ACTUALIZING... BUSINESS CONTINUITY PLAN FOR TREASURY – BEST IN CLASS

As we adjust to extended periods of remote working, clients are realizing how effort previously expended in creating a business continuity plan (BCP) is paying back in spades. Good for them. And it's true having a plan in place to accommodate the loss of access to the main office is one of the critical considerations in formulating an effective BCP plan. A full BCP plan needs to cover much more than planning for remote working. Starting to build out a BCP can be daunting, so we present an approach to defining what a BCP plan should cover for a specific company and how to evaluate and prioritise mitigations and recovery from those events, should they occur.

INITIAL ASSESSMENT

A good starting point is to document the process flow of all the mission-critical activities of the Treasury function along with the frequency of action. If a company makes its payment run on a Thursday only, then an outage on a Tuesday is a much smaller issue than a Thursday.

Secondly, gathering together a list of all relevant artefacts is another initial point of collation. Here we define an artefact both as documents, document libraries, any current BCP plans, communication plans, and contacts as well as physical items such as the relevant systems being used to include banking portals, general ledgers, and the TMS (Treasury Management System).

SCENARIO PLANNING

One tip in devising a scenario plan is to be clear about the coverage that a BCP is aimed for. I recall a BCP planning session early in my career whilst living in Japan. We had a long debate over whether planning for the "big earthquake hitting Tokyo" was a sensible scenario or not. The company had a backup location several miles outside of Tokyo, but if an earthquake occurred, would it not be better to have that location 100 miles away. I do not recall where that ended...Avoid getting too specific in the nature of the scenario but do include the current status. It is not necessary to list out multiple scenarios of how the main office became unavailable; it's enough to state one scenario where the office is unavailable.

The recommendation is to utilise a grid approach to gather the scenarios. Firstly, the scenarios themselves generally fit into for 4 main categories, as shown below, along with a few samples for illustration.

FIGURE 1: Scenario List

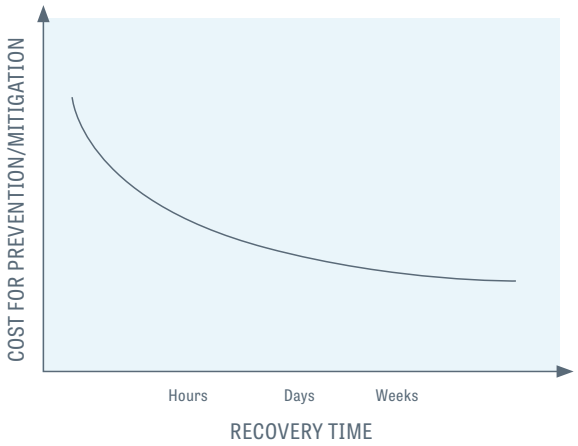
LOSS OF PERSONNEL	LOSS OF FACILITIES	LOSS OF SERVICES	LOSS OF ACCESS
Deputy Treasurer on sick leave.	Main treasury office unavailable. Back up site exists 1-2km away. OR Main treasury office unavailable. No back up site currently exists.	Main TMS is locally installed on client datacenter. No back up datacenter.	TMS no longer accessible. Main payments system no longer accessible.

BCP ACTION PLAN

Once the assessment and scenarios have been defined you can start to formulate a BCP action plan. The scenarios should be reviewed and signed off with stakeholders. At this point, you can formulate an actual BCP action plan. One can think of the cost of implementing a BCP plan akin to an insurance premium. An interesting analogy since business continuity insurance does exist as an offering. However, Global Pandemics are a small print item that are typically not covered.

Continuing the insurance analogy, we are generally comfortable understanding that the higher the level of coverage, the more the cost. In BCP terms, one way to think about this is to understand the relationship between Cost of Prevention versus Cost of Recovery. Research has shown that this relationship is not typically linear at the short end of the timeline.

FIGURE 2: Cost of Prevention vs Recovery time



Thinking about Cost of Recovery itself, one can appreciate that the ability to recover critical systems within minutes requires a significant investment that could be mitigated through other means. For example, making payments through the banking portal as the mitigation to the main Treasury Management System for payment generation is unavailable. To that end, we recommend action plans be articulated for three separate time buckets.

- **Short term (0-72 hours)** – Think of this as the short-term emergency plan.
- **Medium term (3-30 days)** – With items such as payment cycles, management reporting typically falling into monthly cycles and approach to outage over this length requires a different mindset and approach.
- **Long term (30+ days)** – And finally then, the long-term plan requires an adjustment to a new normal.

FIGURE 3: Sample Action Plan

	SHORT (0-72 HOURS)	**MEDIUM** (3-30 DAYS)	**LONG** (30+ DAYS)
LOSS OF SERVICES: Main TMS is locally installed on client datacenter. Application not available.	Work without TMS: Build out extracts from TMS to contain cash viability, upcoming payments, etc. Ensure reports are emailed to team.	Transition back to TMS: Build out cloud based reporting to house reports for team access. Document Data recovery for TMS. Develop data migration plans to ensure TMS is brought back in sync with data.	Back to normal: Datacenter back online. No additional mitigations required.
LOSS OF PERSONNEL: Deputy treasurer leaves.	Redistribute responsibilities: Ensure all key responsibilities have at least 2 personnel able to perform. Cross train all staff.	Reorganize the team: Hire replacement. Ensure procedure docs in place.	Back to normal: New treasurer in place. No additional mitigations required.

For each scenario agreed, an action plan is drawn up. The action plan should define a specific response and address implications to both personnel and infrastructure. The individual action plans can then be formulated into a project plan for implementation (including costings) and presented for funding and implementation. Again, understanding the costs for each scenario individually and collectively is key for stakeholders. There are typically some low cost, quick to implement activities that can be actioned immediately.

Be mindful of security. A disaster scenario should not be an excuse to drop security policies and principles. If multi-factor authentication is being used to access a TMS, it should still be available in said scenario.

TEST, REFINE AND RETEST

Using today's working environment as a potential wake up call, you ideally don't want to wait for an actual disaster to strike before knowing the BCPs are appropriate. The plans must be tested on a regular basis, with results documented and output reviewed for opportunities to enhance the plan. Clearly, it's no fun for the individuals to schedule an outage at 4:30 pm on the Friday of Month End, but perhaps at a minimum that scenario could be enacted around a conference table. If a remote site is available, consider scheduling a day to have the teamwork at the location. This would provide tangible feedback on working space, quality of networks, accessibility to required documents, data, etc. One outcome of good testing will be the identification of the weakest link of the plan which can then be mitigated and retested.

Additionally, whenever a significant change hits an organization, for instance a change of TMS vendor, business acquisition, or key personnel changes occur, this should trigger a review and update to the plan as appropriate.

IT'S GOOD TO TALK

Finally, we must recognize that communication in the event of BCP is paramount. Having a centralized contact list along with a chain of communication structure is a must. It's tempting to think that with work email and our smartphones this information exists in some form already. However, thinking about where this information is held in the event of the scenarios above is vital to a speedy recovery. Privacy concerns must be considered, but if the loss of work email is a scenario to cover, then personal email addresses should be included. It's also important to produce an external contact list for those groups treasury regularly interacts with, relationship bankers, TMS systems contacts, etc.

Preparing for the future starts today with a strong BCP plan fit for purpose for your individual company's criteria. Please contact us for additional planning tips, review of templates and plans, and how to get started.