Contingency Plan for the Treasury Function

1. **Summary:**

We would like to describe the process and the organisation required to prevent any forced interruption of the treasury function for any reason. Having a "BCP" (Business Continuity Plan) is no longer just a luxury, but a real necessity for any multinational business. It is vital to assure the CFO that at any time the treasury function will continue to operate, even under the worst scenarios, especially in the current unstable environment.

2. **Key headlines**

Preparation a BCP can even turn out to be helpful in detecting sources of problems and structural inefficiencies

Technology improves efficiency and productivity, but also creates (over)dependency by treasurers

Common sense can often prevent incidents or mitigate their impact

A BCP is a preventative measure, but could also prove to be curative

3. **ARTICLE**

See next page
It might be worse

The terrible moments, often verging on financial chaos, that we lived through in 2008, sadly remind us that things might be worse. Who would have imagined an earth-shattering event of such proportions? And nevertheless, we could have seen the storm clouds gathering. These events prove to us, should that be necessary, that we should not shelter behind the illusion that such things happen only to others, that they are impossible or we have never seen such things happen before. We may draw a parallel with outside events that might slow down, stop or temporarily prevent the treasury function being carried out. The worst, as we now know, often happens when it shouldn't, following Murphy's Law. That is why we have to prepare meticulously. A "Business Continuity Plan" (BCP) and a Disaster Recovery Plan (DRP) are necessary for all treasury departments. Preparing a BCP can even turn out to be helpful in detecting sources of problems and structural inefficiencies. The work of treasury is by definition a day to day activity which cannot be interrupted without the risk of loss, lost earnings or inefficiency. Treasurers are duty-bound to put in place a tested and effective contingency plan which will give Management the reassurance that even total destruction of the building in which the treasury function is located will not put a stop to the department’s activity or to good cash management.

Treasury structure flowchart

The starting point is fully to flowchart the operations and activities carried out by treasury department. When a complete list has been worked out, a criticality factor has to be applied. Can activity X or Y be closed down for 4 hours, for 1 day, for 3 days or only for 1 hour? Where a greater or lesser criticality level has been decided for each operation, we can try to find a "workaround" that might, at least temporarily, make it possible to continue activity X or Y. Paradoxically, the more the department has been computerised and built up, the greater the technical difficulties that will arise from any stoppage, and the harder it will be to find any workaround. Technology improves efficiency and productivity, but also creates (over)dependency by treasurers. Machines improve work efficiency, but keeping staff numbers to the minimum makes the department more vulnerable, however. We have to distinguish between tasks that cannot suffer any delay, those that can suffer some delay, those for which there is a workaround solution, at least for a short time and finally those for which a reasonable delay would not give rise to much in the way of consequences in the short term. Is there a failsafe mode or some temporary workaround? Would the halted or delayed activity impact downstream on any other vital financial activities or accounting reports? Would complete shutdown threaten the company within a very short time? These are the sorts of questions to ask at the flowcharting stage.

Tasks also need to be sorted by order of priority and importance into the (most) critical, to identify the priorities in the event of an incident. Secondly, operations
for which a delay could be critical need to be identified (for example telephone or electricity being cut off, IT network failure, lack of staff due to food poisoning in the canteen, or server downtime).

This appraisal will enable you to set out backup procedures for personnel, jobs, tasks and systems. It is also an opportunity to draft out any procedures that may not yet have been documented. It is an exercise in self-evaluation, and one that is very healthy for improving your internal structure. Sadly, as is too often the case, the most difficult thing is finding the time to initiate the BCP process, unless this is included in a wider BCP/DRP exercise at group level.

**Setting up a BCP**

Setting up such a BCP may form part of an overall plan deployed throughout the company. It is then quite common to use external consultants. They can coordinate and organise the implementation of an overall plan by entity and for group headquarters. Failing an overall BCP, it is the duty of everyone and of the treasurer in particular, to foresee a potential shutdown of activities, and to take steps to mitigate it. Sometimes, the measures to be taken are straightforward and not burdensome. Common sense can often prevent incidents or mitigate their impact. Simple security measures sometimes need no great amount of work. Others, by contrast, require additional investment (for example a backup server or remote backup hardware).

For example, should the treasurer not have the list of addresses and telephone numbers of his main contacts, particularly banks, what would he do in the morning when he arrives in the office? How much time will be wasted in recreating the contacts and telephone numbers? A (paper) copy kept at home could be a simple prevention measure. Because in the event of fire, there is a high risk that even a BlackBerry, an I-phone or any Smart phone will no longer work.

In addition to the operation’s contingency plan as described in this article, treasurers keen on taking precautions could also think of other scenarios involving the occurrence of external events, such as a bank failure, the merger of two banks resulting in a line of credit being reduced, a “credit crunch” affecting the company’s liquidity or even the collapse of an IT systems supplier resulting in maintenance ceasing.
**BCP objectives:**

1. **Identify critical headquarters functions and recovery time objectives**
2. **Define recovery priorities**
3. **Identify the BCP processes to be maintained**
4. **Establish a migration plan in case of disaster**
5. **Prepare a communication plan**
6. **Evaluate the potential solution of an external disaster recovery site**

**Test the BCP regularly**

A contingency plan that is not tested regularly is just about useless. You have to put yourself into the conditions of a major incident at least once yearly to really test the plan’s effectiveness. It needs to be detailed and documented if it is to be able to be applied at any time, irrespective of the circumstances and people at work on the day of the incident. This general document must also give exact details of the measures to be taken and the migration process in the event of a disaster. A good internal and external communication plan must be drafted out. Banks, suppliers and subsidiaries must be notified of the incident and of the contingency plan, so that the new temporary arrangements do not alarm them. The aim is to ensure activities are not impacted, or are impacted as little as possible, so as not to lose even a single Euro unnecessarily through negligence. There is a high risk, if preparations are not taken, of losing money or losing earnings because funds stay "dormant" for a period of time (not renewing a deposit and non-interest bearing funds or non-delivery of purchased currency or debit balances not being cleared).

A BCP must be updated regularly on the appearance of any new IT solution, for example a new process or procedure. Any new tool may potentially require changes to the BCP. It is helpful to sketch out an impact matrix, on two axes (probability on the horizontal axis and impact as a percentage of interruption on the vertical axis). The treasurer can position the main risks on this matrix depending on their probability (low – medium – high) and their criticality. This chart gives a fuller overview of the risks and the criticality level in relation to day-to-day activity.

**Be prepared!**

Preparing for a major event firstly gives you the chance to conduct a thorough review of your structure. Secondly, it enables you to exorcise the risk of an incident. The best way of fending off or exorcising risk according to some ancient folk beliefs is to address it and prepare for it. The British Army’s 5 Ps applies here: ”Proper Preparation Prevents Poor Performance”. A BCP is a preventative measure, but could also prove to be curative. The risk is one of not thinking up
simple preventative measures that may involve no cost, no particular work and no effort to implement.

François Masquelier
Chairman of ATEL
@FrancoisMasquel