IT Service Continuity Management (ITSCM)

Oh the disaster, the sudden unexpected disaster. Some of us have been through the major ones – Hurricanes, Tornados, and Ice Storms. Others of us have been through the smaller ones – Boiler Exploding in a building, a building falling into the Normanskil, and lightening hitting the building. IT service continuity management (ITSCM) is to proactively assure IT services can be recovered and provisioned based upon the established business continuity management timeframes. Basically once you rate your critical applications, assuring the critical fabulous four are up first within the agreed upon timeframe. This helps to have a pre-defined process in place to help the organization recover to normal operating procedures after a disaster. On the reactive side of the equation, once the disaster has occurred. IT service continuity management is the process responsible for assessing the impact of the disruption on IT services.
ITSCM focuses on the IT services required to support the organizations critical lines of business. For example, in a hospital having the ability to register patients is a critical business process. In the scenario where a disaster has occurred, not only is the patient registration application needed but additionally any supporting IT infrastructure and services such as active directory, networks, telecommunications, technical support, and the service desk. In addition to any census balancing to have the patients referred to the right rooms. Obviously, this pursuit needs to be a join collaboration with patient access and maybe even nursing to assure it is well documented what is needed when.

Commonly the business continuity life cycle is as a foundation building block to help assure that the organization's IT service continuity management process is successful.
The business continuity life cycle consists of four stages:

1. **Initiation** - The initiation stage is starting point for the life cycle. The goal of initiation is to define the ITSCM policy and charter the endeavor. Chartering is the project charter which defines the high-level scope, team needed, and critical success factors for the project. The ITSCM policy is the bought into and formalized plan to influence and determine decisions, actions, and other matters regarding IT continuity. The initiation stage outcome will be the charter, project scope, project timeline, and main ITSCM policy all documents will be referred to in subsequent stages.

2. **Requirements and Strategy** - During the requirements and strategy stage, a business impact analysis (BIA) and risk assessment are conducted. The business impact analysis evaluates the what-if scenarios to consider what might happen after a disaster. BIA points out the critical business processes ad the potential damage which can result from a service disruption. BIA is the requirements part. A business continuity strategy is produced from the results determining which risk reduction measures are necessary and which recovery option supports the organization's needs. This stage typically involves identifying services critical to the business that require additional preventive measures.

3. **Implementation** - During the implementation stage, previous stages outputs are reviewed so that recovery plans can be developed which contain all the details an organization needs to survive a disaster and restore normal services. This stage also defines the actions necessary to prevent, detect, and mitigate the effects of potential disasters. One of the activities conducted in this stage is developing implementation plans, including the emergency response plan, the damage assessment plan, and the salvage plan.

    - **Implementing standby arrangements** - includes defining, creating, and solidifying the underpinning contracts (UCs) with standby providers. A UC is a contract with an external supplier that supports the IT organization in its delivery of services. This contract could be a support or maintenance agreement, and it should be capable of supporting targets agreed to in service level agreements (SLAs). Once completed, the UCs should be listed in the configuration management database and linked to the recovery plan and the associated SLAs. Necessary equipment also needs to be purchased.

- **Developing procedures** – Developing procedures which detail exactly what each member of the disaster recovery (DR) team must do if the plan is invoked. One staff aid may explain the exact steps for immediately transferring data to the backup site if the DR plan is implemented.

- **Undertaking initial tests** - Undertaking initial tests typically involves performing some initial testing of procedures before they are finalized. Actual, final testing occurs in the fourth stage: operational management.

By performing each of these activities, organizations can be sure that they have successfully completed the third stage of the business continuity life cycle. After implementation has been completed, the process needs to be maintained as part of business as usual.

1. **Operational management** – As the ITSCM process needs to be maintained. The operational management stage helps ensure that maintenance occurs. To help maintain the process, a commitment to training, reviewing the process, and testing the process needs to occur. It may be a good idea to have a yearly mock test budgeted. An effective ITSCM plan cannot be developed without taking into consideration the needs of the entire business. When you follow the stages of the business continuity life cycle, a plan which fully supports the organization will be established.

From the business continuity life cycle, one output is the recovery plan. The recovery plan should detail the instructions and procedures to recover or continue the operation of systems, infrastructure, services, or facilities. The ultimate goal of the recovery plan is to maintain service continuity.

The elements of a **recovery plan** are as follows:

- **Strategy –** Strategy explains what systems, infrastructure, services, or facilities will be recovered and how they will be recovered. It also specifies the amount of time it will take for the recovery and when the recovery should be completed.
- **Invocation –** Invocation details everyone who has the authority to invoke the recovery plan.
- **General guidelines** - The general guidelines of behavior for notifying personnel of a potential or actual disaster. It also lists the defined operational escalation procedures.
- **Dependencies** - Dependencies is concerned with the system, infrastructure, service, facility, or interface dependencies in order of importance. Identifying the interdependencies will bring to light other procedures which may need to be enacted in conjunction with the recovery plan. In continuing with our model, census balancing.
- **Team and checklist –** The team and checklist is the list of the staff members who are responsible for enacting the procedures and noting any problems they encounter. It also includes a checklist of key tasks.
- **Procedures** – The procedures for installing and testing hardware and network components, and for restoring applications, databases, and data.

By following this best practice, organizations can have a level of confidence in their recovery plans. Success will be determined by have effective recovery plans which recovery the critical IT services within the agreed to timeframe.

Recovery options need to be considered for IT systems and networks, and critical services such as telecommunications and power. The various **recovery options** are as follows:

- **Do nothing** - However, few organizations can afford to forgo all business activities supported by IT services and simply wait until services are restored.
- **Manual system** - For businesses without a large number of critical IT services, manual workarounds may present a feasible option until IT services can resume.

- **Reciprocal arrangement -** This option involves forming an arrangement with another company that uses similar technology. For instance, a company and its main supplier might discuss an arrangement where they can share facilities in times of disaster.
- **Gradual recovery -** This option is often chosen by organizations that don't need to use the business processes supported by IT services for 72 hours or longer. This often involves the use of a location that provides power and telecommunications, where companies can use their own equipment.
- **Warm start -** This is an option used by organizations that need to recover IT services and facilities within a 24- to 72-hour period. To accomplish this, organizations often use commercial facilities that include operations, system management, and technical support.
- **Hot start** - This is also known as an immediate recovery. This option is used for critical services that cannot be down for any length of time. A hot start provides for immediate restoration of IT services. It is also one of the most expensive options to implement.

One way to warrant that the IT service continuity management (ITSCM) process is both efficient and effective is to assign an **IT service continuity (ITSC) manager**. We all know establishing accountability in a role is necessary for a successful process.
The ITSC manager is responsible for:

- establishing plans to provide agreed-on levels of service within agreed timelines following a disaster
- ensuring that IT service areas are able to respond to an invocation of the continuity plans
- maintaining a comprehensive IT testing schedule and undertaking regular reviews.

Through her primary responsibilities, the ITSC manager will ensure that the ITSCM process is implemented and maintained in accordance with the organization's requirements and business continuity management process. One way ITSC managers can make sure that ITSCM is effective is through continued communication with the other IT service management (ITSM) processes.

ITSCM should not work in isolation from an organization's business requirements, nor should it work in isolation from the other ITSM processes.

Each ITSM process relates to ITSCM in the following ways:

- **Service desk -** ITSCM uses historical data, usually statistics, provided by the service desk. This is a focal point for reporting incidents and making service requests. Whenever possible, many companies use the service desk as the communication center in the invocation of the disaster recovery plan.
- **[Service asset and] Configuration management -** Configuration management helps to define the core infrastructure. Configuration management contains current, accurate, and comprehensive information about all components of the IT infrastructure.
- **Availability management** – Availability management delivers risk reduction measures to maintain business as usual. This process is concerned with designing, implementing, measuring, and managing IT services to ensure that requirements for availability are consistently met.
- **Change management** - The impact of any change to the recovery plan has to be analyzed. Change management works with ITSCM to make sure that any changes made are reflected in the recovery plan and related documents so that documentation is kept up-to-date.
- **Capacity management -** This ensures that business requirements are fully supported by the appropriate IT hardware resources. Through these resources, ITSCM has access to the capacity it needs to develop and test plans.

Like any quality business process, IT service continuity management (ITSCM) has expenses and common problems.

Common problems associated with ITSCM are any issues that prevent an organization from committing to continuity management—in terms of both implementing the process and maintaining it. One example is when firms seem unable to move out of the planning stage and into actual implementation.

Other examples are being unable to find facilities or resources, having someone unfamiliar with the business implement the process, not understanding ITSCM's role in disaster recovery, or thinking IT has already handled continuity planning.

Common costs associated with ITSCM are the expenses incurred from risk management and recovery arrangements. An example of a common cost is the investment required by the introduction of risk management.

Additional examples of common costs are returning operational costs and the hardware needed to support the ITSCM process, and fees for the recovery facility.

There will always be problems and costs associated with implementing ITSCM. But the resulting benefits, especially when a disaster is prevented or quickly controlled, outweigh the associated difficulties and costs.

Bron:
http://www.anticlue.net/archives/000845.htm