tiaa

The Police and Crime Commissioner and Chief Constable for Gwent Police

Assurance Review of Business Continuity Management

January 2025

Final

Executive Summary

OVERALL ASSESSMENT

LIMITED ASSURANCE

- SUBSTANTIAL ASSURANCE
- REASONABLE ASSURANCE
- LIMITED ASSURANCE
- NO ASSURANCE

ASSURANCE OVER KEY STRATEGIC RISK / OBJECTIVE

There is a risk that not having an effective and tested up to date Business Continuity Plan could affect the capability of the force to respond effectively to business disruptions and recover its activities and services under the Civil Contingencies Act 2004. There are currently no risks in relation to business continuity on the force's risk register.

SCOPE

The review considered the effectiveness of the programme of work in relation to emergency preparedness, resilience and response. In summary, this covered the following areas: roles and responsibilities, corporate and department plans, major incident training, emergency plan testing, liaising with partner agencies, risk management, performance monitoring, staff wellbeing and lessons learned for ongoing business continuity.

KEY STRATEGIC FINDINGS

The Strategic Business Continuity Plan needs to be reviewed and updated.

Examples of departmental Business Continuity Plans (BCPs) were found to be out of date and have not been reviewed or tested since the Covid-19 Pandemic and to also lack detail.

Business Impact Analysis within the departmental BCPs also appear to lack or contain the criticality of systems in terms of recovery.

The Terms of Reference for the Strategic Business Continuity Management Group needs to be reviewed and updated.

GOOD PRACTICE IDENTIFIED

Gwent Police has a Business Continuity Strategic Management Group in place to oversee the management, development and implementation of a Business Continuity Management programme.

ACTION POINTS

Urgent	Important	Routine	Operational
0	8	3	2

tiaa

1

Assurance - Key Findings and Management Action Plan (MAP)

Rec.	Risk Area	Finding	Recommendation	Priority	Management Comments	Implementation Timetable (dd/mm/yy)	Responsible Officer (Job Title)
1	Directed	The force's Strategic Business Continuity Plan was last reviewed in December 2020 and is overdue a review. Since the Covid-19 pandemic organisations have reviewed their Business Continuity Plans (BCPs) due to the impact and changes to their working arrangements, systems and processes. There is a risk that not having an effective and tested up to date Business Continuity Plan could affect the capability of the force to respond effectively to business disruptions and recover its activities and services under the Civil Contingencies Act 2004.	The Strategic Business Continuity Plan be reviewed and updated.	2	*Whilst recent retirements have left a gap in our BCM capability and corporate memory, it has also presented an opportunity to refresh and reinvigorate our approach to BCM.* *This coincides with a restructure of the force operating model, which will see new command portfolios and a fresh opportunity to consider BCM in line with our new model.* *Following advice from the TIAA inspector, we have visited Dyfed Powys Police, who have recently gone through the same journey of rebuilding the BCM structure. We are looking at adopting their structures and processes, which are now well established in DPP.*	*Refresh Strategic Business Continuity Plan – 01/03/25*	*Superintendent (Spec Op)* *ACC (Organisational)*

PRIORITY GRADINGS

1	**URGENT**	Fundamental control issue on which action should be taken immediately.
2	**IMPORTANT**	Control issue on which action should be taken at the earliest opportunity.
3	**ROUTINE**	Control issue on which action should be taken.

tiaa

Rec.	Risk Area	Finding	Recommendation	Priority	Management Comments	Implementation Timetable (dd/mm/yy)	Responsible Officer (Job Title)
3	Directed	The Business Continuity Management Policy and Procedure states that: "The Business Continuity Management (BCM) Programme for Gwent Police is guided by a Strategic Business Continuity Group chaired by Supt Roads Policing Specialist Ops'. The Policy also states that: "A Force Planning Unit Civil Contingencies & Emergency Planning Constable has been designated as the BCM Co-ordinator. The BCM Co-ordinator has received BCI training, CBCI qualifications and is the accredited member of staff for the force'. Since the retirement of the previous Assistant Chief Officer – Resources (ACOR), a Superintendent has been given the day-to-day responsibility for BC, reporting into the Temporary Assistant Chief Constable. The Superintendent and deputy do not possess the Certificate of Business Continuity Institute (CBCI) qualification or have not been given appropriate training for the post and hence. There is a risk that business continuity may not be managed effectively.	The Business Continuity lead and deputy be given appropriate training in accordance with the Business Continuity Management Policy and Procedure.	2	*Organisationally, we need to discuss where BCM is best placed to sit, where strategic and tactical governance should be placed and who are the most appropriate personnel to lead on BCM and what professional training and accreditation they require. Other police organisations in Wales employ full time BCM specialists with the appropriate training and accreditation.*	*Agreement on ownership and governance: 01/03/25* *Attendance on external training / accreditation: 01/07/25*	*Superintendent (Spec Op)* *ACC (Organisational)*

Rec.	Risk Area	Finding	Recommendation	Priority	Management Comments	Implementation Timetable (dd/mm/yy)	Responsible Officer (Job Title)
4	Directed	Governance of Business Continuity is undertaken by the Strategic Business Continuity Management Group. Terms of Reference for the Group have been documented and were most recently reviewed and updated in May 2022. The Terms of Reference set out that the Group meet on a quarterly basis and also who are members of the Group. The Group is chaired by the Superintendent Head of Special Operations. The Terms of Reference also sets out that: "The Strategic Business Continuity Management Group terms of reference will be reviewed and updated as required and approved by members at least annually".	The Terms of Reference for the Strategic Business Continuity Management Group be reviewed and updated to reflect current arrangements, and this be undertaken on an annual basis in accordance with the Terms of Reference for the Group.	2	*ToR will naturally be updated as part of adopted DPP BCM structures, templates and processes.*	*Refresh ToR: next BCM meeting scheduled for March 2025*	*Superintendent (Spec Op)* *ACC (Organisational)*
5	Directed	From a review of the Departmental Business Continuity Plans, it could not be determined if Business Impact Analysis (BIAs) had been completed in terms of the criticality of systems and also there was no data collated to provide a force wide analysis and to inform the Strategic Business Continuity Plan.	Business Impact Analysis completed for all departments be summarised within the Strategic Business Continuity Plan to ensure the Response Team and ICT Team have an understanding of the critical functions to restore in terms of criticality.	2	*Our IT provider (SRS) have recently instigated a piece of work to review all IT software/systems used across the organisation and to RAG rate them in terms of BC, from critical impact to low impact. This is an involved piece of work as it relates to 110 different systems but is being progressed and will be managed through the BCM governance structure.*	*01/03/25*	*Superintendent (Spec Op)*

PRIORITY GRADINGS

1	URGENT	Fundamental control issue on which action should be taken immediately.	2	IMPORTANT	Control issue on which action should be taken at the earliest opportunity.	3	ROUTINE	Control issue on which action should be taken.

tiaa

Rec.	Risk Area	Finding	Recommendation	Priority	Management Comments	Implementation Timetable (dd/mm/yy)	Responsible Officer (Job Title)
6	Directed	The Business Continuity lead has oversight of a spreadsheet used to monitor each departmental Business Continuity Plan to record the date of the most recent review of each plan and next planned date. However, it was found that the lead did not hold copies of departmental Business Continuity Plans, which were retained locally. Where departmental Business Continuity Plans are not retained and overseen by the force lead, there is a risk that such plans will have not been completed consistently in terms of organisational requirements and in the event of an incident, impact the ability to enact departmental Business Continuity Plans effectively due to lack of awareness of requirements and recovery plans.	All departmental and business operational Business Continuity Plans be provided to the Superintendent - Special Operations.	2	*New département BCM plans will be created in line with the new operating model. Template being adopted from DPP.* *Plans to be retained centrally – will explore SharePoint.*	*01/04/25*	*Superintendent (Spec Op)*
8	Directed	The review of Business Continuity Plans revealed that most plans were overdue review and update. Where Business Continuity Plans are not kept up to date, there is a risk that the organisation is unable to: prevent or recover from potential threats; ensure business continuity in the event of an interruption; minimise disruption to staff and other stakeholders; to safeguard critical data and records; and, as consequence protect the organisation's reputation.	All Business Continuity Plans not reviewed in the last 12 months be reviewed and updated to reflect current arrangements.	2	*As above, each department/command area will have a refreshed BCM plan in 2025.*	*01/04/25*	*Superintendent (Spec Op)*

PRIORITY GRADINGS

1	URGENT	Fundamental control issue on which action should be taken immediately.

2	IMPORTANT	Control issue on which action should be taken at the earliest opportunity.

3	ROUTINE	Control issue on which action should be taken.

tiaa

Rec.	Risk Area	Finding	Recommendation	Priority	Management Comments	Implementation Timetable (dd/mm/yy)	Responsible Officer (Job Title)
9	Directed	A review of the Business Continuity Plans revealed that they appeared to lack detail and not robust enough. For example, the plans could also include details on Contacts - Activation, staff contacts, activities and services, Equipment (other than ICT) and Communications (setting out in the event of who to communicate with). A review of the Strategic Business Continuity Management reports also noted that that the Assistant Chief Constable (ACC) commented that: "BCM plans appear up to date but not sufficiently robust or detailed enough". Where there is a lack of detail in terms of requirements and how plans are to be enacted, there is a risk plans may not be sufficiently comprehensive to assist departments capability to recover and respond effectively to an incident.	The Business Continuity Plan Template be reviewed and updated to include greater detail to ensure the robustness of the plan.	2	*We had already acknowledged that our BCM plans lacked the required depth to be meaningful.* *Adopting DPP templates.*	01/04/25	*Superintendent (Spec Op)*

PRIORITY GRADINGS

1	URGENT	Fundamental control issue on which action should be taken immediately.
2	IMPORTANT	Control issue on which action should be taken at the earliest opportunity.
3	ROUTINE	Control issue on which action should be taken.

tiaa

Rec.	Risk Area	Finding	Recommendation	Priority	Management Comments	Implementation Timetable (dd/mm/yy)	Responsible Officer (Job Title)
10	Delivery	The review of departmental Business Continuity Plans noted that at the end of each plan there is a box to record the date of when the plan was Validated, Tested, Exercised or Actioned. The dates for the majority of the plans were between 2017 and 2022, with others dated either 2023 or 2024, which implies that the majority of the plans have not been tested with either a desktop exercise or mock exercise to test the robustness and integrity of the plan. Regular testing of Business Continuity Plans helps prepare staff in the event of an incident and can support identification of gaps or weaknesses in places, allowing for necessary adjustments and improvements to be made.	Periodic testing of Business Continuity Plans be implemented. This could include desktop-based or mock live test events.	2	*Testing an exercising is another area where we acknowledge there is a gap.* *The first quarter of 2025 focus will be on getting plans refreshed and an effective BCM governance structure in place. Once this is done, through the strategic group we will look to introduce some meaningful testing and exercising later in 2025.*	*01/08/25*	*Superintendent (Spec Op)* *ACC (Organisational)*

PRIORITY GRADINGS

1	URGENT	Fundamental control issue on which action should be taken immediately.		2	IMPORTANT	Control issue on which action should be taken at the earliest opportunity.		3	ROUTINE	Control issue on which action should be taken.

tiaa

Rec.	Risk Area	Finding	Recommendation	Priority	Management Comments	Implementation Timetable (dd/mm/yy)	Responsible Officer (Job Title)
2	Directed	The Business Continuity Plan does not set out any reference to the 'golden hour'. The actions taken during the first hour after an incident, known as the 'golden hour' when every second may count, and which is seen to lay the foundation for a response and can determine if an event will be a simple (and hopefully isolated) incident versus a full-blown ongoing critical event. Typical 'golden hour' activities may include protecting, preserving, or gathering material that may otherwise be concealed, lost, damaged, altered or destroyed. Where the activities to be performed in the 'golden hour' following the report of an incident, and subsequently the roles and responsibilities for undertaking such activity are no assigned, mitigating the effects of the incident and any consequences of the incident may become prolonged or escalated.	Reference to the actions to be taken during the first hour after an incident, known as 'the golden hour' to be included in the Business Continuity Management Policy and Procedures and in departmental Business Continuity Plans.	3	*We will introduce golden hour action cards – similar to what we have for critical and major incidents – as a simple actionable guide for staff and managers.*	*01/04/25*	*Superintendent (Spec Op)*
7	Directed	Best practice identified in other forces and other TIAA clients includes a standard Business Impact Analysis template to ensure a consistent approach across various departments and functions. The templates may include Critical Services / Activities, Risks, staff and equipment resource requirements, Impact Recovery Time Objectives and Minimum Service Level.	A Business Impact Analysis template be developed and shared with all relevant departments to standardise the process to ensure a consistent approach for managing a force wide incident.	3	*Included within DPP templates.*	*01/04/25*	*Superintendent (Spec Op)*

PRIORITY GRADINGS

1	URGENT	Fundamental control issue on which action should be taken immediately.	2	IMPORTANT	Control issue on which action should be taken at the earliest opportunity.	3	ROUTINE	Control issue on which action should be taken.

Rec.	Risk Area	Finding	Recommendation	Priority	Management Comments	Implementation Timetable (dd/mm/yy)	Responsible Officer (Job Title)
11	Delivery	Good practice identified in other forces and other sectors is to document the aftereffects of an incident, event or business continuity plan test exercise. A standard document could ensure a consistent approach throughout the force, and this could include the overview of the incident, summary of discussions about the incident, lessons learnt and an action log to record and enable monitoring of implementation of the findings and recommendations arising. This can be shared with the Superintendent as the Business Continuity lead.	A standard template document be developed and be made available to all departments with Business Continuity Plans to record the overview, discussion, lessons learnt and actions following an incident or event or business continuity plan test exercise.	3	*Included within DPP templates.*	01/04/25	*Superintendent (Spec Ops)*

PRIORITY GRADINGS

1	URGENT	Fundamental control issue on which action should be taken immediately.

2	IMPORTANT	Control issue on which action should be taken at the earliest opportunity.

3	ROUTINE	Control issue on which action should be taken.

tiaa

Operational - Effectiveness Matter (OEM) Action Plan

Ref	Risk Area	Finding	Suggested Action	Management Comments
1	Directed	Departmental Business Continuity Plans were found to be due for review (see also Recommendation 8). TIAA's work with Dyfed-Powys Police has identified the force's Business Continuity Plans an example of good practice in terms of the form and content.	Consideration be given to contacting Dyfed-Powys Police to request that they share their Departmental Business Continuity Plan template.	*In hand and being progressed with the support of Gaynor.*
2	Delivery	The Business Continuity Lead confirmed that hard copies of Business Continuity plans are retained in the Force Planning Unit. There is a risk that if IT systems were down and there was no access to the Force Planning Unit that the plans may not be accessible. Good practice is to also retain plans that can be access whilst offline on desktops, tablet or mobile phones devices.	Consideration be given to also retain copies of departmental Business Continuity Plans that can be access whilst offline on desktops, tablet or mobile phones devices as further resilience.	*Will ensure this is adopted, in the same way that we retain hard copies of major incident plans within FCR.*

ADVISORY NOTE

Operational Effectiveness Matters need to be considered as part of management review of procedures.

Findings

Directed Risk:

Failure to properly direct the service to ensure compliance with the requirements of the organisation.

Ref	Expected Key Risk Mitigation		Effectiveness of arrangements	Cross Reference to MAP	Cross Reference to OEM
GF	Governance Framework	There is a documented process instruction which accords with the relevant regulatory guidance, Financial Instructions and Scheme of Delegation.	Partially in place	1, 2, 3, & 4	-
RM	Risk Mitigation	The documented process aligns with the mitigating arrangements set out in the corporate risk register.	In place	-	-
C	Compliance	Compliance with statutory, regulatory and policy requirements is demonstrated, with action taken in cases of identified non-compliance.	Partially in place	5, 6, 7, 8, & 9	1

Other Findings

TIAA undertook a review of Business Continuity Recovery Planning in September 2021. The scope of the review was different to this review as it focused on the "planning to deliver for the back log of postponed work and projects due to the pandemic response across all departments". The review was given a Reasonable Assurance assessment with two Important (Priority 2) and one Routine (Priority 3) recommendations. The recommendations have been found to implemented and closed as part of the follow up process.

The force's Strategic Business Continuity Plan (Version 6.4) was last reviewed in December 2020 and is overdue a review. Since the Covid-19 pandemic organisations have reviewed their Business Continuity Plans (BCPs) due to the impact and changes to their working arrangements, systems and processes. **(Recommendation 1 refers).**

The force's Business Continuity Management Policy and Procedure was most recently reviewed, updated and approved by the Assistant Chief Constable in July 2023. The Policy states that: "The Chief Constable of Gwent Police is a Category 1 Responder as defined by the Civil Contingencies Act 2004 (CCA) and has duty to maintain plans to 'ensure that they can continue to perform their functions in the event of an Emergency, so far as is reasonably practicable'".

The force has separate Business Continuity Plans for the Local Policing Areas; one for the East LPA and one for the West LPA plus various Headquarters and Support functions which are all under one BCP.

Other Findings

🔍 The Force has a Property and Business Interruption Insurance Policy in place. The cover is provided by QBE Limited is valid until 31st March 2025. The force also has a Computer Insurance from HSB Engineering Insurance Limited also until 31st March 2025. The cover includes Hardware, Reinstatement of data, Increased cost of working and virus, hacking and denial of service attack.

🔍 The Business Continuity Management (BCM) Policy and Procedures sets out a section on the Media Strategy which states that: "A member of the Corporate Communications Department is an essential part of the BCM Response Team and MUST be contacted (using callout procedures if appropriate) whenever this plan is activated". The section also provides a standard template wording to be used in the event of an incident being activated.

🔍 Governance of business continuity is undertaken by the Strategic Business Continuity Management Group. Terms of Reference for the Group have been documented and were most recently reviewed and updated in May 2022. The Terms of Reference set out that the Group meet on a quarterly basis and also the members of the Group. The Group is chaired by the Superintendent Head of Special Operations. The Terms of Reference state that: "The Strategic Business Continuity Management Group terms of reference will be reviewed and updated as required and approved by members at least annually". **(Recommendation 4 refers).**

🔍 There currently no risks in relation to business continuity on the force's risk register.

🔍 The Business Continuity Management Policy and Procedure and the Business Continuity Policy refer to Business Impact Analysis. A Business Impact Analysis is the process of determining the criticality of business activities to enable an organisation to reduce the risks. A review of the Business Continuity Plans revealed they include the Core Functions and timescales for regaining services in a time of disruption with each function risk assessed and scored. A key and score description is provided to classify each overall score with Blue – Mission Critical, Red – Immediate   Orange – 1 week, and Green – 1 month.

🔍 A review of the East, West LPA B plans plus the Headquarters and Support plans was undertaken. The Plans, which are in MS Excel format, set out tabs for each area within the East. Each tab sets out Management titles, Management Staffing levels, Critical Staffing level per shift, Vehicle Requirements. software and hardware requirements, External Dependencies that are ranked, high, medium and low, Core functions Business Impact Analysis and a scoring matrix table of each function with a key to the scoring methodology.

tiaa

Ref	Expected Key Risk Mitigation		Effectiveness of arrangements	Cross Reference to MAP	Cross Reference to OEM
PM	**Performance Monitoring**	There are agreed KPIs for the process which align with the business plan requirements and are independently monitored, with corrective action taken in a timely manner.	Partially in place	10	-
S	**Sustainability**	The impact on the organisation's sustainability agenda has been considered.	In place	-	-
R	**Resilience**	Good practice to respond to business interruption events and to enhance the economic, effective and efficient delivery is adopted.	In place	11	2

Other Findings

The review of departmental Business Continuity Plans highlighted that the end of each plan there is a box to record the date of when the plan was Validated, Tested, Exercised or Actioned. The dates for the majority of the plans were dated between 2017 and 2022, with others dated either 2023 or 2024, which implies that the majority if the plans have not been tested with either a desktop or mock exercise to test the robustness and integrity of the Plan. Regular testing of a Business Continuity Plan can help identify any gaps or weaknesses, allowing for necessary adjustments and improvements. **(Recommendation 8 refers).**

Good practice identified in other forces and other sectors is to document the aftereffects of an incident, event or test exercise. A standard document for this purpose could ensure a consistent approach throughout the force and this could include the overview of the incident, summary of discussions about the incident, lessons learnt and an action log to record and enable monitoring of actions or recommendations identified. This can be shared with the Superintendent as the Business Continuity lead.

Scope and Limitations of the Review

1. The definition of the type of review, the limitations and the responsibilities of management in regard to this review are set out in the Annual Plan. As set out in the Audit Charter, substantive testing is only carried out where this has been agreed with management and unless explicitly shown in the scope no such work has been performed.

Disclaimer

2. The matters raised in this report are only those that came to the attention of the auditor during the course of the review and are not necessarily a comprehensive statement of all the weaknesses that exist or all the improvements that might be made. This report has been prepared solely for management's use and must not be recited or referred to in whole or in part to third parties without our prior written consent. No responsibility to any third party is accepted as the report has not been prepared, and is not intended, for any other purpose. TIAA neither owes nor accepts any duty of care to any other party who may receive this report and specifically disclaims any liability for loss, damage or expense of whatsoever nature, which is caused by their reliance on our report.

Effectiveness of Arrangements

3. The definitions of the effectiveness of arrangements are set out below. These are based solely upon the audit work performed, assume business as usual, and do not necessarily cover management override or exceptional circumstances.

In place	The control arrangements in place mitigate the risk from arising.
Partially in place	The control arrangements in place only partially mitigate the risk from arising.
Not in place	The control arrangements in place do not effectively mitigate the risk from arising.

Assurance Assessment

4. The definitions of the assurance assessments are:

Substantial Assurance	There is a robust system of internal controls operating effectively to ensure that risks are managed and process objectives achieved.
Reasonable Assurance	The system of internal controls is generally adequate and operating effectively but some improvements are required to ensure that risks are managed and process objectives achieved.
Limited Assurance	The system of internal controls is generally inadequate or not operating effectively and significant improvements are required to ensure that risks are managed and process objectives achieved.
No Assurance	There is a fundamental breakdown or absence of core internal controls requiring immediate action.

Acknowledgement

5. We would like to thank staff for their co-operation and assistance during the course of our work.

Release of Report

6. The table below sets out the history of this report:

Stage	Issued	Response Received
Audit Planning Memorandum:	3rd July 2024	3rd July 2024
Draft Report:	3rd January 2025	16th January 2025
Final Report:	16th January 2025	