# FAQs on Business Continuity and IT Service Continuity

**1. What is meant by business continuity?**
Business continuity implies management processes and integrated plans which maintain the continuity of an organisation's critical processes - those processes which enable a business to deliver key services or products - in the case of a disruptive event. Business continuity encompasses all aspects of an organization which play a role in sustaining critical processes, namely: people, premises, suppliers, technologies, data.

**2. How does business continuity differ from IT service continuity?**
IT service continuity addresses the IT aspect of business continuity. In today's economy, business processes increasingly rely on information and communication technology (ICT) and electronic data (e-data). ICT systems and e-data are, therefore, crucial components of the processes and their safe and timely restoration is of paramount importance. If such systems are disrupted, an organisation's operations can grind to a halt. If the interruption is serious enough, and no risk management planning has occurred, a firm may even go out of business.

**3. What is required for IT service and business continuity?**
Ensuring business and IT continuity requires a deep understanding of the possible threats to an organisation's network and information security (NIS) and having thorough plans in place, should the risk event actually occur, in order to mitigate the impact and allow the organisation to maintain its operations or services. Business continuity is now recognised as an integral part of sound management practice and good corporate governance.

**4. Can you give an example of a disruptive event?**
A disruptive event is any occurrence which limits the ability of an organisation to function effectively. Such events might include a loss of power, an environmental disaster, (e.g. a flood, a fire), a terrorist attack or a malicious IT attack resulting in the loss of critical data.

**5. Why did ENISA write a report on this topic?**
ENISA has written this report in line with one of its key objectives to "promote risk assessment and risk management methods to enhance the capability of dealing with NIS threats." There are several existing and emerging continuity management standards. Many of them overlap, but do not necessarily share the same terminology. For example, although they sound very similar, disciplines such as emergency planning, disaster recovery, incident management and business continuity are all subtly unique. This can be very confusing for organisations which have decided or are required to implement a business continuity plan.

ENISA recognised a need to help organisations understand this complexity and therefore issued the report which aims to provide:

- an overview of the contents and structure of methods, tools and good practices;

- a “common language” (via the glossary) in the area of IT continuity management to facilitate communication among stakeholders.

**6. At whom is this report targeted?**
The report is targeted at ICT and information security professionals, and consultants, including accountants.

**7. What is the process of developing a business continuity plan?**
The organisation needs to understand three fundamental issues to maintain availability of IT and information:

- which processes are critical,
- how quickly they must be restored; and
- the IT and e-data required to keep these critical processes running.

In very simplified terms, these three steps are fundamental to the business continuity plan. As previously mentioned, there is no “one-size-fits-all” method but rather various standards, for different but closely-related disciplines, from around the world.

**8. Which approach does ENISA advocate?**

ENISA does not give priority to any one approach. Instead, the Agency evaluated a number of standards and developed a block diagramme outlining the workflow process and the distinct stages of development. Each step follows and is comprised of several activities. Some activity examples are:

1. define the business continuity management framework (e.g., define the policy and assign responsibilities),
2. conduct a business impact analysis (e.g., assess the risks and impacts),
3. design a business continuity management approach (e.g., design a recovery strategy)
4. deliver the business continuity plan (e.g., incident response plan and communications and media plan)
5. test the plan (e.g., deliver debrief report)
6. sustain the business continuity programme (e.g., train staff)

**9. Why are there so many business continuity standards?**
There are many standards which stem from different, but related, disciplines such as emergency planning, disaster recovery, incident management, risk management, IT service continuity management and business continuity management. It is very difficult to isolate each discipline related to planning for and recovering from a disruptive incident. Often one plan cannot be implemented without another. For example, in the case of an evacuation, a business continuity plan would not be effective to restore critical activities if an emergency plan had not been put into action, staff were not accounted for, the area made secure and the damage assessed. Moreover, it would be difficult to restore critical business processes without implementing an IT service continuity plan to restore technology. ENISA’s aim is therefore not to focus on a single approach. Instead the Agency provides a tool to help organisations understand how to approach the process according to the state-of-the-

art. Factors such as human resources, financial and technological limitations and regulatory constraints will shape the strategy and drive the eventual solution.

**What will ENISA's role be? What are the next steps?**
Based on the overview presented in this report ENISA will:

- *Generate an inventory of methods, tools and good practices*: unlike the work on a risk management / risk assessment inventory, this deliverable will focus on business continuity methods and tools. A first version of the inventory will be generated during 2008;
- *Perform a survey on the usage of continuity measures in e-communication*: in 2008, ENISA plans to survey e-communication providers in order to assess continuity controls and technologies used to guarantee the resilience of networks; and
- *Develop an approach to IT continuity for small- and medium-sized enterprises (SMEs)*: in the future, ENISA plans to develop a framework on business and IT continuity targeted at non-experts in SMEs.