The 20 Critical Questions Series

What Directors should ask about Business Continuity

Updated 2022

Business Continuity – The overarching arrangements to be enacted when a business disruption, disaster situation or crisis has a major impact on business operations that flows to service delivery. It is the process an organisation puts in place so essential activities can continue during and after an unforeseen event or disaster situation. Business continuity planning seeks to prevent interruption to critical services and re-establish operations as quickly and smoothly as possible.

Business Continuity

1. Has the organisation formally assessed risk of potential business disruptions, disaster situations or crises? Does this include a range of potential disruptions and disasters including disease pandemic?
2. Are business continuity management arrangements sufficiently dynamic and do they include scenario analysis at three levels – (a) optimistic 'best case scenario' (b) expected 'likely scenario' (c) pessimistic 'worst case scenario'? Are variables factored into the scenario analysis such as (i) time elapsed before normal operations can resume (ii) economic markers covering severity of the event (iii) workforce health, wellbeing, readiness and connectability (iv) commercial arrangements?
3. Has business impact been assessed should a business disruption, disaster or crisis situation occur? Does it include formal business impact analysis? Does it (a) establish maximum tolerable disruption limits (b) consider certainty of the supply chain (c) consider capacity management including ICT bandwidth?
4. Does the organisation have a business continuity plan independent of the emergency response plan and the ICT disaster recovery plan? Does the business continuity plan span multiple horizons in the event of a serious national or global crisis including (a) initial emergency management response – care, maintenance, survival (b) standing down and ultimately re-establishing business-as-usual (c) adapting to the new normal?
5. Do business continuity management arrangements cover all major risk areas such as (a) people – safety, wellbeing, availability, capability, remote support (b) customer experience (c) supply chain (d) operations (e) financial stewardship including cashflow and solvency (f) communications (g) continuity of critical control arrangements (h) cyber risk management?
6. Is there a specified person or group responsible for business continuity and crisis management, with measurable performance measures in place to continually assess their performance against critical success factors? Is a business continuity annual report prepared for senior management and the audit committee to tell the business continuity story for the year, including results of periodic testing and an assertion on overall preparedness?
7. Does the organisation have a specified crisis management team and defined trigger points that will escalate an incident for the team to stand up? Is there a stepped escalation process to manage an unforeseen event or disaster situation that gets progressively worse or takes a long time to fix?
8. Does the organisation have a designated crisis centre where the crisis management team will meet if organisation facilities are damaged, destroyed or unavailable? Are there alternative sites if required?
9. Are there designated recovery teams for the various parts of the organisation? Do recovery teams maintain crisis kits of important information and resources? Do storage arrangements mean these will be available should a disaster mean the primary site cannot be accessed? Will these be available if the organisation's ICT environment and systems are unavailable?
10. Is there an up-to-date contact list of key management, employees, suppliers and stakeholders? Does it include contractual requirements of suppliers that specify agreed call-out response times and effort?

What Directors should ask about Business Continuity

11. Is there a fit-for-purpose media plan to deal with the media following an unforeseen event, crisis or disaster situation?
12. Is there a formal schedule of business continuity testing and is this actually carried out? Does this include a range of activities from desktop testing through to realistic crisis scenario testing?
13. Are post-test reports written, disseminated throughout the organisation to relevant management and provided to the audit committee?
14. Are improvement actions from business continuity tests recorded, remediated by management in a timely way, and actively followed-up to ensure the actions are properly implemented?

ICT Disaster Recovery

15. Does the organisation have an ICT disaster recovery plan to support the business continuity plan? Does this include a priority list for restoration of the inventory of ICT services following an unforeseen event that disrupts ICT? Is the priority list based on formal business impact analysis?
16. Has the RTO been defined? (recovery time objective – the maximum tolerable duration of time within which a business process must be restored after an ICT disruption in order to avoid unacceptable consequences associated with a break in service continuity).
17. Has the RPO been defined? (recovery point objective – the maximum tolerable amount of data that must be recovered from backup storage for normal operations to resume following an ICT incident).
18. Is there a formal schedule of ICT disaster recovery testing? Has the testing been carried out as scheduled? Does this include a range of activities such as desktop testing, configuration testing, platform testing, multi-platform testing, service testing and realistic crisis scenario testing? Are ICT maintenance activities and ICT disaster recovery activities kept separate as they should be (not counted as tests)? Does the organisation count real-life ICT incidents and disaster occurrences as testing which they should not?
19. Are post-test reports written, disseminated throughout the organisation to relevant management, and provided to the audit committee? Are improvement actions from ICT disaster recovery tests recorded, remediated by management in a timely way, and actively followed-up to ensure the actions are properly implemented?

Review and Audit

20. Are regular reviews and audits of business continuity and ICT disaster recovery arrangements and testing performed and reported to senior management and the audit committee?

The Big Question

Does the organisation clearly know how its business continuity activities fit together, how effective they are, whether they are likely to be successful if a need arises to stand them up, and whether the customer experience sits at the heart of decision-making?