

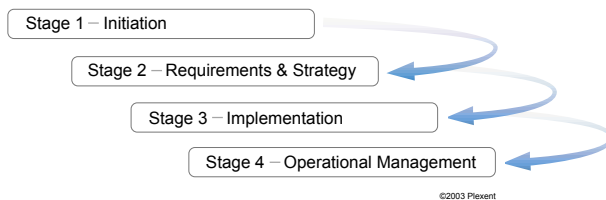
What is Continuity Management?

ITIL defines Continuity Management as:

IT Service Continuity Management (ITSCM) is a sub-set of the Business Continuity Management (BCM) process. ... [and] is concerned with managing an organisation's ability to continue to provide a pre-determined and agreed level of IT Services to support the minimum business requirements following an interruption to the business. This may range from an application or system failure, to a complete loss of the business premises.

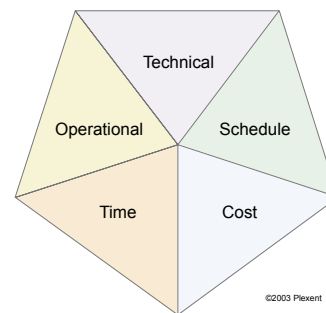
ITIL recommends and prevailing wisdom supports that any and all activities directed toward maintaining IT services must be taken within the larger context of business continuity. Although the pervasive nature of technology and our increasing dependence upon it can often cloud the issue, IT is essentially a business enabler and not an end in itself. Holding fast to this guiding principle will prevent the unnecessary expenditure of time and money when you need it most; when a situation requires that your continuity plans be invoked. To guide you through the process of evaluating your business, assessing risk, developing, implementing and maintaining the viability of an IT continuity plan, ITIL has created a four stage lifecycle.

ITIL Business Continuity Lifecycle



A recurring theme not obvious from a high-level view of the lifecycle, is the prominent role risk management and its associated tools and techniques play in Continuity Management. Risk management is a specialized activity. Therefore, between understanding that business continuity will drive how IT services are prioritized and the ability to evaluate risk in terms of cost, there lies a substantial gulf. The safest way to bridge that gulf is through the systematic use of processes such as Decision Analysis, Expected Monetary Value, and Risk Modeling. It all begins however, with an understanding of the categories of risk and how they apply to your

Categories of Risk



business. The diagram above depicts five basic categories.

Placing the components which comprise the resources, tools and techniques necessary to satisfy your business needs into these categories is the first step. Each category represents lists of items that operate as either a potential risk driver or risk indicator. For example, in the Technical category, might be software design. A critical application, because of its design, may run with full functionality on but a single, specific platform. This becomes a risk driver in that resumption of services is dependent on the availability of a dedicated, preconfigured standby system. Categorization helps bring risk into focus. Even if this risk driver was not immediately obvious, the increased cost associated with buying or leasing the standby system would function as a risk indicator pointing back to the driver which caused it. Keeping track of these interdependencies, while attempting to assign ordinal or cardinal probability/impact values to events in a system, can be daunting. And, while passively accepting risk or doing nothing is always an option, most recognize that active Acceptance, Avoidance, Transfer, or Mitigation strategies offer far better alternatives.

The Plexent Approach

itDNA builds on the Continuity Management concepts outlined in the ITIL standard and, by leveraging our framework, Plexent can apply ITIL to your organization. If you are just getting started with Continuity Management you may need help to identify the proper tools with which to evaluate your business. For example, some changes designed to improve business, such as just-in-time logistics, actually create vulnerability. The associated risks can be easily overlooked if you are not using the correct approach. Or you may be struggling with accurately capturing the various states of nature in preparation for decision-making-under-uncertainty analysis. Whatever your Continuity Management maturity, Plexent can take you to the next level by bringing all of the pieces together.

Much more than just a framework, itDNA brings real-world tools and techniques to bear on your Business Continuity Plan (BCP) and Disaster Recovery (DR) concerns. Backed up by itDNA's maturity models and rich, intellectual property knowledge base, Plexent's project management combines with proven policies and procedures to provide standardized services within the following Continuity Management Elements:

- Requirements
- Develop BCP/DR
- Implement BCP/DR
- Maintain BCP/DR
- BCP/DR Training

Within the larger framework of business continuity planning, Continuity Management complements normal Business Impact Analysis by providing the IT perspective. Additionally, this Discipline interacts with Service Level, Configuration, and Change Management, as well as the Service Desk, to afford total coverage across the organization. Finally, awareness, education and training support the published continuity plan to ensure that it can be executed quickly and effectively in an emergency. Other benefits of a mature Continuity Management program include:

- SLAs targets achieved
- Safety increased
- Financial loss limited or prevented
- IT operational capability preserved
- Preservation of goodwill, credibility, image, or reputation
- Confidentiality, integrity, and availability of data maintained during a crisis

Unless your business can afford to be without IT services for extended periods of time, Continuity Management is a topic that must be addressed. As an extension of your normal business continuity planning, its consideration ensures that critical services will be available when and where you need them. Risk management activities provide the core of what will become the end product, but there is a long road to travel from your business needs to a viable continuity plan. Fortunately, Plexent provides assessment services. Leveraging the intelligence in our itDNA, we can help you evaluate where you are today, where you would like to take your organization, and the surest path to get there.

® ITIL is a registered trademark of OGC.