Using ITIL to Optimize Technology Risk Management

David Ratcliffe
President & CEO
Pink Elephant

Agenda …..

- WHY ITIL?
- WHERE did ITIL come from?
- WHAT exactly is ITIL?
- A definition for "best practices"
- Brief overview of the core ITIL processes & activities
- HOW does ITIL enable TRM?
- WHAT should you be doing?
- Appendix: supplementary planning slides

WHY ITIL?

- In the mid-80s, the UK government decided to stop *"re-inventing the wheel"* for purchasing and operating large scale IT systems
- "Process" and "standards" has been something of a way of life for the Brits
  - BSI ➔ ISO
- In summary: we have an opportunity – and need - to manage IT more like a business, with a focus on marketing & delivering optimized IT services

 3

WHERE did ITIL come from?

- In 1987 the CCTA (now called OGC) initiated a project called GITIMM (Government IT Infrastructure Management Method).
- The term "IT Service Management" was not quite so prevalent at this time – "Infrastructure Management" was the name of the game.
- They began commissioning various consulting firms (Pink Elephant, among many others) to research and document "best practices" for planning & operating IT infrastructures.
- The private sector soon became interested. Just prior to publication of the first ITIL book - "Help Desk" - in 1989, GITIMM was renamed ITIL.

 4

WHAT exactly is ITIL?

- A documented set of *best practices* - not a methodology - for aligning IT services with business requirements
- Provides overall guidance, not a step-by-step how-to manual; therefore the implementation of ITIL processes needs to be adapted & customized from organization to organization
- Provides *optimal service provision* at a *justifiable cost*
- Non-proprietary
- Technology/platform independent

 5

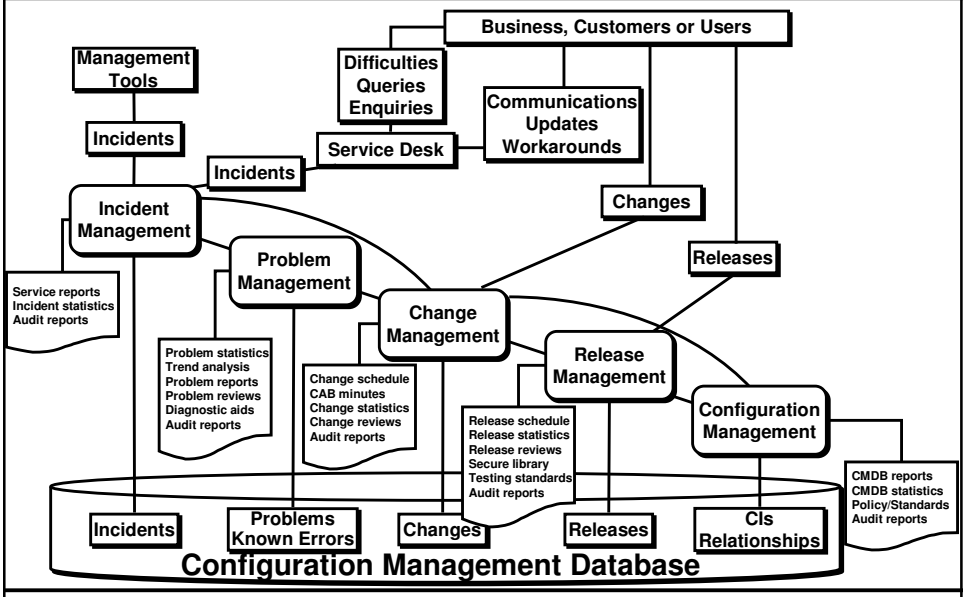
A Definition of Best Practices

- The application of common sense; not rocket-science
- Proven & practical activities which are in common use
- Replaces
  - **"chaos"**
  - **"random results"**
  - **"best efforts"**

    with
  - **"order"**
  - **"predictable quality"**
  - **"optimization"**
- And by the way, when was the last time you needed an ROI justification to apply common sense?

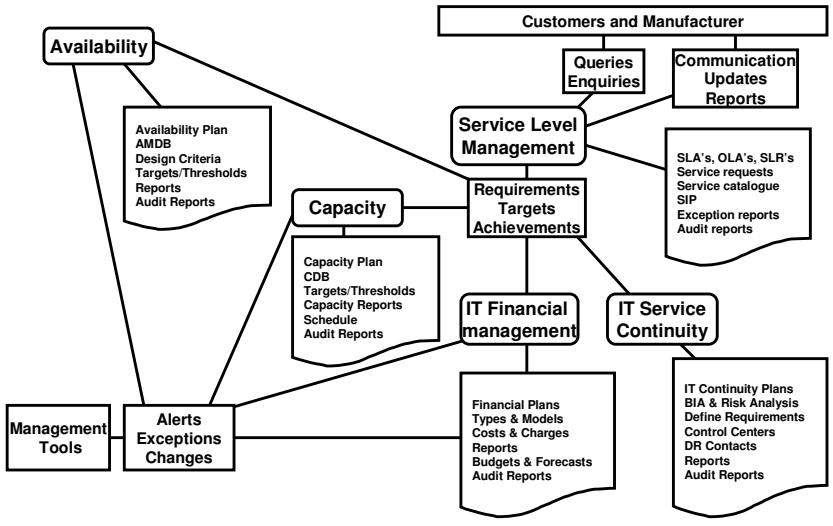
 6

Service Support



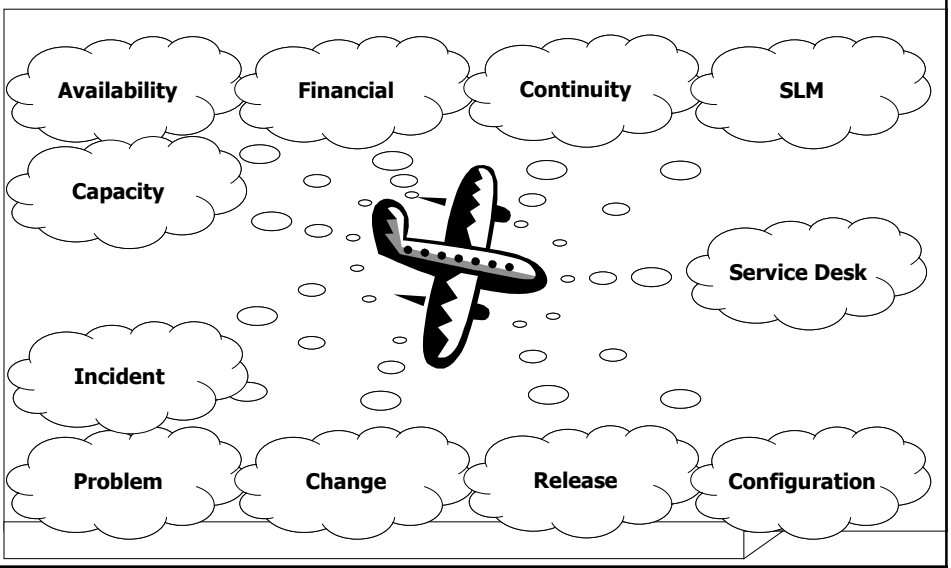
 7

Service Delivery



 8

And just in case you came in late …



 9

HOW does ITIL enable TRM?

- What do we have in the infrastructure?
  - Configuration Management (relationships & impact)
  - Change Management (controlling the evolution)
- What services do we deliver?
  - Service Level Management
- What are our strengths/weaknesses/risks in managing services?
  - Security Management (policies for "CIA")
  - Capacity Management (aligning resources & business demand)
  - Availability Management (reducing operational risks)
  - IT Service Continuity Management (managing through a "crisis")
  - Service Desk (capturing & analyzing data on service quality)

 10

WHAT should you be doing?

Generally:

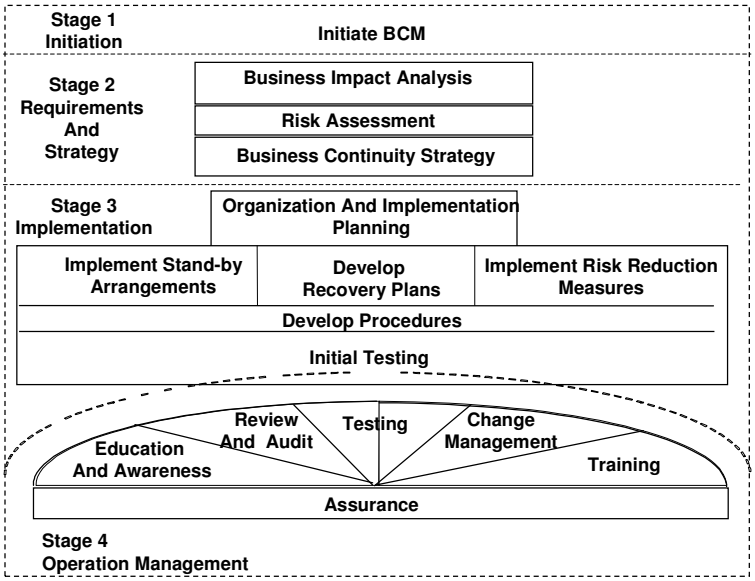
- Increase ITIL awareness
- Evaluate and improve your IT service management processes and tools

Specifically in relation to TRM:

- Improve awareness & control of the IT infrastructure & services
- Embrace the 4 stage IT Service Continuity Lifecycle

 11

Activities – The Four Stages



 12

Using ITIL to Optimize Technology Risk Management

David Ratcliffe
President & CEO
Pink Elephant

Copy of all slides can be found at
www.pinkelephant.com

Review of Key Definitions

- Crisis
  - An unplanned situation in which it is expected that the period during which one or more IT services will be unavailable will exceed threshold values agreed to with the customer.
- Risk = Assets + Threats + Vulnerabilities
- Do nothing
- Manual Work-around
- Reciprocal Arrangements
- Gradual Recovery a.k.a Cold Standby
- Intermediate Recovery a.k.a Warm Standby
- Immediate Recovery a.k.a Hot Standby

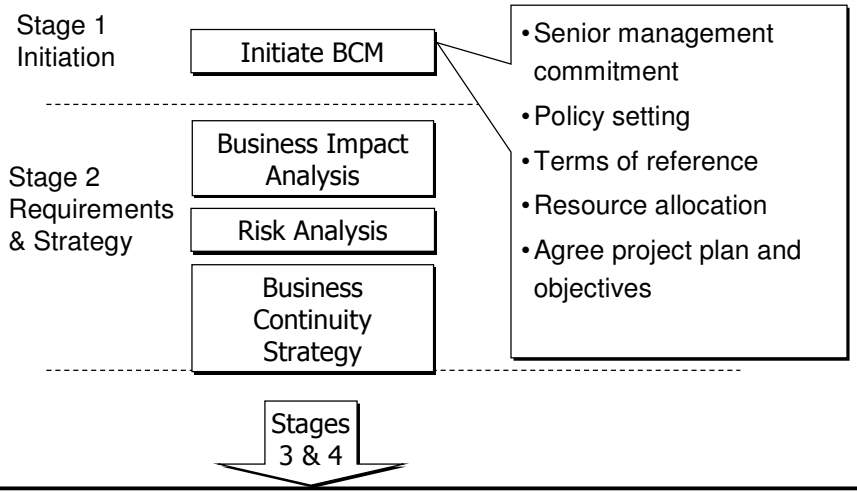
 14

Relationship Between BCM and ITSCM

- Business Continuity Management (BCM) is concerned with the management of business continuity that incorporates all services upon which the business depends, one of which is IT
- IT Service Continuity Management (ITSCM) is focused on the continuity of IT Services to the business
- The dependence upon technology and the greater demands being placed upon organizations require ITSCM to become an integral part of Corporate Management in order for business objectives and targets to be achieved and maintained

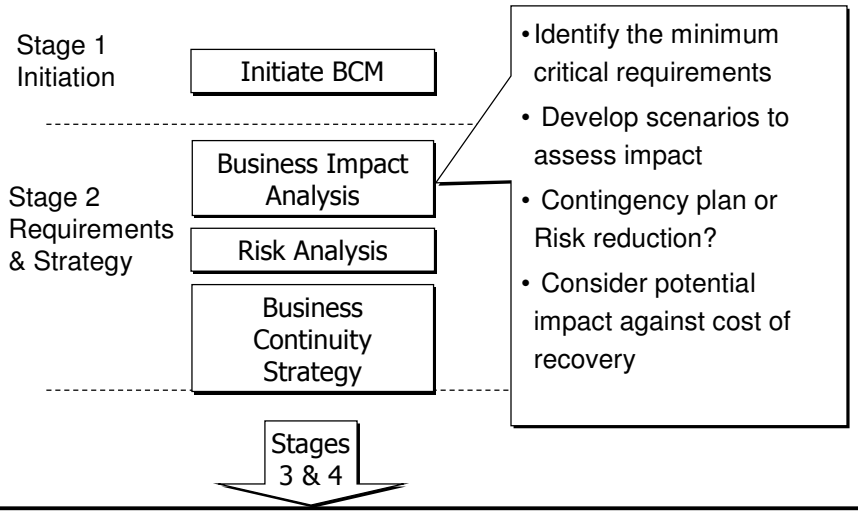
 15

IT Service Continuity Lifecycle



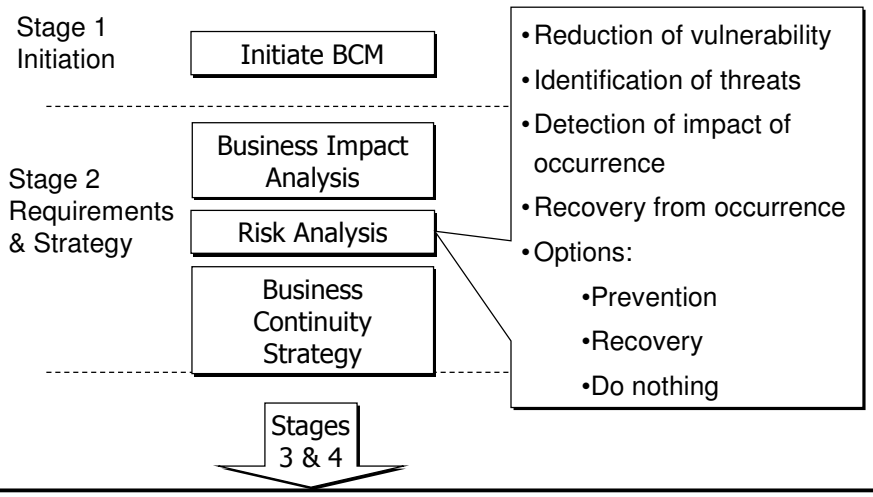
 16

IT Service Continuity Lifecycle



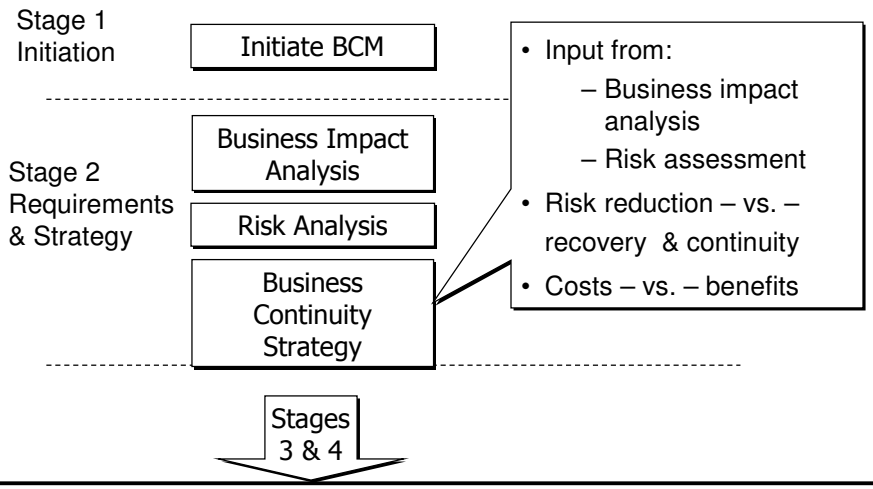
 17

IT Service Continuity Lifecycle



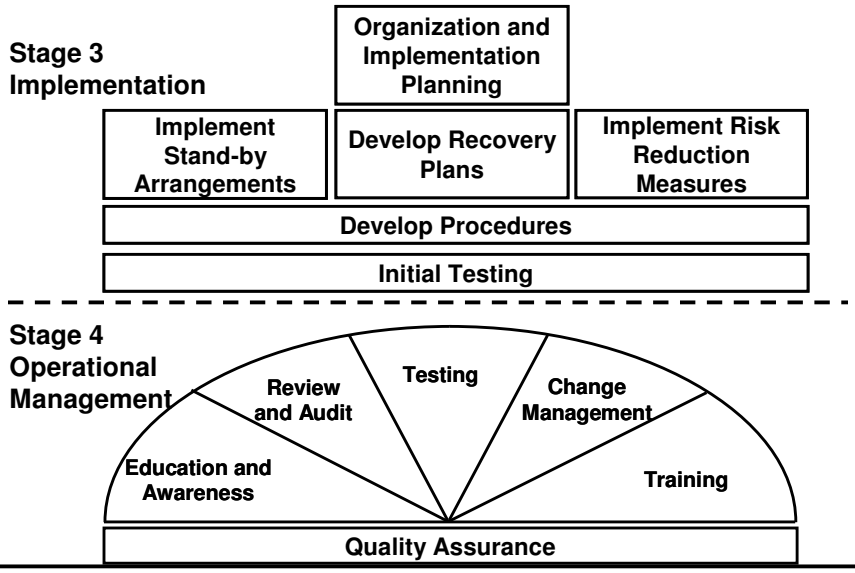
 18

IT Service Continuity Lifecycle



 19

Lifecycle Stages 3 & 4



 20

Implementation planning

Plan development is one of the most important parts of the implementation process and without workable plans the process will certainly fail. At the highest level there is a need for an overall co-ordination plan that includes:

- Emergency Response Plan
- Damage Assessment Plan
- Salvage Plan
- Vital Records Plan
- Crisis Management and Public Relations Plan

Implementation planning

These plans are used to identify and respond to a service disruption, ensure the safety of all affected staff members and visitors and determine whether there is a need to implement the business recovery process. If so, then the next level of plans are invoked which include the key support functions such as:

- Accommodation and Services Plan
- Computer Systems and Network Plan
- Telecommunication Plan
- Security Plan
- Personnel Plan
- Finance and Administration Plan

An ITSCM Generic Recovery Plan

1. **Document Control** — Self-evident
2. Supporting information
   a) Introduction
   b) Recovery strategy
   c) Invocation
   d) General guidance
   e) Dependencies
   f) Recovery teams
   g) Recovery teams checklist
3. Recovery procedure

ITSM Generic Recovery Plan

1. Document control
   a) Document distribution
   b) Document revision
   c) Document approval
2. Supporting information
   a) Introduction
   b) Recovery strategy
   c) Invocation
   d) General guidance
   e) Dependencies
   f) Recovery team
   g) Recovery team checklist
3. Recovery procedure

- This document must be maintained to ensure that the systems, infrastructure and facilities included, appropriately support business recovery requirements.
- This document will be reviewed every X months.
  Current Revision: date
  Next Revision: date
- This document must be approved by the following personnel…

Tactical Inputs

From Availability Management

- System Outage Analysis — SOA
- Fault Tree Analysis — FTA
- Component Failure Impact Analysis — CFIA

From Service Level Management

- Service Level Agreements — SLA
- Underpinning Contracts — UC

From the Business

- Vital Business Functions — VBF

ITSM Generic Recovery Plan

1. Document control
   a) Document distribution
   b) Document revision
   c) Document approval
2. Supporting information
   a) Introduction
   b) Recovery strategy
   c) Invocation
   d) General guidance
   e) Dependencies
   f) Recovery team
   g) Recovery team checklist
3. Recovery procedure

Word from Senior Management
Crisis definitions
Assessment results
Initiatives

ITSM Generic Recovery Plan

1. Document control
   a) Document distribution
   b) Document revision
   c) Document approval
2. Supporting information
   a) Introduction
   b) Recovery strategy
   c) Invocation
   d) General guidance
   e) Dependencies
   f) Recovery team
   g) Recovery team checklist
3. Recovery procedure

- Vital Business Functions
- Recovery times
- Recovery options

 27

ITSM Generic Recovery Plan

1. Document control
   a) Document distribution
   b) Document revision
   c) Document approval
2. Supporting information
   a) Introduction
   b) Recovery strategy
   c) Invocation
   d) General guidance
   e) Dependencies
   f) Recovery team
   g) Recovery team checklist
3. Recovery procedure

- Who can invoke the plan?
- When
- Conditions
- Parameters
- How long it should take

 28

ITSM Generic Recovery Plan

1. Document control
   a) Document distribution
   b) Document revision
   c) Document approval
2. Supporting information
   a) Introduction
   b) Recovery strategy
   c) Invocation
   d) General guidance
   e) Dependencies
   f) Recovery team
   g) Recovery team checklist
3. Recovery procedure

- Roles during normal operations
- Roles during a crisis
- Escalations
- Emergency Response Plan
- Damage Assessment Plan
- Salvage Plan
- Vital Records Plan
- Crisis Management and Public Relations Plan

ITSM Generic Recovery Plan

1. Document control
   a) Document distribution
   b) Document revision
   c) Document approval
2. Supporting information
   a) Introduction
   b) Recovery strategy
   c) Invocation
   d) General guidance
   e) Dependencies
   f) Recovery team
   g) Recovery team checklist
3. Recovery procedure

- Vital Business Functions
- Service Level Requirements
- Accommodation and Services Plan
- Computer Systems and Network Plan
- Telecommunication Plan
- Security Plan
- Personnel Plan
- Finance and Administration Plan

ITSM Generic Recovery Plan

1. Document control
   a) Document distribution
   b) Document revision
   c) Document approval
2. Supporting information
   a) Introduction
   b) Recovery strategy
   c) Invocation
   d) General guidance
   e) Dependencies
   f) Recovery team
   g) Recovery team checklist
3. Recovery procedure

Name	Title	Contact Details

 31

ITSM Generic Recovery Plan

1. Document control
   a) Document distribution
   b) Document revision
   c) Document approval
2. Supporting information
   a) Introduction
   b) Recovery strategy
   c) Invocation
   d) General guidance
   e) Dependencies
   f) Recovery team
   g) Recovery team checklist
3. Recovery procedure

Task	Target Completion	Actual Completion
Confirm Invocation has taken place		
Initiate call tree and establish recovery team		
Identify issues and advise Crisis management Team		
Arrange for backup media, vital records to be shipped from off-site store to recovery site		
Establish recovery team rota		
Confirm progress reporting requirements		
Inform recovery team of reporting requirements		
Confirm liaison requirements with other recovery teams		
Initiate recovery actions		
Advise the estimate for System recovery and commencement of testing		
Advise estimate for when systems will be ready for User processing.		

 32

ITSM Generic Recovery Plan

1. Document control
   a) Document distribution
   b) Document revision
   c) Document approval
2. Supporting information
   a) Introduction
   b) Recovery strategy
   c) Invocation
   d) General guidance
   e) Dependencies
   f) Recovery team
   g) Recovery team checklist
3. **Recovery procedure**

Where necessary, references should be made to supporting documentation (and its location), diagrams and other information sources. This should include the document reference number (if it exists). It is the responsibility of the plan author to ensure that this information is maintained with this plan. If there is only a limited amount of supporting information, it may be easier for this to be included within the plan, providing this plan remains easy to read/follow and does not become too cumbersome.

 33

Items to Review

Is the ITSCM plan updated and related to the business needs?
- Critical Services / Vital Functions
- Critical windows
- Security
- New Services
- SLAs

Is the staffing requirement current and adequately trained?
- Adequate Skills
- Call procedures
- Responsibilities
- Personnel turn over rate

 34

Reporting, Reviewing & Auditing

Management Information

- Historical data on incidents, problems, emergencies and disasters
- Number and details of changes that require updates to the contingency plan
- Percentage of changes that have caused major issues
- CI details including dependencies, relationships and criticality
- Security data and requirements
- SLA review information

Items for reviewing

- Analysis of services
- Test Results – Lessons Learned
- Plan contents

Auditing for compliance

- Test Results Improvements
- Contract review details
- Plans reviewed and updated

 35