APPENDIX C

INTERNAL AUDIT FINAL REPORT – Information Governance, Law and Governance - 2021/22

A. Executive Summary

On the basis of our fieldwork, we are able to provide the following level of assurance on the overall adequacy of the control framework as per our audit scope:

Audit Opinion:	
Substantial Assurance	There is a sound control framework which is designed to achieve the service objectives, with key controls being consistently applied.
Reasonable Assurance	**Whilst there is basically a sound control framework, there are some weaknesses which may put service objectives at risk.**
Partial Assurance	There are weaknesses in the control framework which are putting service objectives at risk.
Minimal Assurance	The control framework is generally poor as such service objectives are at significant risk.

Recommendations:				
PRIORITY	**High**	**Medium**	**Low**	**Total**
Number of Recommendations	0	8	2	**10**

Recommendations from 2019/20 Information Governance Report	
No. of Medium Priority Recs	7
Previously implemented	2
Superseded by new Recs	2
Still to implement	3

Summary of Findings:

Medium Priority

- Responsibility for Information Governance compliance: roles and responsibilities for all areas of information governance compliance not currently defined.
- Self-assessment compliance tool: self-assessment tool has not been implemented and includes areas that require clarification.
- Information Governance Risk Management: responsibility and processes for managing corporate, council-wide, information governance risk are not defined or implemented.
- Children's Services attendance at Information Governance Board: no representatives from any of the Children's Services areas have attended the IGB for a prolonged period.
- Training performance reporting: performance reporting on Information Governance training does not provide a comprehensive assessment of completion.
- Training for Information Asset Advisers: IAAs are not provided with role specific training.
- Data Security Breach Register – Outstanding Breaches: a significant proportion of historic breaches are still categorised as 'outstanding'
- Data Security Breach Register – Completeness of Register: entries in the register are missing risk rating and referral date information.

Low Priority

- Review Schedule for Policy and Guidance documents: there is no schedule in place covering the review and update of all information governance policy and guidance documents.
- Update of Information Governance Policy: the policy contains potentially misleading wording regarding the need to report issues to the Annual Governance Statement.

B. Audit Objectives, Scope & Methodology

The control framework is the system of risk management, internal control and governance put in place by management to ensure that objectives are achieved, waste and inefficiency is minimised and to prevent and detect fraud and corruption.

This audit was conducted as part of the 2021/22 BCP Annual Audit Plan. Our objectives were to provide assurance that the control framework is appropriate and that the controls and processes are operating effectively in BCP Council's Core Information Governance arrangements as outlined in the agreed Terms of Reference including:

- Strategy and Policy
- Governance
- Training
- Operational Activity and Co-ordination
- Follow up of 2019/20 Information Governance internal audit medium priority recommendations

Where weaknesses in the control framework are identified, recommendations have been made for improvement and are detailed in Section C of this report.

We undertake our work on a risk and sample basis in line with Public Sector Internal Audit Standards and as such we do not test all internal controls nor identify all areas of control weakness, fraud or irregularity, however, any issues identified during the course of our work are reported to management

Recommendation Priority Ratings:	
High Priority	High priority recommendations have actual / potential critical implications for achievement of the Service's objectives and/or a major effect on service delivery. Agreed actions should be urgently implemented by the Service within 3 months of the issue of the final audit report and the associated risk(s) added to the Service Risk Register. *Recommendations will be followed-up by Internal Audit as they fall due.*
Medium Priority	Medium priority recommendations have actual / potential significant implications for achievement of the Service's objectives and/or a significant effect on service delivery. Agreed actions should be implemented by the Service within 9 months of the issue of the final audit report and formal consideration should be given to adding the associated risk(s) to the Service Risk Register. *Recommendations will be followed-up by Internal Audit as part of the next audit review or within 12 months after the implementation due date (whichever is sooner).*
Low Priority	Low Priority recommendations have actual / potential minor implications for achievement of the Service's objectives and/or a minor effect on service delivery. *It rests with the Service to implement these actions and advise Internal Audit of the outcome.*

ISSUED ON BEHALF OF:	Nigel Stannard, Head of Audit & Management Assurance (Chief Internal Auditor)	
AUTHOR	James Paterson, Auditor & Ruth Hodges, Audit Manager (Deputy CIA)	
DATE	March 2022	Version Number: Final 1.0
DISTRIBUTION:	Julian Osgathorpe - Corporate Director, Transformation Susan Zeiss - Director, Law and Governance Nigel Channer - Team Leader, Contracts, Commercial and IG	

[redacted]	Simon Milne, Audit Manager (Deputy CIA)

C. Detailed Findings & Recommendations

Ref No.	Finding	Recommendation	Priority	Status / Management Response	Responsible Officer	Target Date
Strategy and Policy						
R1	**Review Schedule for Policy and Guidance** **Issue:** There is no schedule for the reviewing Information Governance policies and associated guidance. As these documents often overlap or make reference to one another, an ad hoc approach to updates could result in inconsistencies emerging between them. **Risk:** There is a risk that information governance arrangements may become ineffective or inconsistent or fail to reflect updated legislative requirements or objectives.	It is recommended that a review schedule, including details of all Information Governance templates, guidance notes and policy documents is established and utilised.	**Low**	Policies have been reviewed and approved by IGB. Next review date August 2023, which is recorded in the policy documents. Guidance notes are annotated when updated (most were reviewed in 2020). Agreed review schedule to be developed by Team.	Information Governance Officer	July 2022
R2	**Update of Information Governance Policy** **Issue:** The BCP Information Governance Policy includes the following wording "Information Asset Owners will also include information risks within their Annual Governance Statements." This is potentially misleading as it indicates that any service exposure to information risk, regardless of how effectively it is being managed, should be included in the Annual Governance Statement. Only those issues that represent a significant governance concern, or a risk exposure that has not been managed effectively, should be included.	It is recommended that the Information Governance Policy is amended to clarify that only significant governance concerns should be included in service Management Assurance Statements.	**Low**	IG risks will be identified by IAOs in SU Risk Registers or (in view of R5 below) a Corporate IG Risk Register, approved and monitored by IGB. SU AGSs will include any high-risk outcomes of the self-assessment compliance checklist.	Team Leader, Contracts, Commercial and IG	July 2022

Ref No.	Finding	Recommendation	Priority	Status / Management Response	Responsible Officer	Target Date
	Risk: There is a risk that unnecessary and potentially confusing information is submitted by services as part of the Annual Governance process, leading to significant issues not being reported on effectively.					
Governance						
R3	**Responsibility for Information Governance Compliance** **Issue:** There are several areas of information governance in the council that are either not subject to active compliance checks and monitoring or where the responsibility for such checks is unclear, including the development, implementation and maintenance of Information Asset Registers, completion of Data Protection Impact Assessments, completion and publication of privacy notices. **Risk:** There is a risk that the council fails to meet its legislative responsibilities, exposing it to reputational damage and legal challenge.	It is recommended that the roles and responsibilities for checking and monitoring the service requirements for Information Governance is reviewed to ensure a comprehensive compliance framework is in place.	**Medium**	This will be taken to IGB to agree an approach where the IGB has overarching responsibility for compliance.	Team Leader, Contracts, Commercial and IG	April 2022
R4	**Self-assessment tool for compliance checks not yet in place** **Issue:** The previous 2019/20 Information Governance audit identified that: Following on from an IGB meeting held on 26/2/2020, the IG team was tasked with researching for a self-assessment tool to enable the team to complete information governance compliance checks throughout the Council as part of their	It is recommended that the self-assessment tool is developed and implemented by Information Governance to support the wider compliance framework. *The above supersedes the 2019/20 recommendation.*	**Medium**	The self-assessment has been issued to services for response. The results will be collated and provided to IGB for analysis and action.	Team Leader, Contracts, Commercial & IG	July 2022

Ref No.	Finding	Recommendation	Priority	Status / Management Response	Responsible Officer	Target Date
	second line of defence role. The team is still in the process of gathering this information. As part of the current audit, it was confirmed that the self-assessment had yet to be implemented. In addition, it is important that the objectives of this document regarding compliance checks, ownership and timeframes for completion are clearly defined. **Risk:** There is a risk that the council fails to meet its legislative responsibilities, exposing it to reputational damage and legal challenge.					
R5	**Information Governance Risk Management** **Issue**: At the October 2020 Audit and Governance Committee, it was agreed that Information Governance risk would be removed from the corporate risk register, on the basis that this would be monitored by the Information Governance Board and escalated back to CMB should the level of risk increase. However, this is not done by the IGB, nor is it part of their terms of reference. There is also no risk assessment or register for corporate information governance risks. **Risk**: There is a risk that corporate information governance risks are not identified and appropriately managed, leading to breaches of legislation, financial penalties, reputational damage, and operational inefficiencies. *Note: The forthcoming BCP Council Risk Management policy will also require corporate risks*	It is recommended that monitoring of corporate information governance risks is included in the Information Governance Board's Terms of Reference, and that this forms part of their standard agenda. It is recommended that the IGB ensures a risk assessment of corporate information risk is undertaken, including consideration of the following areas; • Legislative risk – breaches of compliance with data protection law, leading to censure from government agencies and challenges in the courts • Financial risk – penalties levied on the council due	**Medium**	The Interim Team Leader, Contracts, Commercial & IG will liaise with the SIRO and IGB to facilitate undertaking a risk assessment and producing an information risk register.	Team Leader, Contracts, Commercial & IG	July 2022

Ref No.	Finding	Recommendation	Priority	Status / Management Response	Responsible Officer	Target Date
	to be managed via the responsible governance boards via a key assurance area risk register.	to breaches of governance requirements, financial costs associated with breaches of contract with partners etc • Reputational risk – due to loss or leaks of confidential data and information • Organisation risk – service disruption due to data breaches and failures in information systems • Emerging risk – arising from changes to council structure, service delivery methods and legislative requirements. It is recommended that the above assessment is used to produce, and regularly monitor, an information risk register (as directed in the draft BCP Council Risk Management policy). *The above supersedes the risk register recommendation identified in the 2019/20 audit.*				

Ref No.	Finding	Recommendation	Priority	Status / Management Response	Responsible Officer	Target Date
R6	**Children's Services – Attendance at the IGB** **Issue:** No attendees from any of the Children's service areas, including the Children's Caldicott Guardian, have attended a meeting of the IGB between October 2020 and October 2021. **Risk:** There is an increased risk of non-compliance with legislative requirements, reputational damage and potential financial penalties.	It is recommended that an escalation procedure is put in place to respond to any persistent absence of services from the IGB, especially those with high exposure to information and data risk.	**Medium**	The Interim Team Leader, Contracts, Commercial & IG has agreed with the SIRO that the IGB Chair will monitor and respond to any ongoing lack of attendance by services.	SIRO/Deputy SIRO	Implemented
Training						
R7	**Training Performance Reporting** **Issue:** Performance reporting to the IGB on the completion of training only provides a quarterly snapshot, it does not provide a comprehensive record of the total proportion of officers who have completed it. As such IGB are not made aware of specific services where a significant proportion of staff have failed to complete training. **Risk:** There is a risk that service areas with poor training are more likely to be the source of data protection breaches and are also more likely to be penalised by the ICO.	It is recommended that a comprehensive training performance report, detailing the proportion of officers in each service who have undertaken each module, is produced and provided to the IGB for action.	**Medium**	A comprehensive training report will be produced by the Information Governance Team for presentation to the IGB.	Team Leader, Contracts, Commercial & IG	From April 2022
R8	**Training for Information Asset Advisers** **Issue:** IAAs fulfil a vital role within the council, acting upon the majority of Information Governance activities that are delegated to services. Although guidance documents are made available to IAAs via the IAA network, the often complex demands of the role would benefit from specific training.	It is recommended that IAAs are provided with specific training, pertinent to their roles to ensure they are able to meet corporate expectations.	**Medium**	Agreed.	Team Leader, Contracts, Commercial & IG/IG Team	May 2022

Ref No.	Finding	Recommendation	Priority	Status / Management Response	Responsible Officer	Target Date
	Risk: Without specific training with respect to their role, there is a risk that IAAs will either fail to deliver their roles effectively or will deliver incorrect information/advice to their respective services.					
Operational Activity and Co-ordination						
R9	**Data Security Breach Register – Reporting on Historic Outstanding Breaches:** **Issue**: Review of the data security breach registers for 2019/20 and 2020/21 confirmed the following; 2019/20: total number of recorded breaches (not including cancellations) is 319, of which 103 were categorised as 'outstanding', of which 5 were classified as being of 'high' risk. 2020/21: total number of recorded breaches (not including cancellations) is 309, of which 163 were categorised as 'outstanding', of which 3 were classified as being of 'high' risk. The quarterly reports provided to IGB only detail those new breaches that have been referred during the previous quarter, along with those of that number that are currently outstanding. There does not appear to be a total of historic outstanding breaches that has been reported to IGB. Of particular concern are the 8 outstanding breaches classified as being 'high' risk in 2019/20-2020/21. **Risk**: There is a risk that the issues that have caused breaches persist and that lessons resulting from them fail to be learnt and applied elsewhere in the council.	It is recommended that the quarterly IGB breach performance reports are updated to include all outstanding breach data. In addition, it is recommended that; • The timeframes against which the IG Team will request updates from services if no information has been received are defined. • A procedure for escalating failure to close down outstanding breach reports is put in place.	**Medium**	Automated security breach online tool has been developed by IG Team, using M/S Power Tools application. Consultation and testing with IAAs to be undertaken. System will simplify and streamline process and engage IAAs in direct input of breaches within their SU. In the interim a comprehensive data breach report will be produced by the Information Governance Team for presentation to the IGB.	Team Leader, Contracts, Commercial & or replacement IG/IG Officer	April 2022

Ref No.	Finding	Recommendation	Priority	Status / Management Response	Responsible Officer	Target Date
R10	**Data Security Breach Register – Completeness of Register:** **Issue**: A high proportion of the entries in the Breach register do not have risk ratings allocated to them, including one which had been referred to the ICO. In addition, a high proportion of entries were missing breach dates and referral dates – information that should have been provided as part of the initial processing of the breach. **Risk**: Without complete data breach records there is a risk that the Council's response to them will be inconsistent or ineffective and that reporting will fail to be accurate.	It is recommended that; • all reported breaches are reviewed to assess the risk they present, and for this information to be recorded in the register. • the dates of all breaches and referrals to the IG Team are recorded in the register.	**Medium**	As agreed above.	Team Leader, Contracts, Commercial & IG or replacement/IG Officer	April 2022
Previous Recommendations						
R11	**Information security policy monitoring and reporting process not defined** **Issue**: Information security policy implementation and delivery is the responsibility of both IT and IG. Not clear whether there is a defined collaborative way of working, report production and reporting of information security issues to IGB. Currently the IG Team only report data breaches to IGB, other issues such as monitoring and restrictions, communications security, information security continuity and more are not captured in the current reporting process to IGB. **Risk:** Inadequate monitoring and reporting of issues emanating from implementation of the information security policy.	It is recommended that there be defined monitoring and reporting roles and responsibilities between IG and IT on implementation of the IS policy. In addition, the teams should establish a regular exceptional high-risk reporting mechanism to IGB.	**Medium**	**Agreed with management July 2020.** Liaison with ICT to discuss and resolve this issue will be carried out.	Team Leader, Contracts, Commercial & IG	April 2022

Ref No.	Finding	Recommendation	Priority	Status / Management Response	Responsible Officer	Target Date
R12	**Register of information sharing agreements in place but not up to date.** **Issue:** No up to date Information Sharing Protocols/Agreement register in place. **Risk:** Unauthorised sharing of information with parties not covered under the DISC.	It is recommended that the Information Governance Team maintain an up to date information sharing agreements register which summaries all information sharing agreements for BCP.	**Medium**	The Information Governance Team will contact services to ensure up-to-date records of data sharing agreements are provided and compiled into a Register as suggested.	Team Leader, Contracts, Commercial & IG	September 2022
R13	**Central breach reporting tool not in place** **Issue**: Information Governance should consider producing a portal or central breach reporting tool where Service Units can file and/or populate a breaches log for review by Information Governance. This would allow the IG Team to provide challenge to the Service Units on evidence submitted to the ICO in support of breaches. **Risk**: Failure to provide challenge to the Services on evidence submitted to the ICO in support of breaches	It is recommended that Information Governance put in place a central breach reporting tool/portal which Service Units can use to log breaches. The reporting tool/portal should be visible to the Information Governance Team to allow them to monitor the nature and type of breaches being reported in Service Units and provide the opportunity to challenge the evidence provided to the ICO in support of breaches. It will also inform IG of areas of apparent weakness, so that it can provide additional advice and/or guidance documents to minimise potential information security risks.	**Medium**	Automated security breach online tool has been developed by IG Team, using M/S Power Tools application. Consultation and testing with IAAs to be undertaken.	Team Leader, Contracts, Commercial and IG/IG Officer.	April 2022