The Bad Practice Guidelines
(How Not to Implement BCM)

***Written by Mel Gosling**: "The idea for a Bad Practice Guidelines came about during a meeting of the BCI's GPG Quality Review working group, and was inspired by Mike Hill. What started off as just an amusing idea has a serious purpose. Just because a practice isn't in the Good Practice Guidelines it doesn't mean that it's Bad Practice. By using this Guide, practitioners should be able to identify some of the more common Bad Practices that are still to be found in the world of business continuity. Hopefully, it will also provide some entertainment."*

Business Continuity Management

Business Continuity Management (BCM) is a management process that is used to convince auditors, regulators, and other stakeholders that the organisation has the capability for an effective response to potential impacts that threaten its reputation, brand and value creating activities, even if it hasn't.

BCM Policy and Programme Management

An effective BCM programme will involve no participation by the organisation's executives, and the minimal involvement of managerial, operational, administrative and technical disciplines.

Responsibility for BCM will be given to someone lower down the organisation that has little authority, and whom the Executive feels needs to be given something else to do. This individual will be called the Business Continuity Manager, but will have no staff, and will not be given additional resources to undertake the work.

The lead during incident response will come from the organisation's Executive, who will have taken no interest in the BCM programme and who will have no knowledge of the Incident Management and Business Continuity Plans.

Developing and Implementing a BCM Response

The whole purpose of the BCM process is to produce a Business Continuity Plan (BCP), and this where the BCM process should start. The aim of the BCP will be to give confidence to stakeholders and auditors that the organisation's critical functions will continue to operate during an interruption, whatever its cause, and that the remainder will be recovered in a controlled manner.

The Business Continuity Manager should embark on developing a BCP at the earliest opportunity, and should not be concerned about involving others in the work, as they will probably have more important things to do.

Incident Management Plan

An Incident Management Plan can be developed, but this is an additional expense that is not really necessary. The organisation's Executive will provide effective and timely management of a major incident, and will protect the organisation's brand from financial and reputation damage without the need for an Incident Management Plan.

Business Continuity Plan

The BCP is the foundation on which the whole BCM process is built. It documents the theoretical response of the whole organisation to a disruptive incident rather than the actual arrangements that have been established. Those using the plan should be able to pick it up and use it without ever having seen it before, and to know instinctively how it should be used to select and deploy appropriate strategies from those available to direct the resumption of business units according to the priorities that they see as important at the time.

The components and content of a BCP can vary from organisation to organisation, but as a template obtained from another organisation will be used to develop the BCP, it is likely to be based on the culture of that other organisation and the technical complexity of its solutions.

Business Unit Resumption Plans

Business Unit Resumption Plans provide the operational response to the incident of specific departments or business units. These are usually developed by individual departments with little or no reference to the BCP, and can often conflict with the BCP in terms of objectives, priorities, and recovery processes. A typical example of a Business Unit Resumption Plan is an ICT Disaster Recovery Plan, which should be developed by the ICT department without wasting the time of the users of the facilities by asking what their requirements for ICT might be.

Understanding the Organisation

Once the BCP has been developed, the other elements of the BCM programme that auditors will want to see can be created. A precursor to this though, is to learn the jargon used by Business Continuity professionals so that it can be applied to your organisation, even if nobody else is interested.

Business Impact Analysis

Theoretically, the Business Impact Analysis (BIA) identifies, quantifies and qualifies the business impacts of a loss, interruption or disruption of business processes so that management can determine at what point in time these become intolerable (after an interruption). In practice, this is impossible to achieve.

Undertaking a BIA through interviews, workshops, and questionnaires is expensive and time consuming, and should therefore not be attempted unless there is no other work for the Business Continuity Manager to do. Instead, the objective of the BIA, which is to identify the 'Maximum Tolerable Period of Disruption' (MTPD) of each business process, can be achieved by using information from BCP that has already been developed.

The MTPD of each business process is the same as its recovery time, as shown in the BCP, and this information should be extracted from the BCP into a separate document that can be sent to the Executive as evidence that the BIA has been completed.

Continuity Requirements Analysis

Continuity Requirements Analysis (CRA) collects information on the numbers of resources required to resume and continue the business activities. Again, this can be obtained from the BCP that has already been developed, and does not have to be undertaken as a separate exercise.

Risk Assessment

In the context of BCM, a Risk Assessment estimates the probability and impact of the threats that could cause a business interruption that are most commonly reported in the media, or which appear to concern the Executive most. The Risk Assessment should use a quantitative method, estimating the probability of occurrence of each risk and calculating its impact, and multiplying the two together to provide the illusion of an accurate numeric measure of the risk.

For each risk that has been measured, a number of mitigating actions that reduce the risk should be identified. These should be presented to the Executive as evidence that the organisation understand the risks that threaten it and is taking action to reduce those risks. Following the production of this report to the Executive, the Risk Assessment can be ignored for at least a full year.

Determining BC Strategies

The Business Continuity Management Strategies to be used to maintain the organisation's business activities and processes through an interruption will have already been determined when developing the BCP. These strategies, and the associated tactics for recovering individual activities and processes need to be documented and presented to the Executive.

The strategies selected do not necessarily have to have been implemented, and similarly the tactics used in the BCP do not need to be operational. These represent the aspirations of the organisation regarding resilience and continuity, and should therefore be seen as objectives.

Exercising, Maintenance and Review

A BCM capability can be considered reliable as soon as the BCP has been developed. However, to satisfy the requirements of auditors, regulators, and other stakeholders, evidence that it has been exercised, then maintained and audited will be required.

Exercising

The evidence for the organisation's BCM capability having been exercised is achieved through developing a plan for an exercise programme. The plan does not need to be implemented to be successful, its very existence and a stated intention to undertake the exercises once convenient dates can be found is often all that is required. The planned exercises should begin simply with a walk-through of the BCP by the Business Continuity Manager, and escalate rapidly to complex exercises that are far too expensive ever to be undertaken.

Maintenance

The BCM Maintenance Programme should demonstrate that the organisation remains ready to handle incidents despite the constant changes that all organisations experience.

The most effective way to achieve this is to plan a maintenance schedule for the BCP and to re-issue the BCP with a revised date and version number at the times specified in the schedule, even if nothing in the BCP has actually been changed.

Review

Self-assessment of the organisation's BCM process is the preferred method of review, and so as to be seen as being impartial, the individual who originally appointed the Business Continuity Manager should undertake the review. However, as BCM standards are constantly evolving, the Business Continuity Manager must be prepared to produce whatever evidence of compliance may be required during the review.

Embedding BCM in the organisation's Culture

The fact that a BCP has been developed is evidence of having developed a successful Business Continuity culture. Any attempt to create enthusiasm for Business Continuity within the organisation is unrealistic, but it is important for the Business Continuity Manager to know that the Executive are aware of the BCP and the valuable Business Continuity work that has been undertaken.

Assessing BCM Awareness and training

Before planning, and designing the components of, an awareness campaign for the Executive, it is critical to assume that the Executive know little or nothing about BCM.

Developing BCM within the organisation's culture

Designing education, training and awareness for the Executive is a very difficult task as the time allotted to delivery is usually very small. In many organisations this will be as little as 10 minutes. Concentration on the main message, which is that the organisation has a Business Continuity Manager that has developed and implemented a BCP, is therefore critical.

Monitoring cultural change

The Executive awareness campaign should be reviewed as a one-off task. Success will be measured by the amount of time devoted by the Executive to listening to, and asking questions of, the Business Continuity Manager.