ITSCM (IT Service Continuity Management) Overview: ITIL®'s IT Disaster Recovery and Business Continuity Management

Ellis Holman
IBM

Karla Houser

Session 10043

Abstract

- IT Service Continuity Management (ITSCM) is far more than just Disaster Recovery Planning. It is aligned to the Business Continuity Lifecycle and helps you to prepare for the worst case scenario; that is not just how to recover from a disaster but to stop the disaster from occurring in the first place, if at all possible. ITSCM investigates, develops and implements recovery options when an interruption to service reaches a pre-defined point. It must be a part of the overall Business Continuity Plan and not dealt with in isolation.

  ITSCM helps you determine, for YOUR installation, the “What is a Disaster?” description. Defining the pre-conditions that constitute a disaster is part of the ITSCM process. Such definitions form an integral part of any Service Level Agreement relating to the provision of services.

  ITSCM addresses risks that could cause a sudden and serious impact, items that could immediately threaten the continuity of the business. These typically include things such as:

  - loss, damage or denial of access to key infrastructure
  - application services failures
  - non-performance (including the possibility of your provider experiencing disaster) of critical providers, distributors or other third parties
  - corruption of key information
  - sabotage, extortion or commercial espionage
  - deliberate infiltration
  - attacks on critical information systems

  Our speakers will provide an overview of the ITIL V3 ITSCM process, how it aligns with Business Continuity Management and why you need ITSCM. Businesses today are realizing their dependence upon and their requirements for IT technology and the disciplines that are needed to provide effective and efficient IT services.

Presentation Purpose

- Provide an overview of ITSCM and its alignment with Business Continuity Management
- Provide an overview of why ITSCM is need
- Note: Not all slides in this presentation will be covered in detail. This is an overview presentation and some of the material is intended to be used as a reference after the conference.

Disclaimer:

- *Speakers do not endorse any products/vendors.*
- *Speakers do not recommend the purchase of any products by the participants.*
- *Each participant should make up her or his own mind when evaluating the material.*
- *The views presented in this presentation are solely those of the speakers and not those of any company or organization.*

Agenda

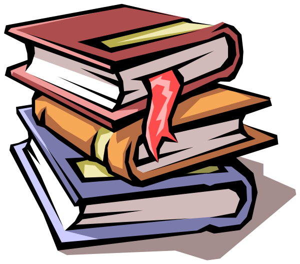
- What is ITIL?
  - And where does ITSCM fit in?
- Terminology
- Defining a Disaster
- ITSCM – Goals, Objectives, Scope
- ITSCM – Lifecycle
- ITSCM is Important …

What is ITIL®?

And where does ITSCM fit in?

Defining ITIL

- ITIL is a public domain, vendor agnostic set of practices for IT Service Management
  - Processes, methods, functions, roles and activities that a service provider uses to enable the deliver of IT services to their customers
    - ITIL "Service" is a business process or function
    - Includes applications and infrastructure as well as processes for delivering these
    - Services defined from a customer's perspective, not IT's perspective
  - Developed by the Central Computer and Telecommunications Agency (CCTA), an Executive Agency within UK government in the 1980's
  - Now "owned" by Office of Government Commerce (OGC), a UK Govt. Department
  - "De-facto standard" for service management
  - Provides a comprehensive, consistent and coherent set of best practices for IT Service Management that promotes a quality approach to achieving business effectiveness and efficiency in the use of information systems
- ITIL = **IT** **I**nfrastructure **L**ibrary
  - A framework for IT Service Management
  - Establishes "good practices"
  - Defines a standard of IT service quality that customers should demand and providers should seek to supply



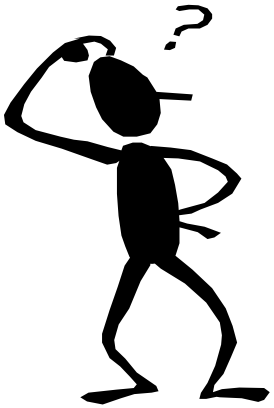
- A set of books
  - Series of publications or "sets" of text ("Library")
  - Library provides "best practices" documentation for IT

Understanding Good versus Best Practices

- A best practice is an innovation
- A good practice is
  - A best practice that has endured the test of time
  - A good practice fits within the framework of how the enterprise does business
  - A generally accepted principle
- Best practices that have become good practices
  - The use of “standard” seat belts in automobiles
- Best practices that have **not** become good practices
  - The use of “five point” seat belts in automobiles
- Good practices become best practices when applied with specificity to your environment

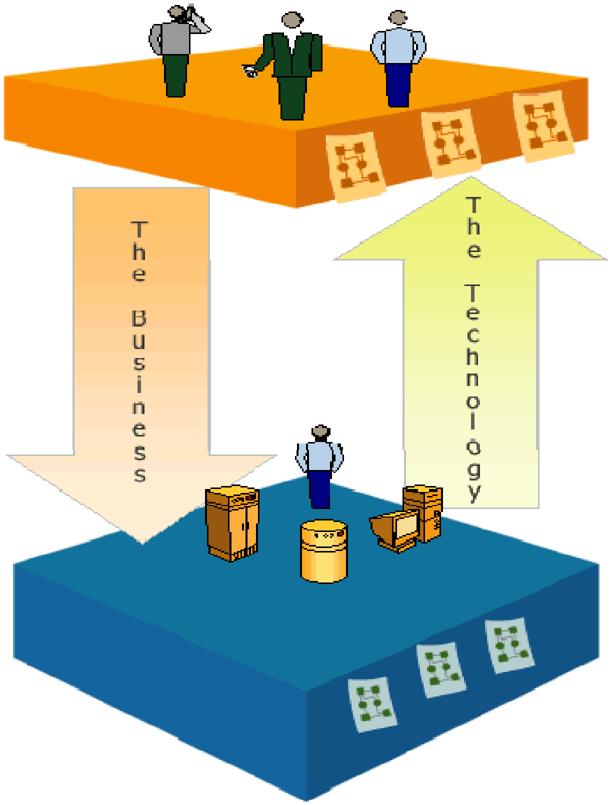
What is ITIL?

- "Good Practices" determined by industry experts, consultants and practitioners
  - Baseline or benchmark
  - MBIT (Managing the Business of IT)
- "Real world" applicability
  - Been there, done that
  - Acknowledges that things can and will go wrong!
    - How often do you receive "thank you the system is up" calls?
- Good ideas on how to manage IT
  - Customer and business, not technology focused
- Framework - goals, general activities, processes
  - Inputs/outputs/relationships documented
  - "What" not "how" guidelines
    - Provides high level guidance on what should be done
  - **Not** list of procedures, these vary by site
    - **You** develop and implement work-level procedures for daily service delivery and service support activities to match **your** unique requirements and internal culture and change them based on the changing needs of **your** organization

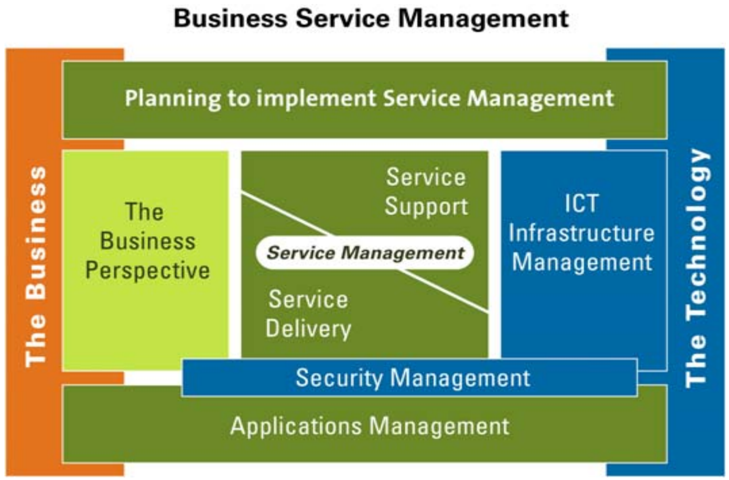


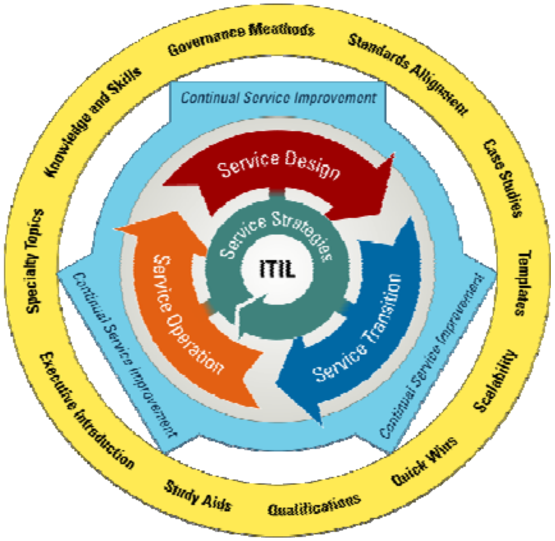
The Goals of ITIL

- Provide “good” practice guidance for IT Service Management
  - Integrate IT to business service
  - Create a framework for management
    - People
    - Processes
    - Technology/Product
    - Partner/Supplier Relationships
  - Improve efficiency
  - Facilitate the quality management of IT services
  - Increase cost effectiveness
  - Reduce risks
  - Focus on the services required by the customer base, not on the technologies



ITIL V2 and ITIL V3

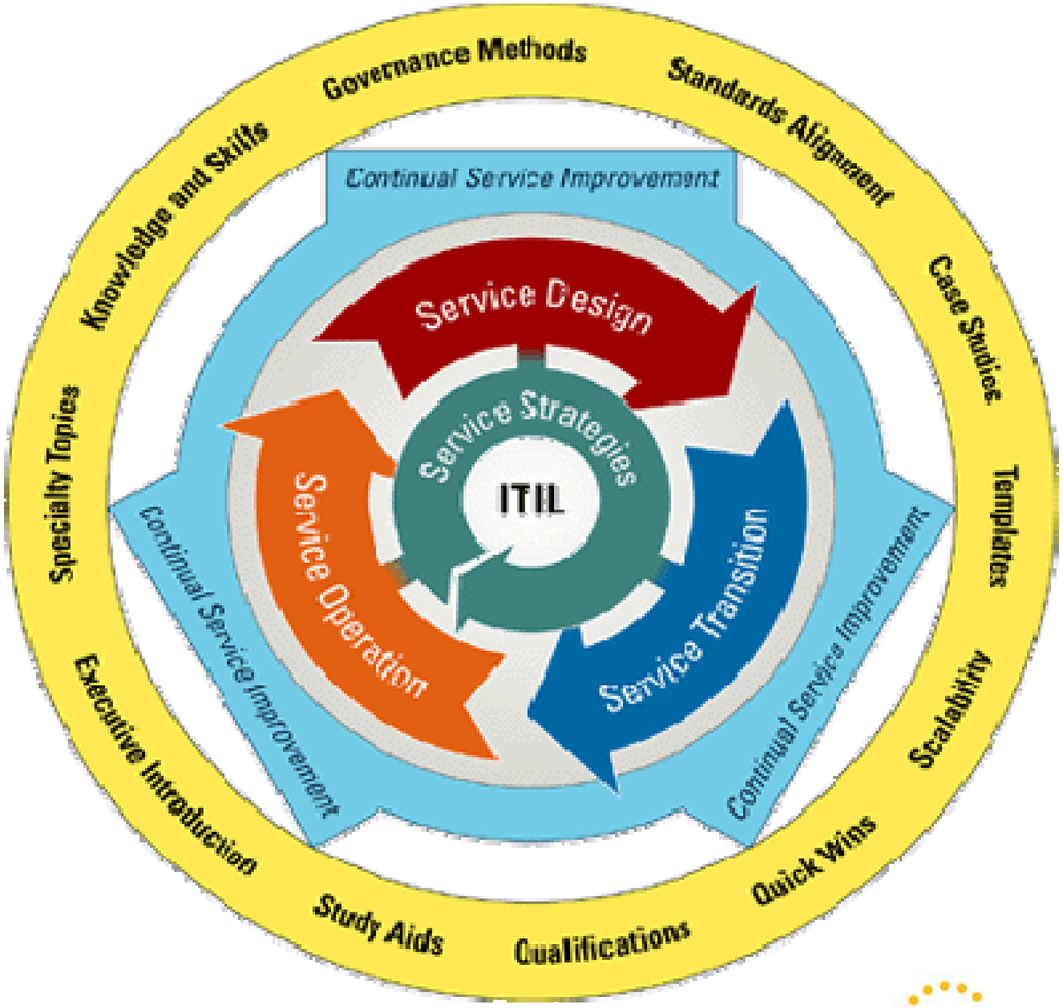




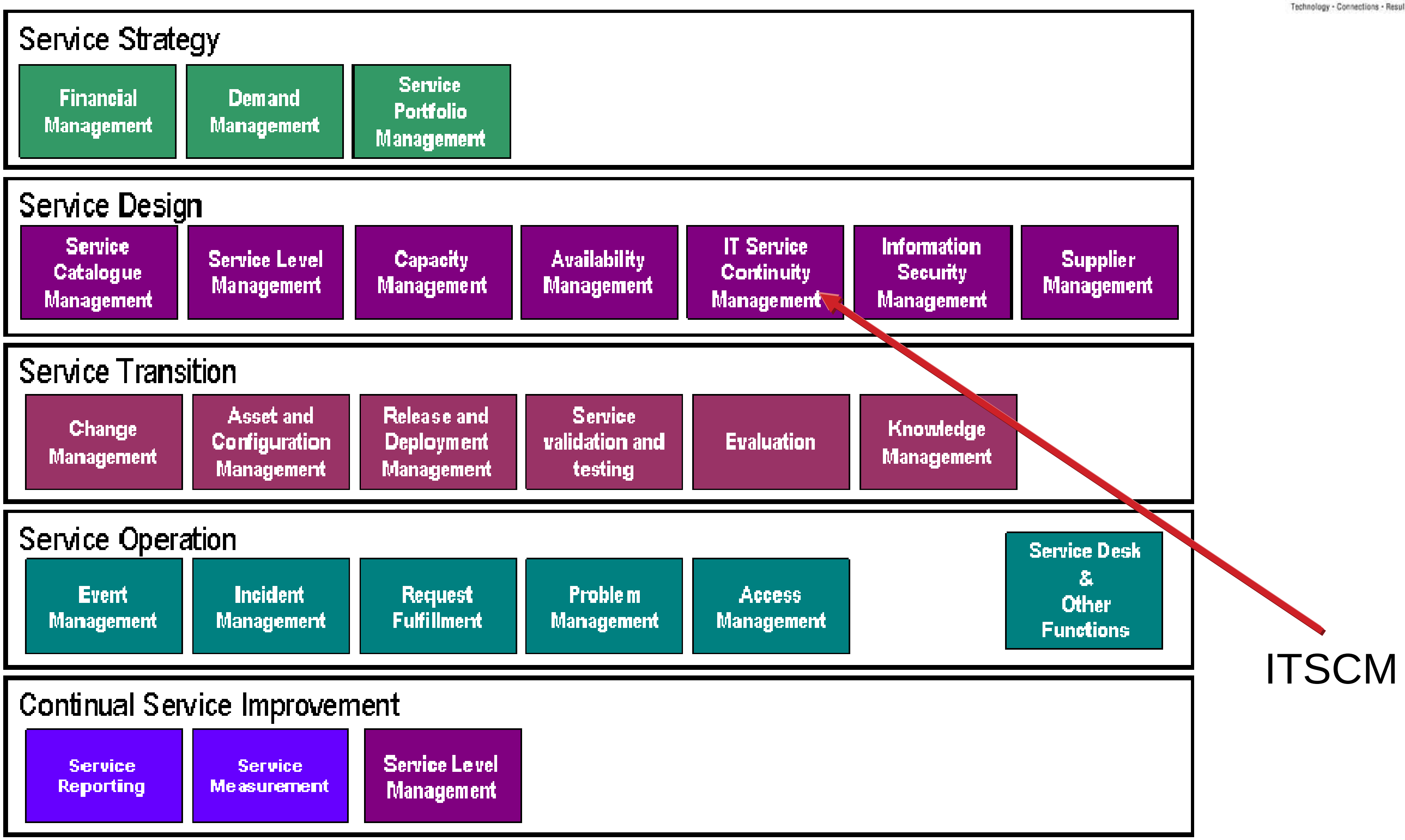
- ITIL V2 = IT-to-Business alignment
  - Core Books
    - Service Support
    - Service Delivery
  - Support Books
    - ICT Infrastructure Management
    - Applications Management
    - Security Management
    - Business Perspective
    - Planning to Implement Service Management
- ITIL V3 = Lifecycle approach
  - Service Strategies: deciding on the services
  - Service Design: requirements & design
  - Service Transition: deployment & activation
  - Service Operations: day-to-day operations
  - Continual Service Improvement: how to improve

ITIL V3 Service Lifecycle

- Service Strategy
- Service Design
- Service Transition
- Service Operation
- Continual Service Improvement



5 Stages of the Service Lifecycle



Service Strategy

- Financial Management
- Demand Management
- Service Portfolio Management

Service Design

- Service Catalogue Management
- Service Level Management
- Capacity Management
- Availability Management
- IT Service Continuity Management
- Information Security Management
- Supplier Management

Service Transition

- Change Management
- Asset and Configuration Management
- Release and Deployment Management
- Service validation and testing
- Evaluation
- Knowledge Management

Service Operation

- Event Management
- Incident Management
- Request Fulfillment
- Proble m Management
- Access Management
- Service Desk & Other Functions

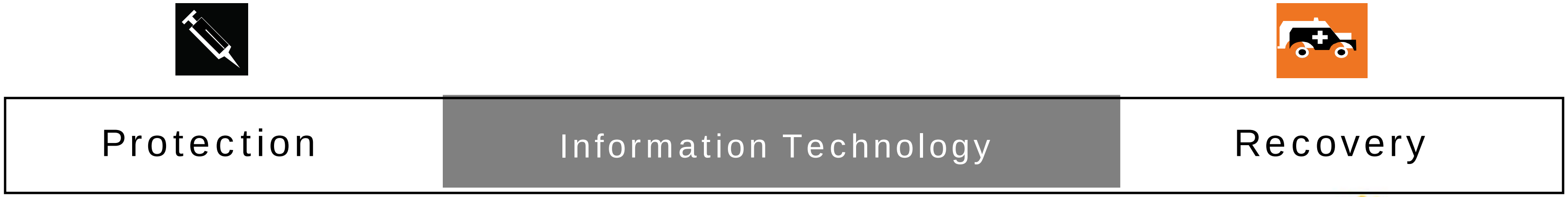
Continual Service Improvement

- Service Reporting
- Service Me asurement
- Service Level Management

ITSCM

IT Service Continuity Management

- Support overall **B**usiness **C**ontinuity **M**anagement (BCM) process by ensuring that the required IT resources can be recovered within business related agreed upon time frames
  - Provide pre-determined levels of service under exceptional conditions
- Common responsibilities
  - Risk management
  - Selection of options based on business requirements
  - Definition of roles and responsibilities
  - Alignment of IT recovery plans and BCM exercising (testing)
  - IT focus
- Resources include hardware, software, staff, and physical environmental
  - The technical and operational aspects of your total Business Continuity Plan



Protection

Information Technology

Recovery

ITSCM and BCM

- ITSCM must be aligned to the Business Continuity Lifecycle
- Business Continuity Management (BCM)
  - Concerned with managing risks to ensure that at all times an organization can continue operating to, at least, a pre-determined minimum level
  - BCM process involves
    - Reducing risk to an acceptable level
    - Planning for the recovery of business processes should a risk materialize and a disruption to the business occur
- ITSCM must be a part of the overall Business Continuity Plan and not dealt with in isolation
  - ITSCM is the “technical component” of BCM

ITSCM and other ITIL Processes

- **Service Level Management**
  - ITSCM is IT Service-oriented.
  - SLM provides a key interface as it defines what are the IT Services within a Service Catalog and at what Service Levels they must be maintained
  - During a continuity ‘event', the Service Level Manager is the interface to the business customers, not the Service Desk. As such, the Service Level Manager should be baked into the ITSCM invocation processes and brought in early during recovery activities
  - Sometimes the Service Level Manager can brief customers during ITSCM exercises

- **Configuration Management**
  - Configuration Management maintains the relationships of IT components that make up each IT Service
  - ITSCM needs to access these service-to-component relationships so that contingency plans can be developed and carried out at the level of a Service
  - If the CMDB is not up-to-date, when changes are assessed for impact, it may not be clear that remote components require similar update
  - During an Incident response, the CMDB provides the impact assessment information necessary to determine if the Incident is severe enough to require ITSCM invocation.

ITSCM and other ITIL Processes

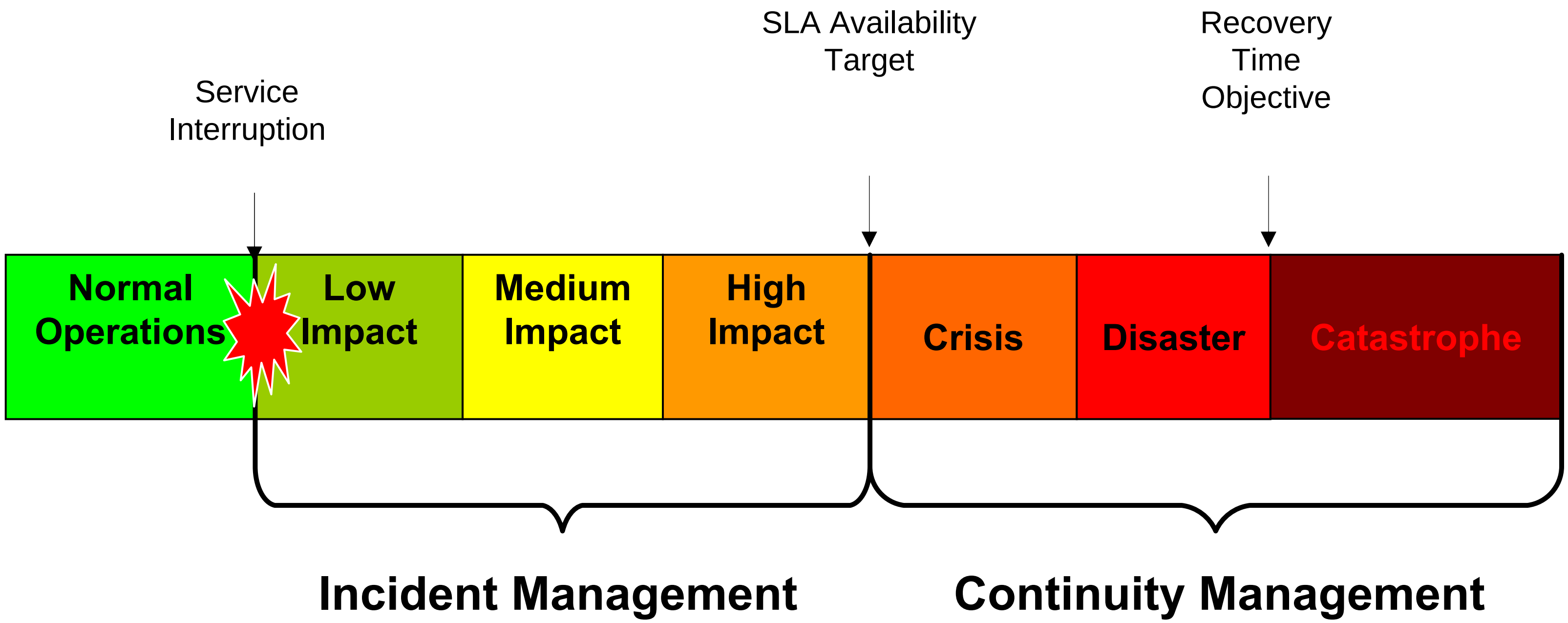
- **Availability Management**
  - Both have a similar focus (after all continuity and availability are two sides of the same coin) and they share a common objective—avoiding IT-related disruptions
  - Availability Management's perspective is to improve high availability through the elimination of single points of failure from components and systems
  - Availability Management leads to robust and redundant configurations in a local data center environment
  - ITSCM's perspective is to cover fail-over/fail-back concerns, any remote replication and remote system mirroring, backup operations, and provide guidance when no automated technological solution is available.
  - Key difference – Availability Management provides an automated capability to avoid taking a casualty to a component in a larger system and ITSCM provides a process of managing risks to the business caused by potential outage or service disruption scenarios and ensuring that the right response mechanism is chosen and acted upon when necessary

- **Incident Management**
  - Entry to ITSCM
  - Incident Management relies on the Service Desk personnel and decisions/classification capabilities defined by Incident Management.
  - The Incident Manager must decide if ITSCM contingencies/capabilities should be used, and when the trigger should be pulled (based on senior management decisions)
  - ITSCM is accountable for ensuring all knowledge, information, and documentation is available to the Incident Manager for making informed recovery invocation decisions

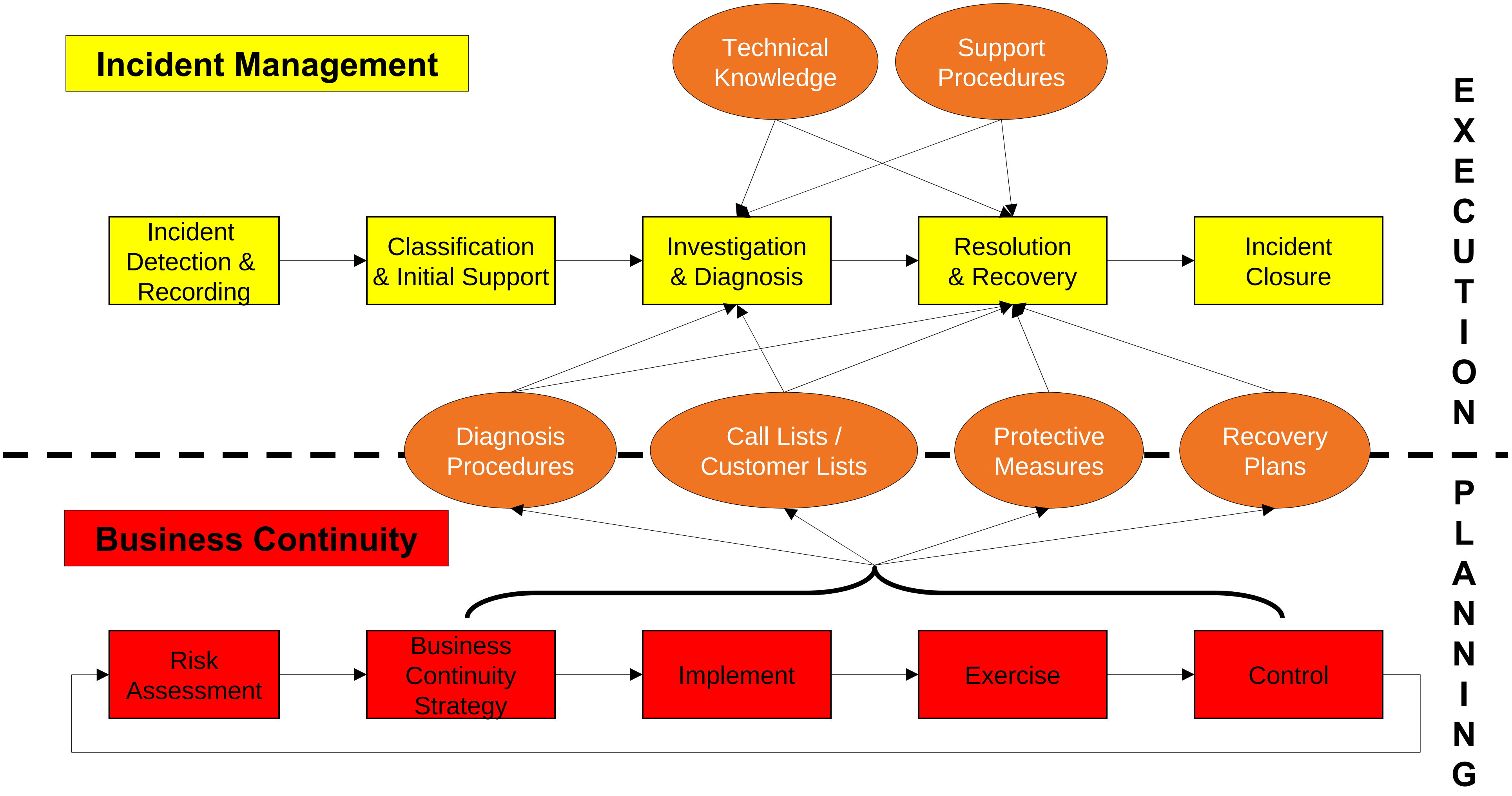
ITSCM and other ITIL Processes

- **Change Management**
  - ITSCM involves many technical components, probably in different locations, that must be kept in synch
    - If a business relies on a remote data center to provide highly or continuously available applications, both centers need to maintain the same levels of code and types of infrastructure
  - A Change Management process that doesn't provide notification when an impending change has an impact on “recovery” or “failover” components will mean failure for ITSCM

Availability, Incident and IT Service Continuity Management



ITSCM & Incident Management



Incident Management

Technical Knowledge

Support Procedures

Incident Detection & Recording

Classification & Initial Support

Investigation & Diagnosis

Resolution & Recovery

Incident Closure

Diagnosis Procedures

Call Lists / Customer Lists

Protective Measures

Recovery Plans

Business Continuity

Risk Assessment

Business Continuity Strategy

Implement

Exercise

Control

EXECUTION

PLANNING

Terminology

Terminology

- Disruption
  - Unplanned event that interrupts the normal flow of a business service for an appreciable length of time
- Disaster
  - Disruption of a critical business service or set of business services for an appreciable length of time
    - Unique to each installation
- Incident Management Plan
  - Documented procedures for recovering a business service from a short term disruption
- IT Disaster Recovery Plan
  - Documented strategy for recovering the IT infrastructure or IT business application after a disaster

Terminology

- Business Continuity Plan
  - “DR” plan that focuses on the business processes rather than the IT infrastructure
- Recovery Time Objective (RTO)
  - How long business process can be without IT application before significant damage to finances or reputation occurs or where required by legal or regulatory requirements
- Recovery Point Objective (RPO)
  - How much data the business process can recreate or afford to loose
- Maximum Tolerable Outage (MTO)
  - The **maximum** amount of time that the business can survive without the business process in any form (manual or automated)

Defining a Disaster

Defining a Disaster

- Defining the pre-conditions that constitute a disaster is part of the ITSCM process
- The definitions form an integral part of any Service Level Agreement relating to the provision of services

What is an IT Disaster?

- **Availability** is related to a component failure and its associated recovery
- A **disaster** may be defined as the prolonged loss of an entire computing center
  - Not a component failure and its associated recovery
- Worse case scenario of a disaster (for above)
  - All equipment and data within the datacenter destroyed
  - Access to the datacenter prohibited due to datacenter damage
  - Staff familiar with the datacenter, equipment, and applications unavailable for the recovery
  - Facility attached to the datacenter relatively undamaged
  - Not a component failure and its associated recovery
- Each organization **must** provide its own “IT disaster” definition

ITSCM > Disaster Recovery Planning

- ITSCM prepares for the worst case scenario
  - Not just how to recovery from a disaster
  - How to prevent/minimize the disaster from occurring in the first place
- Investigates, develops and implements recovery options when a service interruption reaches a pre-defined point

ITSCM – Goals, Objectives, Scope

Why ITSCM?

- IT is a core component of most business processes
  - Key to the survival of the business as a whole
- Risk reduction measures
- Recovery options
  - Maintain the necessary ongoing recovery capability
    - IT services and their supporting components

ITSCM Goals

- Support the overall Business Continuity Management process by ensuring that the required IT technical and services facilities (including computer systems, networks, applications, telecommunications, technical support and Service Desk) can be recovered within required, and agreed, business timescales
  - IT is a core component of most business processes
    - Availability of IT is key to business survival
    - 30% of businesses fail within the first four months after an IT disaster (Gartner)

- Successful implementation requires
  - Senior management commitment & support (IT and Business)
  - Ongoing maintenance, including exercises
  - Design into your processes, not as an afterthought

ITSCM Objectives

- Maintain service continuity plans (including IT) that support the organization’s overall BCP plans
- Complete regular (not OTO) Business Impact Analysis (BIA) exercises
  - Ensure plans are maintained in line with changing business impacts and requirements
- Conduct regular Risk Analysis and Management exercises
  - Business participates
- Provide guidance to other areas of the business and IT on continuity and recovery related issues

ITSCM Objectives (cont.)

- Ensure appropriate continuity & recover mechanisms are in place
  - Meet or exceed agreed to business continuity targets
    - Manual “work-arounds” are acceptable
- Assess the impact of changes on ITSCM
  - Will a change negate recoverability?
- Ensure proactive measures to improve the availability of services are implemented
  - Must be cost justified
- Negotiate and agree to necessary contracts with suppliers to provision your recovery solutions

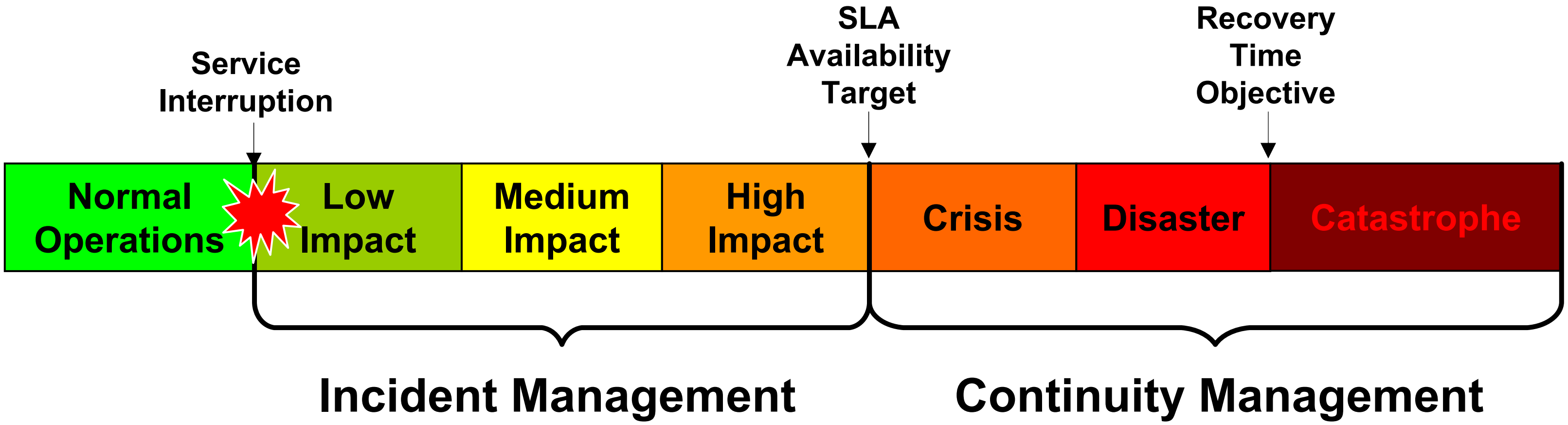
ITSCM Scope Includes

- Focus on events that the business considers significant enough to be considered a disaster
  - Others are incidents
  - Definition of a disaster varies by organization
  - Impact determined by BIAs

- IT technical and service requirements
  - Primary focus is IT assets and configurations that support business processes
  - Alternate work locations

ITSCM Scope Excludes

- Risks related to changes in business direction
  - Diversifications, restructuring, changes to your competitors etc.
- Non-declared disaster technical faults
  - Incident Management / Availability Management responsibilities



ITSCM Value

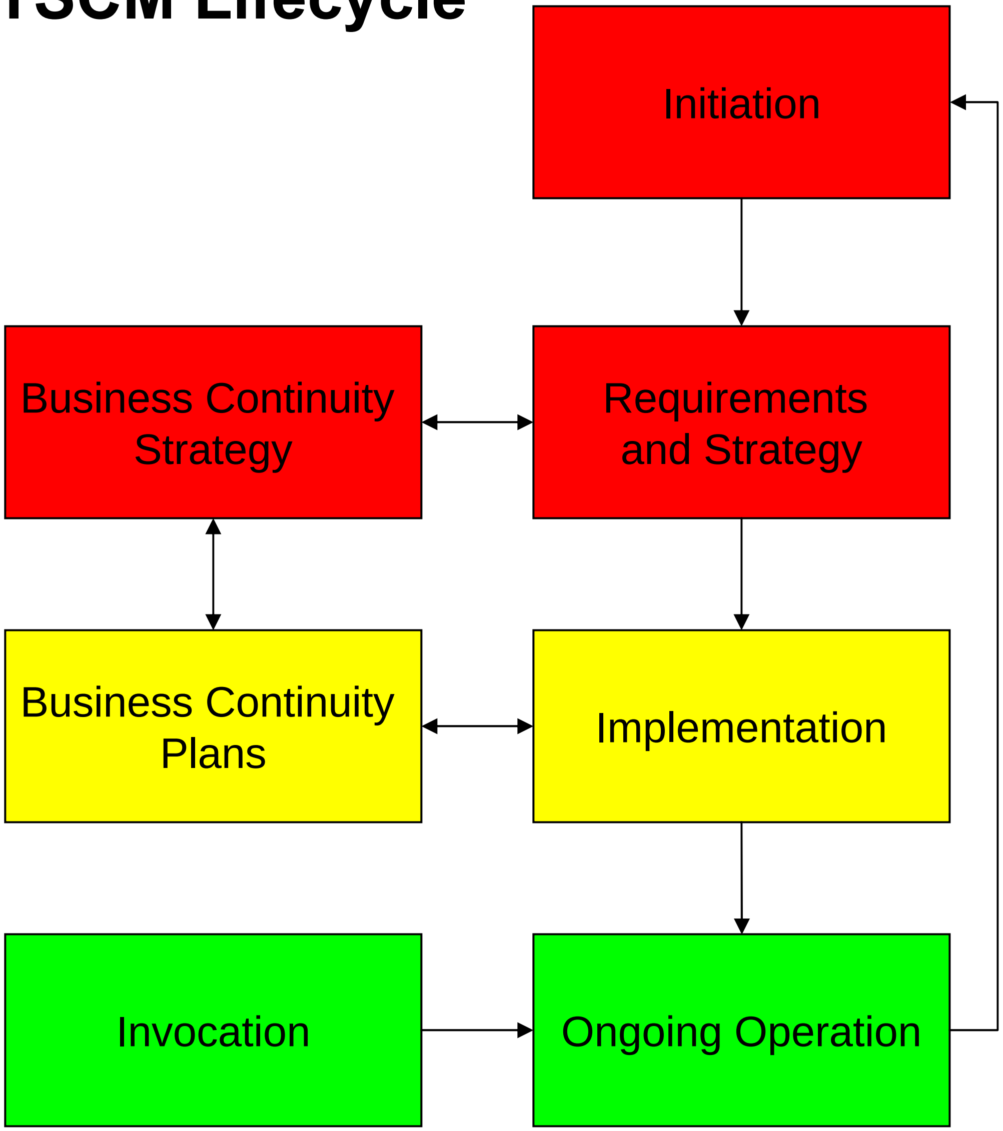
- Allows the business the ability to consciously decide what mitigation strategy to follow
- Although major events and service disruptions such as terrorism have often been the primary concern over recent years, there are many other risks that could result in serious disruption to the business and/or critical services
    - Service disruptions such as IT or telecommunications failure, viruses, failure of key third parties, localized fires and floods have caused much greater damage (overall) than high profile terrorist bombings

The Business Value of ITSCM

- Potential lower insurance premiums
  - The IT organization can help the organization demonstrate to underwriters or insurers that they are proactively managing down their business risks
- Regulatory requirements
  - In some industries a recovery capability is becoming a mandatory requirement such as health, defense, and financial industries
- Business relationship
  - The requirement to work closely with the business to develop and maintain a continuity capability fosters a much closer working relationship between IT and the business areas
- Positive marketing of contingency capabilities
  - Being able to demonstrate effective ITSCM capabilities enables an organization to provide high service levels to clients and customers and thus win business
- Organizational credibility
  - There is a responsibility on the directors of organizations to protect the shareholders’ interest and those of their clients
- Competitive advantage
  - Service organizations are increasingly being asked by business partners, customers and stakeholders to demonstrate their contingency facilities and may not be invited to tender for business unless they can demonstrate appropriate recovery capabilities

ITSCM Lifecycle (Activities)

ITSCM Lifecycle


Initiation
Business Continuity Strategy
Requirements and Strategy
Business Continuity Plans
Implementation
Invocation
Ongoing Operation

Business Continuity Management

IT Service Continuity Management

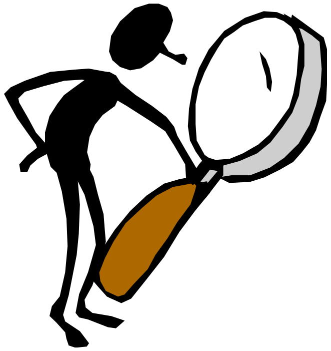
BCM or ITSCM?

- BCM
  - Initiation, Requirements, Business Continuity Strategy
    - BCM provides initial Business Impact and Risk Analysis activities
    - IT is just one service that your business relies on
    - ITSCM supports by producing a supporting ITSCM strategy
- ITSCM
  - Rest of the activities
- No BCM?
  - ITSCM performs all the activities

Initiation

- Policy setting
  - Define management intention and objectives
- Scope setting
  - Roles and responsibilities
  - BIA, Risk Analysis
  - “Command and Control” structure for an interruption
- Resource allocation
  - Don’t forget on-going maintenance
- Define project management structure
- Define metrics

Requirements and Strategy



- Requirements
  - Business Impact Analysis
    - Impact of a loss or damage
    - Damage escalation over time
    - Staffing/skills to enable critical business processes to continue
    - Time for minimal recovery
    - Time for all required processes to be recovered
    - Business process priority
    - RTO and RPO to prioritize
      - Recovery Point Objective – How much data can you lose?
      - Recovery Time Objective – When do you need the IT service?
    - Performance requirements
    - See Session 9222: How to Prepare a Balanced Business Impact Analysis on Thursday at 8 a.m.

Requirements and Strategy

- Requirements
  - Risk Assessment
    - Determine likelihood of a disaster
    - Level of threat and your vulnerability to each threat
    - Can use a simple spreadsheet
      - Category of Risk – Optional (natural disaster, etc.)
      - Issue/Risk - Briefly identify the risk or issue with which you are concerned
      - Risk Description (Explanation of Threat) - Describe the risk associated with the Issue/Risk identified in the previous column. Consider what can go wrong if this risk is not managed.
      - Potential Impact [1 (Low) to 5 (High)] - Identify the impact to your organization if the issue/risk were to occur
      - Likelihood [1 (Low) to 5 (High)] - Identify the likelihood of the issue/risk actually occurring
      - Risk Ranking - Can automatically generates the risk score by multiplying the Potential Impact by the Likelihood. The higher the number, the greater the risk to the organization
      - Risk Owner -Identify the organization or person who is responsible for managing/mitigating/accepting the risk. This can be internal or external to your organization.
      - Risk Mitigation Strategy - Identify how this risk is being managed/mitigated. Possible strategies may consist of existing policies and procedures; manual reviews; and technology to manage the risk.

Risks

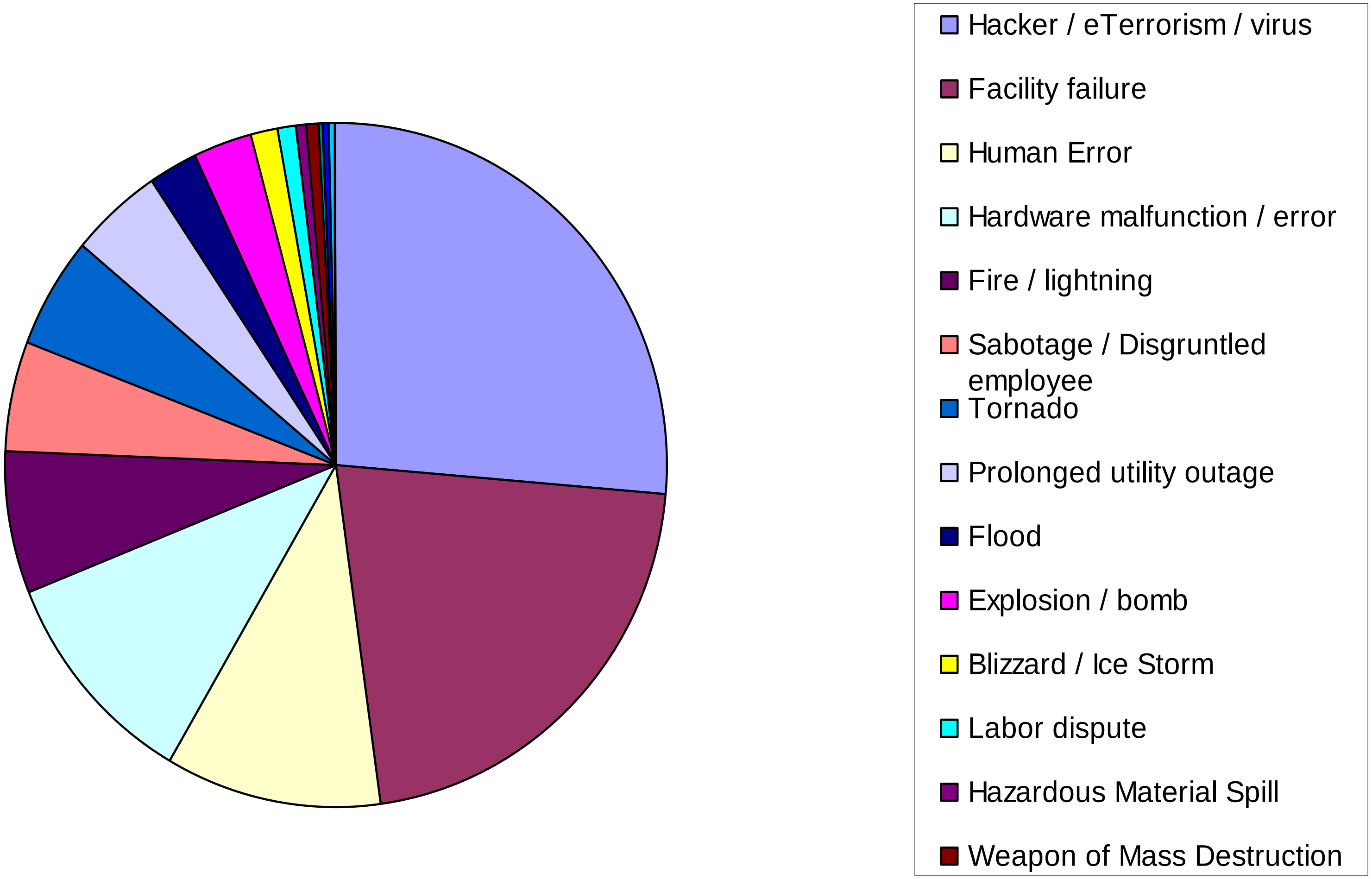
- ITSCM addresses risks that could cause a sudden and serious impact, such that they could immediately threaten the Continuity of the business
- These typically include things such as:
  - Loss, damage or denial of access to key infrastructure services
  - Failure or non-performance of critical providers, distributors or other third parties
  - Loss or corruption of key information
  - Sabotage, extortion or commercial espionage
  - Deliberate infiltration or attack on critical information systems

Some Known Causes for Disasters

A/C Failure
Acid Leak
Asbestos
Bomb Threat
Bomb Blast
Brown Out
Burst Pipe
Cable Cut
Chemical Spill
CO Fire
Condensation
Construction
Coolant Leak
Cooling Tower Leak
Corrupted Data
Diesel Generator
Earthquake
Electrical Short
Epidemic
Evacuation
Explosion
Fire
Flood
Fraud
Frozen Pipes
Hacker
Hail Storm
Halon Discharge
Human Error
Humidity
Hurricane
HVAC Failure
H/W Error
Ice Storm
Insects
Lightning
Logic Bomb
Lost Data
Low Voltage
Microwave Fade
Network Failure
PCB Contamination
Plane Crash
Power Outage
Power Spike
Power Surge
Programmer Error
Raw Sewage
Relocation Delay
Rodents
Roof Cave In
Sabotage
Shotgun Blast
Shredded Data
Sick building
Smoke Damage
Snow Storm
Sprinkler Discharge
Static Electricity
Strike Action
S/W Error
S/W Ransom
Terrorism
Theft
Toilet Overflow
Tornado
Train Derailment
Transformer Fire
UPS Failure
Vandalism
Vehicle Crash
Virus
Water (Various)
Wind Storm
Volcano

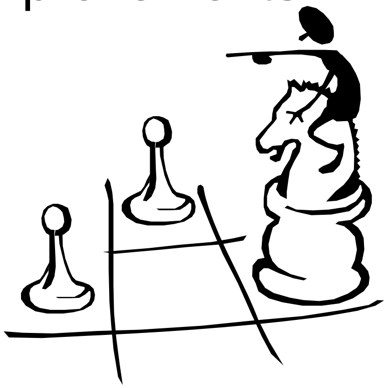
Source: Contingency Planning Research, Inc.

Sample Disaster Profile – Relative Likelihood of Causing a Remote Recovery



Requirements and Strategy

- Strategy
  - Optimum balance of risk reduction and recovery/continuity options
    - Consider priorities by time period
    - If services have high impact, consider availability improvements
    - Elimination of single points of failure
    - Comprehensive backup and recovery strategy
      - Off-site storage (including real-time mirroring)
    - Recovery options
      - May not need to recover all of IT at one time
    - Determine your recovery site **before** you need it
    - See Session 10038: A Business Continuity Solution Selection Methodology on Thursday at 9:30 a.m.
  - It is impossible to eliminate all risks
  - Invocation of a recovery is the last resort
    - Don’t be too quick to declare a disaster
    - More than IT implications in a disaster declaration

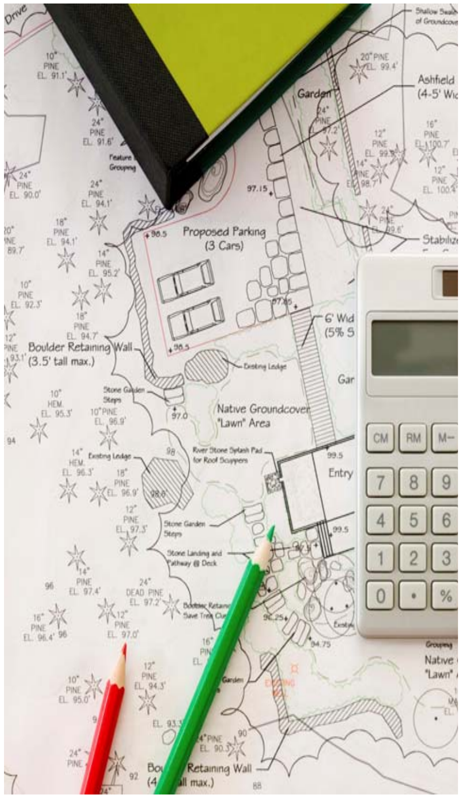


Implementation

- Develop continuity plans
- Develop IT plans, recovery plans and procedures
- Organization planning
- Develop exercise (testing) strategy
- Develop plan management & distribution strategy
- Include checklists in plans
- Don’t base plans on the “experts” being available
  - Assume a reasonable skill set level

Implementation – Continuity Plan

- Overall recovery plan
    - Emergency Response
    - Damage Assessment
    - Salvage
    - Vital Records
    - Crisis Management & Public Relations
    - Accommodation and Services
    - Security
    - Personnel
    - Communication
    - Finance and Administration
- Numerous teams



Implementation – IT Plans

- Ensure that all details related to recovery of the IT services are fully documented
- Contains ALL information needed for recovery the IT resources once a disaster declaration has been made
  - Plans may be “linked” and ordered; not 1 large document
  - RPO & RTO
  - Pre-req and dependent systems
  - Hardware & software requirements
    - Configuration details, etc.
  - Validation checklists
- Infrastructure and business application plans required

Implementation – Contents of an IT Plan

- Preliminary Planning
  - Purpose
  - Scope
  - Assumption
  - Responsibilities
  - Critical events
  - Strategies
- Preparatory Actions
  - People
  - Data
  - Software
  - Hardware
  - Documentation
  - Supplies
- Action Plan
  - Response
  - Recovery
  - Restoration
  - “Return to home”

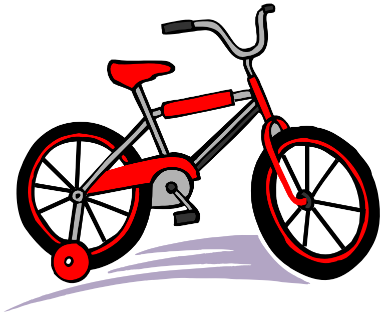
Implementation – Organization Planning

- In the event of a disaster, what will your organizational structure look like?
  - Executive
    - Overall authority and control
    - Responsible for crisis management, coordination with non-IT entities, etc.
  - Coordination
    - Responsible for coordinating the overall IT recovery effort
  - Recovery
    - Various IT and business teams for the critical business services and associated infrastructure that must be recovered
    - Group by IT service and application
- See Session 10037: Managing a Disaster: IT Crisis Management and Emergency Response Teams on Thursday at 11 a.m.

Implementation – Exercises (Testing)

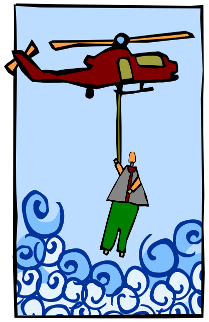
- Ensure that your processes and procedures will work in the event of a true disaster
- Types
  - Walk-throughs
  - Full tests
  - Partial tests
  - Scenario tests
- Involve IT and the business
- Defined objects and critical success factors
- Can’t test everything

Ongoing Operation



- Education, awareness and training
  - Ensure aware of implications of ITSCM
  - ITSCM becomes a way of doing business
- Reviews
  - Periodic review of processes to ensure currency
- Exercises
  - Periodic exercises, at least annually
    - After each major business changes also
  - Focus on critical components (at a minimum)
  - Include crisis management, disaster declaration, etc.
- Change Management
  - Ensure all changes assessed for their ITSCM plan impacts
    - If impacted, update ITSCM plans and test as part of change testing

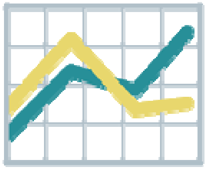
Invocation



- The ultimate test
- Decision typically made by senior management
- Implies disruption to the business
- Must be made in a timely fashion
- Plan should include aids to assist in declaration decision
  - Financial impacts
  - Business impacts
  - Consider recovery time and “return to home” time
- Recognize that recovery will be a time of high activity, long hours, etc.
  - Plan in advance for shifts and turnovers

ITSCM Is Important …

ITSCM is a Critical Tool



- Required to face the challenges of the future
- To continue to operate in spite of the multitude of risks faced, businesses must understand the business impact of service failure
- As businesses strive for greater efficiency, the use of technology and the consequent dependence upon it increases
  - Business must be able to sustain its operations
    - Failure to implement adequate ITSCM measures will impact your organization's ability and its perception following an interruption

ITSCM Must …

- Develop an infrastructure to respond quickly and efficiently to changes in an organization
- Be regularly validated to ensure that the different components of the IT environment will work together
- Consider (be developed with) the business
  - The ultimate choice of which option to choose, is made by the customer as part of the SLA agreements
  - Price has an obvious factor in selected the appropriate recovery option
  - Business processes rely more and more on IT Services and IT components are increasingly targeted for “attacks”

Don’t Forget …

- An important factor to remember when considering ITSCM is where the stakeholders fit into the scheme of things.
  - Not providing ITSCM could be seen as not protecting the stakeholders' investment which could reflect very poorly on senior IT Management, especially should there be a critical Business Continuity failure on an IT Infrastructure component.

Help is Available …

- At SHARE in Orlando
  - Sessions
  - Technology Exchange
  - Informal discussions with peers and technology experts

SHARE Orlando - Disaster Recovery & Business Continuity

	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday
8:00		General Session			9222: How to Prepare a Balanced Business Impact Analysis	9664: Mainframe Tape Without Tapes--Users Share Their Perspective
9:30		9298: Loading and Managing Master Keys on z/OS Hands-on Lab		9636: GDPS Overview and Recent Enhancements (Release 3.7 and 3.8)	10038: A Business Continuity Solution Selection Methodology	9536: I Got My Business Continuity, But Lost My Disaster Recovery
11:00			9406: IMS Disaster Recovery: Simplify and Improve IMS Administration + Coordinated Disaster Recovery for IMS and DB2 Double Session		10037: Managing a Disaster: IT Crisis Management and Emergency Response Teams	
1:30		9671: Managing SAN for Linux on z/VM - a Nationwide perspecive	9221: Compliance: How to Manage (Lame) Audit Recommendations	9947: Preserve System Integrity for Your Business With IBM Replication Solutions for Business Continuity (Part 1 of 2) 9476: Virtual Linux Server Disaster Recovery Planning	9894: Enhanced Disaster Recovery Options	
3:00		9844: Cloud Storage: Backups in the Cloud		9948: Preserve System Integrity for Your Business With IBM Replication Solutions for Business Continuity (Part 2 of 2) 9898: Implementing Oracle's StorageTek Cross TapePlex Replication (Or Not)	9303: Cryptography and Disaster Recovery (DR)	
4:30		10043 ITSCM Overview: ITIL's IT Disaster Recovery and Business Continuity Management	9936: DB2 for z/OS Backup and Recovery Update - V9 and V10	9969: Virtual Tape Replication Multi-Vendor Panel Discussion	9666: Beyond Disaster Recovery: Taking Your Enterprise from High Availability to Continuous Availability 9257: Intelligent Load Balancing with IBM Multi-Site Workload Lifeline	
6:00			9665: z/OS Data Replication as a Driver for Business Continuity			

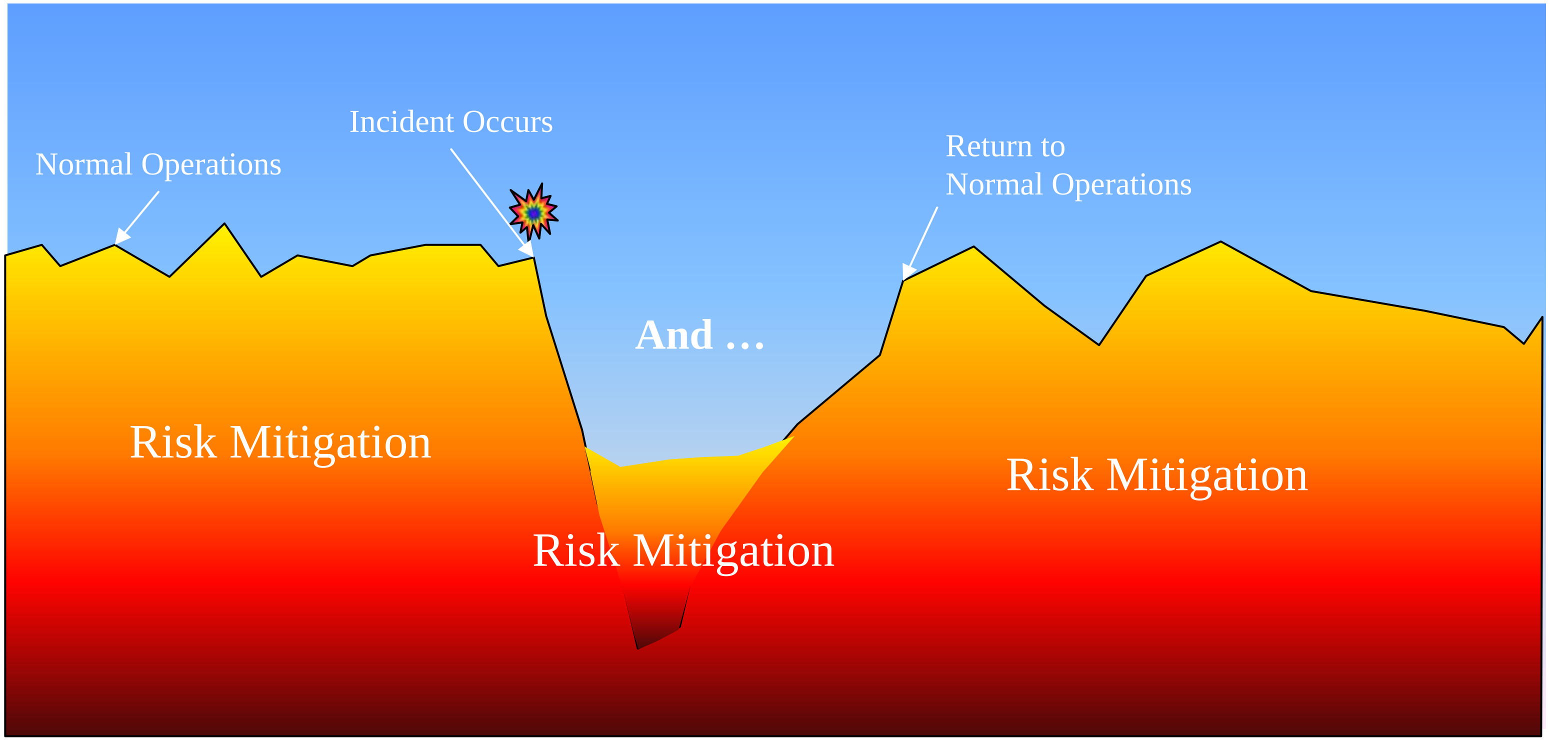
Useful Links

- http://www.itil-officialsite.com/home/home.aspx
- http://www.itilcommunity.com/index.php
- http://www.itilnews.com/IT_service_continuity_management.html
- http://www.conceptsolutionsbc.com/it-articles-mainmenu-34/167-it-service-continuity
- http://wiki.en.it-processmaps.com/index.php/Main_Page
  - http://wiki.en.it-processmaps.com/index.php/ITIL-Checklists#Checklists_for_IT_Service_Continuity_Management
- http://davehawley.com/ITIL/v2pre3/pages/ITIL_KB_Instance_19.html
- http://www.it-director.com/business/security/content.php?cid=9564
- http://www.isaca.lu/?q=system/files/Part%20two-3_Examples_ITIL_COBIT.pdf
- http://www.disasterrecovery.org/
- https://www.drj.com/tools/tools/sample-plans.html
- https://www.drj.com/tools/tools/glossary-2.html
- http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning/introduction.aspx
- Videos
  - http://www.youtube.com/watch?v=hR6jr_AaMUw&feature=related
  - http://www.youtube.com/watch?v=AA10-AMNR8M&feature=related
  - http://www.youtube.com/watch?v=m-5_3Q-3Wsw&feature=related
  - http://www.youtube.com/watch?v=-sj2_tX-dMY&feature=related

In Conclusion …

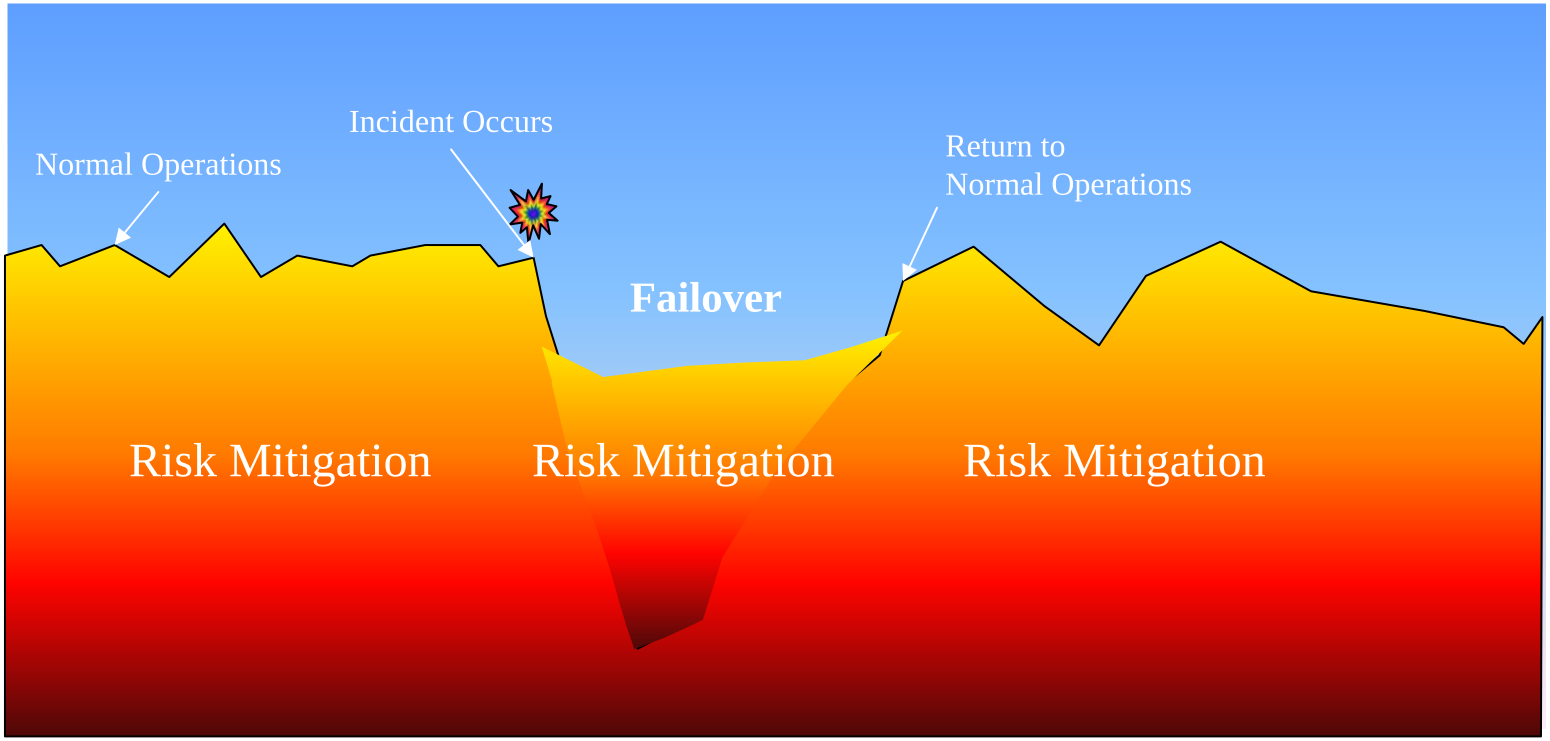
- IT Service Continuity Management is far more than just Disaster Recovery Planning
- IT Service Continuity Management prepares for the worst case scenario
  - Not just how to recover from disaster, but to stop the disaster from occurring in the first place, if at all possible
  - ITSCM investigates, develops and implements recovery options when an interruption to service reaches a pre-defined point

An Incident Occurs

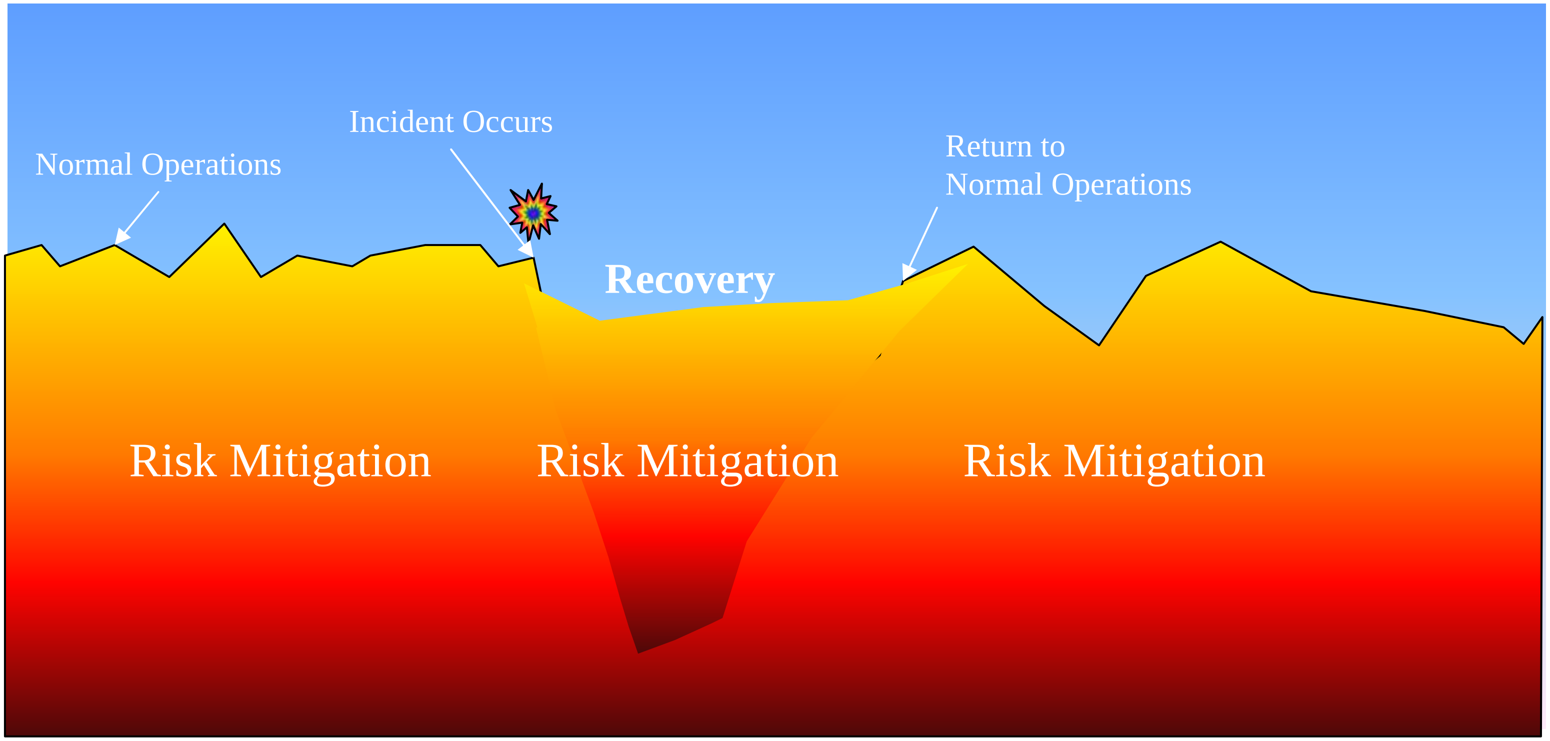


How deep do you want the crater to be?

Availability Management Can Help Some …



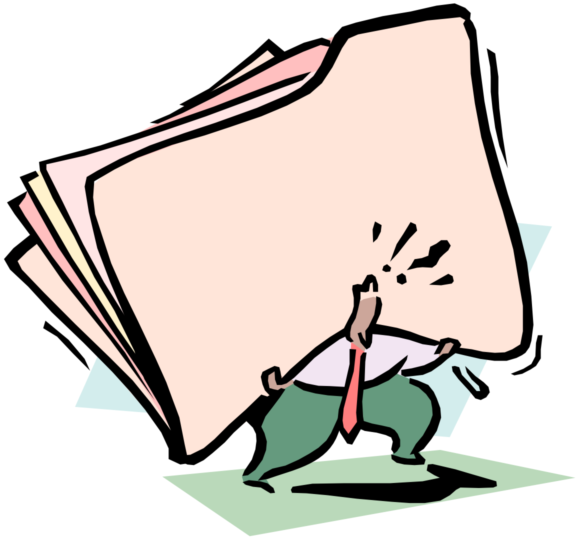
ITSCM Helps When the Incident is Larger Than a Component Failure



Questions and Answers

???

Terminology



ITIL - Acronyms Я Us

- ABC – Activity Based Costing
- ABM – Activity Based Management
- BCM – Business Continuity Management
- BEAST – Baseline, Estimation, Analysis, Simulation, Trends
- BIA – Business Impact Analysis
- BIL – Business Importance Level
- CAB – Change Advisory Board
- CAB/EC – CAB Executive Committee
- CDB – Capacity Database
- CFA – Component Failure Analysis
- CFIA – Component Failure Impact Analysis
- CI – Configuration Item
- CMDB – Configuration Management Database
- CRAMM – CCTA Risk Analysis and Management Method
- CRM - Customer Relationship Management
- DSL – Definitive Software Library
- DHS – Definitive Hardware Store
- FTA – Fault Tree Analysis
- IPKEC – Incident, Problem, Known Error, Change
- IRS-I-OM – Initiation, Requirements and Strategy, Implementation, Operational Management
- ITIL – Information Technology Infrastructure Library
- ITSCM – IT Service Continuity Management
- KPI – Key Performance Indicators

ITIL - Acronyms Я Us (cont.)

- KRA – Key Result Areas
- MARSS – Maintainability, Availability, Reliability, Serviceability, Security
- MTBF – Mean Time Between Failures
- MTTR – Mean Time To Repair
- OGC – Office of Government Commerce
- OLA – Operational Level Agreement
- PCWARD-NMP – Performance, Capacity Database, workload, application Sizing, resource, Demand, Network Management, Modeling, Plan
- RCAP – Resource Capacity Management
- RFC – Request For Change
- SCAP – Service Capacity Management
- SEATOP – Software, Equipment, Accommodation, Transfer, Organization, Provider
- SIP – Service Improvement Plan
- SLA – Service Level Agreement
- SLO – Service Level Objectives
- SLM – Service Level Management
- SLR – Service Level Requirements
- SOA – Systems Outage Analysis
- SOB – Service Opportunity Board
- SPAM – Support, Performance, Availability, Money
- TLA – Three Letter Acronym
- UC – Underpinning Contract
- VBF – Vital Business Function

ITSCM

- Disaster
  - Something that is NOT part of daily operational activities and requires a separate system
  - Not necessarily a flood, fire etc. but may be due to a blackout or power problem and the SLAs are in danger of being breached
- Business Continuity Management (BCM)
  - Strategies and actions to take place to continue Business Processes in the case of a disaster
  - Essential that the ITSCM strategy is integrated into and a subset of the BCM strategy
- Business Impact Analysis (BIA)
  - Quantifies the impact loss of IT service would have on the business
- Risk Assessment
  - Evaluate assets, threats and vulnerabilities that exist to business processes, IT services, IT infrastructure and other assets

Recovery Options

- Manual Workaround
  - Using non-IT based solution to overcome IT service disruption
- Gradual recovery
  - Aka Cold standby
  - >72 hours to recover from a ‘Disaster’
- Intermediate Recovery
  - Aka Warm standby
  - 24 – 72 hours to recover from a ‘Disaster’
- Immediate Recovery
  - Aka Hot standby
  - < 24 hours, usually implies 1 - 2 hours at most to recover from a ‘Disaster’
- Reciprocal Arrangement
  - Agreement with another similar sized company to share disaster recovery obligations