Business continuity scenario exercises - prepared, planned and ready

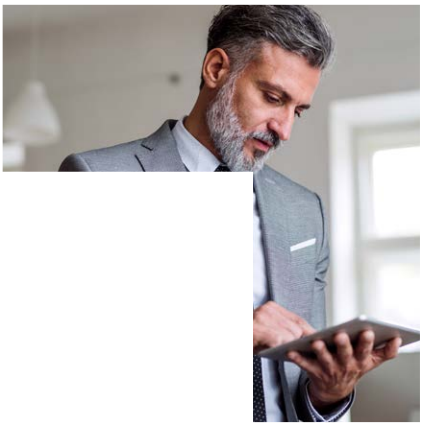
Business continuity scenario exercises can protect your business against disaster and disruption, helping prevent business failure and loss of revenue.

According to ISO 22301, business continuity procedures must be exercised and tested regularly to ensure they are suitable, updated, and consistent with business continuity objectives. In our experience, if you fail to practice and test your plans regularly, then they are likely to fail and what could have been a business continuity issue quickly becomes disaster recovery.

All our exercises and testing methods are aligned to the Business Continuity Management System (BCMS) scope, objectives of your Business. All agreed disaster scenarios that are likely to occur or that will be most damaging to your business are considered. We are experienced in accurately recording exercises and testing data, which allows us to analyse the execution of planned actions and interactions between parties. We then critically evaluate the recorded data to determine if all actions taken were appropriate and in line with the BCMS objectives. The output from our analysis feeds into a lessons learned session for continual improvement, allowing for the correction of vulnerabilities or implementation of improvements.

Why you need to take action

Disruption to business can result in a risk of data loss, loss of revenue, and failure to deliver services. Successful businesses expect the unexpected and plan for it. Knowing how to respond to an incident cannot be deferred until the business is actually impacted by a crisis. Organisations need to be well prepared with practiced cyber media responses. A forward-looking, systematic approach to incident management and response will create structures, train people to work within set regimes and evaluate the approaches being developed in a continuous, purposeful and rigorous manner.



Benefits

- Measure the effectiveness of your security provision by planning and facilitating scenario exercises through various testing methods.
- Upskill your workforce through education, awareness and training of scenario exercises for all members of staff.
- Provide an opportunity for outputs of the scenario exercise to be considered for validation and/or inclusion in your crisis management guidance and share and discuss best practice responses across stakeholders.
- Improve awareness of potential cyber security incidents which may impact the ability to operate ‘business as usual’.

It is imperative you know how to recover from the following potential disruptions:

- Pandemic outbreaks – resulting in a reduced workforce, increased demand on IT infrastructure to facilitate remote working and strong government restrictions on business operations.
- Lockout – physical access to a building or site is denied.
- Loss of computers or equipment – damage or loss of devices used to conduct business.
- Loss of voice, data and/or network services – total or partial loss of communications services.
- Corruption of data – deliberate or accidental loss of access to data due to third party, general user, outsider or admin activity.
- Loss of staff – key personnel who have significant roles within the business, or teams of staff whose loss impacts business operations.
- Loss of critical business partners – issues that are out of your business' control but could have a serious impact on your business.

Organisations that have a BCMS in place are much more likely to reduce the impact of these situations.

Our approach

We understand the effectiveness of testing BCMS using various approaches. Some of our testing methods include:

- Advertising campaigns – raising awareness of business continuity plans to all staff members, suppliers and key persons.
- Auditing – reviewing business continuity plans by various auditing, validation, and verification techniques.
- Tabletop exercise – discussing the theoretical execution of business continuity plans and the actions personnel must take in a dedicated workshop.
- Functional testing – conducting a planned and announced exercise that tests all interrelated plans for specific activities with real resources.
- Full testing – executing an announced or unannounced disaster.

We work with you to develop appropriate, suitable and realistic scenarios allowing staff to discuss and practice how they might respond. Our pre-designed materials and artefacts simulate real news items, which add realism to the exercise and create a realistic workshop that enables staff to rehearse their roles in a safe and controlled environment.

We also have an interactive cyber scenario simulation presentation which can be a useful introduction at cyber security conferences, events and/or meetings where delegates use their mobile phones or laptops to register, participate and vote on how they would respond to the scenario as the situation unfolds. This provides a useful platform for discussion and enables delegates to debate the situation and how they might respond, without the boundaries and time limits of a formal exercise.

About CGI

Insights you can act on

Founded in 1976, CGI is among the largest IT and business consulting services firms in the world.

We are insights-driven and outcomes-based to help accelerate returns on your investments. Across 21 industry sectors in 400 locations worldwide, our 77,000 professionals provide comprehensive, scalable and sustainable IT and business consulting services that are informed globally and delivered locally.

For more information

Visit cgi.com/uk/cyber-security
Email us at cyber.enquiry.uk@cgi.com