Build your tailored business continuity plan

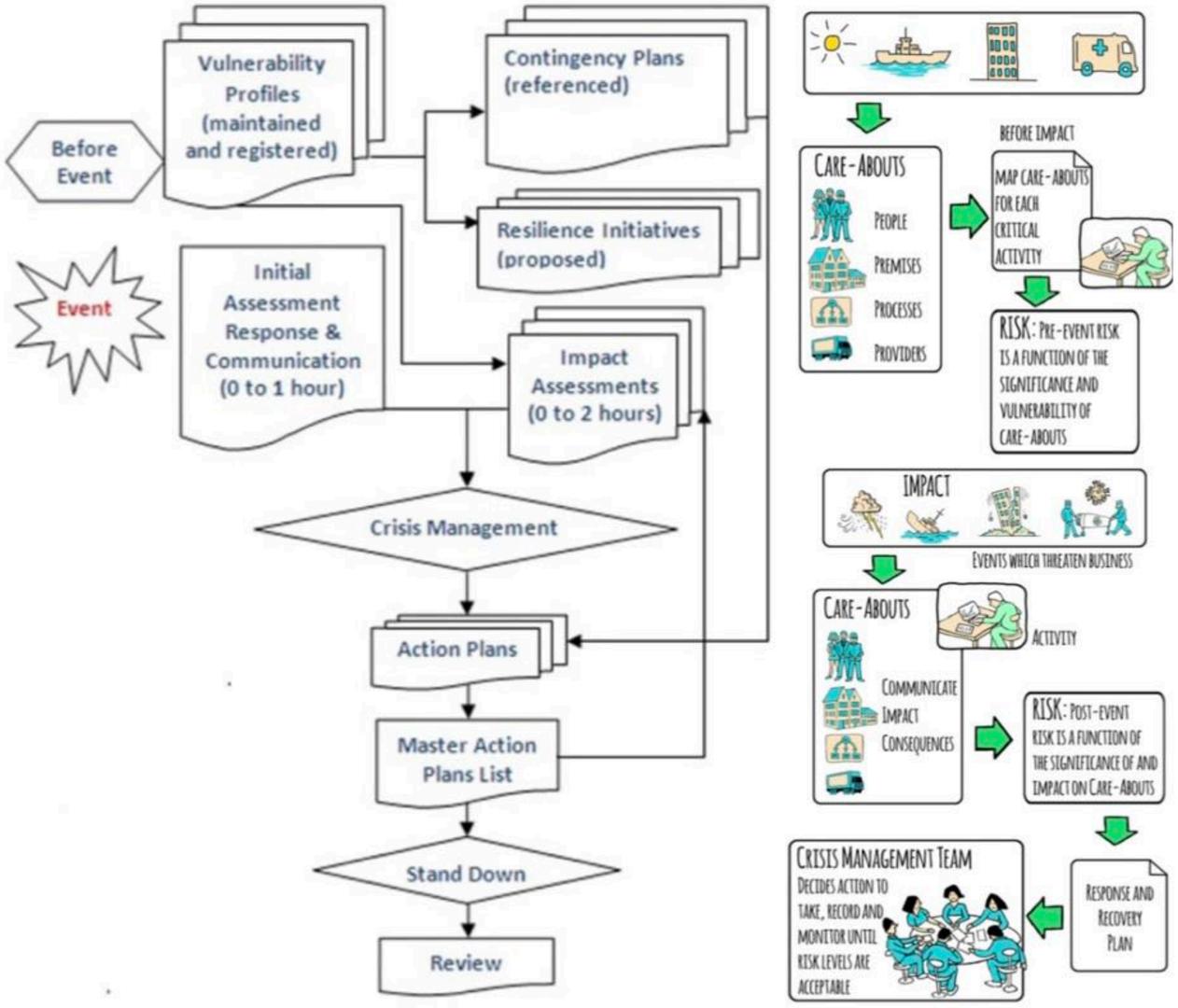


Table of Contents

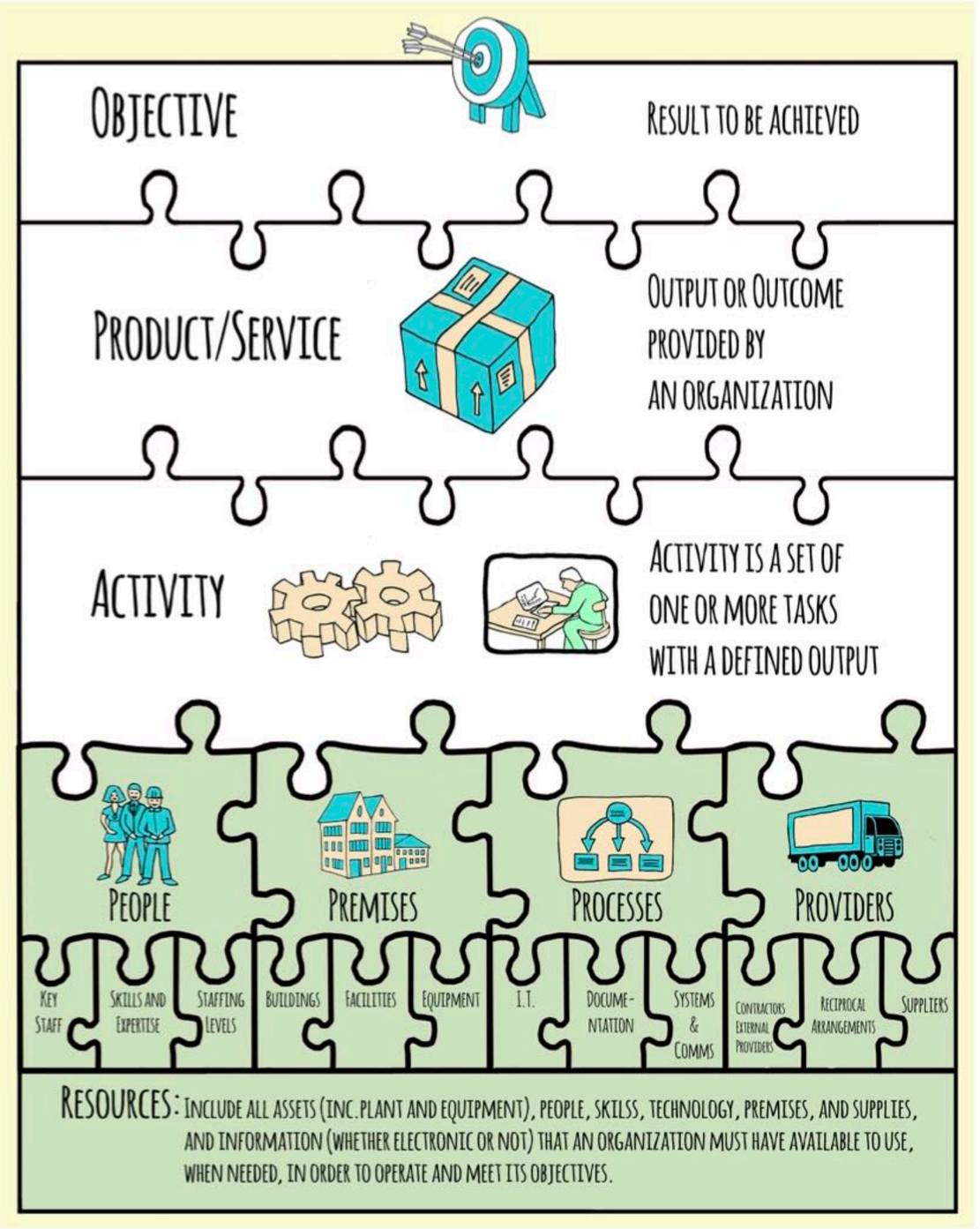
Build your tailored business continuity plan

Basic - we develop a Business Continuity Crisis Management Plan aligned with best practice (as a text document) tailored to reflect your operability needs.

Standard - Basic Plan plus an attachment using this three-tiered structure which can then be used by you to populate AgileBCP SaaS or our FlyingFish Business Continuity app.

- Your PRODUCTS AND SERVICES (Text) - significant to your context.
- Your PRIORITISED ACTIVITIES (Text) - the things you need to keep doing (in order to provide your key products/services).
- Your MUST-HAVES (Text) - the categories we suggest are People, Premises, Processes, and Providers. Please provide descriptions of the things you need in order to support the critical activities you need to keep doing (to provide key products/services).

Premium - using Standard we will build and host (on both the Apple & Google Stores) your dedicated app populated with the three tiers of information from Standard



This risk based plan uses Business Impact Analysis (BIA) - developed from scenarios or Damage Assessments. This provides a sound basis to inform crucial decisions by the Crisis Management Team.

Maximum Acceptable Outage

Maximum Acceptable Outage time is the maximum time a service can be out of commission before the effect imposes risks or outcomes which are unacceptable - as agreed by senior management. **This plan focuses on Key Business Processes with a Maximum Acceptable Outage of <INSERT>**

The achievement of an "acceptable level of functioning" for any Key Business Process should be advised to the Crisis Management Team by the person responsible for that Key Business Process by updating their Impact Status (using images and words to inform the impact score displayed in the FlyingFish app).

Recovery Time Objective

The Recovery Time Objective (RTO) is the planned time, or target, to restore an acceptable level of service delivery. The RTO will be estimated in Action Planning by the Crisis Management Team and form the basis of determining priority actions. These actions will be tracked on the Master Action Plan summarising who needs to do what, and what they need to do it. This plan will also reflect whether it is on time, on budget, and on track.

Note: The RTO should be less than the Maximum Acceptable Outage otherwise restrictions to service levels will apply and those restrictions will therefore need to be managed (communicated to customers). Recovery Time Objectives may also be advised by contract clauses.

Activation

This plan shall be activated by any available member of the Crisis Management Team in the event of any event that in their judgement potentially interrupts ongoing service delivery in a way that puts the organisation at risk. They "declare an event" and "invoke the Business Continuity arrangements".

Upon activation of this plan the Crisis Management Team shall be formed.

- **Crisis Management Team (responsible for decision making);**

The Crisis Management Team shall, in the first instance, be made up from any of the available following people: **<INSERT>**

Key Products / Services in priority order.

Key Products / Services (Described at a High Level and Listed in Priority Order)	*Critical Activities underpinning each Key Product / Service /*

ADD LINES TO THE TABLE ABOVE TO ENSURE COVERAGE OF YOUR BUSINESS

Using the questions below - to prompt thinking – undertake a concise Business Impact Analysis, filling in answers, **for each CRITICAL ACTIVITY**, to the following questions on the blank BIA Sheet (page 9) under the relevant headings

PEOPLE	**Key Staff:** What staff do you require to carry out this Key "must deliver" Product / Service?	**Skills / Expertise / Training:** What skills / level of expertise is required to undertake this Key "must deliver" Product / Service?	**Minimum Staffing Levels:** What is the minimum staffing level with which you could provide some sort of service?
PREMISES	**Buildings:** What locations does this Key "must deliver" Product / Service operate from? (Primary site, alternative premises)	**Facilities:** What facilities are essential to carry out this Key "must deliver" Product / Service? Do you need these to be located at a specific site?	**Equipment / Other Resources:** What equipment / other resources are required to carry out your Key "must deliver" Product / Service?
PROCESSES	**IT:** What IT is essential to carry out this Key "must deliver" Product / Service?	**Documentation:** What documentation / records are essential to carry out your Key "must deliver" Product / Service, and how are these stored?	**Systems & Communications** What systems and means of communication are required to carry out your Key "must deliver" Product / Service?
PROVIDERS	**Reciprocal Arrangements:** Do you have any reciprocal agreements with other organisations?	**Contractors / External Providers:** Do you tender key services out to another organisation? If so - to whom and for what?	**Suppliers:** Who are your priority suppliers and who do you depend on to undertake your Key "must deliver" Product / Service?
PROFILE	**Customers and Reputation:** Who are your key stakeholders?	**Legal Considerations:** What are your legal, statutory and regulatory requirements?	**Vulnerable Groups:** Which vulnerable groups might be affected if your organisation fails to carry out this Key "must deliver" Product / Service?

SHEET: BIA PRO - FORMA to be completed for each CRITICAL ACTIVITY

USE ONE SHEET FOR EACH CRITICAL ACTIVITY

Insert name of Critical Activity here - then list resources required in table below

PEOPLE	*PREMISES*	*PROCESSES*	*PROVIDERS*	*PROFILE*
Key Staff:	**Buildings:**	**IT:**	**Reciprocal Arrangements:**	**Reputation:**
Skills / Expertise / Training:	**Facilities:**	**Documentation:**	**Contractors / External Providers:**	**Legal Considerations:**
Minimum Staffing Levels:	**Equipment / Resources:**	**Systems & Communications**	**Suppliers:**	**Vulnerable Groups:**

CONSIDERATIONS FOR INCREASING YOUR RESILIENCE (BEFORE AN EVENT)

Key Staff: Can staff be contacted out of hours? Could extra capacity be built into your staffing to assist you in coping during an incident?	**Buildings:** Could you operate from more than one premise? Could you relocate operations in the event of a premise being lost or if access to the premise was denied?	**IT:** Is data backed-up and are back-ups kept off site? Do you have any disaster recovery arrangements in place?	**Reciprocal Arrangements:** Do you have agreements with other organizations regarding staffing, use of facilities in the event of an incident?	**Reputational Damage:** How could reputational damage be reduced? How could you provide information to staff and stakeholders in an emergency (e.g. press release)?
Skills / Expertise / Training: Could staff be trained in other roles? Could other members of staff undertake other non-specialist roles, in the event of an incident?	**Facilities:** Are any of your facilities multi-purpose? Are alternative facilities available in the event of an incident?	**Documentation:** Is essential documentation stored securely (e.g. fire proof safe, backed-up)? Do you keep copies of essential documentation elsewhere?	**Contractors / External Providers:** Do you know of alternative contractors or are you reliant on a single contractor? Do your contractors have validated (exercised) contingency plans in place?	**Legal Considerations:** Do you have systems to log decisions; actions; and costs, in the event of an incident?
Minimum Staffing Levels: What is the minimal staffing level to continue to deliver your key functions at an acceptable level? What measures could be taken to minimize impacts of staff shortfalls?	**Equipment / Resources:** Could alternative equipment / resources be acquired in the event of an incident / disruption? Could key equipment be replicated or do manual procedures exist?	**Systems & Communications** Are your systems flexible? Do you have alternative systems in place (manual processes)? What alternative means of communication exist?	**Suppliers:** Do you know of suitable alternative suppliers? Could key suppliers be contacted in an emergency?	**Vulnerable Groups:** How could vulnerable groups be contacted / accommodated in the event of an incident?