

Jaleinius Risk Management



CYCLES

A UNDERTAKE PLAN

Commit to the project or it will falter

B DETERMINE POSITION

Risk tolerance is vital to setting measures

C ASSESS RISKS

Know what you face and where it might come from

D CREATE PLAN

Keep it simple and flexible

E IMPLEMENT PLAN

Prepare for changes and seek their value

F TRAIN STAFF

The most valuable asset of any organisation so make sure they are in the know

G REHEARSE PLAN

Make sure one and all are ready so if an incident happens, you will be ready

H REVIEW PLAN

Staff and situations will change so make sure the plan is up to date

The simple way to plan

Jaleinius Genius

A guide to

Business Continuity Planning

Every organisation should have a Business Continuity Plan (BCP).

Some strong reasons:

- One in five companies will suffer a major disaster in the next five years
- 80% of companies affected by a major incident will close within 18 months
- A biological chemical or nuclear attack on the West by Al Qaida is inevitable. It's just a case of when and where. (Eliza Manningham Buller - Director General of Security Service)
- Less than 40% of businesses with fewer than 50 employees have a plan in place
- In 2005, 38% of companies reported loss of IT; 29% loss of people and 24% loss of telecommunications
- Over 20% of the capital's firms do not have sufficient cash reserves to see them through an avian 'flu epidemic

And the top ten reasons they fail:

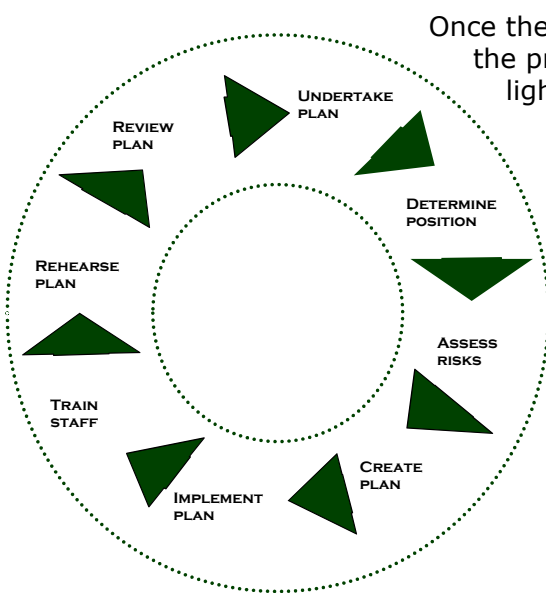
1. It's not my job.
 2. They are simple to do and we will pencil them in for next month
 3. That is an area of management I don't know
 4. It's your job to develop such plans. Let me know when you are finished
 5. I have far too much on my plate
 6. Use this software - let me know when you are finished
 7. Those sort of things don't happen very often and they won't happen to us
 8. We are prepared to deal with this already
 9. The CIO told us to prepare this
 10. An internal audit told us to do it
- (Source: Computing Canada, Feb 28, 2003)

The Jaleinius Genius is a simple to use tool that will guide you through the process of writing and implementing a Business Continuity Plan. By following the clear instructions and guidelines, the result will be a living document that can be used in times of emergency.

Consider the following:

- Can you quickly and simply provide IT and personnel logistics reporting?
- Do you have fast and fail-safe telephone switching?
- Can you generate reports quickly for the emergency services?
- Is your data backup system 'Free from Human Error?'
- Can you cope with losing 'Live Hard-Copy Documents'?

There are eight cycles to a successful plan:



Once the final cycle is reached, it is important to go through the process constantly in order to maintain the plan in the light of the latest developments and information.

The Jaleinius Genius will guide your organisation through the process to mitigate the risks and safeguard your reputation, your business and your shareholders.

You will also receive the Jaleinius Newsletter for twelve months, a monthly update on continuity news and systems. As the majority of continuity planning is based on experience, it is expected that the Jaleinius Genius will be updated and you will be eligible for these updates for a year.

Limitation of Liability

To the maximum extent permitted by applicable law, in no event shall Jaleinius Risk Management or its suppliers be liable for any special, incidental, indirect, or consequential damages whatsoever (including, without limitation, damages for loss of business profits, business interruption loss of business information or any other pecuniary loss) arising out of the use of or inability to use the 'Jaleinius Genius', even if Jaleinius Risk Management has been advised of the possibility of such damages. In any event, Jaleinius Risk Management sole and entire liability under any provision the End User Legal Agreement (EULA) shall be limited to the greater of the amount actually paid by you for the 'Jaleinius Genius'.

Contents

SUBJECT	PAGE
Undertake plan	4
Determine position	6
Assess risks	8
Create plan	13
Implement plan	27
Train staff	29
Rehearse plan	31
Review plan	33
Conclusion	34
Appendices	35
I - Glossary of Terms II - Threats III - Emergency Services IV - Principles of Continuity Planning V - Planning Check List VI - Templates of All Forms	

Phase A

Undertake plan

To implement a BCP is just like any business decision – is it worth it and what will it cost to do?

Look at a simple business case:

Reasons:

The threat to modern businesses have widened considerably over the past five years and now all commercial entities that operate in the West could be affected by incidents, either significant like the London bombings or more common, the loss of valuable resources, such as IT. The usual drivers for continuity planning are:

- Corporate governance
- Existing customers
- Legislation
- Central government
- Insurers
- Auditors
- Regulators
- Potential customers
- Investors suppliers
- Experience with an event or disruption

Options:

A BCP can be done using a consultant or in-house. It is unlikely that a senior employee would be fully conversant with options and therefore might make what may seem like measured decisions but which turn out to be thin on effect. Therefore it is always wise to get advice, in this case, using the Jaleinius Genius.

Expected Benefits:

The security of knowing what to do if the unforeseen happens

An improved reputation

The ability to outbid competition on important contracts

Risks:

There are always going to be opportunity costs to taking on any project. If this process is undertaken, there is also the prospect of impeding the normal business practice. Many organisations can see the benefits of a BCP but weigh up the potential impact on their operations and decide to act as if with their fingers crossed.

Appendix VI - Templates of All Forms

Included are all the forms listed in the Jaleinius Genius in the following order:

Form	Page
Tolerance	54
Impact	55
Business Continuity Team	56
Personnel	57
Visitors	58
Contractors	59
Off site Personnel	60
IT Hardware	61
IT Software	62
IT Support	63
IT Alternative Suppliers	64
Insurance Cover	65
Responses	66
Grab Bag Check List	67
Incident Log	68
PR Officer Check List	69
Post Incident Check List	70