Level 5

**BCM Maturity Assessment Report – Establishing a BCMS**

| **Focus Area** | **Maturity Level** | **Observations** | **Strengths** | **Weaknesses** | **Gaps** | **Recommendations** |
| --- | --- | --- | --- | --- | --- | --- |
| Management Commitment | 5 (Optimised) | Steering Committee is established, meets regularly with agendas and minutes available. | Strong leadership and governance; Regular engagements; Documented oversight. | None observed. | None. | Continue regular reviews and align Steering Committee with emerging risks and industry BCM trends. |
| BCM Policy | 5 (Optimised) | Approved BCM Policy is available and aligned with best practices. | Clearly articulated BCM vision and objectives; Strong policy foundation. | None observed. | None. | Ensure policy is reviewed annually and updated to reflect organisational and regulatory changes. |
| Governance Structure | 5 (Optimised) | Defined roles and responsibilities, formal appointments, and maintained records. | Well-defined structure; Accountability at all levels; Transparent governance. | None observed. | None. | Conduct periodic evaluations of committee performance and effectiveness. |
| BCM Charter | 5 (Optimised) | Charter is formally documented and approved. | Clear alignment to strategic BCM goals; Formal recognition of BCM. | None observed. | None. | Review and update charter as part of the BCM review cycle. |
| BCM Manager/Coordinator | 5 (Optimised) | BCM Coordinator appointed with documented responsibilities. | Strong coordination role established; Clear ownership of BCM activities. | None observed. | None. | Provide continuous training and development opportunities for the BCM Manager. |
| BCM Teams | 5 (Optimised) | All critical teams (ERT, CMT, Disaster Recovery) are established with formal appointments. | Full operational capability for emergency and recovery teams; Defined responsibilities. | None observed. | None. | Conduct regular drills to keep teams agile and prepared. |
| BCM Champions | 5 (Optimised) | BCM Champions appointed in all business units. | Business unit engagement is strong; Decentralized BCM knowledge and accountability. | None observed. | None. | Maintain engagement through quarterly BCM forums and refresher training. |
| Business Continuity Plan | 5 (Optimised) | Approved BCP in place. | Comprehensive planning documented; Response readiness. | None observed. | None. | Regularly test and review BCP scenarios including emerging threats (e.g., cyber, supply chain). |
| BCM Budget | 5 (Optimised) | Dedicated budget allocated. | Financial commitment is evident; Supports sustainability of BCM programme. | None observed. | None. | Ensure BCM budget is tied to risk landscape changes and updated with strategic goals. |
| BCM Programme Work Plan | 5 (Optimised) | Implementation guided by a structured BCM Work Plan. | Planned, consistent and proactive execution of BCM activities. | None observed. | None. | Update work plan quarterly based on internal audits, tests and evolving business priorities. |

**Overall Maturity Level: 5 – Optimised**

**General Observations:**

* The organisation has demonstrated **full compliance** across all Establishing BCMS indicators.
* All required evidence is available and aligns with international best practices such as ISO 22301.
* Stakeholder engagement is mature and well-coordinated.

**General Recommendations:**

* Maintain the current maturity by embedding BCM in corporate culture.
* Benchmark against leading practices periodically.
* Promote continuous improvement through lessons learned, audits, and scenario testing.

BCM Maturity Assessment Report – Embracing Business Continuity

| **Focus Area** | **Maturity Level** | **Observations** | **Strengths** | **Weaknesses** | **Gaps** | **Recommendations** |
| --- | --- | --- | --- | --- | --- | --- |
| Management Commitment | 5 (Optimised) | A formal BCM Steering Committee exists with clearly defined governance. Regular meetings are held and well documented. | Strong governance structure; Demonstrated leadership commitment; Ongoing oversight of BCM. | None observed. | None. | Maintain momentum through quarterly strategic reviews and reporting to executive leadership. |
| BCM Awareness & Induction | 5 (Optimised) | Awareness campaigns are actively conducted and integrated into employee induction processes. | High staff engagement; BCM culture embedded from onboarding phase; Continuous awareness efforts. | None observed. | None. | Refresh awareness materials annually and integrate BCM into e-learning platforms or digital onboarding tools. |
| Competence and Skills | 5 (Optimised) | All key BCM role players have received formal training with effectiveness evaluated through post-training assessments and feedback. | Highly skilled BCM personnel; Ongoing competency development; Continuous improvement based on feedback. | None observed. | None. | Continue annual training refreshers and simulate complex BCM scenarios for advanced development. |
| Training & Awareness Budget | 5 (Optimised) | A dedicated budget supports BCM training and awareness programmes. | Financial sustainability of BCM capacity building efforts; Strategic investment in skills and awareness. | None observed. | None. | Review and adjust budget allocation yearly to align with training needs, scope expansions, or new BCM initiatives. |

**Overall Maturity Level: 5 – Optimised**

**General Observations:**

* The organisation demonstrates a **deeply embedded business continuity culture**, supported by **governance, training, awareness, and investment**.
* Stakeholders show clear alignment with ISO 22301 expectations for organizational resilience.
* BCM is actively promoted at both leadership and employee levels.

**General Recommendations:**

* Maintain and build on current strengths by leveraging BCM champions and ambassadors within departments.
* Incorporate advanced scenario-based learning (e.g., cyber threats, pandemic response).
* Benchmark awareness and training programmes against peer institutions or industry leaders.

BCM Maturity Assessment Report – Analysis

| **Focus Area** | **Maturity Level** | **Observations** | **Strengths** | **Weaknesses** | **Gaps** | **Recommendations** |
| --- | --- | --- | --- | --- | --- | --- |
| Business Impact Analysis | 5 (Optimised) | Critical business activities have been thoroughly identified via BIA, with detailed analysis and prioritisation completed. | Clearly defined critical functions; RTOs and RPOs are well-documented; Analysis aligns with strategic priorities. | None observed. | None. | Periodically update BIA (at least annually or when major changes occur). Integrate BIA results into strategic planning and risk registers. |
| Detailed Impact Assessment | 5 (Optimised) | BIA reports include time-based impact scenarios and dependencies, including financial, legal, and reputational impact analysis. | Comprehensive understanding of impact thresholds; Informed response planning; Well-developed continuity planning basis. | None observed. | None. | Extend impact modelling to third parties (vendors, partners) to cover supply chain continuity. |
| RTOs and RPOs | 5 (Optimised) | Documented RTOs and RPOs for each critical function are in place, validated and communicated to stakeholders. | Precise recovery expectations; Informed IT and process recovery strategies; Business-aligned recovery goals. | None observed. | None. | Conduct RTO/RPO testing through simulation or system recovery validation; ensure continual alignment with business changes. |
| Risk Assessment | 5 (Optimised) | BCM risk assessments are regularly performed and integrated into the enterprise risk management framework. | Comprehensive identification of BCM threats; Strong link to organisational risk profile; Risk-driven BCM planning. | None observed. | None. | Continue to update BCM risk assessments in line with emerging threats (e.g., cybersecurity, climate, geopolitical risks). |

**Overall Maturity Level: 5 – Optimised**

**General Observations:**

* The organisation has demonstrated a highly mature approach to **business continuity analysis**, with **strong alignment between business priorities and continuity strategies**.
* Stakeholders provided complete evidence supporting the analytical phase of the BCM lifecycle.
* The BIA and Risk Assessment processes are clearly institutionalised and updated as part of normal business operations.

**General Recommendations:**

* Maintain periodic BIA and risk review cycles aligned with major changes (systems, services, regulations).
* Use BIA/Risk outputs to inform scenario-based BCM exercises and investment decisions.
* Leverage technology (e.g., BIA software or dashboards) to improve reporting and traceability of recovery dependencies and risk trends.

BCM Maturity Assessment Report – Solutions Design

| **Focus Area** | **Maturity Level** | **Observations** | **Strengths** | **Weaknesses** | **Gaps** | **Recommendations** |
| --- | --- | --- | --- | --- | --- | --- |
| Business Continuity Strategy Development | 5 (Optimised) | Strategies for sustaining critical activities are well-documented and formally approved. | Strategies are risk-informed and BIA-driven; Strong alignment with operational priorities; Robust documentation exists. | None observed. | None. | Maintain ongoing alignment of strategies with changes in technology, business models, and regulatory demands. |
| Use of BIA & Risk Inputs | 5 (Optimised) | Strategy documents directly reference findings from BIA and BCM risk assessments. | Evidence-based decision-making; Risk-informed planning enhances resilience; Transparent link to analysis phase. | None observed. | None. | Institutionalise periodic reviews of strategies to accommodate evolving risks or BIA changes. |
| Tactical Adequacy (Resources/SLAs) | 5 (Optimised) | Continuity strategies have been evaluated and shown to meet service-level and resource requirements for all critical operations. | Clear understanding of resource needs; Tactical solutions meet or exceed continuity objectives; Well-integrated with IT and facilities planning. | None observed. | None. | Continue scenario-based validation (e.g., stress tests) to confirm tactical adequacy under extreme conditions. |
| Solution Implementation Planning | 5 (Optimised) | Implementation projects are well-resourced and funded, with defined plans for deploying BCM solutions. | Strong project planning and execution capability; Adequate resourcing supports long-term resilience goals. | None observed. | None. | Link project outcomes to BCM performance metrics and ensure executive oversight remains active during implementation. |

**Overall Maturity Level: 5 – Optimised**

**General Observations:**

* The organisation has a **comprehensive and well-integrated BCM strategy development process**.
* Strategy selection is directly based on **BIA and risk assessment** results, ensuring relevance and priority alignment.
* **Funded initiatives** exist to implement the solutions, reflecting strategic commitment to continuity and resilience.

**General Recommendations:**

* Regularly review strategies and implementation projects against **changing business landscapes and new threats** (e.g., cyber risks, environmental hazards).
* Develop metrics to measure the **effectiveness and ROI of implemented solutions**.
* Ensure continued coordination between IT, facilities, HR, and operations for end-to-end solution coverage.

BCM Maturity Assessment Report – Enabling Solutions

| **Focus Area** | **Maturity Level** | **Observations** | **Strengths** | **Weaknesses** | **Gaps** | **Recommendations** |
| --- | --- | --- | --- | --- | --- | --- |
| Incident Response | 5 (Optimised) | A documented incident response structure exists and outlines roles, responsibilities, and procedures. | Clear command structure; Rapid response capabilities; Well-integrated into BCM framework. | None observed. | None. | Conduct regular incident response drills and post-incident reviews to ensure agility and readiness. |
| Business Continuity Plan | 5 (Optimised) | An up-to-date and approved BCP exists, covering all critical operations and functions. | Robust documentation; Well-aligned with organisational priorities and BIA findings. | None observed. | None. | Review and test BCP at least annually and after major business or operational changes. |
| Emergency Response Plan | 5 (Optimised) | Emergency Response Plan is documented, accessible, and aligned to site-specific threats and scenarios. | Quick response readiness; Clear evacuation, safety, and communication protocols. | None observed. | None. | Regularly conduct emergency drills and include third-party tenants or site occupants in planning and testing. |
| Disaster Recovery Plan | 5 (Optimised) | DRP is approved and supports IT service continuity across all key systems and infrastructure. | Strong IT-business alignment; Tested and validated recovery procedures; Integration with overall BCM. | None observed. | None. | Continue periodic recovery testing (e.g., failover simulations) and ensure DRP reflects latest system configurations and risks. |
| Crisis Management Plan | 5 (Optimised) | CMP is formalised and provides guidance for executive response during major disruptions. | High-level leadership involvement; Clear communication and decision-making framework; Media and stakeholder communication considered. | None observed. | None. | Ensure periodic tabletop exercises involving executive leadership to maintain confidence and effectiveness. |
| Pandemic Response Plan | 5 (Optimised) | A COVID-19 or equivalent pandemic plan was developed, implemented, and documented. | Demonstrated agility during health crises; Health, safety, and operational continuity well addressed; Lessons learned documented. | None observed. | None. | Review pandemic plan for relevance to future public health, biosecurity, or widespread workforce disruption events. |

**Overall Maturity Level: 5 – Optimised**

**General Observations:**

* The organisation has **comprehensive and well-integrated continuity response plans** that enable resilience across multiple disruption scenarios.
* Documentation is not only complete but is actively maintained, reviewed, and embedded in operational practice.
* All key functional plans (BCP, ERP, DRP, CMP, Pandemic) are aligned and complementary, supporting a cohesive response structure.

**General Recommendations:**

* Maintain current documentation maturity by scheduling **annual reviews and scenario-based testing** across all plans.
* Strengthen coordination through **integrated multi-plan exercises** (e.g., combining ERP, CMP, and DRP into a complex crisis scenario).
* Continue to track **lessons learned** from actual incidents or global disruptions to update and refine response strategies.

BCM Maturity Assessment Report – Validation

| **Focus Area** | **Maturity Level** | **Observations** | **Strengths** | **Weaknesses** | **Gaps** | **Recommendations** |
| --- | --- | --- | --- | --- | --- | --- |
| Exercising and Testing | 5 (Optimised) | The organisation has a formal, well-documented testing and exercising programme that covers all major BCM components. | Regular testing schedule; Wide participation across business units; Use of varied exercise types (tabletop, simulation, live). | None observed. | None. | Incorporate more complex and cross-functional scenarios; track lessons learned and update plans accordingly. |
| Review and Assurance | 5 (Optimised) | BCM arrangements have undergone comprehensive review through internal audits, self-assessments, or third-party evaluations in the past year. | Strong governance and oversight; Transparent and verifiable assurance practices; Issues identified and acted upon effectively. | None observed. | None. | Continue annual audits and consider rotating external reviewers for a fresh perspective; integrate BCM findings into enterprise risk reporting. |

**Overall Maturity Level: 5 – Optimised**

**General Observations:**

* The organisation has **institutionalised its validation process**, ensuring that BCM capabilities are not only documented but **tested, reviewed, and continually improved**.
* A structured testing programme and recent audits confirm a high level of **preparedness and compliance**.

**General Recommendations:**

* Evolve testing to include **advanced threat scenarios** (e.g., coordinated cyberattacks, critical supplier failures).
* Ensure **post-exercise reporting** includes measurable metrics and that improvement actions are tracked to completion.
* Align BCM validation cycles with **IT DR and crisis communication plans** for full-spectrum resilience validation.