Information Governance (CIS3005-N)

Week 11

Business Continuity and Disaster Recovery Planning

School of **Computing, Engineering & Digital Technologies**

tees.ac.uk/computing

Lecture Aims

- Consider how business continuity and disaster recovery planning link with risk management, and how they relate to one another
  - What are business continuity and disaster recovery planning?
  - Why are they important?
  - How do we do it?
  - How does they link with our assessment?

Business Continuity Planning

- Some experts describe needing a BCP (Business Continuity Plan) or BCMS (Business Continuity Management System) where there is a “Business Emergency” or “Disruptive Incident”.

- Examples describing the types of emergency or incident:
  - https://invenioit.com/continuity/4-real-life-business-continuity-examples/
    - Ransomware, virus, fire, loss of internet, hurricane etc.

- In your ICA: what types of emergency or incident have the capacity to disrupt normal business operations?

Business Continuity Planning

- Thinking back to Covid-19 lockdown, what measures do you think Teesside University (and other educational institutions) put into place to ensure business continuity?
- How prepared do you think the organisations were?
- How different might a risk assessment look today, compared to 2020?

- The NHS Wannacry ransomware attack in 2017 cost the organisation an estimated £92m. Can we measure the human cost?

What is a Business Continuity Plan?

- The examples below include an outline of critical business functions, recovery processes, stakeholder information, and helpful emergency response checklists.

- Business Continuity Plan Templates and Toolkits
  - UK Government Business Continuity Management Toolkit
  - NHS Business Continuity Toolkit

Disaster Recovery Planning

- A Disaster Recovery Plan forms ***part of*** a Business Continuity Plan – a disaster has potential to disrupt business continuity
- Some organisations describe it as a **formal document** that provides detailed instructions to follow in the event of an **unplanned incident**, to **minimise impact** and help ensure **business continuity**

- **ITIL v4** defines a disaster as: "A sudden unplanned event that causes great damage or serious loss to an organization. A disaster results in an organization failing to provide critical business functions for some predetermined minimum period of time."
- How will you ensure that only **true disasters** are handled by your Disaster Recovery Process (ICA Part 3)?

Why is it important?

- To preserve reputation
- Ensure continuity of services offered
- To ensure organisational resilience (being able to return to normal working practices after an incident)
- To reduce the time taken to return to normal working practices
- To reduce cost
- To improve the capability of a business to identify and respond to threats
- To improve redundancy within system(s)

Hojat Rezaei Soufi, S. Ali Torabi & Navid Sahebjamnia (2019)

Examples of Business Continuity gone wrong

- Ten business continuity disasters that cost the UK billions (including serious storm damage and unforeseen closure of the Forth Road Bridge):
  - https://www.information-age.com/ten-biggest-business-continuity-disasters-cost-uk-businesses-billions-123461455/

- Crisis Communications –Communication should be considered and included in Part 3 (Poster)

Reviewing a BCP

- Every 6 months or year
- If major changes occur within the organisation
  - Location/venue change
  - Major expansion/contraction
  - Change in significant contracts (suppliers etc.)
  - Corporate changes such as a takeover
  - Regulatory changes (e.g. GDPR)
  - Lessons learned (e.g. Grenfell Disaster)

Applying it to your ICA

- You do NOT need to create a BCP!
- You can simply refer to it as though it exists (like you will with other named documentation in the scenario)
- You may/will need to revisit ICA task 1 (Risk Assessment Analysis) to include detail relating to a BCP
- Refer to a professional body such as The Business Continuity Institute (BCI)
- Identify a known approach, and reference it
- A major part of Disaster Recovery is likely to be ‘backup and restore’, and ensuring all formal documentation is in place

Applying it to your ICA

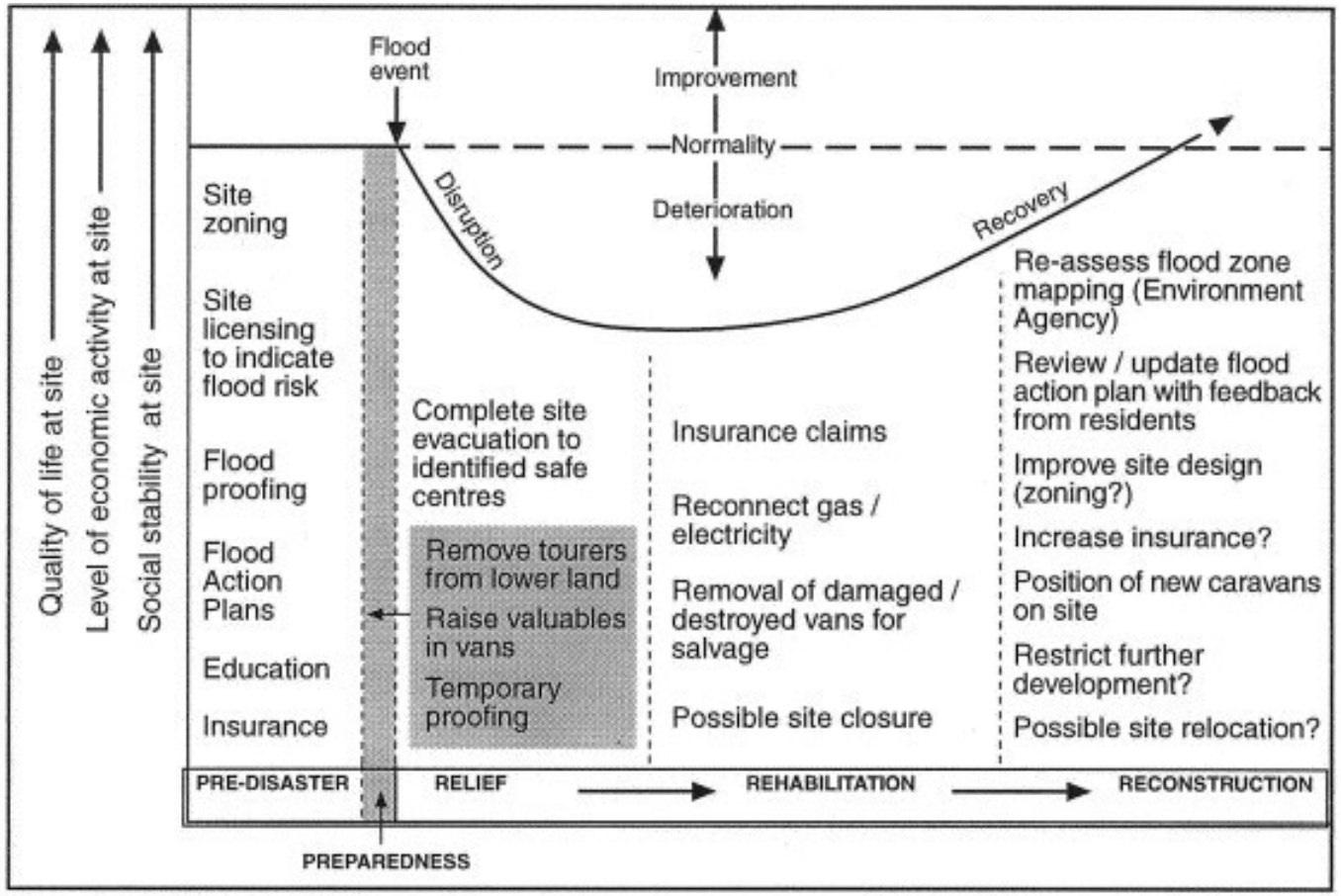
- In **Part 1** (Risk assessment): BCP will form part of your mitigation, linked to specific risks. Is there indication that the company have a BCP?
- In **Part 2** (Issues and Controls): BCP could be incorporated into your controls
- In **Part 3** (Disaster Recovery Poster): BCP could be a step “Refer to BCP”
- In **Part 4** (Reflection): e.g. you could consider whether you considered a BCP in enough detail etc.

Further Reading

- Info Entrepreneurs: Crisis Management and Business Continuity Planning - a useful site in plain English
  - https://www.infoentrepreneurs.org/en/guides/crisis-management-and-business-continuity-planning/#2

Further Reading

- Improving disaster recovery planning processes over time:
  - https://www.cutover.com/blog/how-mature-it-disaster-recovery-testing-process
- Check out various sources online for Disaster Response Curves (e.g. Park's Model) – typically used in natural disaster situations



References

- Continuity Central, https://continuitycentral.com/, (accessed on 25/04/24).
- Soufi, H. J.,Torabi, S.A., Sahebjamnia, N., (2019), *Developing a novel quantitative framework for business continuity planning*, International Journal of Production Research, 57:3, pp. 779-800.
- The Business Continuity Institute, https://www.thebci.org/, (accessed on 25/04/24).