Business Continuity

By Rich Schiesser in conjunction with Harris Kern's Enterprise Computing Institute

The state of business continuity and disaster recovery planning is dismal in most organizations, and even nonexistent in many. Moreover, most plans in place simply won't work. This is not surprising since disaster recovery has not been given sufficient consideration. Until now disaster recovery has been among CIOs' lower priorities. This article is the first in a series covering business continuity. It presents an overview of the business continuity framework.

It is important to note the difference between the terms "*business continuity*" and "*disaster recovery*", as they are used interchangeably in the industry. We view the terms in a hierarchical perspective for the purposes of ensuring continuity of your key business processes, delivery services, and information technology (IT) services. IT disaster recovery is a significant component of business continuity, but there is more to consider when planning for expected events. Consider the following:

Business Continuity Hierarchy

Business	**Services**	**Information Technology**
Continuity of key: ▪ Business outcomes ▪ Business process	Continuity of key: ▪ Delivery services ▪ Delivery processes	Continuity of key: ▪ Delivery services ▪ Delivery processes
Business Continuity		

In an emergency there are many *continuity* requirements within the organization's business and services covering processes, facilities, personnel and others. IT and a variety of business units across the organization must work in concert, both in planning for continuity and in its execution.

Today, the disaster recovery capabilities in many organizations contribute little to their real objectives and operations. But with rising threats to our socio-politico-economic infrastructures, government and business leaders are more aware of their dependencies and risks regarding information technology. They are beginning to recognize the extent of their vulnerabilities, and, as such, are becoming more amenable to allocating the resources to reduce their risks. There is now a window of opportunity to gain control of business continuity and disaster recovery, and build programs that contribute to desired business outcomes.

To move forward there are a few challenges that you will want to address. When organizations think about disaster recovery, they commonly think about technology, like tape backup systems, storage systems, and hot sites. Technology, particularly high availability technology, is an important part of business continuity and disaster recovery. However, there is more - much more. IT executives need a way to ensure that plans are relevant and

realistic, accurate and up-to-date, workable and manageable, and cost-effective. In effect you need to *productionalize* business continuity.

This means you will want to build and manage a process to ensure that business continuity strategies, plans and procedures are always appropriate. You will have to manage business continuity as a service to ensure the business gets what it needs, when it needs it, at a reasonable cost. To do so you will need to help the business define the components depicted in the diagram above.

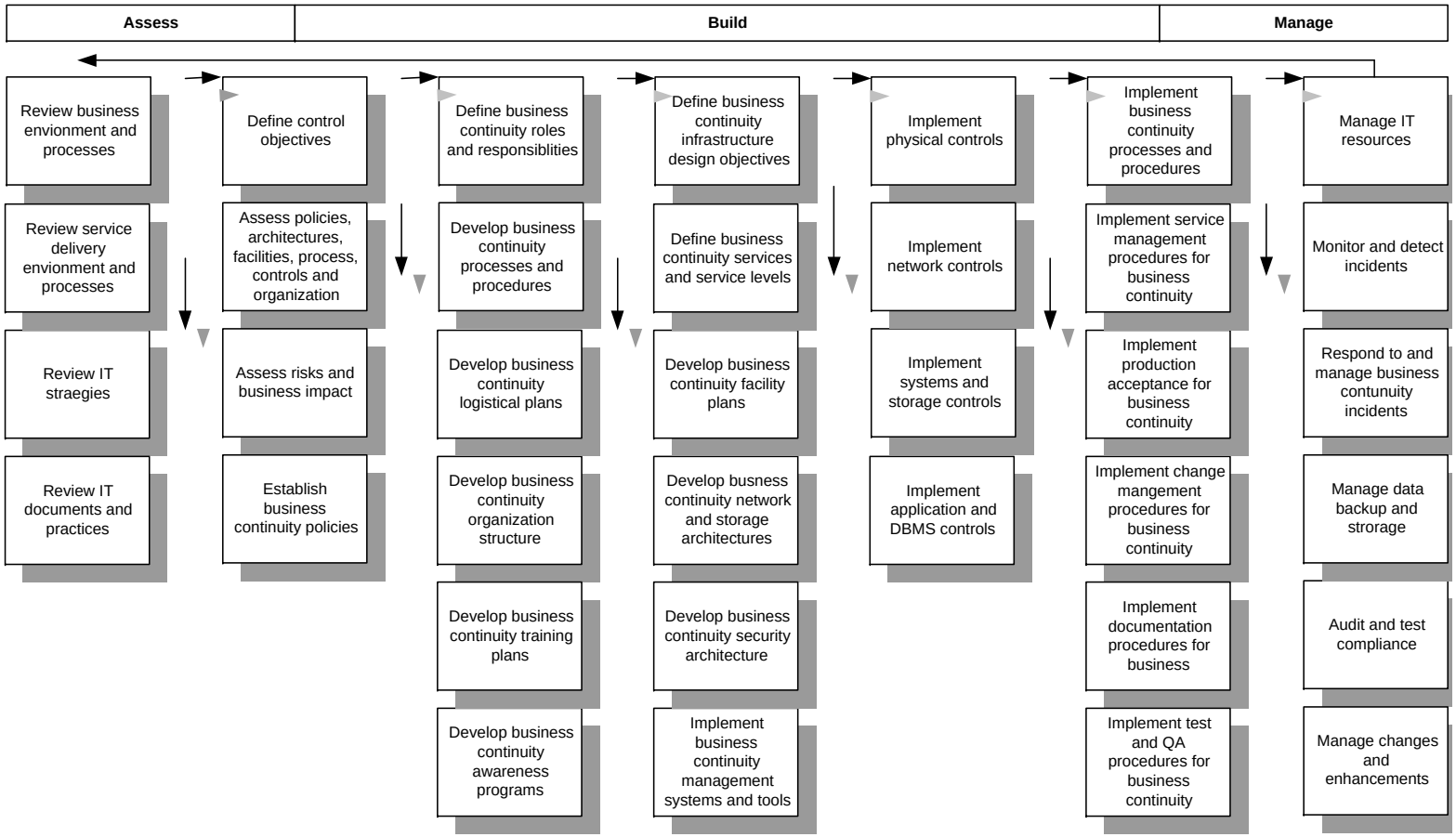
The business continuity framework described in this series is a way to ensure that key aspects of the business, service delivery and technology infrastructure, including the business continuity process, are assessed, built and managed in a comprehensive and logical manner by placing emphasis on process, technology and organization.

The diagram below shows one manifestation of the assess, build, manage model. Some of the key components of the business continuity framework are underscored:

- *Business impact analysis* – Business continuity planning depends on a clear understanding of business processes and data, and associated risks. The business continuity process formalizes procedures to 1) identify important business processes, data and technology infrastructure, 2) identify associated risks and impact, and 3) develop scenarios and business continuity strategies. With formal procedures you can ensure business continuity strategies are evaluated and updated continuously.
- *Service management* – Business continuity is a service and, as such, must be driven by service levels. These include descriptions of continuous (no downtime allowed) and resilient (some downtime allowed) systems with time-to-restore and point-of-restoration metrics.
- *Production acceptance* – To be effective, business continuity planning must be an integral part of the applications and IT infrastructure development processes. For example policies and procedures need to be in place to ensure that business continuity and high availability requirements are identified early in the software development lifecycle. Production acceptance procedures also ensure that all required provisions for business continuity (technologies, processes and organization) are ready and tested *before* applications are released for production.
- *Change management* – Like any other critical application and IT infrastructure component, business continuity strategies, plans and documentation are subject to change management. This is the only way to ensure that changes are captured in a timely and accurate way.
- *Technology architectures* – Tape backup has always been an important part of disaster recovery, but it is no longer sufficient. It is too slow and cannot handle high volumes of data. With greater emphasis on business continuity, other technologies must be considered. High-availability servers, storage systems, networks and DBMS's, among others, have prominent roles in many business continuity plans.
- *Detection and response management* – This is the essence of any business continuity plan. It comprises all the guidelines and detailed procedures for emergency decision-making, preparation, initial emergency responses and system recovery.

- *Security management* – Security and business continuity are closely related. Business continuity plans must be reviewed with respect to security policies and requirements.

Business Continuity
Assess, Build, Manage Model



Unification Framework > Informaiton Technology Dimension > IT Process Domain > Business Continuity Element					
IT Services	**IT Policies**	**IT Organization**	**Technology Architectures**	**IT Facilities**	**IT Processes**

- *Organization* – Roles and responsibilities must be well defined. This covers a variety of technical staff (programmers, administrators and operators), executive managers (emergency decision makers), facilities managers (power, cooling, cabling), human resources (staff issues and needs), business units (business processes) and external organizations (outsourcers, telcos and suppliers).
- *Facilities* – You must make provisions to ensure that appropriate facilities are in place. You must consider guidelines that address high-availability power, cooling and fire protection systems and facilities that are physically secure. These guidelines must also cover different types of offsite facilities for processing, storage and workspace.
- *Logistics* – Systems and data recovery are only part of business continuity planning. There are many logistical issues to consider, *before an emergency occurs*. You will want to make special provisions for your organization's staff. They need adequate workspace, furniture, workstations, communications and supplies. In many cases you need to make special arrangements for living accommodations, food, personal security and transportation. You might have to make special arrangements for their families. If you don't productionalize these tasks, they won't get done
- *Testing* – Many organizations rarely test their business continuity plans. If they do it is not adequate. Having guidelines and procedures to ensure that testing is frequent, comprehensive and systematic is a must.
- *Assessments* – Business continuity must be assessed continuously for improvements. Also, it must be audited for compliance with polices and regulations.