Business Continuity Management

Business Impact Analysis (BIA)

This BIA identifies and documents the key products and services of PAS Ltd; the critical activities required to deliver these; the impact that a disruption of these activities would have on our organisation; and the resources required to resume the activities.

Key Products and Services

This section lists the key products and services PAS Ltd provides which if disrupted for any reason will have the greatest impact. For each product or service identified, we have tried to consider what the impact of a disruption would be both in terms of our organisation's ability to meet its aims and objectives, and the consequences. These are:

1. Customer support
2. Software development
3. Hosted customer solutions
4. Accounts management and billing
5. Sales and marketing

Impact Durations

Given the above list of Key Products and Services, this section looks at the effects each of these would have over varying time scales.

1. **Customer Support** – Loss of the ability to support our customers for short periods of time (up to 24hrs) would likely not have huge effects, the software we support, although time critical, does not require immediate attention in a majority of cases. It should also be noted that support activities are primarily focused on the period between April and early July and can be conducted from other sites.

   If the interruption was to extend beyond 24hrs into multiple days, or possibly weeks, the effect would be more substantial, often meaning customers could not complete activities that could result in fines.

2. **Software Development** – Many of the time issues are the same as detailed above, however it is unlikely that loss of development activities would have such crucial effects. The key software development period for the business is fairly flexible.

3. **Hosted Customer Solutions** – As in point 1, interruption of our infrastructure for short periods of time (up to 24hrs) would likely not have huge effects, the service we offer, although time critical, does not require 100% uptime in a majority of cases. It should also be noted that 'business critical' activities are primarily focused on the period between April and early July.

If the interruption was to extend beyond 24hrs into multiple days, or possibly weeks, the effect would be more substantial, often meaning customers could not complete activities that could result in fines.

4. **Account Management and Billing** – Although a key part of running the business, an interruption of our ability to invoice customers and look after customers is non-critical even over longer periods of time.

5. **Sales and Marketing** – Although a key part of running the business, an interruption of our ability to sell and market our products is non-critical even over longer periods of time.

Understanding the organisation and impact

Given the above, it appears that the Maximum Tolerable Period of Disruption (MTPD) would be in the order of 24-48 hours. During this time activities would not threaten the organisation's viability, either financially or through a loss of reputation.

This indicates that PAS Ltd has a goal (or Recovery Time Objective) of 48 hours maximum, with areas 1 and 3 being treated as a priority.

The rest of this plan seeks to document the critical activities that are required to deliver our key products and services, and looks into four key areas:

1. **People** – Customer support and hosting services can be handled with a skeleton staff of 2-3 people even at the busiest time. The range of skills required would include a mix of 1st, 2nd and 3rd line support people.

2. **Premises** – PAS has only one key location for support, should the issues be with the location of the office itself, we could provide key services from any remote location with Internet access (such as employee's homes). Should the issue be with the hosting facility, we would have to reconfigure services at another location, possibly from backup systems.

3. **Technology** – Staff would need access to PCs, Internet connectivity and phones to be able to successfully carry out both support and managed service maintenance. These are all based on standard hardware.

4. **Information** – It would be crucial to have access to the core customer records and support systems that are used. Both systems are run from a remote hosting facilities, meaning they are independent of the core office location, and are also backed up to off-site locations.

5. **Suppliers and partners** – PAS Ltd has a number of partners that resell our products and for whom we offer backup support activities. These would need to be kept updated on any issues or disruption to service.

Risk Assessment

This risk assessment looks at the likelihood and possible impacts of a variety of risks that could cause a business interruption for PAS Ltd. The aim is to assess these risks and therefore be able to prioritise any risk reduction activities. The focus of this risk assessment is the critical activities and supporting resources identified in the BIA stage.

The key risks identified are:

1. **Loss of staff** – It is very unlikely that there would be a complete loss of staff in the business. We have cover plans in place for staff not being able to be in the office, and for the period mentioned there is adequate cover to handle most situations. It would be logical to ensure we have 'doubled up' on all key delivery areas to minimise risk. Solutions for high levels of absence from long-term sickness, sickness clashing with annual leave, include:

   - Increased staff flexibility to ensure that staff within the support section can effectively switch roles at short notice
   - Regular training to ensure that all staff are kept up to date with processes and legislation

   Solutions for high incidence of staff turnover resulting in a lack of experience include:

   - Clear and up to date documentation of all procedures
   - Regular staff development reviews to identify areas of knowledge shortfall
   - Full commitment to staff training by the company, with the aim of providing cover at every level of operation

2. **Loss of systems (IT and telecommunications)** – This section is broken into further elements as it is the most crucial and would have the most dramatic effect on the business.

   Computer hardware - PAS Ltd server systems are based upon the use of standard hardware platforms and virtual environments, with standard configurations. A small number of these of these are located at the main offices; others are hosted at ioMart and Equinix data centres (who also provides infrastructure and technical backup). This policy facilitates rapid repair/recovery in the event of system failure. Replacement would take place using either on-site spare components or JIT delivery of necessary parts. All work would be carried out by qualified service engineers and all work would be carried out under strict supervision of trained PAS Ltd personnel. Standard platforms minimise the number of spare parts required, with parts experiencing the highest failure rate being kept on site.

   In the event of a total Server failure, replacement would take place using a standby standard server. If necessary, data would be restored from backup storage. The required software will be loaded onto the standby server by PAS Ltd personnel.

   WAN link loss/fault – The main office and the hosting facilities have multiple inbound/outbound connection to the internet, meaning that a single failure is covered by redundancy. In the event of a total loss of connectivity at the main office, operations would be moved to another location (or employee's homes).

   Power failure at Data Centre/Main Office – Loss of power to the main office would invoke the need to relocate operations to another site (or employee's homes). The hosting centre is based at Reynolds House and/or Turing House, which are sister buildings located on the Manchester Technopark on the periphery of Manchester City Centre. These two buildings comprise their primary hosting facilities, and both ioMart and Equinix have long-term leases on these spaces, and have fitted out the hosting space to their own specifications. ioMart and Equinix are in complete control and are not resellers of another company's data centre space.

   Data corruption – In the event of data corruption caused by a system failure, the data would be restored from backup storage. These are both stored locally on-site and off-site for added redundancy.

Firewall failure/fault – The firewalls used are 'High Availability Pairs'. This allows the automatic switch-over from one device to the stand-by unit with no service loss in the event of failure.

Telecommunication failure – The telephone equipment in use at the PAS Ltd offices is covered by a fully managed VoIP telephony provider and covered under a complete SLA for any hardware failures or problems. The VoIP based service allows calls and 'extensions' to be remapped to other offices or employee's homes should that be deemed appropriate.

Summary - There is a reasonable risk of this instance occurring, with all systems being based around technology, critical failures can occur. This is covered in nearly every case by having redundant systems in place to allow continuity of work. Risk avoidance measures that ensure equipment is well maintained would reduce risk considerably.

3. **Loss of utilities eg water, gas or electricity or fire** – Loss of water and gas are unlikely, and would also have a minimal effect on business; however loss of electricity supply would be a problem. If this was over an extended period (more than 24hrs) it would mean we would need to relocate operations to other offices or locations. There is not much we can do to reduce this risk.

   Other strategies to manage these incidents are:

   - Back-up discs of code and data (where appropriate) are kept initially in a fireproof safe away from the server location and the daily back-up are transferred to an off-site facility
   - All records kept in locked cupboards
   - Staff on site trained in fire prevention and security implementation
   - Testing and timed building evacuation procedures
   - Smoke detectors in place
   - Detailed company policy on Health and Safety
   - All electrical equipment tested once a year to minimise electrical faults

4. **Loss of, or access to, premises** – This would generate short term inconvenience to customers but all facilities necessary are internet based and flexible in their delivery capabilities. It would be hard to reduce the risk level. PAS Ltd's premises have secure locks; all keys are allocated and documented only to PAS Ltd staff. The Manchester Science Park has CCTV running 24hrs per day, and on-site security staff.

5. **Disruption to transport** – Again this would generate few problems for PAS Ltd, a large percentage of the staff live locally to the office and can walk in if necessary.

Business Continuity Management

This stage of the BCM process is concerned with the development and implementation of appropriate plans and arrangements to ensure the management of an incident and continuity and recovery of critical activities that support PAS Ltd's key products and services. As a very small organisation, this is a single plan which incorporates all the above elements. There are 4 key areas to the plan:

1. **Purpose and scope** – The aim is to get as many functional services back up and running within the 24-48hr period as possible. The key services to be resumed are customer support and hosting provisions, followed by development and ancillary services.

2. **Document owner and maintainer** – The owner of the process and the person with responsibility for maintaining the plans is Graham Whitehouse. The plan will be regularly reviewed and tested.

3. **Roles and responsibilities** – There are three key people with roles and responsibilities in this plan, being Matthew Beech, Graham Whitehouse and Andrew Jones. In the event of a disaster/incident within either PAS Ltd or the hosted operational area the contacts listed below should be informed. Telephone contact should be made, supported by an email giving detailed explanation of the disaster/incident.

   a. **PAS Ltd Primary contact:**

Name:	Graham		Whitehouse
Phone:	0161	232	5475
Mobile:	07766		308983
email:	graham.whitehouse@p11dorganiser.co.uk		

   b. **PAS Ltd Secondary contact:**

Name:	Andrew		Jones
Phone:	0161	232	5478
Mobile:	07432		088769
email:	andrew.jones@p11dorganiser.co.uk		

   c. **PAS Ltd Escalation contact:**

Name:	Matthew		Beech
Phone:	0161	232	5470
Mobile:	07973		729469
email:	matthew.beech@p11dorganiser.co.uk		

   It is the responsibility of all those above to ensure that each person listed is made aware of the disaster event. It is then the responsibility of the primary and secondary contacts within the business to ensure that the disaster recovery procedures detailed in this document are instigated (in a timely manner after the appropriate consultation). Any third party suppliers would be contacted by the primary or secondary contacts at PAS Ltd.

   The escalation contact will be kept informed about incidents and will be available should any issues arise that are not covered in this plan.

4. **Plan invocation** – The BCM can only be invoked by agreement of at least two of the individuals named in section 3 (above). Once the plan is invoked, a 'call tree' is implemented to ensure all individuals (and partners and suppliers) are notified as appropriate.

Exercising BCM arrangements

A BCM plan cannot be considered reliable until it is exercised and has proved to be workable. Exercising will involve:

- Validating plans
- Rehearsing key staff
- Testing systems which are relied upon to deliver resilience

PAS Ltd would aim to ensure this plan is exercised annually. Not all aspects of the plan can be tested without business disruption, but crucial elements can, such as the contact list and the activation process. We would anticipate being able to test back-up power, communications equipment and information management arrangements regularly.

PAS Ltd would have Live exercises where a necessity for components (such as evacuation) that cannot be tested effectively in any other way.

After any test we will record and evaluate the event, through a debriefing immediately after the exercise and that will be written up in a 'lessons learned' report with actions if required.

Maintaining BCM arrangements

A maintenance programme will be put in place that ensures these plans are updated:

- If there are any changes to any part of the organisation, including restructurings, changed methods of the delivery of your critical activities
- If there is a change to the external environment in which the organisation operates
- Following lessons learned from an incident or exercise
- Changes to staff

Reviewing BCM arrangements

We plan to review the BCM arrangements through a self-assessment process at a regular interval. This review will be documented and will verify that:

- All key products and services and their critical activities and supporting resources have been identified
- Arrangements accurately reflect your organisation's objectives; arrangements are fit for purpose, and appropriate to the level of risk your organisation faces
- BCM maintenance and exercising programmes have been effectively implemented
- BCM arrangements incorporate improvements identified during incidents and exercises and in the maintenance programme
- An effective programme for training and awareness raising is in place;

- Change control procedures are in place and working effectively

BCM Log

The following table is to be completed after tests are completed.

Reason/Incident	Style	Date	Outcome
Annual Test	Full	03/04/2014	Pass
Annual Test	Full	02/03/2015	Pass
Power Outage	Partial	15/09/2015	Pass
Annual Test	Partial	12/05/2015	Pass
Phone	Partial	17/08/2015	Pass
Annual Test	Full	28/01/2016	Pass
Annual Test	Full	28/01/2017	Pass
Annual Test	Partial	20/04/2018	Pass
Annual Test	Full	25/09/2018	Pass
Power Outage	Partial	14/11/2018	Pass
Annual Test	Full	03/09/2019	Pass
Annual Test	Full	16/03/2020	Pass
Power Outage	Partial	18/12/2020	Pass