Programme within Our Future Council.
- 8.8 The Council will review and respond to recommendations within the UK Government Resilience Action Plan and the Strategic Defence Review.
9. **Alternative options considered**
- 9.1 None
10. **Legal considerations**
- 10.1 The Council meets its obligations under the Civil Contingencies Act 2004 as a Category One Responder, alongside associated legislation.

11. Financial implications

- 11.1 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 emergency financial assistance programme designed to help local authorities recover from the immediate costs of responding to major emergencies. When a local authority incurs significant unbudgeted expenditure while protecting life or property during a disaster—such as flooding, severe weather, or major fires—it may be eligible for reimbursement under this scheme. The scheme typically covers up to 85% of eligible costs above a set threshold, which is calculated based on the authority's annual budget. The scheme only applies to immediate response costs and does not cover longer-term recovery or infrastructure repair.

12. Natural environment, climate & ecology implications

- 12.1 The changing climate informs weather events, and as an example 2024/25 presented a significant number of storm challenges. Emergency response plans need to keep pace with the changing environment.

13. Well-being and health implications

- 13.1 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.

14. Other implications

- 14.1 None

15. Risk implications

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

Current Risk: Low

Residual Risk: Low

- 15.2 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 a very high 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.

16. Equalities

- 16.1 None

17. **Appendices**

17.1 Appendix A – Background Information

18. **Background papers**

18.1 None

19. **Report sign-off**

19.1 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)

Emergency Management and Resilience – Dorset Council

Civil Contingencies Act

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.

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).

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.

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).

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.

A range of other legislation also apply. Both REPIR and COMAH are referenced in the main report. The Council also has duties under the PSR (Pipeline Safety Regulations) which are being discharged via Major Accident Hazard Pipelines (MAHP) planning. Dorset Council is the lead duty holder authority for both REPIR, COMAH and MAHP offsite plans.

Emergency Management at Dorset Council

Emergency Management and Resilience 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) and Silver (Tactical) officers (Heads of Service level).

The Emergency Management and Resilience 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 Management and Resilience Officer function for the Council.

Dorset Council Emergency Plans / Workstreams

Each of the Emergency Management 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; Communicable disease, pandemic and public health emergencies 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; 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 Events Safety Advisory Group (SAG)

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.

In cases of national security, lead on planning and response is provided by central government.

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.

The Role of Councillors

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 Management and Resilience sits within the “Planning and Emergency Management and Resilience” 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.

In the event of incident notification, the Duty Emergency Management and Resilience Officer will endeavour to inform the portfolio holder, Leader and relevant ward members. However, the level of contact will vary, as the primary focus of the officer is to respond to the incident.

Business Continuity

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.

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 Management and Resilience 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.

The '[Dorset Prepared](#)' website provides tools and guidance to support businesses and voluntary organisations.

Societal resilience

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.

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

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, however this contract expired and future funding is currently unclear. Prior to the contract, the CRLO was engaged in the development of several Community Emergency Response Plans. Community resilience remains a team priority, but is being delivered on a "best endeavours" basis by team members at present, as the work is primarily outside of normal working hours.

The '[Dorset Prepared](#)' website has been redeveloped and provides tools and guidance for communities.

Audit and Governance Committee

04 August 2025

Risk Management Update

For Review and Consultation

Cabinet Member:

Cllr N Ireland, Leader of the Council, Climate, Performance and Safeguarding

Executive Director:

A Dunn, Executive Director, Corporate Development

J Mair, Director, Legal & Democratic Services

Report author and job title:

- Chris Swain, Risk Management & Reporting Officer
- Liz Crocker, Head of Strategy

Email:

- chris.swain@dorsetcouncil.gov.uk
- liz.crocker@dorsetcouncil.gov.uk

Report status: Public

1. Executive summary

Dorset Council is continuing to strengthen the way it measures, monitors, and reports on performance and risk. Over the past six months, steady progress has been made in embedding a more strategic and transparent approach to risk management aligned with the Council's strategic performance and risk reporting framework.

Key developments include the full implementation of Principal and Strategic Risks, the timely completion of all audit actions, and the integration of risk and performance reporting. This unified approach enhances strategic alignment, supports informed decision-making, and improves organisational accountability.

The draft Risk Appetite Statement (Appendix A), developed through consultation with Cabinet and senior leaders, outlines Dorset Council's high-level strategic intent regarding the level of risk it is willing to accept in pursuit of its objectives. While the statement will be approved under delegated authority, feedback from the Committee is welcomed on both the content of the statement and the administration's proposed appetite for risk.

Further work is underway to finalise a new Corporate Risk Register and enhanced Risk Dashboard, with a demonstration planned for a future meeting. These developments will be consolidated into a revised Risk Management Strategy for Committee review in October 2025.

The role of the Audit and Governance Committee remains central in ensuring that the right areas of focus are maintained and that continuous improvement is embedded across the organisation.

2. Recommendation(s)

2.1 That the Audit and Governance Committee:

- Note the progress made in strengthening Dorset Council's risk management framework over the past six months, including the timely completion of all risk audit actions.
- Provide feedback on the draft Risk Appetite Statement (Appendix A), recognising that final approval rests with the Leader of the Council under delegated authority.
- Support the proposed approach to embedding the risk appetite principles across the organisation, including directorate-level interpretation and the escalation of out-of-appetite risks through existing governance structures.
- Note the ongoing development of the new risk register and enhanced risk dashboard and agree to receive a demonstration at a future meeting.
- Note the risk reporting compliance for August 2025 and the updated presentation of strategic risks and escalate any matters to the relevant Scrutiny Committees where appropriate.

3. Reason for the recommendation(s)

3.1 To ensure that the council's risk management methodologies support informed, risk-based decision-making while remaining proportionate and aligned with organisational objectives and key deliverables.

4. The report

4.1 Over the past 6 months, we have made steady, incremental improvements to Dorset Council's overall risk management framework, including the timely completion of all risk audit actions.

Principal Risks

- 4.2 Following the finalisation of the Council Plan, Dorset Council adopted its [Principal Risks](#) as the top tier within its risk management framework, under which all other risks are aligned as subsets. These 11 Principal Risks are adapted from the Orange Book (HM Treasury and Government Finance Function), the UK Government's standard for risk management in the public sector. Their purpose is to provide a structured approach to identifying key areas of organisational risk, thereby enhancing strategic insight and supporting more informed decision-making. All risks within the Corporate Risk Register are now aligned to **one or more** Principal Risk areas, offering deeper insight into the interrelationships between risks. Appendix B of this report provides a breakdown of how Corporate Risk Register entries align with the Principal Risks.

Strategic Risks

- 4.3 Strategic risks have been identified in collaboration with senior leaders, using a defined set of criteria to guide discussions, as outlined in section 1.3 of the Audit and Governance Committee Risk Management Update, 14 April 2025.

A risk may be classified as strategic if it meets **one or more** of the following:

- Will have a noticeable impact on achieving strategic priorities as documented in the council plan or key organisational deliverables.
- Is rated 20 or more according to the Council's risk matrix (see Appendix C) based on the existing controls that are in place.
- Has a noticeable impact upon the use of the Council's key resources (finance, people etc).
- May result in significant attention from external stakeholders with the potential to cause significant reputational and or political damage.

- 4.4 Appendix D confirms the Strategic Risks that are now embedded into reporting cycles across the organisation. These risks form part of quarterly performance and risk reports to the Senior Leadership Team (SLT), and flow into the respective Scrutiny Committee, in accordance with our Strategic Performance and Risk Reporting Framework (Appendix E), unifying risk and performance reporting within public reports. Strategic Risks have replaced simply reporting on the "Very High" risks in isolation and provide a better rounded and proportionate view of the organisation's risks.

- 4.5 Bringing together risk and performance reporting provides a more holistic and transparent view of how the organisation is progressing toward its objectives. This integrated approach offers several key benefits:

- **Improved Decision-Making.** By viewing risks alongside performance data, leaders can better understand the context behind performance trends and make more informed, risk-aware decisions.
- **Strategic Alignment.** It ensures that risk considerations are embedded in the delivery of strategic priorities, helping to balance ambition with realism.
- **Early Warning Signals.** Performance shortfalls often signal underlying risks. Reporting them together allows for earlier identification and proactive management of emerging issues.
- **Efficiency and Clarity.** A unified reporting structure reduces duplication, streamlines oversight, and provides a clearer narrative for senior leaders, members, and stakeholders.
- **Transparency and Accountability.** Presenting risk and performance together in public reports enhances transparency. It shows not only how the Council is performing, but also the risks it is managing in pursuit of its goals, supporting open governance and public trust.

Risk Appetite

- 4.6 Following the presentation of the Risk Appetite Framework to the Audit and Governance Committee on 14 April 2025, consultation with Cabinet and senior leaders has resulted in the development of the Risk Appetite Statement, detailed in Appendix A(i).
- 4.7 The risk appetite level was identified for each Principal Risk in Appendix A(ii). These individual assessments were then brought together to form a comprehensive statement that reflects the organisation's overall approach to risk.
- 4.8 This statement outlines Dorset Council's high-level strategic intent regarding the level of risk it is willing to accept in pursuit of its objectives.
- 4.9 The statement will be approved under delegated authority. Cllr Nick Ireland, Leader of the Council and Cabinet Member for Climate, Performance and Safeguarding, holds delegated authority to approve the Risk Appetite Statement. However, he welcomes feedback from the Committee on both the statement itself and the administration's proposed appetite for risk.
- 4.10 Once approved through delegated authority, it will serve as a guiding tool for risk-based decision-making across the organisation.

Embedding the Risk Appetite

4.11 To ensure the Risk Appetite Statement is effectively embedded across the Council, the following steps will be taken:

- **Assessment of Existing Risks.** Through enhancements to the Corporate Risk Register, all risks owners will be required to determine whether the risk falls within the agreed risk appetite levels. Any risks identified as outliers, those exceeding the defined appetite, will be escalated to SLT for review and resolution.
- **Directorate-Level Interpretation.** Each directorate will be supported in interpreting the Risk Appetite Statement and understanding its practical implications. A template to guide this process is provided in Appendix F.

Further Work

4.12 The Risk Management & Reporting Officer, supported by the wider Policy, Intelligence and Performance (PIP) service, is working at pace to finalise the new Risk Register, alongside an enhanced reporting Risk Dashboard designed to improve user experience and reporting functionality. A testing phase is currently underway to inform final refinements ahead of the planned 'go live' launch in Quarter 3. A demonstration of the risk register and dashboard will be provided to Committee members.

4.13 The various themes of progress outlined throughout this report will be consolidated within a revised Risk Management Policy, which is scheduled for presentation for review by the Audit and Governance Committee in October 2025.

Risk Reporting Compliance

4.14 Dorset Council's overall compliance with the Corporate Risk Register over a rolling 12-month period since September 2024, as reported in the published Audit and Governance Committee papers:

Month	September 2024	January 2025	April 2025	August 2025
Overall Compliance	100%	100%	100%	100%

- 4.15 Appendix C provides a detailed overview of Dorset Council's Corporate Risk Register compliance, while Appendix D outlines the Strategic Risks and their respective ratings across each directorate. Together, these appendices offer essential insights into compliance and present a proportionate view of the risks most pertinent to the organisation.

5. Legal considerations

- 5.1 There are no direct legal implications arising from this report. However, uncontrolled risks may pose a threat to Dorset Council's ability to comply with statutory obligations.

6. Financial implications

- 6.1 There are no direct financial implications arising from this report. However, uncontrolled risks may pose a threat to Dorset Council's financial stability. Additionally, implementing risk controls may have budgetary impacts, which should be evaluated through a cost-benefit analysis prior to adoption.

7. Natural environment, climate & ecology implications

- 7.1 There are no specific natural environment, climate or ecological implications associated with this report; however, the Corporate Risk Register identifies several risks in this category.

8. Well-being and health implications

- 8.1 There are no specific well-being or health implications associated with this report; however, the Corporate Risk Register identifies several risks in this category.

9. Other implications

- 9.1 None.

10. Risk implications

- 10.1 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 report outlines the Risk Management Framework, Principal and Strategic Risks for Dorset Council. It therefore does not have a rating to consider related to a decision. The appendix provides an update on the current Principal and Strategic Risks.

11. Equalities

11.1 There are no specific equality implications associated with this report; however, the Corporate Risk Register identifies several risks in this category.

12. Appendices

12.1 Appendix A – Dorset Council Risk Appetite Statement and Framework

12.2 Appendix B – Dorset Council Principal Risks

12.3 Appendix C – Dorset Council Risk Scoring Matrix and Overall Summary

12.4 Appendix D – Dorset Council Strategic Risks

12.5 Appendix E – Dorset Council Strategic Performance and Risk Framework

12.6 Appendix F – Applying Risk Appetite

13. Background papers

13.1 [Audit and Governance Committee Risk Management Update, 14 April 2025](#)

14 Report sign-off

14.1.1 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

04 August 2025



Dorset Council Risk Appetite Statement and Framework

i) Dorset Council Risk Appetite Statement:

“Dorset Council is committed to building a secure, resilient, and forward-looking organisation, where risk is not only managed but also embraced as a catalyst for innovation and improvement. We are shaping a future where thoughtfully considered opportunities for change drive better outcomes for our communities, services, and workforce.

We maintain strong safeguards to protect our people, property, assets and information, from harm or unauthorised use.

We accept that some financial uncertainty may be necessary to unlock significant improvements in service delivery and operate within a robust legal and regulatory framework, preparing for a future where adaptability and resilience are key to success.

Our open approach to commercial and procurement activity demonstrates a willingness to pursue innovation, with some non-critical decisions being made via devolved authority. We actively promote the legitimate transparency, openness, and information sharing to support effective decision-making and collaboration in providing better services to our communities. Our Operational stance empowers local managers to make non-critical decisions and encourages evidence-based experimentation, fostering a culture of responsible innovation.

Dorset Council's people policies provide a strong and stable foundation, while remaining open to flexible, people-centred approaches that foster innovation, adaptability, and growth. Dorset Council is committed to investing in its workforce, developing a diverse range of skills to meet evolving needs and challenges. We ensure that all projects and programmes display demonstrable benefits, so that every initiative actively contributes to building a thriving, future-ready council.

In property and asset management, we are exploring diverse, adaptive solutions to meet evolving organisational needs in delivering services to our communities. We are eager to develop new models, partnerships, and technologies that can enhance our impact and outcomes for communities.

Dorset Council is preparing for the future with a clear focus on resilience, adaptability, and continuous improvement. By taking a thoughtful and balanced approach to risk, and aligning our efforts with long-term priorities, we aim to build a council that is responsive to change and committed to delivering the best outcomes for our communities.”

ii) Dorset Council Risk Appetite Framework:

The highlighted areas represent the selections made following consultation with Cabinet and Senior Leaders:

Risk Appetite Level Definitions					
	Averse (1)	Minimal (2)	Cautious (3)	Open (4)	Eager (5)
Commercial	Dorset Council has a strong preference for engaging in tested and established commercial agreements with close management controls and oversight.	Dorset Council accepts low-scale commercial / procurement activity via devolved authority, with medium and high-level activity validated by senior management.	Dorset Council tends to stick to the status quo. Commercial innovations are avoided unless necessary, with decisions generally held by senior management.	Dorset Council has a willingness to pursue innovation, which has previously showed benefit. Its non-critical decisions may be devolved to local managers.	Dorset Council has a desire to innovate and break the mould. Commercial initiatives are pursued in improving services with high levels of devolved authority to increase business agility.
Data and Information Management	Dorset Council 's data and information are secured through strict access controls and extensive monitoring.	Dorset Council ensures minimal distribution of data and information to reduce risks and damages because of disclosure.	Dorset Council's data is distributed cautiously, and only when required to maintain operational effectiveness.	Dorset Council accepts that openness and information sharing is needed for effective operations in a controlled environment.	Dorset Council's data and information is subject to minimal controls. Its data is open and easily accessible in the pursuit of operational effectiveness.

Risk Appetite Level Definitions					
	Averse (1)	Minimal (2)	Cautious (3)	Open (4)	Eager (5)
Finance	Dorset Council safeguards its financial resources as a priority and avoids any activities that could lead to financial loss or impact.	Dorset Council considers financial impacts and risk are only acceptable when related to the essential delivery of services.	Dorset Council's financial decisions accept some uncertainty related to loss or impact, only if they yield upside opportunities in service delivery.	Dorset Council is willing to invest and take on higher financial risks to support the business where they have been appropriately managed with controls.	Dorset Council seeks to invest for the best possible benefit in opportunities, acknowledging that there may be significant financial loss or impact.

Risk Appetite Level Definitions					
	Averse (1)	Minimal (2)	Cautious (3)	Open (4)	Eager (5)
Legal	Dorset Council avoids areas that could be potentially challenged legally, even if the chances of winning any case are high.	Dorset Council operates on a basis that ensures it would be successful in any legal challenge.	Dorset Council takes decisions where it must be reasonably certain that it would be able to win any legal challenge.	Dorset Council takes tough decisions and accepts that any legal challenge is likely to be difficult, but the potential benefits outweigh the downsides.	Dorset Council accepts the possibility of losing any legal case is high, but the potential benefits that could be realised in the event of success are exceptional.

Risk Appetite Level Definitions					
	Averse (1)	Minimal (2)	Cautious (3)	Open (4)	Eager (5)
Operations	Dorset Council adopts a “tried and tested” approach to operational delivery, with close management control.	Dorset Council pursues innovations only in the instance that it is deemed essential for operational delivery and validated by senior management.	Dorset Council tends to stick to the status quo. Operational innovations are carefully selected where necessary, and decisions are generally held by senior management.	Dorset Council pursues innovation that has evidence of previous benefits. There is a willingness to innovate and responsibility for non-critical decisions may be devolved to local managers.	Dorset Council seeks innovative approaches to operational delivery by constantly challenging current practices. This is supported by high levels of devolved authority.

Risk Appetite Level Definitions					
	Averse (1)	Minimal (2)	Cautious (3)	Open (4)	Eager (5)
People	Dorset Council maintains close management control, with little devolved authority. There is limited flexibility in working practices and development of staff is limited to “essential” services only.	Dorset Council’s Senior Leadership hold decision-making authority. The organisation adopts strict recruitment and retention strategies to minimise disruption and development is limited to being role specific.	Dorset Council’s decision-making is generally controlled by senior management. There is acceptance of safe and standard people / working policies.	Dorset Council adopts devolution of certain work-related decision-making responsibilities. The organisation is willing to invest in its people to create a variety of skills in its workforce.	Dorset Council adopts high levels of devolved authority. The organisation constantly challenges working practices to pursue innovation and invests significantly in staff development to create a broad skillset.

Risk Appetite Level Definitions					
	Averse (1)	Minimal (2)	Cautious (3)	Open (4)	Eager (5)
Project/ Programme	Dorset Council prioritises projects / programmes with almost certain outcomes that are supported by close management control and oversight. There is a preference for maintaining and protecting rather than creating or innovating.	Dorset Council prioritises only the most essential innovations. Decision making is held by senior management with projects / programmes needing to demonstrate clear links to the organisation's strategic priorities.	Dorset Council tends to stick to the status quo and innovations are generally avoided unless necessary. Decision making is typically made by senior management with projects and programmes aligned to strategic priorities.	Dorset Council pursues innovation when projects / programmes display demonstrable benefits. Decision making may be devolved to local managers, with plans aligned to functional standards.	Dorset Council constantly pursues innovation to achieve the best working practices and "break the mould". There are high levels of devolved authority with plans largely aligned to organisational governance.

Risk Appetite Level Definitions					
	Averse (1)	Minimal (2)	Cautious (3)	Open (4)	Eager (5)
Property	Dorset Council complies with strict policies for purchase, rental, disposal, construction, and refurbishment of property, that ensures it is producing good value for money.	Dorset Council is recommended to follow strict policies for purchase, rental, disposal, construction, and refurbishment of property that ensures it is producing good value for money.	Dorset Council can adopt a range of agreed solutions for purchase, rental, disposal, construction and refurbishment of property that ensures it is producing good value for money.	Dorset Council can adopt a range of agreed solutions for purchase, rental, disposal, construction and refurbishment of property that ensures it meets organisational needs.	Dorset Council applies dynamic solutions for the purchase, rental, disposal, construction and refurbishment of property that ensures it meets organisational needs.
Reputation	Dorset Council has no appetite for any decisions with a high chance of repercussion to the organisation's reputation.	Dorset Council's appetite for risk taking is limited to those events where there is no chance of any significant repercussion to the organisation's reputation.	Dorset Council's appetite for risk taking is limited to those events where there is little chance of any significant repercussion to the organisation's reputation.	Dorset Council has appetite to take decisions with the potential to expose the organisation to additional scrutiny, but only where appropriate steps are taken to control the risk.	Dorset Council has an appetite to take decisions which are likely to bring additional Governmental / organisational scrutiny, only where potential benefits outweigh the risks.

Risk Appetite Level Definitions					
	Averse (1)	Minimal (2)	Cautious (3)	Open (4)	Eager (5)
Security	Dorset Council has no tolerance for security risks causing loss or damage to its property, assets, information or people with stringent control measures in place.	Dorset Council aims to minimise loss or damage to property, assets, information or people with significant control measures in place.	Dorset Council accepts limited security risks to support business need, with industry standard controls in place to protect its property, assets, information or people.	Dorset Council accepts some security risks to support business need with tailored controls in place to protect its property, assets, information or people.	Dorset Council accepts security risks to support business need with the minimum level of controls in place to support agile use of its property, assets, information or people.
Technology	Dorset Council generally avoids developments in systems and technology.	Dorset Council considers development in systems and technology that is deemed vital to protect current operations.	Dorset Council implements the use of established / mature systems and technology to enhance the organisations performance.	Dorset Council welcomes new systems and technologies in the pursuit of improved service delivery and organisational performance.	Dorset Council views new systems and technology as essential for organisational development and service delivery.

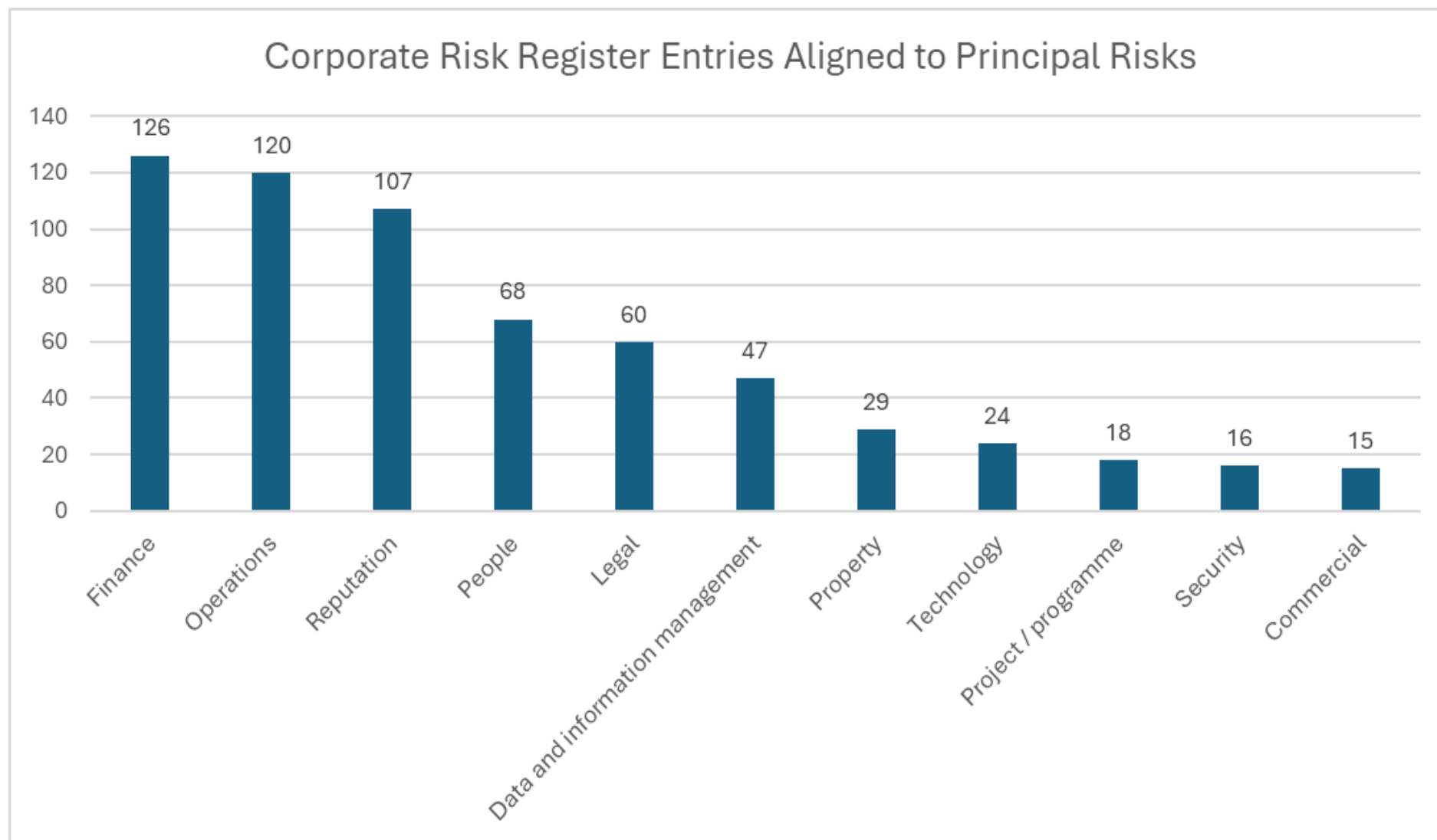
Audit and Governance Committee

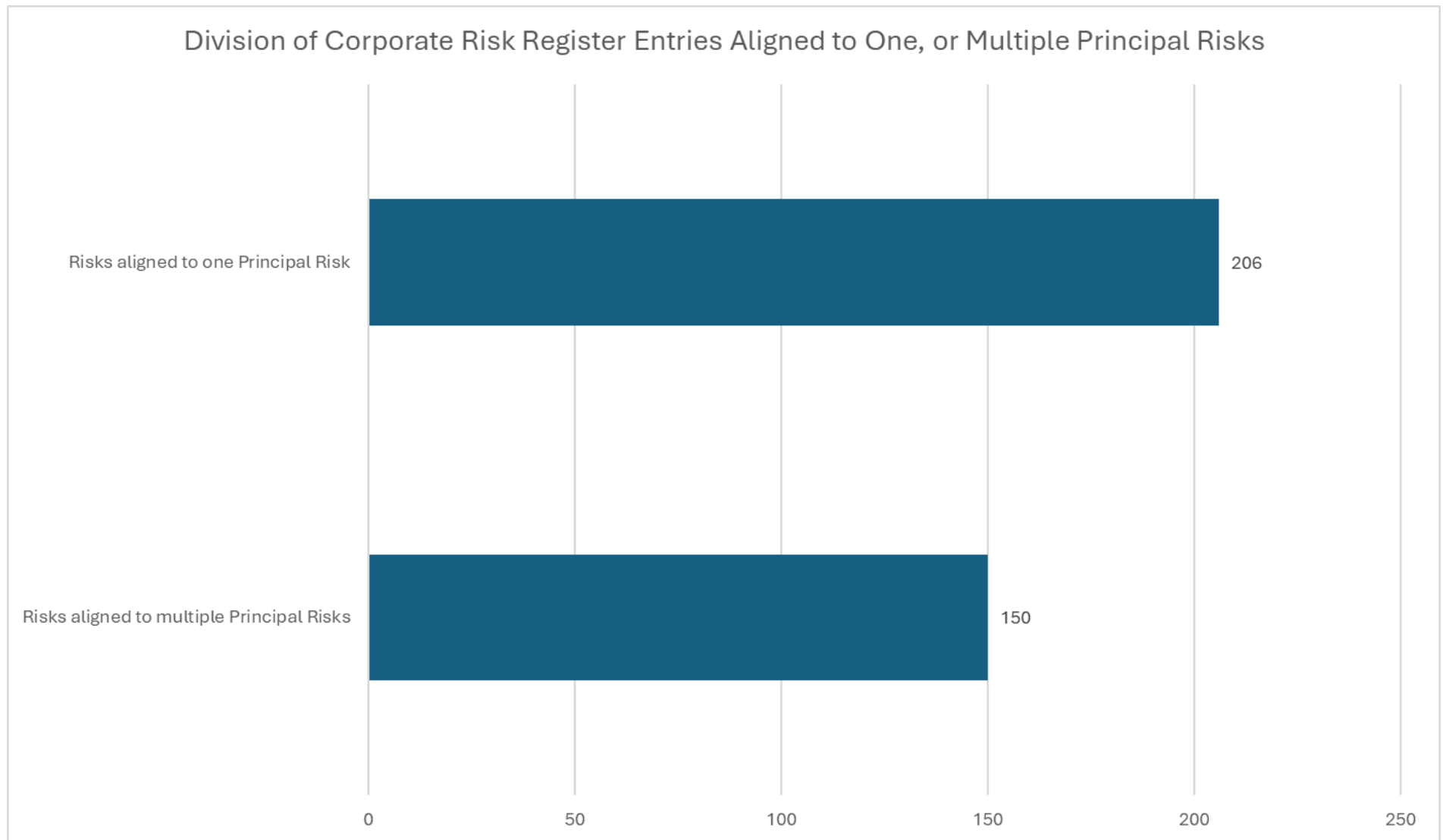
04 August 2025



Dorset Council Principal Risks

As of 07 July 2025





Audit and Governance Committee

04 August 2025



Dorset Council Risk Scoring Matrix and Overall Summary

As of 07 July 2025

Dorset Council Risk Scoring Matrix:

Dorset Council Risk Scoring Matrix								
Impact	Catastrophic	5	10	15	20	25		Risk Rating
	Major	4	8	12	16	20	Risk Score	Very High
	Moderate	3	6	9	12	15	20 to 25	High
	Slight	2	4	6	8	10	12 to 16	Medium
	Limited	1	2	3	4	5	5 to 10	Low
		Very Unlikely	Unlikely	Possible	Likely	Almost Certain		
		Likelihood						
							1 to 4	

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

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

Overall Summary:

The table illustrates the spread of all Corporate Risk Register entries:

Impact	Catastrophic	1	1	3	2	0
	Major	4	36	12	10	1
	Moderate	11	54	81	10	0
	Slight	6	69	28	11	2
	Limited	4	6	4	0	0
		Very Unlikely	Unlikely	Possible	Likely	Almost Certain
		Likelihood				

Total Risks	Overdue	Strategic Risk Compliance	Overall Compliance
356	0	100%	100%

Audit and Governance Committee

04 August 2025



Dorset Council Strategic Risks

As of 07 July 2025

Strategic Risks According to Impact and Likelihood Scores:

The table illustrates the spread of all Strategic Risks (identified by their ID's).

All Strategic Risks are reported to SLT and relevant Scrutiny Committees. Strategic Risks that are aligned with Council Plan priorities and will be reported via the Council Plan performance monitoring dashboards when published later this year.

Impact	Catastrophic			201	272, 286	
	Major		144, 213	140, 180, 814	348, 560, 805, 808	612
	Moderate		112, 244, 273, 342, 372, 729	167, 182, 229, 230, 798, 803, 804, 812	101, 339, 723	
	Slight	806		765		
	Limited	279, 821*	816, 807, 810	811		
		Very Unlikely	Unlikely	Possible	Likely	Almost Certain
		Likelihood				

*Detail to be finalised with risk owners

Adults and Housing

ID	Adults and Housing Risk	Strategic Priority	Principal Risk(s)	Risk Rating
167	Failure to keep adults safe who have care and support needs and are at risk of harm or abuse	Communities for all	Legal, Operations, Reputation	Medium
180	The supply of temporary accommodation is insufficient to meet statutory homelessness demand	Provide high quality and affordable housing	Commercial, Operations, Project / programme, Property, Reputation	High
182	Poor quality private rented sector housing may lead to increased social, health and economic pressure on households and therefore higher demand for Council services	Provide high quality and affordable housing	Project / programme, Property, Reputation	Medium
244	The Local Plan does not support future development in the appropriate areas to meet the community need	Provide high quality and affordable housing	Reputation	Medium
339	Due to the demand on hospital bed stock, patients with higher complexity needs may be delayed hospital admission, leading to increased demand for Council run services	Communities for all	Operations, Reputation	High
342	As a result of capacity in the voluntary and community sector, Dorset council may not be able to provide sufficient care and support to residents, leading to a failure to deliver communities for all	Communities for all	Commercial, Operations, Reputation	Medium

ID	Adults and Housing Risk	Strategic Priority	Principal Risk(s)	Risk Rating
723	The impact on the Adult Social Care Service user budget of funding for people who previously funded their own care in residential/nursing care settings and now require funding by the local authority	Communities for all	Finance, Operations	High
798	Impact of rises in 25/26 Employers NI & NMW on the social care market, increase risk of service failure and / or contract handback. May limit new capacity available to meet incoming (and increasing) demand.	Communities for all	Commercial, Reputation, Operations	Medium
808	Due to the abolition of NHS England, commissioning arrangements for local health services may be disrupted, leading to service delivery and financial sustainability consequences for social care	Communities for all	Commercial, Finance, Operations	High
814	Due to corporate, market and partnership conditions, the home-in on housing programme may not achieve the housing strategy objectives, leading residents being unable to access affordable, suitable, secure homes	Provide high quality and affordable housing	Finance, Operations, Reputation	High

Children's Services

ID	Children's Services Risk	Strategic Priority	Principal Risk(s)	Risk Rating
112	An inability to attract and retain suitably qualified staff may lead to unmanageable workloads leading to a failure to safeguard children and meet their needs early	Communities for all, Key organisational deliverable	Finance, Legal, Operations, People, Reputation	Medium
272	Instability in the High Needs Block budget may create an increased deficit in the Dedicated Schools Grant (DSG) resulting in a deficit in Dorset Councils financial position.	Key organisational deliverable	Finance, Legal, Reputation	Very High
273	Due to demand for service provision, Education, Health and Care Plans may not be delivered within statutory timescales, leading to a failure to deliver children's educational needs and an increase in SEND tribunals	Communities for all	Operations, People, Reputation	Medium
279	As a result of a lack in financial or strategic commitment, the Early Help Partnership may fail, resulting in the increased demand for statutory services including child protection and the number of children in care	Communities for all	Operations	Low
811	Due to the transition of some schools to Academy Trusts, Dorset Council may face challenges in influencing KS2 attainment, potentially resulting in a limited ability to improve results beyond the national average	Communities for all	Operations, Reputation	Low
812	Due to the removal of the ability for Early Years (EY) settings to charge 'top ups' for early education funded places, there may be insufficient early education places	Communities for all	Operations, Reputation	Medium

ID	Children's Services Risk	Strategic Priority	Principal Risk(s)	Risk Rating
	available			
816	As a result of insufficient numbers of young care leavers engaging with education, employment or training, care leavers may develop social and economic isolation, leading to increased levels of demand on the local authority and strategic partners	Communities for all	Finance, Operations, Reputation	Low

Corporate Development

ID	Corporate Risk	Strategic Priority	Principal Risk(s)	Risk Rating
140	Due to the effects of climate change and extreme weather events, Dorset Council may be unable to adapt its services and infrastructure leading to reduced resilience in service delivery to residents and in our communities	Respond to the climate and nature crisis	Finance, Legal, Property, Reputation	High
286	A successful cyber-attack to IT systems causes loss of service or data	Key organisational deliverable	Data and information management, Finance, Legal, Operations, Reputation, Security, Technology	Very High

ID	Corporate Risk	Strategic Priority	Principal Risk(s)	Risk Rating
348	There is a business continuity risk from delayed ICT recovery after a disruption such as a power failure	Key organisational deliverable	Date and information management, Finance, Legal, Operations, Reputation, Security, Technology	High
803	Due to the organisations finances, Dorset Council may have to reduce its workforce in lieu of transformation, leading to insufficient resource to deliver services	Key organisational deliverable	Finance, Operations, People	Medium
804	As a result of transformation, Dorset Council may be unable to retain staff and preserve employee wellbeing, leading to a skills gap and reduced employee health in the organisation	Key organisational deliverable	Operations, People	Medium
805	Due to current levels of resourcing, the organisations transformation work may not achieve its objectives, leading to incomplete benefits to service delivery, customer experience and cost savings	Key organisational deliverable	Finance, Operations, People, Project / programme, Reputation	High
806	Due to the nature of Dorset's economy if economic growth slows, Dorset Council may see a stagnation in Council Tax and Business Rate revenue, leading to increased pressure on budgets to fund service delivery	Grow our economy	Finance, Reputation	Low
807	As a result of a breach in, or lack of, internal controls with insufficient progress in addressing the weaknesses, Dorset Council's external audit report may lead to Government intervention	Key organisational deliverable	Finance, Operations, Reputation	Low

Legal and Democratic

ID	Legal and Democratic Risk	Strategic Priority	Principal Risk(s)	Risk Rating
101	Emergency Planning - Lack of robust business continuity framework (policy and processes; testing and leadership) results in service failure	Key organisational deliverable	Data and information management, Legal, Operations, Reputation, Security, Technology	High
213	Information Compliance - Dorset Council may not be able to demonstrate evidence such as required training levels to support the NHS Digital Toolkit leading to a withdrawal of access to NHS data and systems	Key organisational deliverable	Data and information management, Security, Technology	Medium
612	Loss of the ability to find, open, work with, understand or trust Dorset Council's digital information causes disruption to business operations	Key organisational deliverable	Data and information management, Operations, Reputation, Security, Technology	Very High

Place

ID	Place Risk	Strategic Priority	Principal Risk(s)	Risk Rating
144	Lack of resources results in failure to deliver the Councils' Priorities on Economy	Grow our economy	Commercial, Finance, Reputation	Medium

ID	Place Risk	Strategic Priority	Principal Risk(s)	Risk Rating
201	As a result of sea level rise driven by climate change, Dorset Council may not have the resources to adapt its coastal defences, leading to low lying areas of the county being uneconomical to defend	Respond to the climate and nature crisis	Finance, Legal, Property, Reputation	High
229	Dorset Innovation Park is unable to attract additional investment and growth causing loss of income to Dorset Council	Grow our economy	Commercial, Finance, Property, Reputation	Medium
230	Failure to engage with education sector results in the pipeline of skilled labour in the Dorset Council area reducing, increasing the skills shortage and businesses exiting the Dorset Council area	Communities for all, Grow our economy	Finance, Project / programme, Reputation	Medium
372	Due to current levels of resourcing, Dorset Council may fail to maintain the county's natural environment, leading to a failure to halt the areas nature decline	Respond to the climate and nature crisis	Finance, Operations, People	Medium
560	Because of reduced levels of funding, timely Flood and Coastal Erosion Risk Management (FCERM) activities may not be undertaken, leading to an increased risk of asset failure	Respond to the climate and nature crisis	Operations, Property	High
729	Due to the virulence of ash dieback within the highway extent, there may be a danger for highways users from fallen trees	Respond to the climate and nature crisis	Finance, Operations, People	Medium
810	As a result of a reduction to staff capacity, the renewal of the rights of way improvement plan may be delayed, leading to	Communities for all, Grow our	Finance, Project /	Low

ID	Place Risk	Strategic Priority	Principal Risk(s)	Risk Rating
	a failure to link communities and support the local economy	economy, Respond to the climate and nature crisis	programme	

Public Health and Prevention

ID	Public Health and Prevention Risk	Strategic Priority	Principal Risk(s)	Risk Rating
765	Major incident involving synthetic opiates leads to disruption of normal business for the Public Health team	Communities for all	Operations, People, Reputation	Medium
821*	As a result of health service reform, Dorset Council may incur additional unprovisioned responsibilities, leading to increased resourcing and budgetary pressures	Communities for all, Key organisational deliverable	Commercial, Finance, Operations, Reputation	Low*

*Detail to be finalised with risk owners

Public Health and Prevention Strategic Risks will be reevaluated following completion of their Business Planning processes, following their introduction into Dorset Council as the fifth Directorate.

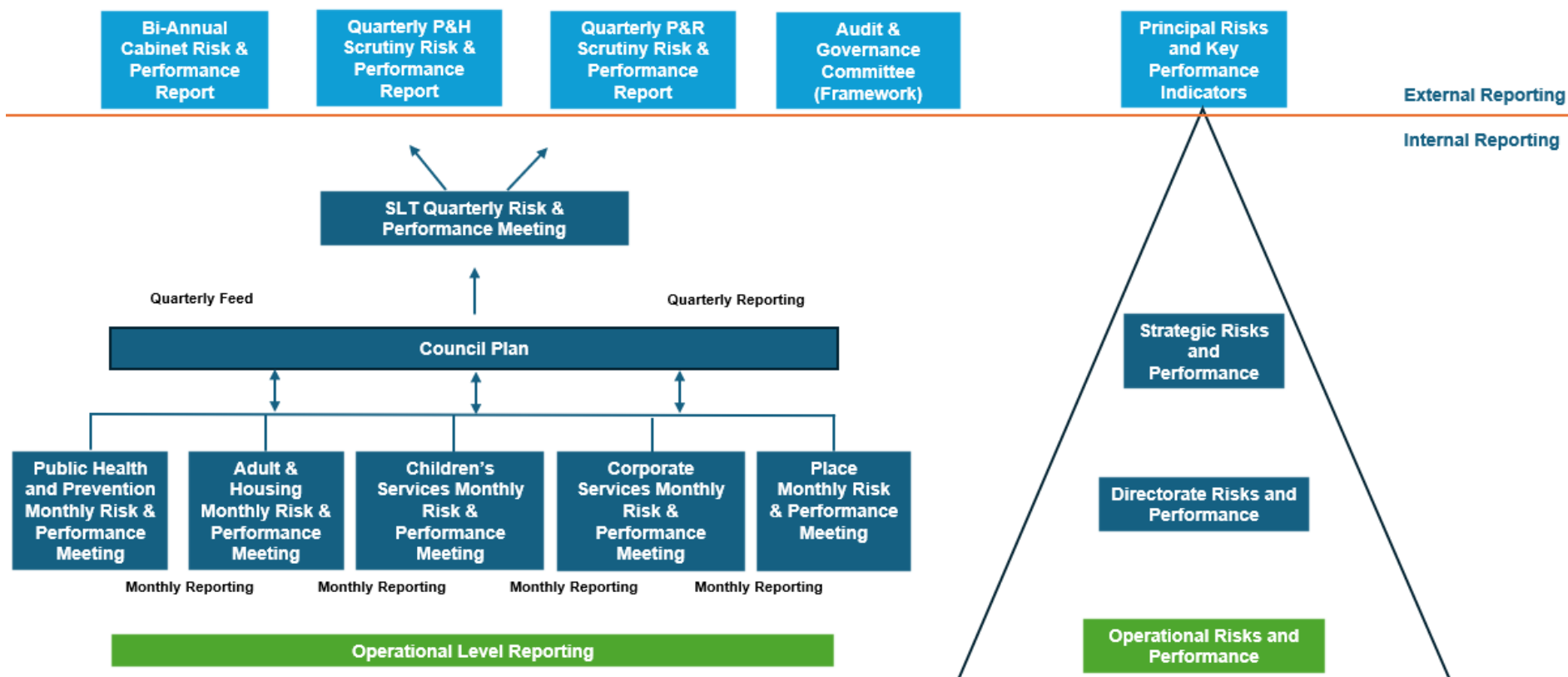
Audit and Governance Committee

04 August 2025



Dorset Council Strategic Performance and Risk Framework

Dorset Council Strategic Performance and Risk Framework



Audit and Governance Committee

04 August 2025



Applying Risk Appetite

To implement Dorset Council's risk appetite statement effectively, each principal risk area must have defined parameters that distinguish between acceptable and

unacceptable levels of risk taking and identify when escalation is necessary in line with the organisation's existing governance structures. The following template is designed to support business areas in aligning their operational risk taking with the organisations strategic steer provided by the risk appetite statement and framework.

Principal Risk	Risk Appetite	Will Accept	Will Not Accept	Escalate
<u>Commercial</u>	Open: Dorset Council has a willingness to pursue innovation, which has previously showed benefit. Its non-critical decisions may be devolved to local managers.			
<u>Data and Information Management</u>	Open: Dorset Council accepts that openness and information sharing is needed for effective operations in a controlled environment.			
<u>Finance</u>	Cautious: Dorset Council's financial decisions accept some uncertainty related to loss or impact, only if they yield upside opportunities in service delivery.			

Principal Risk	Risk Appetite	Will Accept	Will Not Accept	Escalate
<u>Legal</u>	Cautious: Dorset Council takes decisions where it must be reasonably certain that it would be able to win any legal challenge.			
<u>Operations</u>	Open: Dorset Council pursues innovation that has evidence of previous benefits. There is a willingness to innovate and responsibility for non-critical decisions may be devolved to local managers.			
<u>People</u>	Open: Dorset Council adopts devolution of certain work-related decision-making responsibilities. The organisation is willing to invest in its people to create a variety of skills in its workforce.			
<u>Project / Programme</u>	Open: Dorset Council pursues innovation when projects / programmes display demonstrable benefits. Decision making may be devolved to local managers, with plans aligned to functional standards.			

Principal Risk	Risk Appetite	Will Accept	Will Not Accept	Escalate
<u>Property</u>	Open: Dorset Council can adopt a range of agreed solutions for purchase, rental, disposal, construction and refurbishment of property that ensures it meets organisational needs.			
<u>Reputation</u>	Open: Dorset Council has appetite to take decisions with the potential to expose the organisation to additional scrutiny, but only where appropriate steps are taken to control the risk.			
<u>Security</u>	Averse: Dorset Council has no tolerance for security risks causing loss or damage to its property, assets, information or people with stringent control measures in place.			
<u>Technology</u>	Eager: Dorset Council views new systems and technology as essential for organisational development and service delivery.			

This page is intentionally left blank

Audit and Governance Committee Monday, 4 August 2025 Treasury Management Annual Report 2024/25

For Decision

Portfolio Holder: Cllr S Clifford, Finance & Capital Strategy

Local Councillor(s): All

Executive Director: A Dunn, Executive Director, Corporate Development

Report Author: David Wilkes
Title: Service Manager (Treasury and Investments)
Tel: 01305 224119
Email: david.wilkes@dorsetcouncil.gov.uk

Report Status: Public

Brief Summary

This report summarises the treasury management performance and position information for Dorset Council for the year ended 31 March 2025.

Treasury management at the Council is conducted within the framework of CIPFA's Treasury Management Code of Practice. In adopting the code, recommended best practice is for members to approve an annual treasury management strategy report, and to then receive a mid-year update on progress against the strategy and a year-end review of actual performance against the strategy (this report).

All treasury management activity in the year complied with the limits and parameters included in the Treasury Management Strategy for 2024/25 approved by full Council February 2024.

All capital expenditure must be financed, either from external sources (government grants and other contributions), the Council's own resources (revenue, reserves and capital receipts) or debt (borrowing, leasing and Private

Finance Initiative). The Council's cumulative outstanding amount of debt finance is measured by the Capital Financing Requirement (CFR).

The Council's Capital Financing Requirement (CFR) at 31 March 2025 was £434m, up £46m from £388m at the start of the year but £49m below the budget of £483m when the capital strategy was approved by full Council in February 2024.

As at 31 March 2025, the Council had outstanding external borrowing of £292m plus other capital financing liabilities of £34m equalling £326m total external debt, with £9.8m total interest paid servicing this external debt for the year.

The difference between the CFR and external debt was approximately £115m, financed by 'internal borrowing' which is the use of reserves, working capital and other balance sheet resources that would otherwise have been invested had they not been used to 'offset' the Council's borrowing requirement.

As at 31 March 2025 the Council held cash and cash equivalents of £36m and treasury investments valued at £27m, in total £63m, down from £69m from 31 March 2024. The total interest receivable and investment income for the Council for the year was approximately £6.4m.

Recommendation:

That the Committee note and comment upon the report.

Reason for Recommendation:

To better inform members of treasury management activity, in accordance with the corporate requirement to ensure money and resources are used wisely.

1. Introduction

- 1.1 The Council's treasury management strategy for 2024/25 was approved by a meeting of Dorset Council on 13 February 2024.
- 1.2 The Council has borrowed and invested substantial sums of money and is therefore exposed to financial risks including the loss of invested funds and the revenue effect of changing interest rates. The successful identification, monitoring and control of risk remains central to the Council's treasury management strategy.
- 1.3 Treasury risk management at the Council is conducted within the

framework of the Chartered Institute of Public Finance and Accountancy's Treasury Management in the Public Services: Code of Practice 2021 Edition (the CIPFA Code) which requires the Council to approve a treasury management strategy before the start of each financial year and, as a minimum, a semi-annual and annual treasury outturn report. This report fulfils the Council's legal obligation under the Local Government Act 2003 to have regard to the CIPFA Code.

- 1.4 The Council employs professionally qualified and experienced staff with responsibility for making borrowing and investment decisions. Officers are supported by external advisers who are specialists in their fields. The Council currently employs Arlingclose Limited as treasury management advisers.
- 1.5 This approach ensures that the Council has access to a wide pool of relevant market intelligence, knowledge and skills that would be very difficult and costly to replicate internally. However, whilst advisers provide support to the internal treasury function, final decisions on treasury matters always remain with the Council.

2. External Context

- 2.1 Treasury management decisions made by the Council must take into consideration external factors, particularly the wider economic backdrop and the outlook for financial markets and interest rates, and the wider regulatory framework.
- 2.2 Over the course of the financial year the Bank of England's Monetary Policy Committee (MPC) reduced Bank Rate from 5.25% to 4.5%, with three cuts of 0.25% in August 2024, November 2024 and March 2025. The Bank Rate is important for the Council's treasury activities because the returns on cash balances tend to follow this quite closely as do short term borrowing rates. Interest rates on long term borrowing are more closely aligned to interest rates on government borrowing ('gilts') which held up higher than expected due to upward pressure on the level of expected government borrowing.
- 2.4 A detailed commentary on the external context provided by Arlingclose is included in Appendix 1.

3. Local Context

- 3.1 The Council's balance sheet is summarised in table 1 below.

Table 1: Balance Sheet Summary

	31-Mar 2024 Actual £m	31-Mar 2025 Budget £m	31-Mar 2025 Forecast £m	31-Mar 2025 Actual £m	2024/25 Annual Change £m
Capital Financing Requirement (CFR)	388	483	450	434	46
Less PFI other debt liabilities	19	20	20	34	15
Loans CFR (underlying borrowing requirement)	370	463	430	400	30
External borrowing	225	313	325	292	68
Internal borrowing	145	150	105	107	-38
Cash and investments	69	65	60	63	-6

- 3.2 All capital expenditure must be financed, either from external sources (government grants and other contributions), the Council's own resources (revenue, reserves and capital receipts) or debt (borrowing, leasing and Private Finance Initiative). The Council's cumulative outstanding amount of debt finance is measured by the Capital Financing Requirement (CFR).
- 3.3 Debt is only a temporary source of finance, since loans and leases must be repaid, and this is therefore replaced over time by other financing, usually from revenue which is known as Minimum Revenue Provision (MRP). Alternatively, proceeds from selling capital assets (known as capital receipts) may be used to replace debt finance. The CFR increases with new debt-financed capital expenditure and reduces with MRP and capital receipts used to replace debt.
- 3.4 The CFR has risen by £45m over the year to £434m, which is £49m less than budgeted due to slippage in delivering the capital programme. External borrowing has increased by £63m over the year, which is higher than the increase in CFR as the Council has less reserves available to support 'internal borrowing' than it did at the beginning of the year.
- 3.5 The treasury management position at 31 March 2025 and the change during the year is shown in Table 2 below.

Table 2: Treasury Management Summary

	31.03.24 Balance £m	2024/25 Movement £m	31.03.25 Balance £m
Long-term borrowing			
PWLB*	78.4	67.1	145.6
LOBO loans**	11.0	0.0	11.0
Other	85.6	0.0	85.6
Short-term borrowing	49.5	0.5	50.0
Total borrowing	224.5	67.6	292.2
Long-term investments	19.0	0.3	19.3
Short-term investments	32.5	-24.0	8.4
Cash and cash equivalents	17.9	17.6	35.5
Total investments	69.4	-6.2	63.2
Net borrowing	155.1	73.8	228.9

* Public Works Loan Board loans from the UK Debt Management Office.

**Lender Option Borrower Option loans.

4. External Borrowing

4.1 At 31 March 2025 the Council held £293m of loans, a net increase of £68m from 31 March 2024, as part of its strategy for funding previous and current years' capital programmes. Outstanding loans as at 31 March 2025 are summarised in Table 3 below.

Table 3: External Borrowing

	31.03.24 Balance £m	Net Change £m	31.03.25 Balance £m	31.03.25 Weighted Average Rate %	31.03.25 Weighted Average Maturity (years)
Public Works Loan Board	91.0	54.6	145.6	4.6%	11.5
Banks (LOBO)	11.0	0.0	11.0	4.6%	51.6
Banks (fixed-term)	25.6	0.0	25.6	4.7%	52.1
Local authorities (long-term)	15.0	0.0	15.0	4.4%	34.5
Local authorities (short-term)	37.0	13.0	50.0	4.8%	0.4
Other lenders (fixed-term)	45.0	0.0	45.0	3.3%	41.6
Total borrowing	224.6	67.6	292.2	4.5%	27.4

- 4.2 The chief objective of Dorset Council and its predecessors when borrowing has been to strike an appropriately low risk balance between securing low interest costs and achieving cost certainty over the period for which funds are required, with flexibility to renegotiate loans should long-term plans change being a secondary objective.
- 4.3 The Council's borrowing decisions are not predicated on any one outcome for interest rates and a balanced portfolio of short and long-term borrowing has been maintained.
- 4.4 The Council held £11m of Lender's Option Borrower's Option (LOBO) at 31 March 2025. These are loans where the lender has the option to propose an increase in the interest rate at set dates (lender's option), following which the Council has the option to either accept the new rate or to repay the loan at no additional cost (borrower's option).
- 4.5 In addition, capital finance may be raised by the following methods that are not borrowing but are classed as other debt liabilities: leasing, hire purchase, Private Finance Initiative (PFI) and sale and leaseback. Total debt other than borrowing at 31 March 2025 was £26.2m.
- 4.6 CIPFA's 2021 Prudential Code is clear that local authorities must not borrow to invest primarily for financial return and that it is not prudent for local authorities to make any investment or spending decision that will increase the capital financing requirement and so may lead to new borrowing, unless directly and primarily related to the functions of the Council. PWLB loans are no longer available to local authorities planning to buy investment assets primarily for yield unless these loans are for refinancing purposes.
- 4.7 The Council has not invested in assets primarily for financial return or that are not primarily related to the functions of the Council.

5. Cash and Treasury Investments

- 5.1 The CIPFA Treasury Management Code defines treasury management investments as those investments which arise from an authority's cash flows or treasury risk management activity that ultimately represents balances that need to be invested until the cash is required for use in the course of business.
- 5.2 Cash, cash equivalents and treasury investments held on 31 March 2025 are summarised in Table 4 below.

Table 4: Cash and Treasury Investments

	31.03.24 Balance £m	Net Movement £m	31.03.25 Balance £m
Cash & Cash Equivalents	17.9	17.6	35.5
Investments:			
Short-dated bond funds	2.8	0.0	2.9
Strategic bond funds	10.0	-4.4	5.6
Equity income funds	13.7	-13.7	0.0
Property funds	19.0	0.3	19.3
Multi asset income funds	6.0	-6.0	0.0
Total Investments	51.5	-23.8	27.7
Total Cash & Investments	69.4	-6.2	63.2

5.3 Both the CIPFA Code and government guidance require the Council to invest its funds prudently, and to have regard to the security and liquidity of its treasury investments before seeking the optimum rate of return, or yield. The Council's objective when investing money is to strike an appropriate balance between risk and return, minimising the risk of incurring losses from defaults and the risk of receiving unsuitably low investment income.

5.4 The Council holds investments in bond, equity, multi-asset and property funds which were 'inherited' from a number of the predecessor councils. These investments are held for the longer term with the acceptance that capital values will fluctuate over the short term but with the expectation that over a three to five-year period total returns will exceed cash interest rates. These 'strategic investments' were valued at £27.7m in total as at 31 March 2025.

6. Treasury Performance

6.1 The Council measures the financial performance of its treasury management as shown in table 5 below.

Table 5: Treasury Performance

	Budget 31.03.25 £m	Actual 31.03.25 £m	Variance £m	
Interest Payable	10.3	9.8	0.5	F
Interest and Investment Income	-7.0	-6.4	-0.6	A
Net Payable / (Receivable)	3.3	3.4	-0.1	A
Realised (Gains) / Losses in Fair Value	0.0	-0.8	0.8	F
Unrealised (Gains) / Losses in Fair Value	0.0	-0.3	0.3	F
Net (Surplus) / Deficit	3.3	2.3	1.0	F

6.2 Realised gains or losses in fair value result from the sale of units in pooled investment funds at a different price to that which they were purchased at. Total net realised gains in fair value from the sale of units in such funds in the financial year were £0.8m.

6.2 Unrealised gains or losses in fair value result from the holding of units in pooled investment funds that are valued at a different price to that which they were purchased at. Total net unrealised gains in fair value from holding units in such funds at the financial year end were £0.3m.

6.3 Unrealised gains or losses in the fair value of pooled investment funds, that otherwise must be recognised in profit or loss under International Financial Reporting Standard (IFRS) 9, are not charged to the revenue account, and must be taken into an unusable reserve account.

7. Compliance

7.1 All treasury management activities undertaken during the year complied with the CIPFA Code of Practice and the Council's approved Treasury Management Strategy.

7.2 Compliance with the limits on cash and treasury investments is demonstrated in the table below.

Table 6: Cash and Investments Limits

	2024/25 Maximum £m	31.03.25 Actual £m	2024/25 Limit £m	Complied Yes/No
Any single organisation, except the UK Government	11.8	1.1	20	Yes
Any group of organisations under the same ownership	11.8	1.1	20	Yes
Any group of pooled funds under the same management	29.1	17.0	50	Yes
Negotiable instruments held in a broker's nominee account	0.0	0.0	50	Yes
Limit per non-UK country	0.0	0.0	20	Yes
Registered providers and registered social landlords	0.0	0.0	50	Yes
Unsecured investments with banks and building societies	11.8	1.1	20	Yes
Loans to unrated corporates	0.0	0.0	20	Yes
Money Market Funds	103.9	37.2	unlimited	Yes
Strategic pooled funds	51.8	27.7	unlimited	Yes
Real Estate Investment Trusts	0.0	0.0	50	Yes

7.3 The Council is legally obliged to set an affordable “authorised limit” for external debt each year. In line with statutory guidance, a lower “operational boundary” is also set as a warning level should debt approach the limit. Compliance with the authorised limit and operational boundary for external debt is demonstrated in the table below.

Table 7: Debt Limits

	2024/25 Maximum £m	31.03.25 Actual £m	2024/25 Operational Boundary £m	2024/25 Authorised Limit £m	Complied Yes/No
Total External Debt	326	326	507	532	Yes

8. Treasury Management Indicators

8.1 The Council measures and manages its exposures to treasury management risks using the following indicators.

- 8.2 **Liability Benchmark:** This indicator compares the Council's actual existing borrowing against a 'liability benchmark' that has been calculated to show the lowest risk level of borrowing. The liability benchmark is an estimate of the minimum amount of external borrowing the Council must hold to fund its current capital and revenue plans while keeping cash and investments at a minimum 'liquidity allowance' to manage day-to-day cash flows.

Table 8: Liability Benchmark

	31.03.24 Actual £m	31.03.25 Actual £m
Loans CFR	370	400
Less balance sheet resources	214	171
Net loans requirement	155	229
Plus liquidity allowance	30	30
Liability benchmark	185	259
Actual borrowing	225	292

- 8.3 **Security:** The Council has adopted a voluntary measure of its exposure to credit risk by monitoring the value-weighted average credit score of its investment portfolio. This is calculated by applying a score to each investment (AAA = 1, AA+ = 2 etc.) and taking the average, weighted by the size of each investment. Unrated investments are assigned a score based on their perceived risk.

Table 9: Security

	2024/25 Target	31.03.25 Actual	Complied? Yes/No
Portfolio average credit rating	< 6	4.95	Yes

- 8.4 **Liquidity:** The Council has adopted a voluntary measure of its exposure to liquidity risk by monitoring the amount of cash available to meet unexpected payments within a rolling three-month period without additional borrowing. In addition, the Council aims to hold a minimum of £30m readily available in same day access bank accounts and Money Market Funds.

Table 10: Liquidity

	2024/25 Target	31.03.25 Actual	Complied? Yes/No
Total cash available within 100 days	> 30%	50%	Yes

- 8.5 Interest Rate Exposure: This indicator is set to control the Council's exposure to interest rate risk. Bank Rate reduced by 0.75% from 5.25% on 1 April 2024 to 4.50% by 3 March 2025. The upper limits on the one-year revenue impact of a 1% rise or fall in interests were:

Table 11: Interest Rate Exposure

Interest rate risk indicator	2024/25 Target £000s	31.03.25 Actual £000s	Complied? Yes/No
Upper limit on one-year revenue impact of a 1% <u>rise</u> in interest rates	< 1,000	255	Yes
Upper limit on one-year revenue impact of a 1% <u>fall</u> in interest rates	< 1,000	-255	Yes

- 8.6 The impact of a change in interest rates is calculated on the assumption that maturing borrowing and investments will be replaced.
- 8.7 Sums invested for periods longer than a year: The purpose of this indicator is to control the Council's exposure to the risk of incurring losses by seeking early repayment of its investments. The limits on the long-term principal sum invested to final maturities beyond the period end were:

Table 12: Investments longer than one year

	2024/25	2025/26	2026/27	No fixed date
	£m	£m	£m	£m
Limit on principal invested beyond one year	20.0	20.0	20.0	100.0
Actual principal invested beyond one year	0.0	0.0	0.0	27.7
Complied (Yes/No)	Yes	Yes	Yes	Yes

- 8.8 Maturity Structure of Borrowing: This indicator is set to control the Council's exposure to refinancing risk. The upper and lower limits on the maturity structure of borrowing were:

Table 13: Maturity Structure of Borrowing

	31.03.25 Actual £m	% of Total Borrowing	Upper Limit	Lower Limit	Complied Yes/No
Under 12 months	50.0	17.1%	30%	0%	Yes
1 to 2 years	20.0	6.8%	30%	0%	Yes
2 to 5 years	52.6	18.0%	30%	0%	Yes
5 to 10 years	30.1	10.3%	35%	0%	Yes
10 to 20 years	1.3	0.4%	35%	0%	Yes
20 to 30 years	41.8	14.3%	45%	0%	Yes
30 to 40 years	15.0	5.1%	45%	0%	Yes
40 to 50 years	45.0	15.4%	45%	0%	Yes
50 years and above	36.4	12.5%	50%	0%	Yes
Total	292.2	100.0%			

9. Financial Implications

This report summarises the performance of the Council's treasury management activity in 2024/25. There are no other financial implications arising from this report.

10. Natural Environment, Climate & Ecology Implications

There are no direct natural environment, climate and ecology implications arising from this report.

11. Well-being and Health Implications

There are no well-being and health implications arising from this report.

12. Other Implications

There are no other implications arising from this report.

13. Risk Assessment

Having considered the risks associated with this decision, the level of risk has been identified as:

Current Risk: HIGH

Residual Risk: Medium

Treasury management is an inherently risky area of activity and a number of controls are embedded in its operation. The key treasury management risks are

highlighted as part of the treasury management strategy approved by Council as part of the budget setting process. This report highlights any variances from this strategy and draws out any specific risks which have arisen

14. Equalities Impact Assessment

There are no equalities implications arising from this report.

15. Appendices

Appendix 1: External Context (Arlingclose April 2025)

Appendix 2: Glossary of Treasury Management Terms

16. Background Papers

Capital Strategy 2024/25

Treasury Management Strategy 2024/25

Appendix 1: External Context (Arlingclose April 2025)

Economic background: Both the UK and US elected new governments during the period, whose policy decisions impacted the economic outlook. The Chancellor of the Exchequer delivered her Spring Statement in March 2025, following her Budget in October 2024. Based on the plans announced, the Office for Budget Responsibility downgraded its predictions for UK growth in 2025 to 1% from 2%. However, it upgraded its predictions for the four subsequent years. Inflation predictions for 2025 were pushed up, to 3.2% from 2.6%, before seen as falling back to target in 2027. The market reaction to the Spring Statement was more muted compared to the Budget, with very recent market turbulence being driven more by US trade policy decisions and President Trump.

After revising its interest rate forecast in November following the Budget, the council's treasury management advisor, Arlingclose, maintained its stance that Bank Rate will fall to 3.75% in 2025.

UK annual Consumer Price Index (CPI) inflation continued to stay above the 2% Bank of England (BoE) target in the later part of the period. The Office for National Statistics (ONS) reported headline consumer prices at 2.8% in February 2025, down from 3.0% in the previous month and below expectations. Core CPI also remained elevated, falling slightly in February to 3.5% from 3.7% in January, just below expectations for 3.6% but higher than the last three months of the calendar year.

The UK economy Gross Domestic Product (GDP) grew by 0.1% between October and December 2024, unrevised from the initial estimate. This was an improvement on the zero growth in the previous quarter, but down from the 0.4% growth between April and June 2024. Of the monthly GDP figures, the economy was estimated to have contracted by 0.1% in January, worse than expectations for a 0.1% gain.

The labour market continued to cool, but the ONS data still require treating with caution. Recent data showed the unemployment rate rose to 4.4% (3mth/year) in the three months to January 2025 while the economic inactivity rate fell again to 21.5%. The ONS reported pay growth over the same three-month period at 5.9% for regular earnings (excluding bonuses) and 5.8% for total earnings.

The BoE's Monetary Policy Committee (MPC) held Bank Rate at 4.5% at its March 2025 meeting, having reduced it in February. This follows earlier 0.25% cuts in November and August 2024 from the 5.25% peak. At the March MPC meeting, members voted 8-1 to maintain Bank Rate at 4.5%, with the one dissenter

preferring another 25 basis points cut. The meeting minutes implied a slightly more hawkish tilt compared to February when two MPC members wanted a 50bps cut. In the minutes, the Bank also upgraded its Q1 2025 GDP forecast to around 0.25% from the previous estimate of 0.1%.

The February Monetary Policy Report (MPR) showed the BoE expected GDP growth in 2025 to be significantly weaker compared to the November MPR. GDP is forecast to rise by 0.1% in Q1 2025, less than the previous estimate of 0.4%. Four-quarter GDP growth is expected to pick up from the middle of 2025, to over 1.5% by the end of the forecast period. The outlook for CPI inflation showed it remaining above the MPC's 2% target throughout 2025. It is expected to hit around 3.5% by June before peaking at 3.7% in Q3 and then easing towards the end of the year but staying above the 2% target. The unemployment rate was expected to rise steadily to around 4.75% by the end of the forecast horizon, above the assumed medium-term equilibrium unemployment rate of 4.5%.

Arlingclose, the authority's treasury adviser, maintained its central view that Bank Rate would continue to fall throughout 2025. From the cuts in August and November 2024 and February 2025, which took Bank Rate to 4.50%, May is considered the likely month for the next reduction, with other cuts following in line with MPR months to take Bank Rate down to around 3.75% by the end of 2025.

The US Federal Reserve paused its cutting cycle in the first three months of 2025, having reduced the Fed Funds Rate by 0.25% to a range of 4.25%-4.50% in December, the third cut in succession. Fed policymakers noted uncertainty around the economic outlook but were anticipating around 0.50% of further cuts in the policy rate in 2025. Economic growth continued to rise at a reasonable pace, expanding at an annualised rate of 2.4% in Q4 2024 while inflation remained elevated over the period. However, growth is now expected to weaken by more than previously expected in 2025, to 1.7% from 2.1%. The uncertainty that President Trump has brought both before and since his inauguration in January is expected to continue.

The European Central Bank (ECB) continued its rate cutting cycle over the period, reducing its three key policy rates by another 0.25% in March, acknowledging that monetary policy is becoming meaningfully less restrictive. Euro zone inflation has decreased steadily in 2025, falling to 2.2% in March, the lowest level since November 2024. Over the current calendar year, inflation is expected to average 2.3%. GDP growth stagnated in the last quarter of the 2024 calendar year, after expanding by 0.4% in the previous quarter. For 2025, economic growth forecasts were revised downwards to 0.9%.

Financial markets: Financial market sentiment was reasonably positive over most of the period, but economic, financial and geopolitical issues meant the trend of market volatility remained. In the latter part of the period, volatility increased and bond yields started to fall following a January peak, as the economic uncertainty around likely US trade policy impacted financial markets. Yields in the UK and US started to diverge in the last month of the period, with the former rising around concerns over the fiscal implications on the UK government from weaker growth, business sentiment and higher rates, while the latter started falling on potential recession fears due to the unpredictable nature of policy announcements by the US President and their potential impact.

The 10-year UK benchmark gilt yield started the period at 3.94% and ended at 4.69%, having reached a low of 3.76% in September and a high of 4.90% in January in between. While the 20-year gilt started at 4.40% and ended at 5.22%, hitting a low of 4.27% in September and a high of 5.40% in January. The Sterling Overnight Rate (SONIA) averaged 4.90% over the period.

(The period in question ended shortly before US President Donald Trump announced his package of 'reciprocal tariffs', the immediate aftermath of which saw stock prices and government bond yields falling and introduced further uncertainty over the economic outlook.)

Credit review: In October 2024, Arlingclose revised its advised recommended maximum unsecured duration limit on most banks on its counterparty list to six months. Duration advice for the remaining five institutions, including the newly added Lloyds Bank Corporate Markets, was kept to a maximum of 100 days. This advice remained in place at the end of the period.

Credit default swap prices generally trended lower over the period but did start to rise modestly in March, but not to any levels considered concerning. Once again, price volatility over the period remained generally more muted compared to previous periods.

Financial market volatility is expected to remain a feature, at least in the near term and, credit default swap levels will be monitored for signs of ongoing credit stress. As ever, the institutions and durations on the Authority's counterparty list recommended by Arlingclose remain under constant review.

Appendix 2: Glossary of Treasury Management Terms

Annuity	A method of repaying a loan where the cash payment remains constant over the life of the loan, but the proportion of interest reduces and the proportion of principal repayment increases over time. Repayment mortgages and personal loans tend to be repaid by the annuity method.
Balance sheet resources	Arlingclose term for the sum of <i>usable reserves</i> and <i>working capital</i> . Equal to the difference between the <i>loans CFR</i> and the <i>net loans requirement</i> .
Bank Rate	The official interest rate set by the <i>Monetary Policy Committee</i> , and the rate of interest paid by the <i>Bank of England</i> on commercial bank deposits. Colloquially termed the “base rate”.
Bond	A certificate of <i>long-term</i> debt issued by a company, government, or other institution, which is tradable on financial markets.
Bond fund	A <i>collective investment scheme</i> that invests mainly in <i>bonds</i> .
Call account	A <i>deposit</i> account that can be called back, normally on instant access.
Capital	(1) Long-term, as in <i>capital expenditure</i> and <i>capital receipt</i>. (2) Principal, as in <i>capital gain</i> and capital value. (3) Investments in <i>financial institutions</i> that will absorb losses before <i>senior unsecured creditors</i>.
Capital expenditure	Expenditure on the acquisition, creation or enhancement of fixed assets that are expected to provide value for longer than one year, such as property and equipment, plus expenditure defined as capital in legislation such as the purchase of certain investments and expenditure directed by the government to be treated as capital.
Capital finance	Arranging and managing the cash required to finance <i>capital expenditure</i> , and the associated accounting.
Capital financing requirement (CFR)	A local authority’s underlying need to hold debt for capital purposes, representing the cumulative capital expenditure that has been incurred but not yet financed. The CFR increases with <i>capital expenditure</i> and decreases with <i>capital finance</i> and <i>MRP</i> .
Capital receipt	Cash obtained from the sale of an item whose purchase would be <i>capital expenditure</i> . The law only allows local authorities to spend capital receipts on certain items, such as new capital expenditure. They are therefore held in a capital receipts reserve until spent.
Capital strategy	An annual report required by the <i>Prudential Code</i> that sets out a local authorities’ high-level plans for capital expenditure, debt and investments and its <i>Prudential Indicators</i> for the forthcoming financial year.
Cash equivalent	Accounting term for short-term investments readily convertible to cash with an insignificant risk of change in value.

Collective investment scheme	Scheme in which multiple investors collectively hold units or shares. The investment assets in the fund are not held directly by each investor, but as part of a pool (hence these funds are also referred to as 'pooled funds').
Commercial investment	An investment whose main purpose is generating income, such as <i>investment property</i> .
Cost of carry	When a loan is borrowed in advance of need, the difference between the interest payable on the loan and the income earned from investing the cash in the interim.
Counterparty	The other party to a loan, investment or other contract.
Counterparty limit	The maximum amount an investor is willing to lend to a <i>counterparty</i> , in order to manage <i>credit risk</i> .
Country limit	The maximum amount an investor is willing to lend to all <i>counterparties</i> based in a foreign country, in order to manage <i>credit risk</i> .
Coupon	The contractual interest rate payable on a <i>bond</i> , as a percentage of the <i>nominal</i> amount. This normally reflects market conditions when the bond was originally issued.
Credit default swap (CDS)	<i>Derivative</i> for swapping <i>credit risk</i> on a particular issuer, similar to an insurance policy where the buyer pays a <i>premium</i> against the risk of default. Also used as an indicator of credit risk: the higher the premium, the higher the perceived risk.
Credit rating	Formal opinion by a <i>credit rating agency</i> of a <i>counterparty's</i> future ability to meet its financial obligations. As it is only an opinion, there is no guarantee that a highly rated organisation will not default.
Credit rating agency	An organisation that publishes <i>credit ratings</i> . The three largest agencies are Fitch, Moody's and Standard & Poor's but there are many smaller ones.
Credit risk	The risk that a <i>counterparty</i> will <i>default</i> on its financial obligations.
DMADF	Debt Management Account Deposit Facility – a facility offered by the <i>DMO</i> enabling local authorities to deposit cash at very low <i>credit risk</i> . Not available in Northern Ireland.
DMO	Debt Management Office – an executive agency of HM Treasury that deals with central government's debt and investments.
EIP	Equal instalments of principal. A method of repaying a loan where the principal is repaid over the life of the loan, in equal instalments. Interest payments reduce over time as the principal is repaid.
Equity fund	A <i>collective investment scheme</i> that mainly invests in company <i>shares</i> .
FCA	Financial Conduct Authority – UK agency responsible for regulating financial markets and the conduct of <i>financial institutions</i> , <i>brokers</i> , <i>custodians</i> , <i>fund managers</i> and <i>treasury management advisors</i> .

Gilt	Bond issued by the UK Government, taking its name from the gilt-edged paper they were originally printed on.
Gilt yield	<i>Yield on gilts</i> . Commonly used as a measure of risk-free long-term interest rates in the UK.
Interest rate risk	The risk that unexpected changes in interest rates cause an unplanned loss, for example by increased payments on borrowing or lower income on investments.
Internal borrowing	A local government term for when actual “external” <i>debt</i> is below the <i>capital financing requirement</i> , indicating that difference has been borrowed from internal resources instead; in reality this is not a form of borrowing.
Liability benchmark	Term in CIPFA’s <i>Treasury Management Code</i> which refers to the minimum amount of borrowing required to keep investments at a minimum liquidity level. Used to compare the actual and forecast levels of borrowing.
Liquidity risk	The risk that cash will not be available to meet financial obligations, for example when investments cannot be recalled and new loans cannot be borrowed.
Loans CFR	The <i>capital financing requirement</i> less the sum met by <i>other long-term liabilities</i> ; i.e. the underlying need to borrow for capital purposes.
LOBO	Lender’s option borrower’s option – a long-term loan where the lender has the option to propose an increase in the interest rate on pre-determined dates. The borrower then has the option to either accept the new rate or repay the loan without penalty. LOBOs increase the borrower’s interest rate risk and the loan should therefore attract a lower rate of interest initially.
Market risk	The risk that movements in market variables will have an unexpected impact. Usually split into <i>interest rate risk</i> , <i>price risk</i> and <i>foreign exchange risk</i> .
Maturity	(1) The date when an investment or borrowing is scheduled to be repaid. (2) A type of loan where the principal is only repaid on the maturity date.
Maturity profile	A table or graph showing the amount (or percentage) of debt or investments maturing over a time period.
Monetary Policy Committee (MPC)	Committee of the <i>Bank of England</i> responsible for implementing <i>monetary policy</i> in the UK by changing <i>Bank Rate</i> and <i>quantitative easing</i> with the aim of keeping <i>CPI</i> inflation at around 2%.
Money market fund (MMF)	A <i>collective investment scheme</i> which invests in a range of short-term assets providing high credit quality and high liquidity. Usually refers to <i>CNAV</i> and <i>LVNAV</i> funds with a <i>WAM</i> under 60 days which offer instant access, but the European Union definition extends to include <i>cash plus funds</i> .
MRP	Minimum revenue provision - an annual amount that local authorities are required to set aside and charge to revenue for the repayment of debt associated with capital expenditure. Local authorities are required by law to have regard to government guidance on MRP. Not applicable in Scotland, but see <i>Loans Fund</i> .

Municipal bonds agency	Company that issues <i>bonds</i> in the <i>capital market</i> and lends the proceeds back to local authorities. The bonds are guaranteed by the local authorities.
Net borrowing	<i>Borrowing</i> minus <i>treasury investments</i> .
Net loans requirement	CIPFA term for the forecast amount of borrowing required to generate zero <i>treasury investments</i> .
Other long-term liabilities	<i>Prudential Code</i> term for <i>credit arrangements</i> .
Operational boundary	A <i>prudential indicator</i> showing the most likely, prudent, estimated level of external <i>debt</i> , but not the worst-case scenario. Regular breaches of the operational boundary should prompt management action.
Pension Fund	Ringfenced account for the income, expenditure and investments of the local government pension scheme. Pension fund investments are not considered to be part of <i>treasury management</i> .
Pooled fund	See <i>collective investment scheme</i> .
PRA	Prudential Regulation Authority – the part of the <i>Bank of England</i> that regulates UK banks.
Principal	The amount of money originally lent on a <i>debt</i> instrument.
Private Finance Initiative (PFI)	A government scheme where a private company designs, builds, finances and operates assets on behalf of the public sector, in exchange for a series of payments, typically over 30 years. Counts as a <i>credit arrangement</i> and <i>debt</i> .
Property fund	A <i>collective investment scheme</i> that mainly invests in property. Due to the costs of buying and selling property, including <i>stamp duty land tax</i> , there is usually a significant fee charged on initial investment, or a significant difference between the <i>bid</i> and <i>offer</i> price.
Prudential borrowing	Another term for <i>unsupported borrowing</i> .
Prudential Code	Developed by CIPFA and introduced in April 2004 as a professional code of practice to support local authority capital investment planning within a clear, affordable, prudent and sustainable framework and in accordance with good professional practice. Local authorities are required by law to have regard to the Prudential Code.
Prudential indicators	Indicators required by the <i>Prudential Code</i> and determined by the local authority to define its capital expenditure and asset management framework. They are designed to support and record local decision making in a manner that is publicly accountable.
PWLB	Public Works Loans Board – formerly a statutory body operating within the <i>DMO</i> that lent money from the National Loans Fund to local authorities and other prescribed bodies and collected the repayments. The term now refers to the replacement facility operated by the DMO. Not available in Northern Ireland.
Realised gain or loss	Gain or loss that will not be reversed later, e.g. because the instrument has been sold. See also <i>unrealised gain or loss</i> .

Redemption	The process of withdrawing cash from a <i>collective investment scheme</i> and cancelling the units of shares. Redemptions can be suspended in certain circumstances detailed in the <i>prospectus</i> .
Refinancing risk	The risk that maturing loans cannot, be refinanced, or only at higher than expected interest rates leading to an unplanned loss. Managed by maintaining a smooth <i>maturity profile</i> .
Revenue expenditure	Expenditure to meet the ongoing cost of delivering public services including salaries and the purchase of goods and services, as opposed to <i>capital expenditure</i> .
Service investments	Investments made to promote a local authority's public service objectives, for example a <i>loan</i> to a local charity or <i>shares</i> in a local company.
Strategic funds	<i>Collective investment schemes</i> that are designed to be held for the long-term, comprising <i>strategic bond funds</i> , <i>diversified income funds</i> , <i>equity funds</i> and <i>property funds</i> .
Temporary borrowing	Borrowing with a term of less than one year.
Term deposit	A <i>deposit</i> that is repayable after a fixed period of time.
Treasury investments	Investments made for <i>treasury management</i> purposes, as opposed to <i>commercial investments</i> and <i>service investments</i> .
Treasury management	The management of an organisation's cash flows, investment and borrowing, with a particular focus on the identification, control and management of risk. Specifically excludes the management of pension fund investments.
Treasury management advisor	Regulated firm providing advice on <i>treasury management</i> , <i>capital finance</i> and related issues.
Treasury Management Code (TM Code)	CIPFA's Code of Practice for Treasury Management in the Public Services and Cross-Sectoral Guidance Notes, to which local authorities are required by law to have regard.
Treasury management indicators	Indicators required by the <i>Treasury Management Code</i> to assist in the management of <i>credit risk</i> , <i>interest rate risk</i> , <i>refinancing risk</i> and <i>price risk</i> .
Treasury management strategy	Annual report required by the <i>Treasury Management Code</i> covering the local authority's <i>treasury management</i> plans for the forthcoming year.
Unrealised gain or loss	Gain or loss that may be reversed later, e.g. from <i>marking to market</i> . Also called a paper gain or loss. See also <i>realised gain or loss</i> .
Unsupported borrowing	Borrowing where the cost is self-financed by the local authority. Sometimes called prudential borrowing since it was not permitted until the introduction of the <i>Prudential Code</i> in 2004. See also <i>supported borrowing</i> .
Usable reserves	Resources available to finance future <i>revenue</i> and/or <i>capital expenditure</i> . Some usable reserves are ringfenced by law for certain expenditure such as on schools or council housing.

Vanilla	A simple instrument without any additional features such as <i>embedded derivatives</i> .
Working capital	The cash surplus or deficit arising from the timing differences between income/expenditure in accounting terms and receipts/payments in cash terms.
Yield	A measure of the return on an investment, especially a <i>bond</i> . The yield on a fixed rate bond moves inversely with its price.



IT Audit Findings

Dorset Council and Pension Fund

Year ended 31 March 2025

Issued July 2025

Sumit Saroha

Engagement Lead, IT Audit

T: +44 (0) 20 7865 2210

E: Sumit.Saroha@uk.gt.com

Alex Korolchuk

Engagement Manager, IT Audit

T: +44 (0) 20 7184 4459

E: Alex.Korolchuk@uk.gt.com

Rupanshu Singh

Associate, IT Audit

T: +44 (0) 20 7865 2501

E: Rupanshu.Singh@uk.gt.com

Edward O Hodgson

Associate, IT Audit

T: +44 (0) 11 7305 7604

E: Edward.O.Hodgson@uk.gt.com



Contents

Section	Page
1. Executive summary	3
2. Scope and summary of work completed	4
3. Summary of IT audit findings	5
4. Detail of IT audit findings	7

Section 1: Executive summary

01. Executive summary	
02. Scope and summary of work completed	
03. Summary of IT audit findings	
Details of IT audit findings	

To support the financial statement audit of Dorset Council and Pension Fund (“Dorset”) for year ended 31 March 2025, Grant Thornton has completed a design and implementation review of the IT General Controls (ITGC) for applications identified as relevant to the audit.

This report sets out the summary of findings, scope of the work, the detailed findings and recommendations for control improvements.

We would like to take this opportunity to thank all the staff at Dorset for their assistance in completing this IT Audit.

Section 2: Scope and summary of work completed

01. Executive summary

02. Scope and summary of work completed

Summary of IT audit findings

Details of IT audit findings

Page 180

The objective of this IT audit was to complete a design & implementation controls review over Dorset's IT environment to support the financial statement audit. The following applications were in scope for this audit specific to Dorset Council:

- SAP
- Capita
- Active Directory

The following applications were in scope for this audit specific to Dorset Pension Fund:

- SAP
- UPM

We completed the following tasks as part of this IT Audit:

- Evaluated the roll forward ITGC assessment for security management and change management controls and cybersecurity;
- Performed high level walkthroughs, inspected supporting documentation and analysis of configurable controls in the above areas;
- Completed a detailed technical security and authorisation review of Dorset's SAP system as relevant to the financial statements audit, and
- Documented the test results and provided evidence of the findings to the IT team for remediation actions where necessary.

Section 3: Summary of IT audit findings

- 01. Executive summary
- 02. Scope and summary of work completed
- 03. Summary of IT audit findings**
- Details of IT audit findings

Summary of IT audit findings

This section provides an overview of results from our assessment of the relevant Information Technology (IT) systems and controls operating over them which was performed as part of obtaining an understanding of the information systems relevant to financial reporting. This includes an overall IT General Control (ITGC) rating per IT system and details of the ratings assigned to individual control areas.

Page 182

IT system	Level of assessment performed	Overall ITGC rating	ITGC control area rating			Related significant risks / other risks
			Security management	Technology acquisition, development and maintenance	Technology infrastructure	
SAP	Roll Forward ITGC assessment					n/a
Capita	Roll Forward ITGC assessment					n/a
UPM	Roll Forward ITGC assessment					n/a
Active Directory	Detailed ITGC assessment					n/a

Assessment

-  Significant deficiencies identified in IT controls relevant to the audit of financial statements
-  Non-significant deficiencies identified in IT controls relevant to the audit of financial statements / significant deficiencies identified but with sufficient mitigation of relevant risk
-  IT controls relevant to the audit of financial statements judged to be effective at the level of testing in scope
-  Not in scope for testing

Section 4: Details of IT audit findings

- 01. Executive summary
- 02. Scope and summary of work completed
- 03. Summary of IT audit findings
- Page 183**
Details of IT audit findings

SAP ITGC Assessment Findings

1.



Assessment

Issue and risk

Users with inappropriate access to ABAP debugger in production

GT noted that access to perform debug in the system had been provided to 8 users from Payroll team to run payroll activities and 3 users from the Business Solutions Engineer team to manage the application respectively, while it should not have been granted to any user in perpetual mode.

Refer to Appendices file, tab "SAP - ABAP Debugger" for further information.

Risks

Unauthorised access to ABAP debugger increases the risk of:

- unauthorised change or deletion of table entries including tables that are typically protected.
- the ability to perform debugging functions by inserting break-point statements into program code
- the ability to bypass authority checks and execute transactions

Recommendations

The Council has taken initial steps to mitigate the risks previously identified from our work and findings in the prior period, by reviewing the specific debugger users and reducing these from 26 to 11 users. Per discussion with management and control owners it was noted that debug access was retained for the Council's payroll team as they need to manage Z tables (customised tables) and run the payroll. Due to the high frequency of occurrence of these payroll activities, FireFighter IDs or breakglass controls were deemed not feasible to be embedded in the current set up. By removing the debug access from these remaining 11 users, it was found to impact the payroll run activities to the point they were unable to run the Council's payroll.

Management are seeking to identify alternate controls to mitigate the high risk of debug access in system for these remaining users. This should be implemented either by effecting the breakglass technology and/or GRC controls mechanism and/or automating certain elements of the payroll process. Whilst this level of access currently remains, this continues to present a risk to the Council of unauthorised access and change functions within SAP, as highlighted in our risk assessment.

Management response

From the recommendation made by Grant Thornton in last year's audit, we have significantly reduced the access to the debug authorisation to mitigate the risk that this issue poses. We have removed it from standard IT support roles and introduced the process that debug needs to be requested and approved, before it is granted and logged. There are still some specific scenarios where operationally certain authorisations are still required, which we are working on how we can minimise the access required as much as possible.

Page 184

Assessment

- Significant deficiency – ineffective control/s creating risk of significant misstatement within financial statements and / or directly impact on the planned financial audit approach.
- Deficiency – ineffective control/s creating risk of inconsequential misstatement within financial statements and not directly impacting on the planned financial audit approach
- Improvement opportunity – improvement to control, minimal risk of misstatement within financial statements and no direct impact on the planned financial audit approach

SAP ITGC Assessment Findings

Assessment	Issue and risk	Recommendations
2. 	Segregation of Duties Conflict as developers have access to production GT compared all users with the ability to develop changes in development with those with the ability to create/import transports in production and identified the following: • there were 2 user accounts with no longer required access to develop changes in development environment as well as 19 background system user accounts; • there were 2 accounts with access to import transport requests (via STMS) belonging to a former member of SAP Support Team and a background user account; • there were 3 developers with access to implement changes in production environment, having access to both development and transport changes to production. GT verified that all users were members of the SAP Support or HR Systems teams, hence a general recommendation has been made to remove access for the generic background system accounts and those users no longer requiring SAP development functionality. <i>Refer to Appendices file, tab "SAP - Developer Implementer SOD" for further information.</i> Risks The combination of access to develop and implement those changes in the production environment creates a risk that inappropriate or unauthorised changes are made to data and/ or programs	Management should segregate a user's ability to develop and implement changes. Privileged access to the production environment should be revoked from users that are involved in development. If for operational reasons access cannot be fully segregated, alternative options to mitigate the risk could include performing a review of change implementation activity logs. These should be regularly reviewed for appropriateness by an independent individual with evidence retained. Management response At the point the two development users left the authority, they no longer had access to the SAP system by virtue of the fact that their network account was locked and corporate devices were returned. Also, no development changes have been made with those users since they left, and suspicion would have been raised had any transports been created with those users and so would not have subsequently been released into production. The two users have now been locked. The 19 background system user accounts have now been set from dialog to system users to stop the ability for them to be used to log into the system. The two accounts with access to import transport requests (via STMS) belonging to a former member of SAP Support Team and a background user account were both locked at the point the person left the organisation and when the background account was no longer required, so both were not active and could not be used to log into the system. Authorisations have now also been removed as well. The three developers having access to both development and transport changes to production is due to capacity in the support team. We have minimised the number of people that can transport changes into production as much as possible, but still allowing us to operate. These three members of the SAP support team do also need to be able to make changes as well, so we're unable to place a segregation in this area. The alternative would be for someone outside of the SAP support team to apply transport changes to production, which is seen as a greater risk. The mitigations in place are that we record the transports that have been promoted to the production system in our monthly audit report and highlight if an exception occurs, which is either an unexpected user transports a change, or a transport was created and transported by the same person. This happens very rarely and has only occurred in the past through a patching activity, where we are in "firefighting mode".

Assessment

-  Significant deficiency – ineffective control/s creating risk of significant misstatement within financial statements and / or directly impact on the planned financial audit approach.
-  Deficiency – ineffective control/s creating risk of inconsequential misstatement within financial statements and not directly impacting on the planned financial audit approach
-  Improvement opportunity – improvement to control, minimal risk of misstatement within financial statements and no direct impact on the planned financial audit approach

SAP ITGC Assessment Findings

3.



User access within SAP was kept valid after the user's termination date

A leaver with a leaving date of 30 August 2024, we confirmed that the account was deactivated on 02 September 2024, 2 business days after the leaving date.

GT confirmed that this was due to the leaving date occurring on a Friday and the request being actioned the following Monday.

Risk

Where system access for leavers is not disabled in a timely manner, there is a risk that former employees will continue to have access and can process erroneous or unauthorised access transactions.

There is also a risk that these accounts may be misused by valid system users to circumvent internal controls.

Recommendations

Management should ensure that a comprehensive user administration procedures are in place to revoke application and AD access in a timely manner, before or on the leavers last working date. For a user administration process to be effective, IT must be provided with timely notifications from HR and/ or line managers

Management should consider performing user access reviews on all terminated accounts to ensure all accounts have been disabled in a timely manner.

Where old or unused accounts have been identified, these should be immediately revoked.

Management response

Our standard leaver process is that all system access is automatically removed from the account on the day the employee leaves. In this example, this means on Friday 30th August 2024, the account had no roles or authorisations and so was unable to do or see anything in the system. We then locked the account as part of our weekly leavers process on Monday 2nd September 2024, which then completes the deactivation process. The second stage to this is a manual step and so would not be feasible to carry this action out more frequently than a weekly basis, but with the first stage of removing all access from the account having already completed, means this is an extremely low risk.

Page 186

Assessment

- Significant deficiency – ineffective control/s creating risk of significant misstatement within financial statements and / or directly impact on the planned financial audit approach.
- Deficiency – ineffective control/s creating risk of inconsequential misstatement within financial statements and not directly impacting on the planned financial audit approach
- Improvement opportunity – improvement to control, minimal risk of misstatement within financial statements and no direct impact on the planned financial audit approach

SAP ITGC Assessment Findings

4.



Assessment

Issue and risk

Ineffective production client configuration settings

GT identified that the Global System Change Option (SE06) settings were set to 'Modifiable' within production client. This setting allows direct changes to objects associated with ABAP software components in production.

GT have confirmed that the setting was changed as part of an approved request SR4010905 on 04 June 2024 and the 'Changes and Transports for client specific objects' is set as 'No changes allowed'.

Risk

If client settings are not configured to restrict direct changes to repository objects or cross client customising objects in production, there is a risk that there could be unauthorised changes to financially critical production data.

Recommendations

Management should ensure that the parameter 'SE06 – System Change Option' settings are consistently set to 'Non-Modifiable' in production client.

Management response

On this occasion SE06 was left open at the point SCC4 was closed. Our standard process is to open and close the production client in both SE06 and SCC4 simultaneously. SCC4 being closed greatly reduced any risk that SE06 being open posed, however, this is not our standard practice and so we will monitor that both SCC4 and SE06 are both closed together to ensure we minimise any future risk.

Page 187

Assessment

- Significant deficiency – ineffective control/s creating risk of significant misstatement within financial statements and / or directly impact on the planned financial audit approach.
- Deficiency – ineffective control/s creating risk of inconsequential misstatement within financial statements and not directly impacting on the planned financial audit approach
- Improvement opportunity – improvement to control, minimal risk of misstatement within financial statements and no direct impact on the planned financial audit approach

General Applications ITGC Assessment Findings

Assessment	Issue and risk	Recommendations
1.	Lack of oversight over third-party users assigned privileged systems access in UPM GT has identified the following Civica vendor user and generic accounts with privileged access assigned in both application and MS SQL database layers of UPM system: • Application - 1 user and 2 generic accounts; • Database - 32 user and 2 generic accounts. <i>Refer to Appendices file, tab "UPM Accounts" for further information.</i> Due to the lack of SOC 1 Type II attestation for UPM system provider Civica, GT is unable to gain assurance over appropriateness of the user access for these accounts or of any activity performed. We noted that the access for these accounts is provided on a permanent basis and neither activity monitoring nor user access reviews are performed by Dorset. Separate inquiry procedures were conducted with the Civica vendor regarding their change management process and privileged access controls. However, no additional evidence was provided to substantiate the high-level control procedures outlined. Risks Without adequate oversight over the third-party users of system administration accounts, there is an increased risk of unauthorised or inappropriate changes to the underlying data. In addition, usage of shared/ generic third-party accounts create a lack of accountability around changes made within the system.	Management should undertake a review for all IT support partners to confirm how they obtain assurance over appropriate IT controls being implemented / operated by third-party service organisations. This should, as a minimum, include the controls over privileged production or database access, such as: - approving vendor access for specific requirements and disabling after completion - reviewing account activities performed Where independent service organisation assurance reports are available, management should assess the findings and consider whether complementary user entity controls are effective. Management response Dorset follow the guidance of our System Provider CIVICA on how to grant them access, maintaining individual access will create more of a risk to the Pension Fund (UPM) if CIVICA neglect to inform us when users leave their business. We are not informed in a timely manner of staff turnover at CIVICA which raises the risk of unauthorised users if they have left the business, and we are not notified.

Assessment

- Significant deficiency – ineffective control/s creating risk of significant misstatement within financial statements and / or directly impact on the planned financial audit approach.
- Deficiency – ineffective control/s creating risk of inconsequential misstatement within financial statements and not directly impacting on the planned financial audit approach
- Improvement opportunity – improvement to control, minimal risk of misstatement within financial statements and no direct impact on the planned financial audit approach

General Applications ITGC Assessment Findings

2.



Lack of oversight over a privileged generic account in Active Directory

GT was not provided with complete evidence relating to the management of the password to 1 generic AD account, such as:

- account last log in date;
- whether the password is held in secure location/password manager;
- whether the password is changed after each use.

Furthermore, GT has confirmed that this generic user ID is used as a support account, however, its activity is not logged and monitored.

Refer to Appendices file, tab "Active Directory Accounts" for further information.

Risks

The use of generic or shared accounts with high-level privileges increases the risk of unauthorised or inappropriate changes to the application or database. Where unauthorised activities are performed, they will not be traceable to an individual.

The excessive use of accounts with privileged access increases the risk of end-users being able to:

- change system configuration settings without authorisation and approval
- read and modify sensitive data,
- create, modify or delete user accounts without authorisation,
- delete or disable system audit logs.

Recommendations

Management should undertake a review of all user accounts on the AD to identify all generic privileged accounts. For each account identified management should confirm:

- requirement for the account to be active and be assigned privileged access;
- which users have access to the account and business justification for retaining such access;
- controls in place to safeguard the account from misuse.

Where possible, privileged generic accounts should be removed, and individuals should have their own uniquely identifiable user accounts created to ensure accountability for actions performed. Alternately, management should implement suitable controls to limit access and monitor the usage of these accounts (i.e. through increased use of password vault tools / logging and periodic monitoring of the activities performed). Where monitoring is undertaken, this should be formally documented and recorded.

Management response

The account identified is an application service account. The application captures the AD account name of the logged in user, verifies and logs the action taken. Entra ID logs the actions of this account within the rest of the infrastructure. Whilst a complete log is not stored in one place combining these logs show a complete picture of the account activity.

Users are only able to use this account to carry out tasks for which they are approved, and this is controlled by the application using the service account rather than the specific permissions of the AD account.

The account is managed by the application owner. The account is recorded in a secure location and was last used 30/01/2025 18:43:47. This account is monitored in AD in the same way as any other and is subject to the same controls and restrictions as required by the council policy.

Assessment

- Significant deficiency – ineffective control/s creating risk of significant misstatement within financial statements and / or directly impact on the planned financial audit approach.
- Deficiency – ineffective control/s creating risk of inconsequential misstatement within financial statements and not directly impacting on the planned financial audit approach
- Improvement opportunity – improvement to control, minimal risk of misstatement within financial statements and no direct impact on the planned financial audit approach

General Applications ITGC Assessment Findings

Assessment	Issue and risk	Recommendations
3. 	Lack of formal activity monitoring over generic user ID in Capita GT confirmed a lack of formal activity monitoring review documentation for the following privileged generic accounts: • 2 generic administrative accounts that are shared by 6 members of the Technical Support and Development Service. • 1 generic user ID with privileged access to the application, which is used by Capita vendor to provide remote support. Furthermore, GT was not provided with last log in dates for these accounts to verify whether their activity falls within the April 2024 to March 2025 audit period. <i>Refer to Appendices file, tab "Capita Accounts" for further information.</i> Risks Without formal and routine reviews of security event logs, inappropriate and anomalous activity may not be detected and resolved in a timely manner. Additionally, unauthorised system configuration and data changes made using privileged accounts will not be detected by management.	It is recommended that security event logs are reviewed on a regular basis for example daily or weekly, ideally by an IT security personnel / team who are independent of those administering Capita and its underlying database. Any issues identified within these logs should be investigated and mitigating controls implemented to reduce the risk of reoccurrence. Management response Security event logs for privileged user accounts used by Technical Support and Development Team are now reviewed by Business Development Team who are familiar with the software but do not have administrative rights, to mitigate the risk of not detecting inappropriate an anomalous activity in a timely manner. Security event logs for privileged user accounts 'academy' used by Capita/MRI Remote Support Team are now reviewed by Technical Support and Development Team to mitigate the risk of not detecting unauthorised system configuration and data changes in a timely manner.

Assessment

-  Significant deficiency – ineffective control/s creating risk of significant misstatement within financial statements and / or directly impact on the planned financial audit approach.
-  Deficiency – ineffective control/s creating risk of inconsequential misstatement within financial statements and not directly impacting on the planned financial audit approach
-  Improvement opportunity – improvement to control, minimal risk of misstatement within financial statements and no direct impact on the planned financial audit approach

General Applications ITGC Assessment Findings

4.



Assessment

Issue and risk

Capita Access Termination Process and System Limitation Review

Upon inspection of user access termination request sample, GT noted the following:

- the request was raised for Revenues Officer staff, who left the organisation on 19 July 2024 (Friday).
- the request was submitted by a business user on 22 July 2024 (Monday) and was disabled by Technical Support and Development Team.

GT noted a system limitation was whereby the system does not maintain the date and time stamp of the user's access revocation; hence, we could not verify that the user access from the system was revoked on 22/07/2024.

Additionally, although the IT Team actioned the leave request in a timely manner and the access was revoked within 1 business day after the user's termination date, it is best practice to disable users at the end of the users last working day.

Risks

Where system access for leavers is not disabled in a timely manner, there is a risk that former employees will continue to have access and can process erroneous or unauthorised access transactions.

There is also a risk that these accounts may be misused by valid system users to circumvent internal controls.

Recommendations

It is recommended the notification by business users to Technical Support and Development Team to be submitted before the user's termination date, so that the IT personnel can revoke access at the end of the users last working day. Furthermore, consider the possibility of extending the system tracking to include a date and time stamp for access revocations. This feature will allow for better verification of when access was terminated, thereby improving accountability.

Management response

The Technical Support and Development Team proactively reminds managers to notify them of upcoming changes ahead of the effective date. However, when information is not received in advance, revocation is promptly actioned (1 business day) to mitigate the risk of unauthorised account access by a former employee. When advance notice is provided, the team ensures that access is revoked on or before the user's last working day, or if the user is working beyond normal business hours, it has been actioned on the immediate next working day. We will now communicate that revocation will happen by 4pm on the last employment day. While this approach may result in some access being forfeited on the final day, in most cases, the user's last working day precedes their official employment end date.

GT recognised the system limitation within the batch program User Permissions as it does not output a timestamp on revoked accounts. This is out of our control as dependent on Capita/MRI software development. We can however record this manually at the time of revocation to improve accountability and will start to do this upon the next revocation.

Page 191

Assessment

- Significant deficiency – ineffective control/s creating risk of significant misstatement within financial statements and / or directly impact on the planned financial audit approach.
- Deficiency – ineffective control/s creating risk of inconsequential misstatement within financial statements and not directly impacting on the planned financial audit approach
- Improvement opportunity – improvement to control, minimal risk of misstatement within financial statements and no direct impact on the planned financial audit approach

Controls for which assurance could not be provided

Expected control name and description	Reason/Justification
1. Segregation of duties for UPM and Capita Administrative privileges (including generic super user access rights) to the network, applications and their associated databases are restricted to those users requiring this level of access (in line with their roles and responsibilities). Privileged duties do not conflict with other roles. Creation and modification of vendor accounts for UPM Access to any application (in line with the starter's roles and responsibilities) is requested and approved by the new starter's line manager (or equivalent person) before being granted by someone from IT. Vendor change management for UPM and Capita Vendor develops changes which are tested in an environment separate from the production environment. Vendor developers do not have continuous access to the production environment and cannot implement their own changes into the production environment.	GT was unable to obtain SOC 1 Type II reports for Capita and UPM systems, as the vendors Capita One and Civica do not undergo the level of attestation required to gain assurance over the design and effectiveness of the vendor-related controls. Within the audit period of 2024/2025, GT was not able to provide assurance over the vendor segregation of duties controls in relation to privileged accounts on Capita and UPM application and database layers. Additionally, the lack of assurance applies to change management controls of both systems, such as those specifically governed by the Capita and Civica vendors. These include development and implementation of changes, segregation of development, testing and production environments as well as developer vs. implementor segregation of duties. <i>Please note, this observation is subject to GT obtaining further evidence of Civica vendor controls as requested on 24/04/2025.</i>
2. User access termination for UPM For leaver control, requests to revoke access to any in scope application is initiated by HR and / or their line manager ahead of the actual leave date and access revoked in a timely manner.	For UPM system, in the course of 2025 IT audit activities, it has been indicated that there were no leavers during the 2024/25 financial year. However, GT noted a system limitation whereby the date when users were terminated from the system is not displayed on the deleted users' page. Consequently, GT was unable to verify the resolution of the control finding from the previous year, and thus, cannot obtain assurance regarding this matter. <i>Please note, this observation is subject to GT obtaining complete HR list for the full audit period in review and subsequent analysis of UPM user list and HR leaver data as requested on 10/04/2025.</i>
3. Generic user accounts management UPM and Active Directory Access to generic or shared accounts must be strictly controlled, justified, and approved. Only authorised users should be allowed to access passwords for privileged generic IDs, and only for specific, approved purposes. Generic credentials should be stored in a password vault. Access should be time-limited, with credentials automatically rotated or expired after use.	Specific to privileged generic accounts identified for UPM and Active Directory, GT was unable to gain assurance over the password keeper software. Specifically, this is in relation to identifying the personnel managing access to the following keepers: Server/Storage, Client Devices, Place - DBA, Place - GIS, SAP - Windows PWDs, Cireson & Server Manager, and Place – Applications. Additionally, GT was not able to verify whether the keeper software is in-house, or vendor developed. <i>Please note, this observation is subject to GT obtaining further evidence regarding the password keeper software, as requested on 22/04/2025.</i>

Review of findings raised in prior year – SAP

Assessment	Issue and risk previously communicated	Update on actions taken to address the issue
X	Users with inappropriate access to ABAP debugger in production ABAP debugger is used for performing debugging functions such as inserting a code to correct any errors in the source code. Users are therefore able to execute unauthorised transactions through these amendments to code. We noted that there were 26 active Dialog(A) accounts and 1 Service (S) assigned with access to ABAP Debugger in production granted via S_DEVELOP authorisation object. We further observed that 20 users had made program attributes changes, accounting header documents changes and master data changes during the audit period. The 7 others have access to ABAP debugger in production but have not made any changes during the period. Risk Unauthorised access to ABAP debugger increases the risk of: • unauthorised change or deletion of table entries including tables that are typically protected by SCC4, • the ability to perform debugging functions by inserting break-point statements into program code • the ability to bypass authority checks and execute transactions	• This deficiency has been partially remediated. • The number of users with ABAP debugger has been reduced from 26 to 11 in 2024/2025 audit period. • Refer to SAP ITGC Assessment Finding 1.

Page 193

Review of findings raised in prior year – SAP

Assessment	Issue and risk previously communicated	Update on actions taken to address the issue
X	Segregation of Duties Conflict as developers have access to production We compared all users with the ability to develop changes in development with those with the ability to create/import transports in production and identified the following: • there were 4 users with the ability to develop changes in development and create/import transports in production via STMS. • of the 4 users, 3 users had the ability to develop changes in development and import them into production via Standard Transport Management System (STMS). In response, we compared the list of users that created transports in development and those that created/imported transports in production and noted that there was 1 user that had created transports in development and released the same transports in production. Risk The combination of access to develop and implement those changes in the production environment creates a risk that inappropriate or unauthorised changes are made to data and/ or programs	• This deficiency has been partially remediated. • Refer to SAP ITGC Assessment Finding 2.
	User access within SAP was kept valid after the user's termination date It was noted during the audit, that a user was terminated on the 21st of December 2023, however their SAP account was still valid to 30th of January 2024. Upon reviewing the last login dates, we noted that this account had not been accessed since date of departure. Risk Where system access for leavers is not disabled in a timely manner, there is a risk that former employees will continue to have access and can process erroneous or unauthorised access transactions. There is also a risk that these accounts may be misused by valid system users to circumvent internal controls.	• This improvement point has not been remediated. • Refer to SAP ITGC Assessment Finding 3.

Assessment

- ✓ Action completed
- X Not yet addressed

Review of findings raised in prior year – SAP

Assessment	Issue and risk previously communicated	Update on actions taken to address the issue
✓	Password settings not in line with the organisation's password policy We noted that the following password settings were not configured in line with the organisations password policy and/or the National Cyber Security Centre (NCSC): - The password policy states that the password length should be 15 characters. The System User Defined value is only set at 8 characters. - The password policy states that users no longer enforce password expiration, which is in compliance with the NCSC, however the system is set for password expiration of 180 days. Risks A lack of robust password settings may allow financial information to be compromised by unauthorised users.	This finding has been remediated upon further analysis of the password settings of SAP. The password length has been increased to 15 and the password expiration has been set to appropriate parameters.
✓	Users with inappropriate access to maintain all SAP Standard or Customised tables in production Our IT audit procedures identified 22 Dialog user accounts that were assigned access to maintain all SAP standard or customised tables via SM30 or SM31. Risks Access to maintain all standard or customised SAP tables creates a risk that unauthorised table maintenance functions can be performed and result in data integrity issues.	This deficiency has been remediated, upon further evaluation provided within the roll forward scope of the IT audit period of April 2024 to March 2025.

Assessment

- ✓ Action completed
- ✗ Not yet addressed

Review of findings raised in prior year – General Applications

Assessment	Issue and risk previously communicated	Update on actions taken to address the issue
Page 196	X User access within Capita and UPM are not appropriately revoked for terminated employees Application access is not revoked for terminated employees in a timely manner. For a sample terminated user in Capita, we observed that the request to terminate a leaver was submitted 2 business days after the user had left the Council. For a sample terminated user in UPM, we observed that the sample user was deleted from the system 4 business days after they transferred out of the Pensions department Risk Where system access for leavers is not disabled in a timely manner, there is a risk that former employees will continue to have access and can process erroneous or unauthorised access transactions. There is also a risk that these accounts may be misused by valid system users to circumvent internal controls.	- This deficiency has been partially remediated. - Refer to General Applications ITGC Assessment Finding 4 and section “Controls for which assurance could not be provided”, point 2.
	X Lack of review of audit logs for Capita Information security event logs, which capture the monitoring of activities performed by users with privileged access within Capita were not reviewed. Risk Without formal and routine reviews of security event logs, inappropriate and anomalous activity may not be detected and resolved in a timely manner. Additionally, unauthorised system configuration and data changes made using privileged accounts will not be detected by the Council.	- This improvement point has not been remediated. - Refer to General Applications ITGC Assessment Finding 3. The finding additionally applies to UPM and Active Directory – refer to General Applications ITGC Assessment Finding 1 and 2.

Assessment

- ✓ Action completed
- X Not yet addressed

Review of findings raised in prior year – General Applications

Assessment	Issue and risk previously communicated	Update on actions taken to address the issue
X	Lack of formal review of the Service Auditor Report We noted that the Council does not review the Service Auditor Report (SOC1 Type 2 or a ISAR3402) provided for Capita. Risk Without adequate oversight and monitoring over the service auditor report on business controls procedures, there is an increased risk that controls over financial reporting operated by the service providers might not be designed, implemented and operating effectively	- This improvement point has not been remediated. However, there has been additional information obtained during the 2024 to 2025 audit period, thus providing further context to this deficiency. - Refer to section “Controls for which assurance could not be provided”, point 1.
✓ Page 197	Lack of formal cybersecurity policies or procedures Upon review of the cybersecurity control environment, we have identified the entity does not perform active backup testing. Risk The absence of a specific process to conduct active backup testing pose a control risk to the entity's cybersecurity posture. This deficiency could lead to vulnerabilities and increased likelihood of successful cyber-attacks.	This deficiency has been remediated upon further analysis and evaluation of the cybersecurity environment and the specific industry context of Dorset Council & Pension Fund.
✓	Inadequate control over privileged accounts within Capita We observed that the Capita administrative generic accounts are shared by 6 members of the Technical Support and Development Service. We performed mitigating procedures to confirm that the usage of the accounts were restricted to the 6 members. Risk The use of generic or shared accounts with high-level privileges increases the risk of unauthorised or inappropriate changes to the application or database. Where unauthorised activities are performed, they will not be traceable to an individual.	- This deficiency has been remediated. - We have confirmed user access to generic user accounts is appropriately restricted to members of Technical Support & Development team and the activities performed on these accounts are traceable to individuals logging in, which was verified by the review of the Capita system audit logs.

Assessment

- ✓ Action completed
- X Not yet addressed



Document is Restricted

This page is intentionally left blank

Audit and Governance Committee Work Programme 2025-26

13 Oct 2025		
SWAP Update Report	Update Report	Officer Contact- Sally White/Angie Hooper
Period 4 Financial Management Report 2025/26	Report	Officer Contact- Sean Cremer
Quarterly Risk Management Update	Update Report	Officer Contact- Chris Swain, Liz Crocker
Grant Thornton – External Audit Progress Report	Update Report	Officer Contact - Julie Masci/Sam Harding
Update on Our Future Council Work	Update	Officer Contact- Aidan Dunn

17 Nov 2025		
Quarter 2 Financial Management Report 2025/26	Report	Officer Contact- Sean Cremer
Treasury Management Mid-Year Review 2025/26	Report	Officer Contact- David Wilkes
Grant Thornton - Dorset Council Audit Findings Report 2024-25	Report	Officer Contact - Julie Masci/Sam Harding
Grant Thornton – Dorset Pension Fund Audit Findings Report 2024-25	Report	Officer Contact - Julie Masci/Chrissa Viente
Grant Thornton – Auditors Annual Report 2024-25	Report	Officer Contact – Julie Masci/Sam Harding
Grant Thornton – Dorset Council - Letter of Representation	Management Letter	Officer Contact – Julie Masci/Sam Harding
Grant Thornton – Dorset Pension Fund – Letter of Representation	Management Letter	Officer Contact – Julie Masci/Chrissa Viente
Update on Our Future Council Work	Update	Officer Contact- Aidan Dunn

12 Jan 2026		
SWAP Update Report	Update Report	Officer Contact – Sally White/Angie Hooper

Risk Management Update	Update Report	Officer Contact-Chris Swain, Liz Crocker
Update on Our Future Council Work	Update	Officer Contact- Aidan Dunn

23 March 2026		
Quarter 3 Financial Management Report 2025/26	Report	Officer Contact- Sean Cremer
Grant Thornton – 2025-26 Audit Plan Dorset Council	Report	Officer Contact - Julie Masci/Sam Harding
Grant Thornton – 2025-26 Audit Plan Dorset Council	Report	Officer Contact - Julie Masci/Chrissa Viente
Update on Our Future Council Work	Update	Officer Contact- Aidan Dunn

27 April 2026		
Annual Governance Statement	Statement	Officer contact- Marc Eyre
SWAP Update Report	Update Report	Officer Contact – Sally White/Angie Hooper
Planning Paper 2026-27 & Internal Audit Charter	Planning Paper	Officer Contact – Sally White/Angie Hooper
Annual Internal Audit Opinion 2025-26	Opinion Report	Officer Contact – Sally White/Angie Hooper
Quarterly Risk Management Update	Update Report	Officer Contact- Chris Swain, Liz Crocker
Grant Thornton – External audit progress report	Update Report	Officer Contact - Julie Masci/Sam Harding
Update on Our Future Council Work	Update	Officer Contact- Aidan Dunn

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

Issue	Notes	Date raised