What is Business Continuity?

Business Continuity enables an organisation to keep operating in the event of a disruption to its operations. It limits the impact of a disruptive event, and enables the organisation to survive.

It is implemented through a process known as Business Continuity Management (BCM), which delivers a framework for building resilience to disruptive events. It provides the capability for an effective response to events that might threaten the organisation, and aims to ensure that disrupted operations are resumed or recovered to pre-planned levels of service within agreed timescales.

Business Continuity is an important element of organisational resilience, which is the ability of an organization to anticipate, prepare for, and respond and adapt to incremental change and sudden disruptions in order to survive and prosper. It is both related to and overlaps other management disciplines aimed at making an organisation more resilient:

- **Risk Management** is the process of identifying, quantifying, and managing the risks that an organisation faces. Business Continuity reduces the impact of a risk should it materialise, and is an essential risk mitigation strategy for low probability high impact events.
- **Emergency Management** is the process of preparing for, mitigating, responding to and recovering from an emergency, both to an organisation and the wider community. Most, if not all, organisations have implemented procedures for dealing with emergencies, and these should be integrated with Business Continuity to provide a seamless response to events that have the potential to disrupt operations.
- **Crisis Management** is the process of dealing with a major event that threatens to harm the organisation and its stakeholders. It has a wider application than Business Continuity in that it also covers events that do not disrupt operations (such as those that cause only reputational damage), and is a key element of any implementation of Business Continuity.
- **Security Management** is the process of identifying an organisation's assets (including information assets), and developing, documenting, and implementing policies and procedures for protecting those assets. Business Continuity provides the policies and procedures to recover from the loss of these assets.
- **IT Disaster Recovery** is a subset of Business Continuity that covers the resumption of IT services following a disruption and the recovery IT infrastructure (hardware, software, networks, and data).
- **Crisis Communications** is the process of protecting and defending an organisation facing a public challenge to its reputation. It is an essential element of Business Continuity and should be part of any response to a disruptive event.