Leveraging ITIL to improve Business Continuity and Availability

Samuel Lo  MBA, MSc, CDCP, PMP, CISSP, CISA
Data Centre Services Manager
COL Limited

itSMF Conference 2009
25 February 2009
Agenda

- Availability Management
- ITSM and Business Continuity
- The critical considerations on integration for Business Continuity and Availability management
- Impact on/of the standards – ISO/IEC 20000, ISO/IEC 27001 and BS25999
Business Downtime

Business concerns

- Cost of downtime
- Causes of downtime such as human error, hardware availability, fires, floods or virus attacks

Availability management and Business Continuity management are in line with the organization’s needs.
ITIL and Availability Management

- ITIL can provide best practices on IT operations by
  - Minimizing people, technology and process issues that cause downtime and
  - Defining and maintaining appropriate service levels.

- ITSM can provide assurance of specific performance and availability outcomes for business-critical IT services.

- Availability management should ensure the agreed level of availability is provided.
Business Requirements for IT Availability

- A definition of the Vital Business Functions (VBFs) supported by the IT services
- A definition of IT services downtime, i.e. the conditions under which the business considers the IT services to be unavailable
- The business impact caused by loss of services, together with the associated risk
- Quantitative availability requirements, i.e. the extent to which the business tolerates IT services downtime or degraded service
- The required service hours, i.e. when the service is to be provided
- An assessment of the relative importance of different working periods
- Specific security requirements
- The service backup and recovery capability.
Availability Management Process

Availability Management Process should include

- Monitoring of all aspects of availability, reliability and maintainability of IT services
- Maintenance of a set of methods, techniques and calculations for all availability measurement, metrics and reporting
- Collection of measurements, analysis and production of regular and ad hoc reports on service and component availability
Certain Vital Business Functions (VBFs) need special designs, incorporating:

- **High availability**: a characteristic of the IT services that minimizes or masks the effects of IT component failure to the users of a service.

- **Fault tolerance**: the ability of an IT services to continue to operate correctly after failure of a component part.

- **Continuous operation**: an approach or design to eliminate planned downtime of an IT services.

- **Continuous availability**: an approach or design to achieve 100% availability.
VBFs and Availability

- The greatest level of availability should be included in the design of those services supporting the most critical of the VBFs.

The relationship between levels of availability and overall cost
Availability Measurement

1. Agreed Service Time (AST)
2. Mean Time Between Service Incidents (MTBSI)
3. Mean Time Between Failures (MTBF)
4. Mean Time to Restore Service (MTRS)

Value to the business
The Availability Management Process ensures that the availability of systems and services matches the evolving agreed needs of the business.
The Mission of ITSCM

- To manage the risks of key IT services failing by avoiding risks (Risk Management)
- To recover key IT services in a contingency (Disaster Recovery)
- To support the continued functioning of the business to a specified level within a stated set of circumstances (Business Continuity)
ITSCM and BCP Processes

- Review the agreement of the scope of the IT Service Continuity Management (ITSCM) process and the policies adopted, especially Business Continuity Policy
- Prioritize the business processes by Business Impact Analysis
- Conduct Risk Analysis (RA) to identify the assets, threats, vulnerabilities and countermeasures
- Evaluate the options for recovery
- Produce the Business Continuity Plan (BCP)
- Test, review and maintain BCP on regular basis
ITSCM Process Goals

- ITIL-aglied ITSCM policies, processes and procedures
- Dedicated ITSCM process owner
- Holistic recovery of IT services to ensure business services are recovered versus technologies
- Alignment of IT service recovery plans with Vital Business Functions
- Actions to ensure Operational Level Agreements and Underpinning Contracts with IT suppliers will support recovery services
- Periodic testing and audits of BCP
- Communications for IT service recovery needs and requirement across the organization
- Staff awareness and education on BCP and actions to be taken in event of a major business disruption
Business Continuity and Availability

- Identify and correct continuity problems within IT and achieve greater alignment with the business continuity plan
- Ensure that proactive measures to improve the availability of services are implemented
- Negotiate and agree the necessary contracts with suppliers for provision of the necessary recovery capability to support all continuity plans in conjunction with the Supplier Management process
Relationships between other ITIL processes

- Infrastructure and business Change Management need to assess the impacts of changes on the BC and DR plans.
- Configuration Management data (CMDB) is required to facilitate planning.
- Both the BC and DR plans should be subject to Change management procedures and Configuration Management for production and DR sites.
- Incidents reported to the Service Desk should be available to ITSCM planners for impact analysis purposes.
Facilities and Data Centre Management

Beside IT systems, in order to have high availability for IT services we should also ensure sufficient control on facilities and data centre management.

The main components includes

- Building Management
- Power Management such as duel power supply from separate isolated transformers, UPS, diesel generator
- Environmental Conditioning such as CRAC, backup chiller plant
- Facilities Monitoring such as Building Management Systems
- Fire Protection System such as FM200 and zone partitioning
- Physical Access Control
- Scheduled Preventive Maintenance
- Contract & SLA management
- Safety
- Operational Training
ISO-ITIL Relationship

ISO 20000 Part 1
Compulsory requirements

ISO 20000 Part 2
Code of Practice

ITIL
Best Practice Guidance

In house Policies, Processes, Procedures and Practices
Deploy Services
## Variations between ITIL and ISO 20000

- ISO/IEC 20000 is the first worldwide standard aimed specifically at IT Service Management
- Adopted ISO/IEC 20000 in 2005
- ISO/IEC 20000 is strongly aligned with the ITIL
- ISO/IEC 20000 provides an independent standard suitable for third-party certification
- ITIL provides best practices in IT Service Management
- ISO/IEC 20000 consists of a auditable specification and code of practice
- Service Continuity and Availability Managed are separate in ITIL
- ISO/IEC 20000 includes Information Security Management (ISO/IEC 27001) for security requirement
Relationship between ISO 20000/ISO 27001 and ITIL

A way to understand the relationship is to look at the relationship between ITIL and Information Security Management

- How the Service Support processes relate to Security Management
- How the Service Delivery processes relate to Security Management
Service Support and Security Management

Service Desk
- Security Incident identification and resolution
- Access Management

Incident Management
- Security Incident Management

Problem Management
- Security Problem

Change Management
- Approval for Request of Change about security
- Impact on Security Controls

Configuration Management
- Identification of IT assets
- CIA of Configuration Items

Release Management
- Compliance control e.g. licenses
- Security Policy Compliance
- Security Emergency Release procedure

Service Support
Service Delivery and Security Management

Service Level Management
- Security OLA/SLA
- Service Improvement Plan

Availability Management
- Risk Management & Business Impact Analysis
- Recovery Strategies

Capacity Management
- Monitoring thresholds
- Capacity Plan

Financial Management
- Security Infrastructure Cost
- Security Operation Cost

IT Service Continuity Management
- Risk Management & Business Impact Analysis
- Security of Recovery Solution
- Data Security
- Business Continuity Plans
BS25999 and IT Service Continuity Management

- BS25999 comprises two compatible and aligned parts: **BS 25999-1:2006** (Part One) is a *Code of practice* that takes the form of guidance and recommendations. It establishes the process, principles and terminology of BCM and provides a comprehensive methodology based on BCM best practice. **BS 25999-2:2007** (Part Two) is a *Specification* that details the requirements for a BCMS.

- ITSCM processes and other ITIL processes provide many best practices for preparing certification on BS25999.
Questions
Thank You!

Samuel Lo
samuelleo@col.com.hk
(852) 2118-3888
www.wharftt.com
www.col.com.hk