IT Risk Management Guide

Risk Management Implementation Guide - Presentations Blueprints, Templates; Complete Risk Management Toolkit Guide for Information Technology Processes and Systems

Gerard Blokdijk

IT Risk Management Guide

Risk Management Implementation Guide,
Presentations, Blueprints, Templates;

Complete Risk Management Toolkit Guide for
Information Technology Processes and Systems

Gerard Blokdijk,
Claire Engle & Jackie Brewster

Notice of Rights

Notice of Liability

The information in this book is distributed on an “As Is” basis without warranty. While every precaution has been taken in the preparation of the book, neither the author nor the publisher shall have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the instructions contained in this book or by the products described in it.

Trademarks

Many of the designations used by manufacturers and sellers to distinguish their products are claimed as trademarks. Where those designations appear in this book, and the publisher was aware of a trademark claim, the designations appear as requested by the owner of the trademark. All other product names and services identified throughout this book are used in editorial fashion only and for the benefit of such companies with no intention of infringement of the trademark. No such use, or the use of any trade name, is intended to convey endorsement or other affiliation with this book.

Table of Contents

1 INTRODUCTION ROADMAP

Many organizations are looking to implement Risk Management as a way to improve the structure and quality of the business.

This document describes the contents of the Risk Management Guide. The information found within the Guide is based on the ITIL Version 3 framework, focusing on the processes of Information Security Management and IT Service Continuity Management. In addition, to these processes are the methodologies supported by ITIL Version 3 e.g. M_o_R and CRAMM which are considered 'best practice' all over the world.

There are also valuable insights into managing risks within Project Management.

The Guide is designed to answer a lot of the questions about Risk Management and provide you with useful guides, templates and essential, but simple assessments.

The assessments and questionnaire will help you identify the areas within your organization that require the most activity in terms of change and improvement.

Presentations can be used to educate or be used as the basis for management presentations or when making business cases for Risk Management implementation.

The additional information will enable you to improve your organizations methodology knowledge base.

The book serves to act as a starting point. It will give you a clear path to travel. It is designed to be a valuable source of information and activities.

The Risk Management Guide:

- Flows logically,
- Is scalable,
- Provides presentations, templates and documents,
- Saves you time.

1.1 Step 1

Start by reviewing the PowerPoint presentations in the following order:

1. **Risk Management Intro Presentation**

   This concise presentation gives a great introduction to the book, covering definitions, general concepts and the foundations of Risk Management.

2. **Risk Management ITIL V3 – ITSCM**

3. **Risk Management ITIL V3 – ISM**

4. **Risk Management – Project Management**

   Presentations 2 – 4 provide a detailed and comprehensive overview of Risk Management in each of the specialist areas of ITIL Version 3 IT Service Continuity Management, Information Security Management and Project Management.

These presentations will give you a good knowledge and understanding of all the terms, activities and concepts required within Risk Management. They can also be used as the basis for management presentations or when making a formal business case for Risk Management implementation. Make sure you pay close attention to the notes pages, as well as the slides, as references to further documents and resources are highlighted here.

1.2 Step 2

If you did not look at the supporting documents and resources when prompted during the PowerPoint presentations, do this now. Below is an itemized list of the supporting documents and resources for easy reference. You can use these documents and resources within your own organization or as a template to help you in prepare your own bespoke documentation.

Risk Management ITIL V3 – ITSCM:

1. **ITSCM Reciprocal Arrangements**

   Concise example of a user friendly agreement that can be used as a template for your organization.

2. **ITSCM Business Impact Assessment**

   Example of a complete and easy to use assessment that can be used as a template for your organization.

3. **Management of Risk Framework M_O_R**

   A detailed overview of the M_o_R methodology with written explanation and supporting diagrams. This methodology is supported within the ITIL version 3 framework.

4. **IT Risk Assessment Planning**

   An easy to follow guide on what should and should not be covered within your Risk Assessment.

5. **IT Risk assessment Score Sheet**

   A comprehensive and ready to use score sheet, to score your risk factors.

6. **Risk Assessment and Control Form**

   A detailed and user friendly template that include prompts and advice and can be used within your organization.

7. **Risk Assessment Questionnaire**

   This is am extremely useful document that is ready to use and distribute for the purpose of obtaining feedback from staff within your organization.

8. **ITSCM Business Continuity Strategy**

   A comprehensive and user friendly template and procedure that can be used as a resource within your organization.

9. **Typical Contents of a Recovery Plan**

   In accordance with the ITIL Version 3 framework and the ITSCM process. This is a list of the typical contents for a continuity recovery plan.

10. **ITSCM Communication Plan**

    Concise example of a user friendly template and procedure that can be used as a template for your organization.

11. **ITSCM E-Mail Text**

    Concise example of a user friendly template and procedure that can be used as a template for your organization.

12. **ITSCM Emergency Response Plan**

    A detailed and comprehensive example of a user friendly template that can be used as a template for your organization.

13. **ITSCM Salvage Plan Template**

    Concise example of a user friendly template and procedure that can be used as a template for your organization.

Step 2 continued...

Risk Management ITIL V3 – ISM:

1. **CRAMM**

   Overview of the widely used CRAMM methodology and how it can be effective when used within a work environment.

Risk Management – Project Management:

1. **Checklist on Assignment of Risk Ownership**

   Complete checklist you can use to ensure conformance to the PRINCE2 methodology, when assigning Risk Owners.

2. **Generic Project Risk Assessment**

   Concise example of a user friendly template and procedure that can be used as a template for your organization.

Alternatively, continue by working through the **Risk Management Framework** document and the **Conducting a Risk Management Review** document with the focus on your organization. This will help you ascertain the Risk Management maturity for your organization. You will able to identify gaps and areas of attention and/or improvement.

The supporting documents and resources found within the book will help you fill these gaps by giving you a focused, practical and user-friendly approach to Risk Management.

1.3 Risk Management – INTRO PRESENTATION

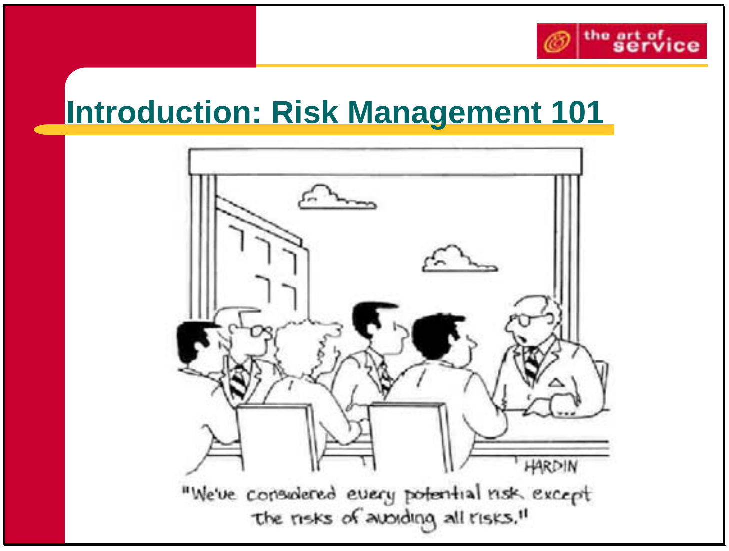
1.3.1 Slide 1: Intro to Risk Management (RM)

Introduction to Risk Management

Welcome

the art of service

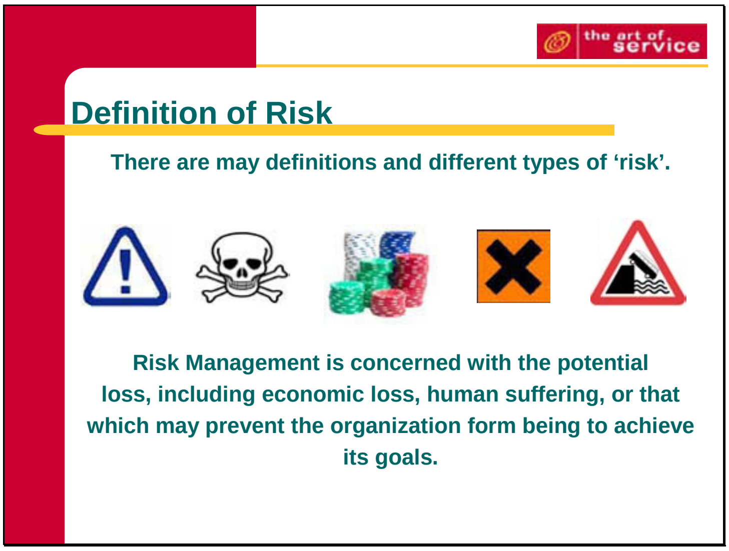
1.3.2 Slide 2: RM 101



Introduction: Risk Management 101

"We've considered every potential risk except the risks of avoiding all risks."

1.3.3 Slide 3: Definition of Risk

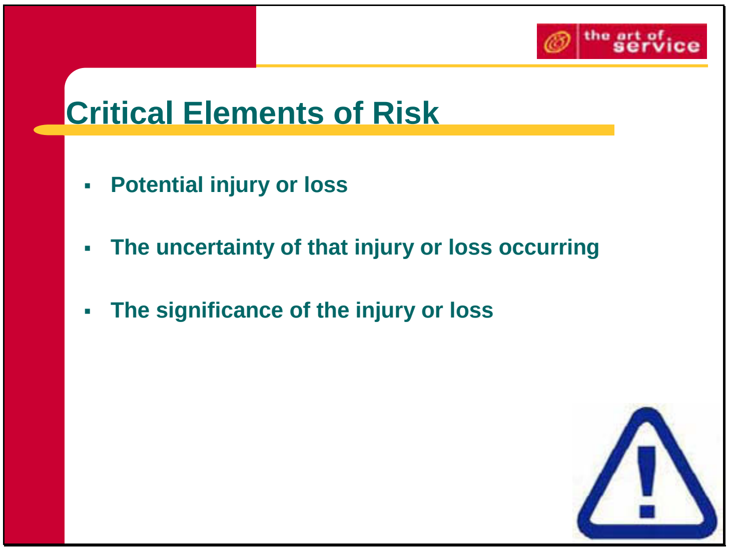


Definition of Risk

There are may definitions and different types of ‘risk’.

Risk Management is concerned with the potential loss, including economic loss, human suffering, or that which may prevent the organization form being to achieve its goals.

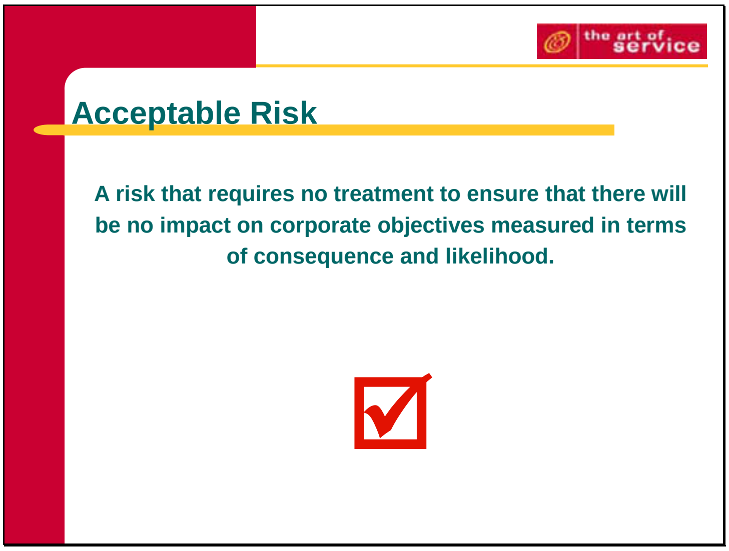
1.3.4 Slide 4: Critical Elements of Risk



Critical Elements of Risk

- Potential injury or loss
- The uncertainty of that injury or loss occurring
- The significance of the injury or loss

1.3.5 Slide 5: Acceptable Risk

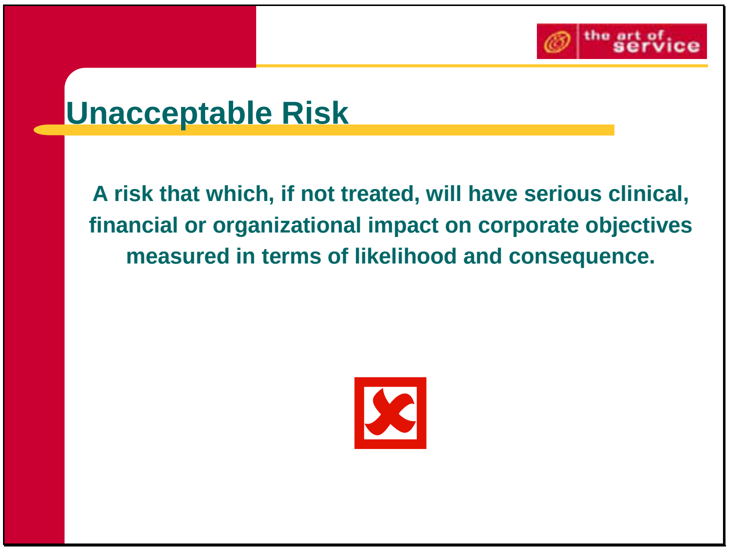


Acceptable Risk

A risk that requires no treatment to ensure that there will be no impact on corporate objectives measured in terms of consequence and likelihood.

☑

1.3.6 Slide 6: Unacceptable Risk

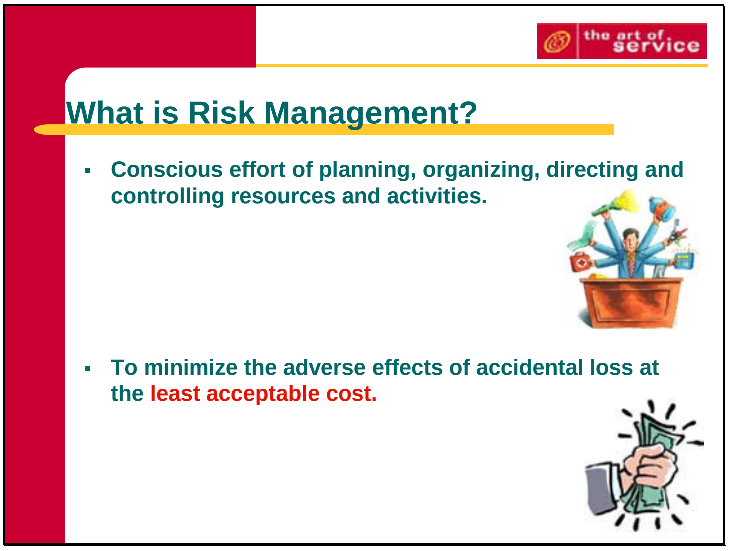


the art of service

Unacceptable Risk

A risk that which, if not treated, will have serious clinical, financial or organizational impact on corporate objectives measured in terms of likelihood and consequence.

1.3.7 Slide 7: What is RM?

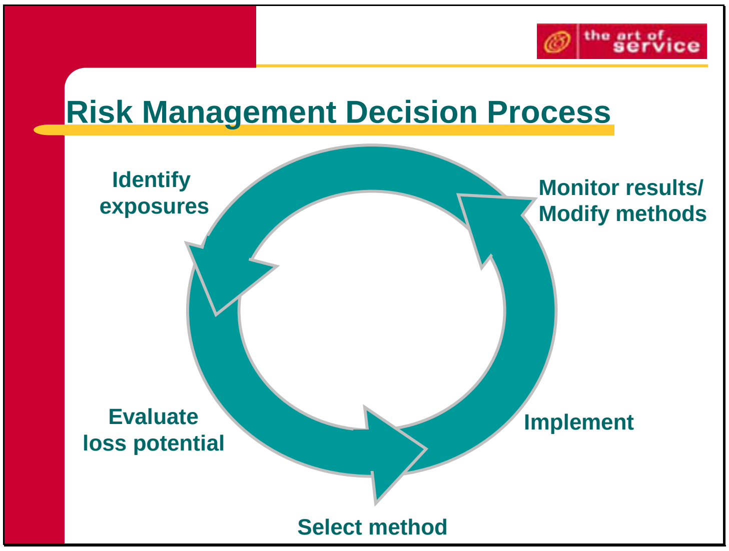


What is Risk Management?

- Conscious effort of planning, organizing, directing and controlling resources and activities.
- To minimize the adverse effects of accidental loss at the least acceptable cost.

To meet the organization's specific needs, a successful risk management program must balance risk control and risk financing techniques while considering the organization's mission, vision, values and goals.

1.3.8 Slide 8: RM Decision Process



Risk Management Decision Process

Identify:

- Possible losses and damages to human and physical resources
- Where the exposure comes from
- How frequently they occur and their severity.

Evaluate:

Risk Management techniques – we take calculated risks.

Select:

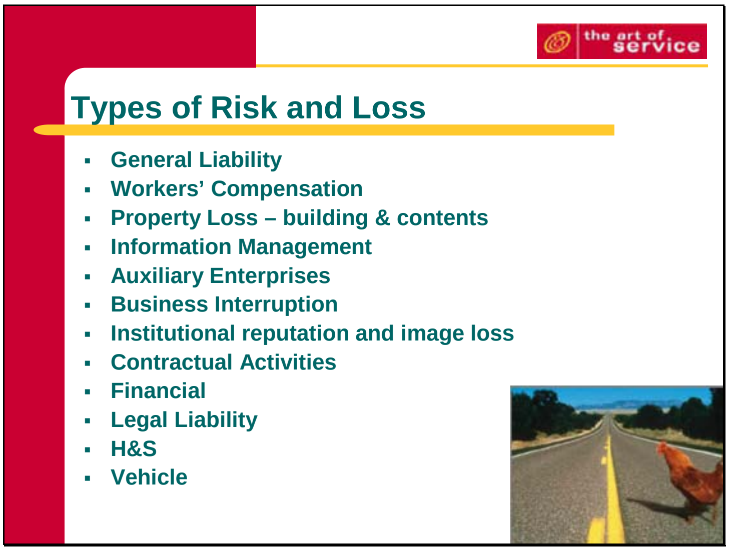
Appropriate techniques

Implement:

Chose and use techniques.

Monitor and **Modify** as required.

1.3.9 Slide 9: Types of Risk & Loss

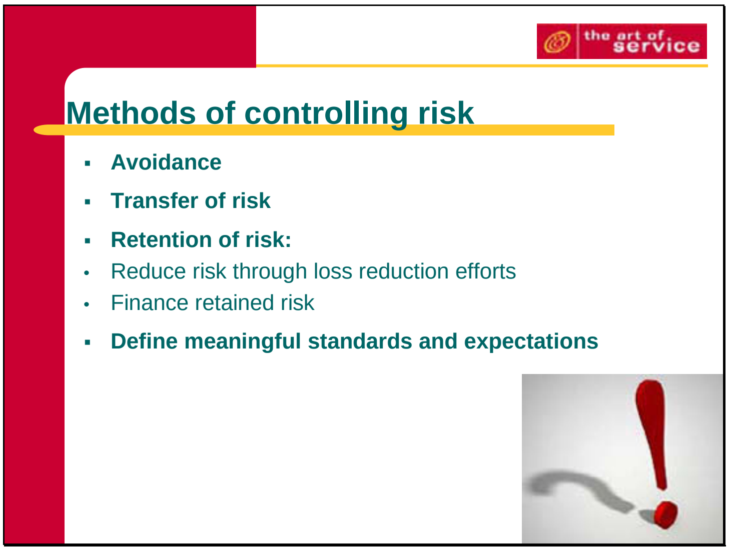


the art of service

Types of Risk and Loss

- General Liability
- Workers' Compensation
- Property Loss – building & contents
- Information Management
- Auxiliary Enterprises
- Business Interruption
- Institutional reputation and image loss
- Contractual Activities
- Financial
- Legal Liability
- H&S
- Vehicle

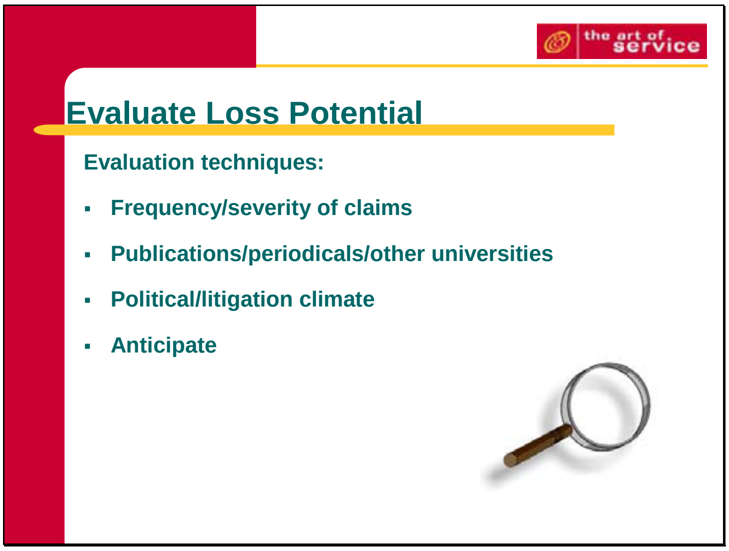
1.3.10 Slide 10: Methods of Controlling Risk



Methods of controlling risk

- **Avoidance**
- **Transfer of risk**
- **Retention of risk:**
- Reduce risk through loss reduction efforts
- Finance retained risk
- **Define meaningful standards and expectations**

1.3.11 Slide 11: Evaluate Loss Potential

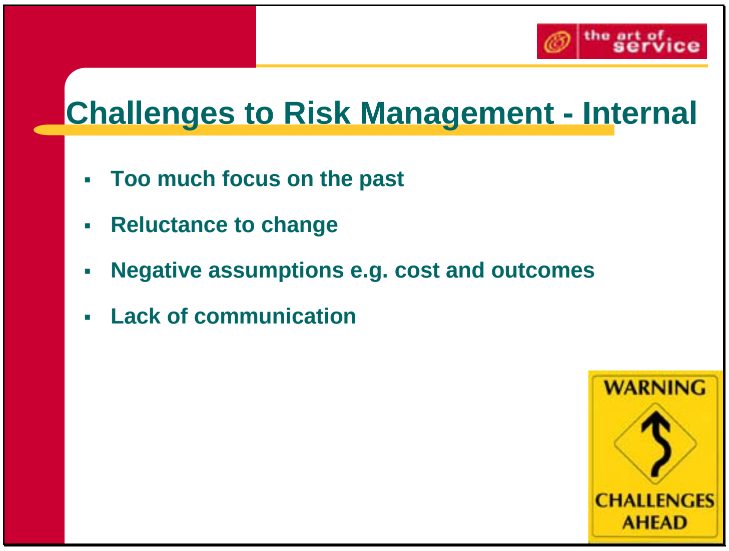


Evaluate Loss Potential

Evaluation techniques:

- Frequency/severity of claims
- Publications/periodicals/other universities
- Political/litigation climate
- Anticipate

1.3.12 Slide 12: Challenges to RM – Internal

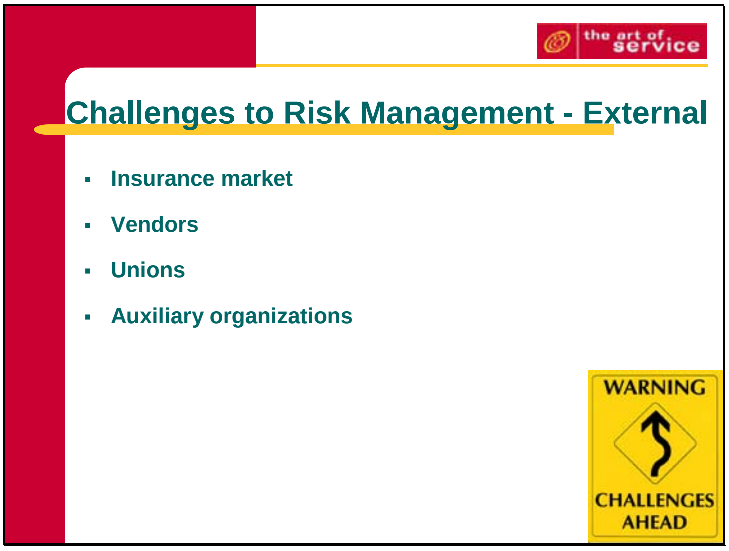


Challenges to Risk Management - Internal

- Too much focus on the past
- Reluctance to change
- Negative assumptions e.g. cost and outcomes
- Lack of communication

the art of service
WARNING
CHALLENGES
AHEAD

1.3.13 Slide 13: Challenges to RM – External



the art of service

Challenges to Risk Management - External

- Insurance market
- Vendors
- Unions
- Auxiliary organizations

WARNING
CHALLENGES AHEAD

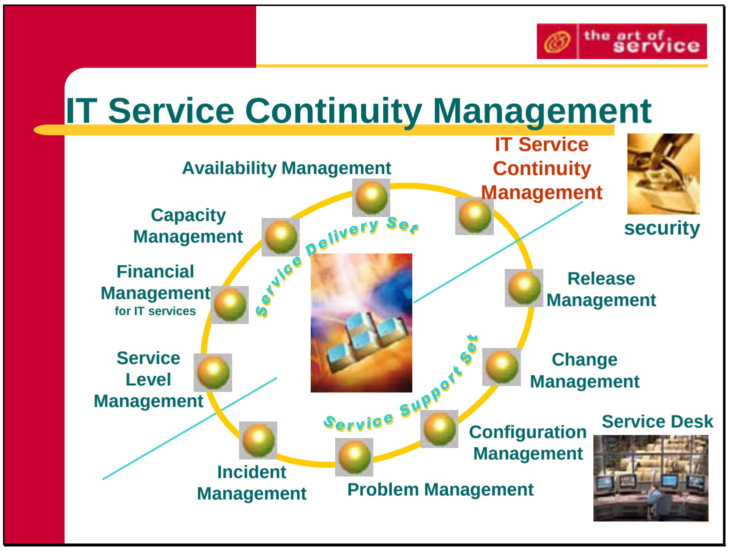
1.4 Risk Management ITIL V3 – ITSCM

1.4.1 Slide 1: Risk Management & ITIL

Risk Management and ITIL

the art of service

1.4.2 Slide 2: IT Service Continuity Management



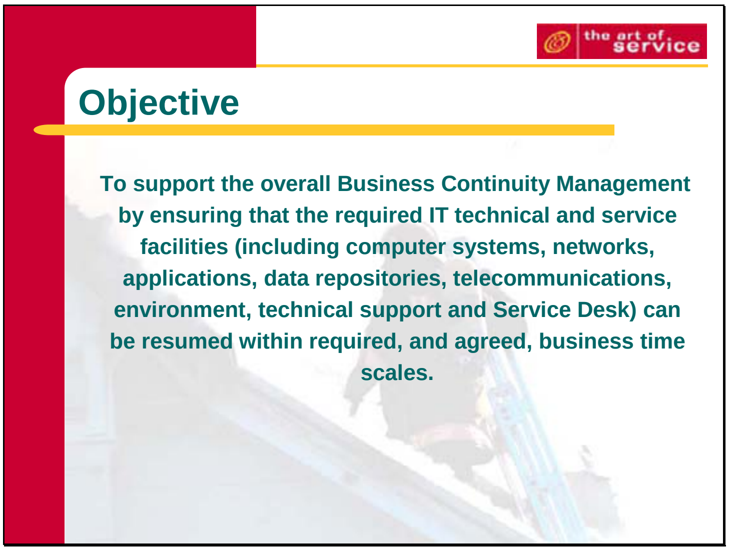
IT Service Continuity Management

1.4.3 Slide 3: IT Service Continuity Management

IT Service Continuity Management

the art of service

1.4.4 Slide 4: Objective

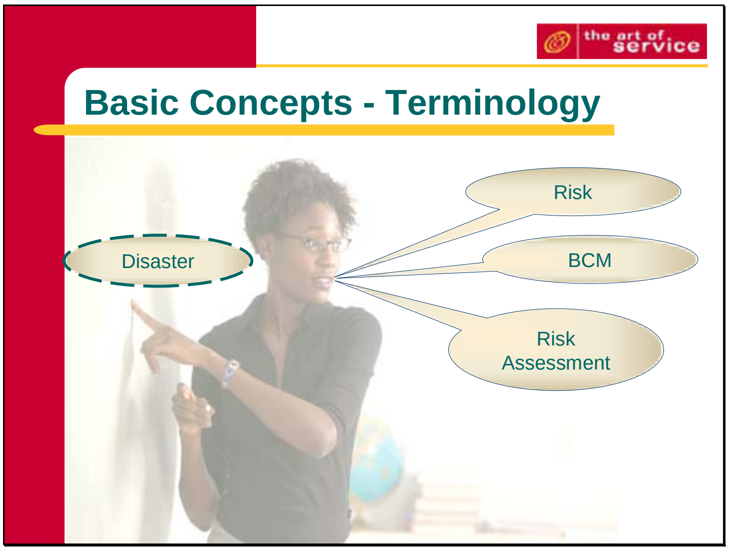


Objective

To support the overall Business Continuity Management by ensuring that the required IT technical and service facilities (including computer systems, networks, applications, data repositories, telecommunications, environment, technical support and Service Desk) can be resumed within required, and agreed, business time scales.

As technology is a core component of most business processes, continued or high availability of IT is critical to the survival of the business as a whole. This is achieved by introducing risk reduction measures and recovery options. Like all elements of ITSM, successful implementation of ITSCM can only be achieved with senior management commitment and the support of all members of the organization. Ongoing maintenance of the recovery capability is essential if it is to remain effective.

1.4.5 Slide 5: Basic Concepts – Terminology



Basic Concepts - Terminology

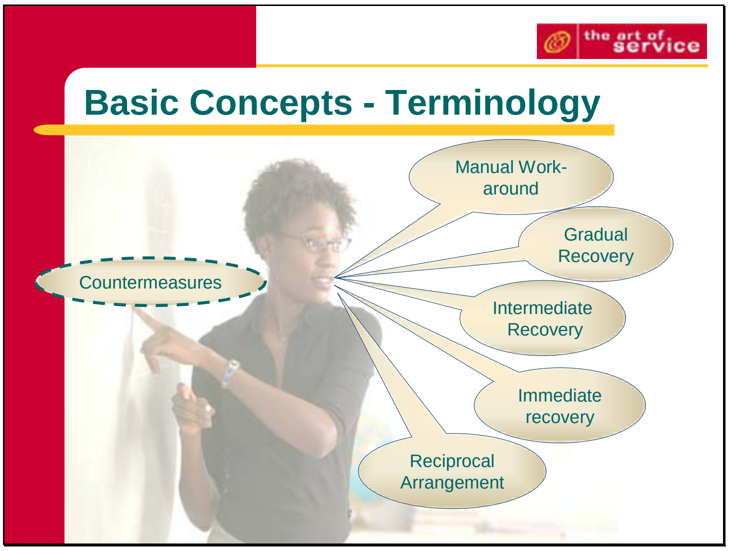
Disaster: NOT part of daily operational activities and *requires a separate system.*

Risk: A possible event that could cause harm or loss, or affect the ability to achieve objectives. A risk is measured by the probability of a threat, the vulnerability of the asset to that threat, and the impact it would have if it occurred.

BCM: Business Continuity Management: The business process responsible for managing risk that could seriously affect the BCM safeguards and interests of key stakeholders, reputation, brand and value-creating activities. The BCM Process involves reducing risks to an acceptable level and planning for the recovery of business processes should a disruption to the Business occur. BCM sets the objectives, scope and requirements for IT Service Continuity Management.

Risk Assessment: The initial steps of risk management. Analysing the value of assets to the business, identifying threats to those assets, and evaluation how vulnerable each asset is to those threats. Risk Assessment can be quantitative (based on numerical) or qualitative.

1.4.6 Slide 6: Basic Concepts – Terminology



Basic Concepts - Terminology

Manual Work-around
Gradual Recovery
Countermeasures
Intermediate Recovery
Immediate recovery
Reciprocal Arrangement

Counter Measures: Measures to prevent or recover from disaster

Manual Workaround: Using non-IT based solution to overcome IT service disruption

Gradual recovery: aka cold standby (>72hrs)

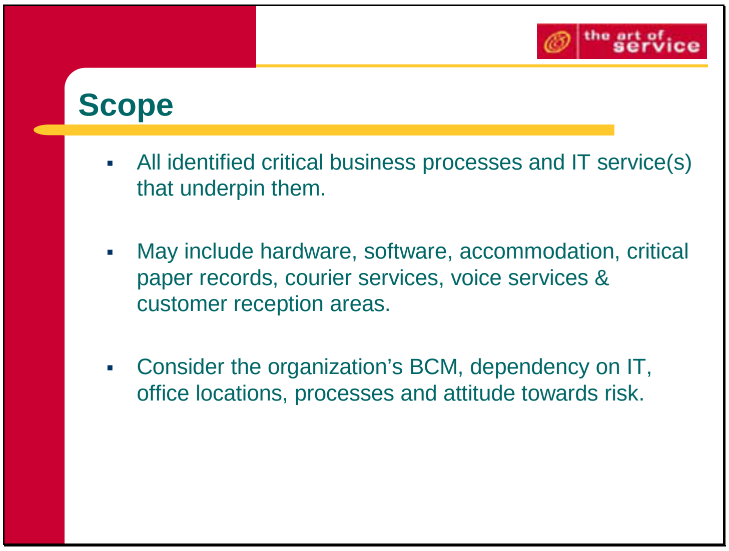
Intermediate Recovery: aka warm standby (24-72hrs)

Immediate Recovery: aka hot standby (< 24hrs, usually implies 1-2 hrs)

Reciprocal Arrangement: Agreement with another similar sized company to share disaster recovery obligations.

A detailed and usable example of an ITSCM Reciprocal Agreement is available on page 98.

1.4.7 Slide 7: Scope



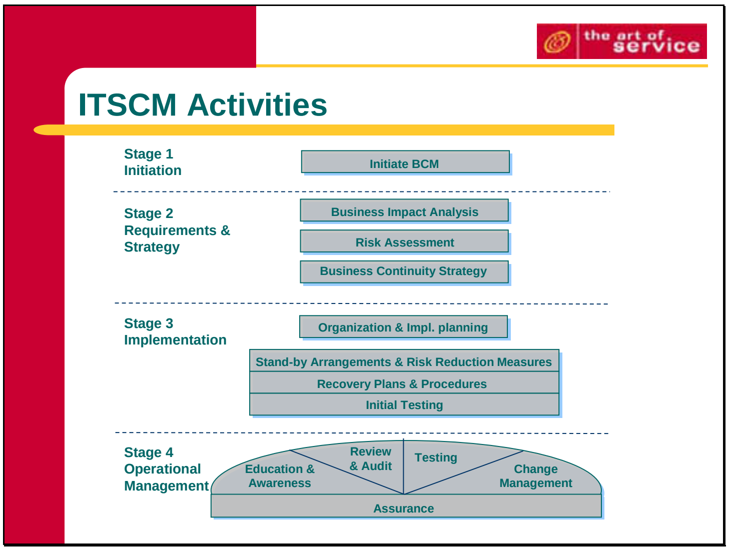
Scope

- All identified critical business processes and IT service(s) that underpin them.
- May include hardware, software, accommodation, critical paper records, courier services, voice services & customer reception areas.
- Consider the organization's BCM, dependency on IT, office locations, processes and attitude towards risk.

The ITSCM process includes:

- Agreement of the scope of the ITSCM process and the policies adopted.
- Business Impact Analysis (BIA) to quantify the impact loss of IT service would have on the business.
- Risk Analysis: the risk identification and risk assessment to identify potential threats to continuity and the likelihood of the threats becoming a reality. This also includes taking measures to manage the identified threats where this can be cost justified.
- Production of the overall ITSCM strategy. This can be produced following the two steps identified above, and is likely to include elements of risk reduction as well as a selection of appropriate and comprehensive recovery options.
- Production of an ITSCM plan, which again must be integrated with the overall BCM plans.
- Testing of the plans.
- Ongoing operation and maintenance of the plans.

1.4.8 Slide 8: ITSCM Activities



ITSCM Activities

Stage 1
Initiation

Initiate BCM

Stage 2
Requirements &
Strategy

Business Impact Analysis

Risk Assessment

Business Continuity Strategy

Stage 3
Implementation

Organization & Impl. planning

Stand-by Arrangements & Risk Reduction Measures

Recovery Plans & Procedures

Initial Testing

Stage 4
Operational
Management

Education & Awareness

Review & Audit

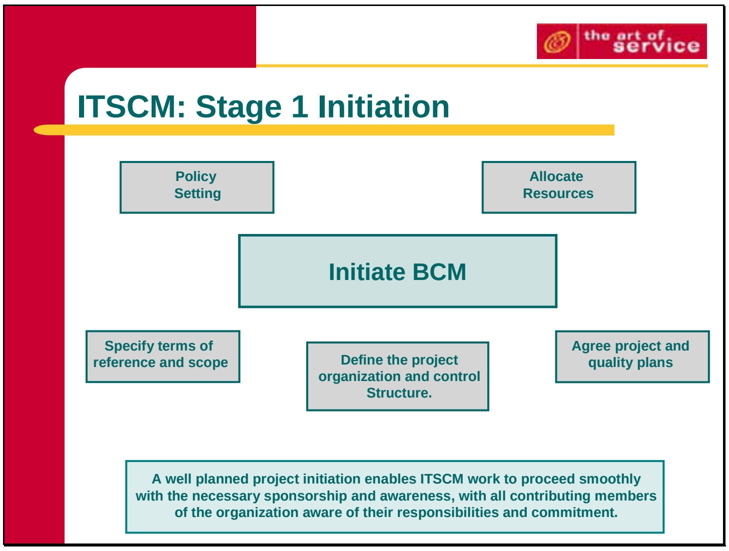
Testing

Change Management

Assurance

It is not possible to have effective ITSCM without support from the business. These are the four stages of the Business Continuity lifecycle that have particular emphasis on IT aspects.

1.4.9 Slide 9: ITSCM - Stage 1



ITSCM: Stage 1 Initiation

Policy Setting

Allocate Resources

Initiate BCM

Specify terms of reference and scope

Define the project organization and control Structure.

Agree project and quality plans

A well planned project initiation enables ITSCM work to proceed smoothly with the necessary sponsorship and awareness, with all contributing members of the organization aware of their responsibilities and commitment.

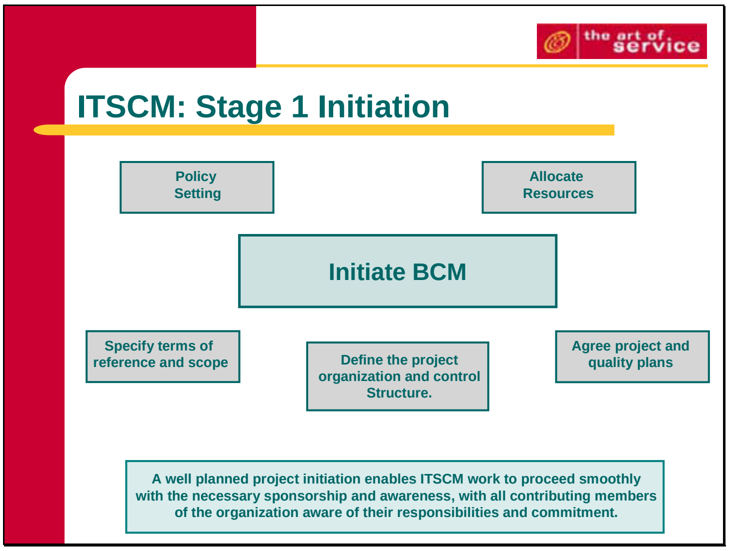
Policy setting – should be established and communicated ASAP so all member of the organization BCM issues are aware of their responsibilities to comply and support ITSCM. As a minimum the policy should set out management intention and objectives.

Specify terms of reference and scope – inc. defining scope and responsibilities of managers and staff, and work methods. Also covers risk assessment, BIA and the 'command and control' structure required to support business interruption. Other issues to consider are; outstanding audit issues, regulatory, insurance or client requirements and compliance with other standards such as BS7999 (Security Management) or ISO 20000.

Allocate Resources – effective BCM and ITSCM requires considerable resource in terms of money and manpower. Depending on the maturity of the organization, external consultants may be required to assist with BIA etc.

Define the project org control structure – It is advisable to use a standard project planning methodology such as PRINCE 2 complemented with project-planning tool. The appointment of an experienced project manager who reports to a steering committee and guides the work groups is the key to success.

1.4.10 Slide 9 cont…



ITSCM: Stage 1 Initiation

Policy Setting
Allocate Resources
Initiate BCM
Specify terms of reference and scope
Define the project organization and control Structure.
Agree project and quality plans

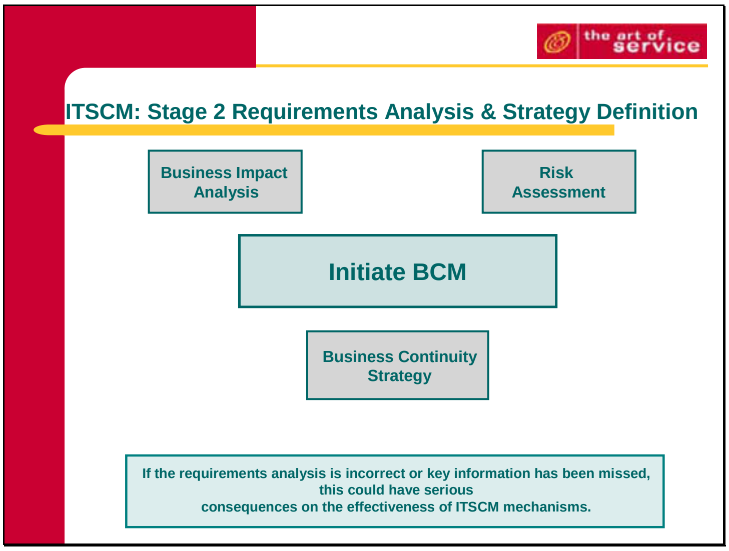
A well planned project initiation enables ITSCM work to proceed smoothly with the necessary sponsorship and awareness, with all contributing members of the organization aware of their responsibilities and commitment.

Agree project and quality plans – to enable the project to be controlled and variances addressed. Quality plans ensure that deliverables are achieved and to an acceptable level of quality.

The extent to which these activities need to be considered during the initiation process depends on the contingency facilities that have been applied within the organization.

Some parts of the business may have an established continuity plan based on manual workarounds, and the IT Organization may have developed their own disaster plans for supporting critical systems. However, effective ITSCM is dependent on supporting critical business functions and ensuring that the available budget is applied in the most appropriate way.

1.4.11 Slide 10: ITSCM – Stage 2

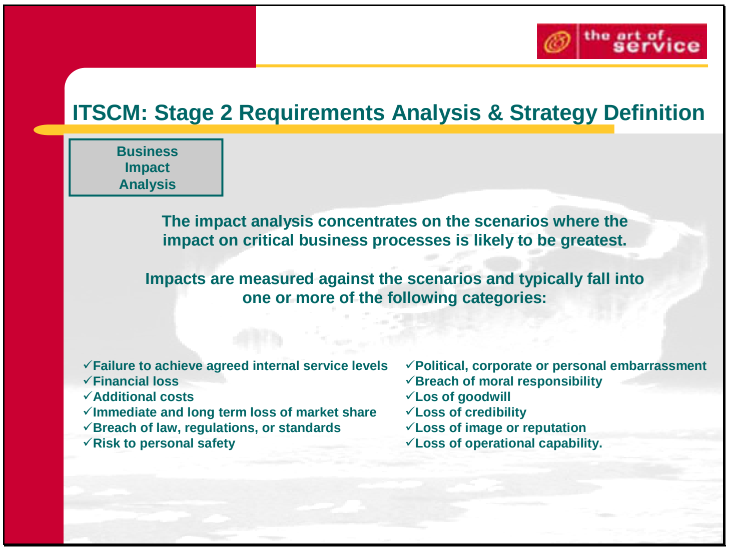


ITSCM: Stage 2 Requirements Analysis & Strategy Definition

If the requirements analysis is incorrect or key information has been missed, this could have serious consequences on the effectiveness of ITSCM mechanisms.

This stage provides the foundation for ITSCM and is a critical component in order to determine how well an organization will survive a business interruption or disaster and the costs that will be incurred.

1.4.12 Slide 11: ITSCM – Stage 2



ITSCM: Stage 2 Requirements Analysis & Strategy Definition

Business Impact Analysis

The impact analysis concentrates on the scenarios where the impact on critical business processes is likely to be greatest.

Impacts are measured against the scenarios and typically fall into one or more of the following categories:

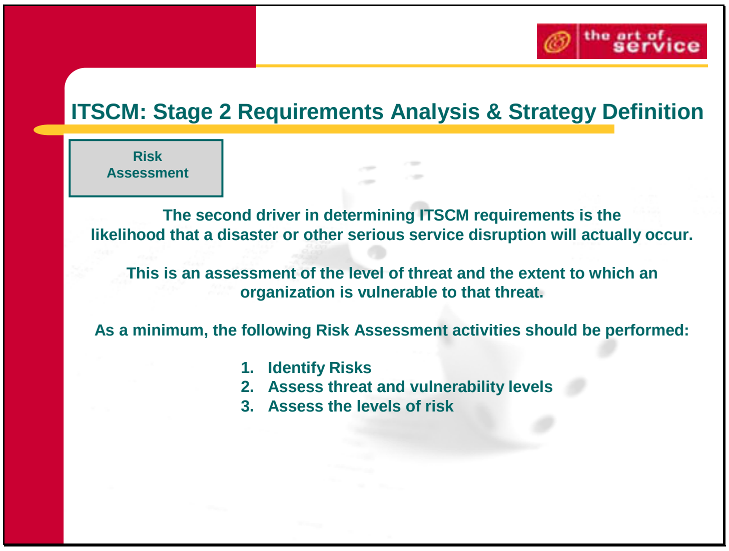
- ✓Failure to achieve agreed internal service levels
- ✓Financial loss
- ✓Additional costs
- ✓Immediate and long term loss of market share
- ✓Breach of law, regulations, or standards
- ✓Risk to personal safety
- ✓Political, corporate or personal embarrassment
- ✓Breach of moral responsibility
- ✓Los of goodwill
- ✓Loss of credibility
- ✓Loss of image or reputation
- ✓Loss of operational capability.

The Business Impact Analysis (BIA) identifies the minimum critical requirements to support the business.

This assessment enables the mapping of critical service, application and technology components to critical business processes, therefore helping to identify the ITSCM elements that need to be provided. The business requirements are ranked and the associated ITSCM elements confirmed and prioritized in terms of risk reduction and recovery planning. The results of the BIA are invaluable input to several areas of process design including Service Level Management to understand the required service levels.

A detailed and usable example of an ITSCM Business Impact Assessment is available on page 117.

1.4.13 Slide 12: ITSCM – Stage 2



ITSCM: Stage 2 Requirements Analysis & Strategy Definition

Risk Assessment

The second driver in determining ITSCM requirements is the likelihood that a disaster or other serious service disruption will actually occur.

This is an assessment of the level of threat and the extent to which an organization is vulnerable to that threat.

As a minimum, the following Risk Assessment activities should be performed:

1. Identify Risks
2. Assess threat and vulnerability levels
3. Assess the levels of risk

Identify Risks

i.e. Risks to particular IT Service components (assets) that support the business process which cause an interruption to service.

Assess Threat and Vulnerability Levels

The threat is defined as 'how likely it is that a disruption will occur' and the vulnerability is defined as' whether, and to what extent, the organization will be affected by the threat materializing'.

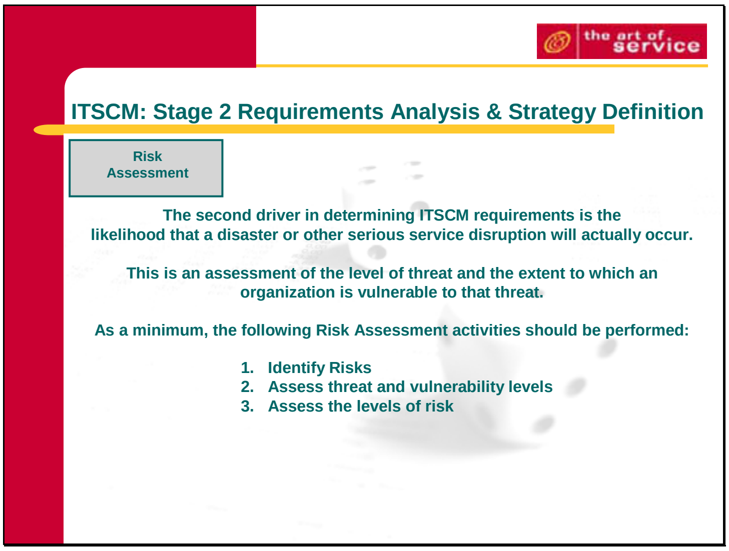
Assess the Levels of Risk

the overall risk can then be measured. This may be done as a measurement if quantitative data has been collected, or qualitative using a subjective assessment of, for example, low, medium or high.

Following the Risk Assessment

It is possible to determine appropriate countermeasures or risk reduction measures to manage the risks, i.e. reduce the risk to an acceptable minimum level or mitigate the risk.

1.4.14 Slide 12 cont…



ITSCM: Stage 2 Requirements Analysis & Strategy Definition

Risk Assessment

The second driver in determining ITSCM requirements is the likelihood that a disaster or other serious service disruption will actually occur.

This is an assessment of the level of threat and the extent to which an organization is vulnerable to that threat.

As a minimum, the following Risk Assessment activities should be performed:

1. Identify Risks
2. Assess threat and vulnerability levels
3. Assess the levels of risk

A standard methodology, such as the Management of Risk (M_O_R), should be used to assess and manage risks within the organization.

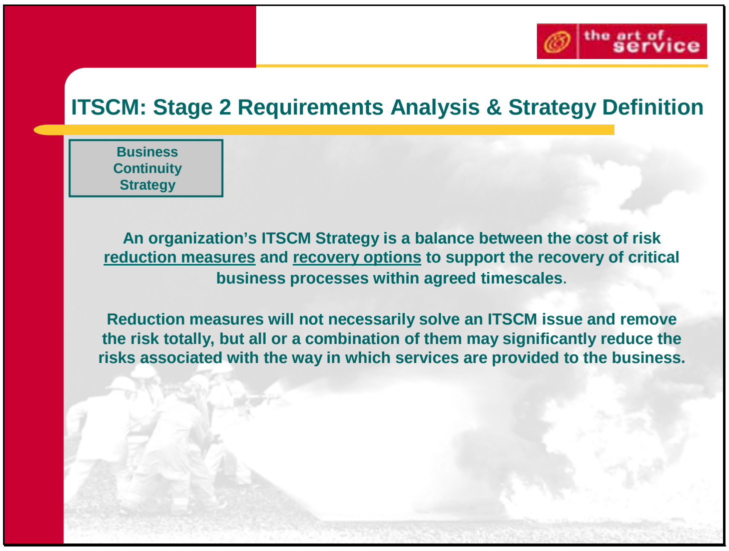
The Management of Risk Framework M_O_R is illustrated and explained on page 125.

Detailed and usable examples of IT Risk Assessment Planning are available on page 128.

A Risk Assessment Score Sheet is available on page 131 and more information on Risk Assessment and Control Form is available on page 134.

A Risk Assessment Questionnaire is available on page 138.

1.4.15 Slide 13: ITSCM – Stage 2



ITSCM: Stage 2 Requirements Analysis & Strategy Definition

Business Continuity Strategy

An organization's ITSCM Strategy is a balance between the cost of risk reduction measures and recovery options to support the recovery of critical business processes within agreed timescales.

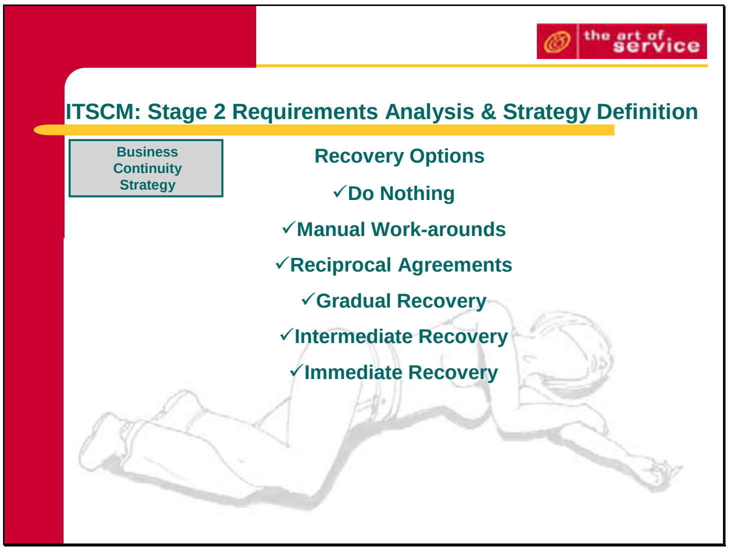
Reduction measures will not necessarily solve an ITSCM issue and remove the risk totally, but all or a combination of them may significantly reduce the risks associated with the way in which services are provided to the business.

Risk reduction measures include:

- A comprehensive backup and recovery strategy, including off-site storage
- Elimination of single points of failure e.g. single power supply from a single utility organization.
- Outsourcing services to more than one provider
- Resilient IT systems and networks constantly change-managed to ensure maximum performance in meeting the increasing business requirements.
- Greater security controls e.g. physical access control using swipe cards
- Better control to detect local service disruptions e.g. fire detection systems linked with suppression systems
- Improving procedures to reduce the likelihood of errors or failures e.g. Change control.

A detailed and usable example of an ITSCM Business Continuity Strategy is available on page 144.

1.4.16 Slide 14: ITSCM – Stage 2



ITSCM: Stage 2 Requirements Analysis & Strategy Definition

Business Continuity Strategy

Recovery Options

- ✓Do Nothing
- ✓Manual Work-arounds
- ✓Reciprocal Agreements
- ✓Gradual Recovery
- ✓Intermediate Recovery
- ✓Immediate Recovery

IT Recovery Options need to be considered for:

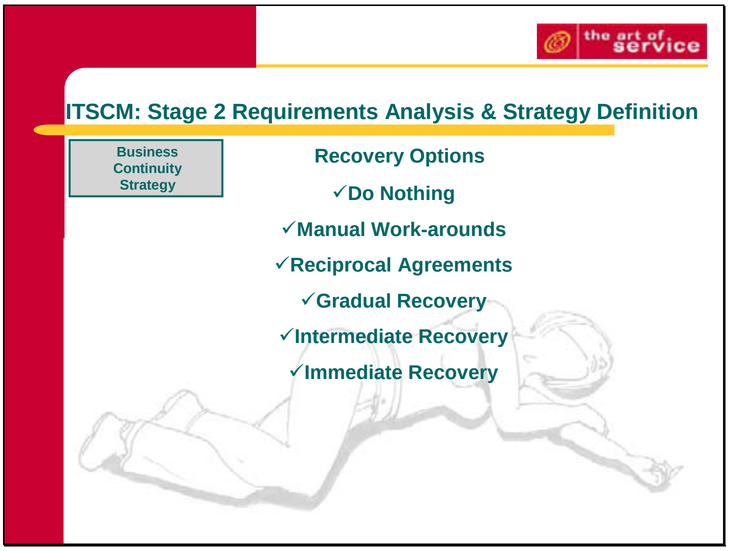
- People and accommodation
- IT systems and networks
- Critical Services e.g. power, water, telecommunications etc
- Critical assets e.g. paper records and reference material

Costs and benefits of each option need to be analyzed. Inc comparative assessment of:

- Ability to meet business recovery objectives
- Likely reduction in the potential impact
- Costs of establishing the option
- Costs of maintaining, testing and implementing the option
- Technical, organizational, cultural and administrative implications.

It is important that the organization checks the recovery options that are chosen are capable of implementation and integration at the time they are required, and that the required service recovery can be achieved.

1.4.17 Slide 14 cont…



ITSCM: Stage 2 Requirements Analysis & Strategy Definition

Recovery Options

✓Do Nothing

✓Manual Work-arounds

✓Reciprocal Agreements

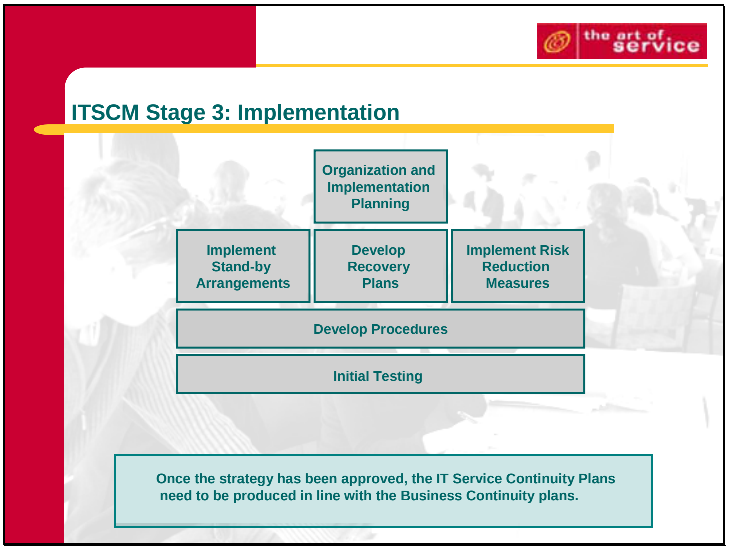
✓Gradual Recovery

✓Intermediate Recovery

✓Immediate Recovery

As with Recovery Options, it is important that the reduction of one risk does not increase another. The risk of Availability systems and data may be reduced by outsourcing to an off-site third party. However, this potentially increases the risk of compromise of confidential information unless rigorous security controls are applied.

1.4.18 Slide 15: ITSCM – Stage 3



ITSCM Stage 3: Implementation

Organization and Implementation Planning
Implement Stand-by Arrangements
Develop Recovery Plans
Implement Risk Reduction Measures
Develop Procedures
Initial Testing

Once the strategy has been approved, the IT Service Continuity Plans need to be produced in line with the Business Continuity plans.

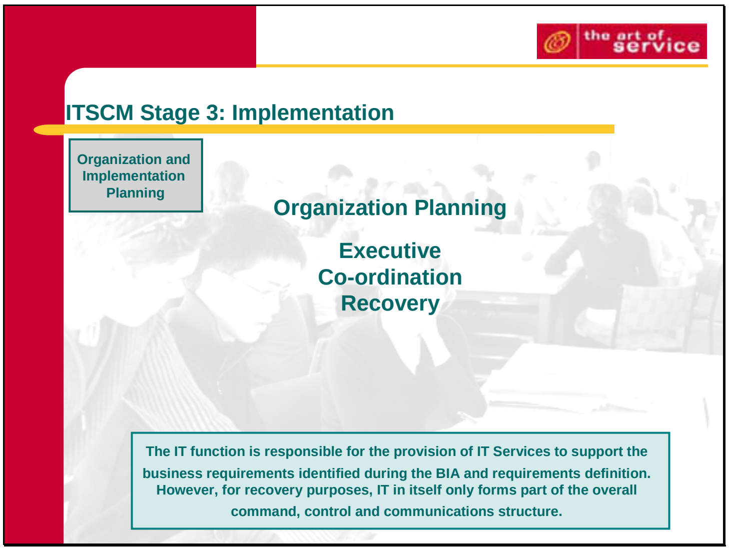
ITSCM plans need to be developed to enable the necessary information for critical systems, services and facilities to either continue to be provided or to be reinstated within an acceptable period of the business.

The implementation Stage consists of the following processes:

- Establish the organization and develop implementation plans
- Implement stand-by arrangements
- Implement risk reduction measures
- Develop IT recovery plans
- Develop procedures
- Undertake initial tests.

Each of the above is considered with respect to the specific responsibilities that IT must action.

1.4.19 Slide 16: ITSCM – Stage 3



ITSCM Stage 3: Implementation

Organization and Implementation Planning

Organization Planning

Executive
Co-ordination
Recovery

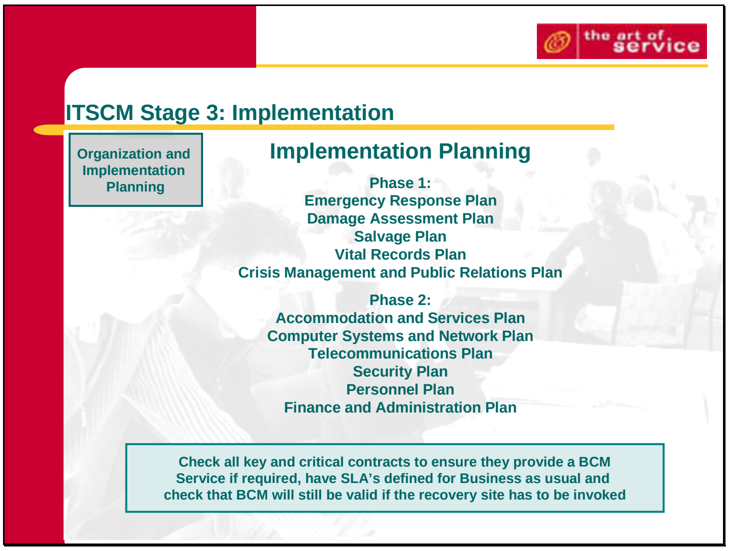
The IT function is responsible for the provision of IT Services to support the business requirements identified during the BIA and requirements definition. However, for recovery purposes, IT in itself only forms part of the overall command, control and communications structure.

Organization Planning

- **Executive** – including senior management/executive board with overall authority and control within the organization and responsible for crisis management and liaison with other departments, divisions, organizations, the media, regulators, emergency services etc.
- **Co-ordination** – typically one level below the Executive group and responsible for co-coordinating the overall recovery effort within the organization.
- **Recovery** – a series of business and service recovery teams representing the critical business functions and the services that need to be established to support these functions. Each team is responsible for executing the plans within their own areas and for liaison with staff, customers and third parties. Within IT the recovery teams should be grouped by IT Service and application.

Detailed and usable examples of <u>Typical Contents of a Recovery Plan</u> are available on page 156.

1.4.20 Slide 17: ITSCM – Stage 3



ITSCM Stage 3: Implementation

Organization and Implementation Planning

Implementation Planning

Phase 1:
Emergency Response Plan
Damage Assessment Plan
Salvage Plan
Vital Records Plan
Crisis Management and Public Relations Plan

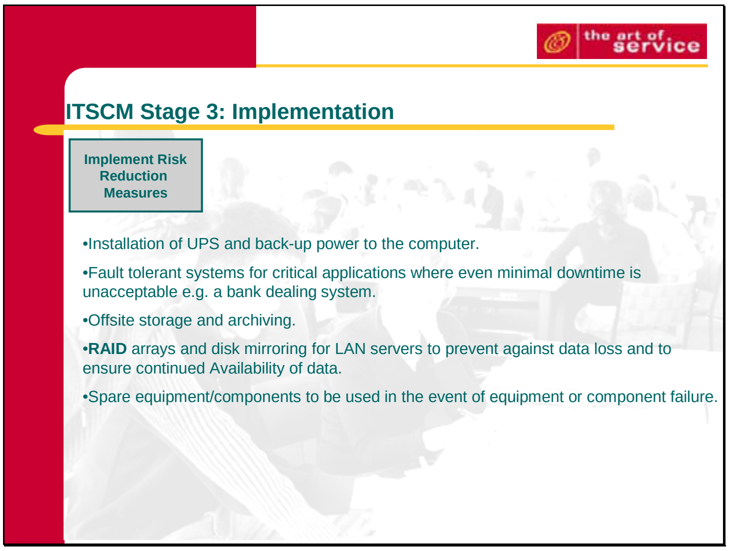
Phase 2:
Accommodation and Services Plan
Computer Systems and Network Plan
Telecommunications Plan
Security Plan
Personnel Plan
Finance and Administration Plan

Check all key and critical contracts to ensure they provide a BCM Service if required, have SLA's defined for Business as usual and check that BCM will still be valid if the recovery site has to be invoked

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.

Phase 1: These plans are used to identify and respond to 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 there is a need, Phase 2 plans need to take place. These will include the key support functions.

1.4.21 Slide 18: ITSCM – Stage 3

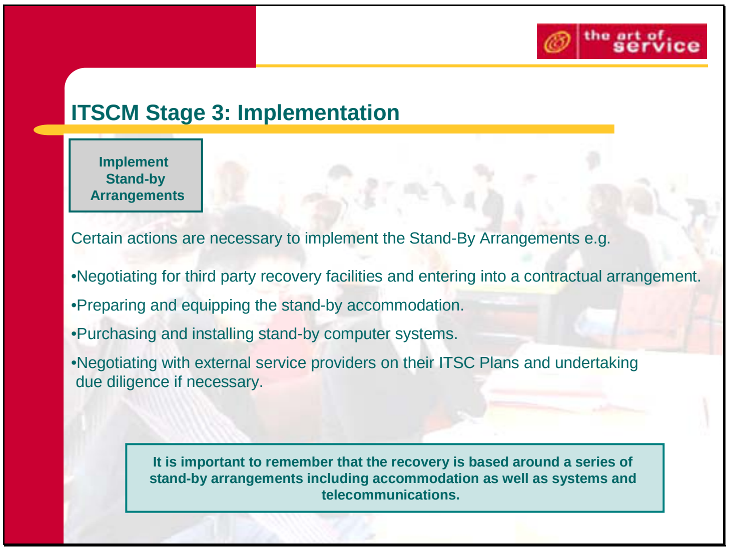


ITSCM Stage 3: Implementation

Implement Risk Reduction Measures

- Installation of UPS and back-up power to the computer.
- Fault tolerant systems for critical applications where even minimal downtime is unacceptable e.g. a bank dealing system.
- Offsite storage and archiving.
- **RAID** arrays and disk mirroring for LAN servers to prevent against data loss and to ensure continued Availability of data.
- Spare equipment/components to be used in the event of equipment or component failure.

1.4.22 Slide 19: ITSCM – Stage 3



ITSCM Stage 3: Implementation

Implement Stand-by Arrangements

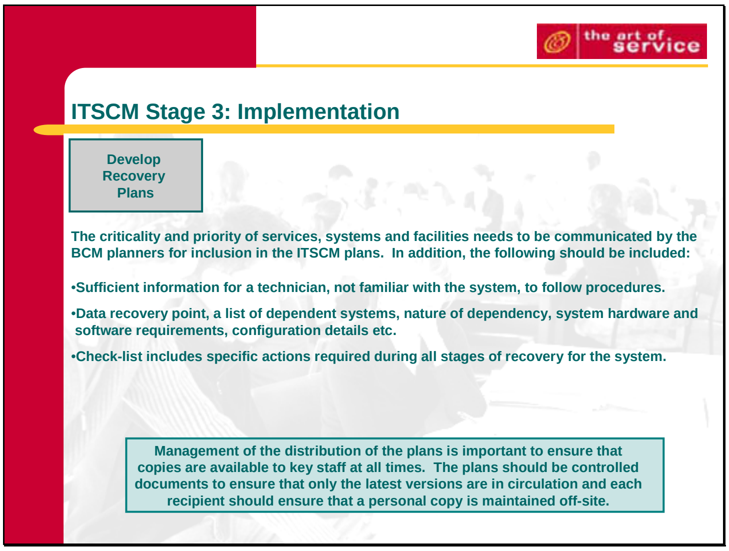
Certain actions are necessary to implement the Stand-By Arrangements e.g.

- Negotiating for third party recovery facilities and entering into a contractual arrangement.
- Preparing and equipping the stand-by accommodation.
- Purchasing and installing stand-by computer systems.
- Negotiating with external service providers on their ITSC Plans and undertaking due diligence if necessary.

It is important to remember that the recovery is based around a series of stand-by arrangements including accommodation as well as systems and telecommunications.

Training and new procedures may be required to operate, test and maintain the stand-by arrangements and to ensure that they can be initiated when required.

1.4.23 Slide 20: ITSCM – Stage 3



ITSCM Stage 3: Implementation

Develop Recovery Plans

The criticality and priority of services, systems and facilities needs to be communicated by the BCM planners for inclusion in the ITSCM plans. In addition, the following should be included:

•Sufficient information for a technician, not familiar with the system, to follow procedures.

•Data recovery point, a list of dependent systems, nature of dependency, system hardware and software requirements, configuration details etc.

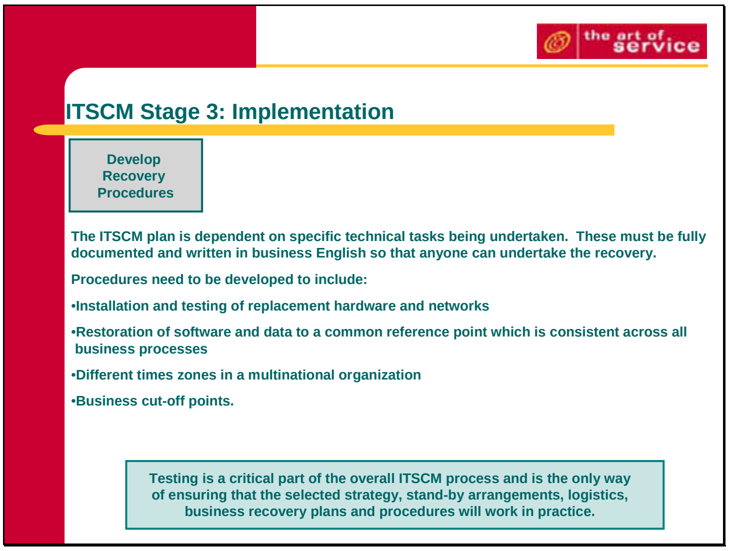
•Check-list includes specific actions required during all stages of recovery for the system.

Management of the distribution of the plans is important to ensure that copies are available to key staff at all times. The plans should be controlled documents to ensure that only the latest versions are in circulation and each recipient should ensure that a personal copy is maintained off-site.

The recovery plans include key detail such as the data recovery point, a list of dependent systems, the nature of dependency and the data recovery points, system hardware and software requirements, configuration details and references to other relevant or essential information about the system etc.

A check-list is included that covers specific actions required during all stages of recovery for the system, for example after the system has been restored to an operational state, connectivity checks, functionality checks or data consistency and integrity checks should be carried out prior to handling the system over to the business.

1.4.24 Slide 21: ITSCM – Stage 3



ITSCM Stage 3: Implementation

Develop Recovery Procedures

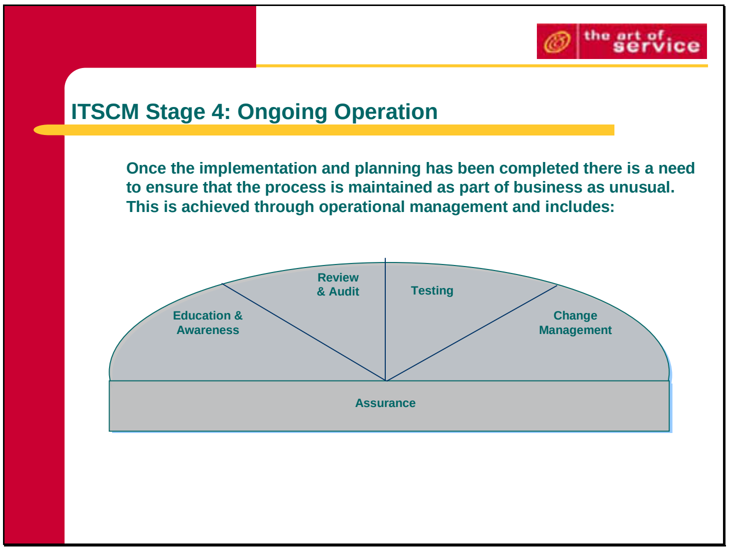
The ITSCM plan is dependent on specific technical tasks being undertaken. These must be fully documented and written in business English so that anyone can undertake the recovery.

Procedures need to be developed to include:

- Installation and testing of replacement hardware and networks
- Restoration of software and data to a common reference point which is consistent across all business processes
- Different times zones in a multinational organization
- Business cut-off points.

Testing is a critical part of the overall ITSCM process and is the only way of ensuring that the selected strategy, stand-by arrangements, logistics, business recovery plans and procedures will work in practice.

1.4.25 Slide 22: ITSCM – Stage 4



ITSCM Stage 4: Ongoing Operation

Once the implementation and planning has been completed there is a need to ensure that the process is maintained as part of business as unusual. This is achieved through operational management and includes:

Education & Awareness

Review & Audit

Testing

Change Management

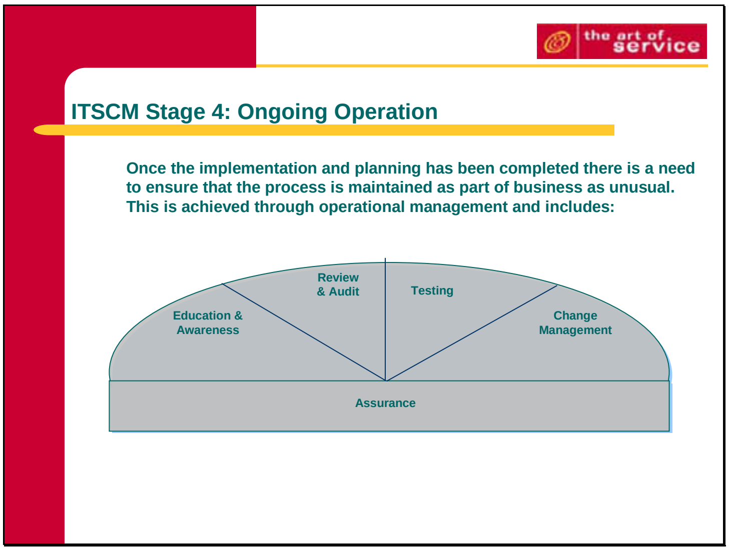
Assurance

Education and Awareness – this should cover the organization and the IT organization, for service continuity specific items. This ensures that all staff are aware of the implications of Business and Service Continuity and consider them part of their normal routine and budget.

Review – regular review of all of the deliverable from the ITSCM process needs to be undertaken to ensure that they remain current. With respect to IT this is required whenever there is a major Change to the IT Infrastructure, assets or dependencies such as new systems or networks or a change in service providers, as well as there is a change on business direction and strategy or IT strategy.

Testing – following the initial testing it is necessary to establish a program of regular testing to ensure that the critical components of the strategy are tested at least annually or as directed by senior management or audit. It is important that any changes to the IT Infrastructure are in included in the strategy, implemented appropriately and tested to ensure they function correctly.

1.4.26 Slide 22 cont…



ITSCM Stage 4: Ongoing Operation

Once the implementation and planning has been completed there is a need to ensure that the process is maintained as part of business as unusual. This is achieved through operational management and includes:

Education & Awareness

Review & Audit

Testing

Change Management

Assurance

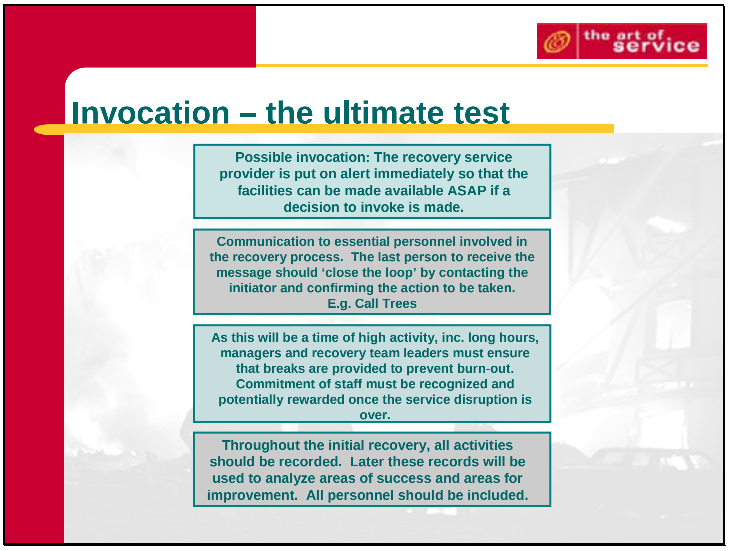
Change Management – following tests and reviews, and day to day changes, there is a need for the ITSCM plan to be updated. ITSCM must be included as part of the change management process to ensure all changes are reflected in the contingency arrangements provided by IT or 3rd parties. **Inaccurate plans and inadequate recovery capabilities may result in failure of ITSCM.**

Training – IT may be involved in training non-IT literate business recovery team members to ensure they have the necessary level of competence to facilitate recovery.

Assurance – The final process in the ITSCM lifecycle involves obtaining assurance that the quality of the ITSCM deliverables is acceptable to senior business management and that operational management processes are working satisfactorily.

A detailed and usable example of an <u>ITSCM Communication Plan</u> and <u>ITSCM Email Template</u> are available on pages 161 and 167.

1.4.27 Slide 23: Invocation – The Ultimate Test



Invocation – the ultimate test

Possible invocation: The recovery service provider is put on alert immediately so that the facilities can be made available ASAP if a decision to invoke is made.

Communication to essential personnel involved in the recovery process. The last person to receive the message should 'close the loop' by contacting the initiator and confirming the action to be taken. E.g. Call Trees

As this will be a time of high activity, inc. long hours, managers and recovery team leaders must ensure that breaks are provided to prevent burn-out. Commitment of staff must be recognized and potentially rewarded once the service disruption is over.

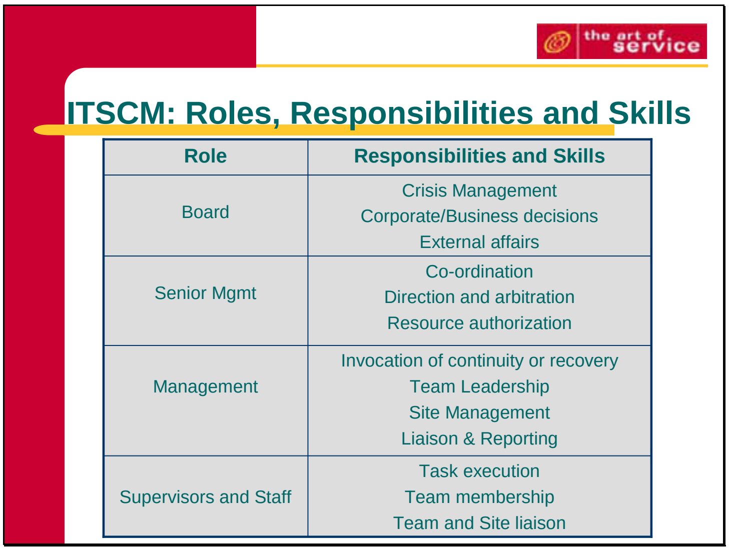
Throughout the initial recovery, all activities should be recorded. Later these records will be used to analyze areas of success and areas for improvement. All personnel should be included.

The decision to invoke needs to take into account a number of factors:

- The extent of the damage and scope of the potential invocation
- The likely length of the disruption and unavailability of the premises and/or services.
- The time of day/month/year and the potential business impact. At year end the need to invoke may be more pressing to ensure that year end processing is completed on time.
- Specific requirements of the business depending on work being undertaken at the time.

A detailed and usable example of an ITSCM Emergency Response Plan and ITSCM Salvage Plan Template are available on pages 171 and 180.

1.4.28 Slide 24: Roles, Responsibilities & Skills



ITSCM: Roles, Responsibilities and Skills

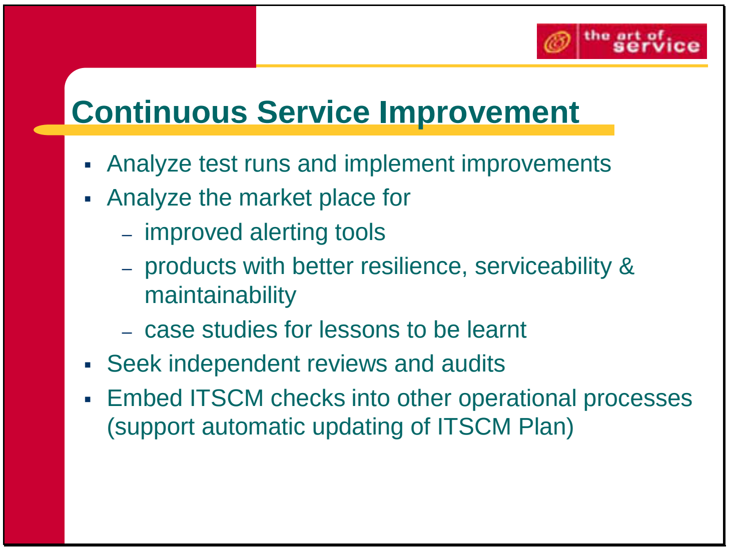
Role	Responsibilities and Skills
Board	Crisis Management Corporate/Business decisions External affairs
Senior Mgmt	Co-ordination Direction and arbitration Resource authorization
Management	Invocation of continuity or recovery Team Leadership Site Management Liaison & Reporting
Supervisors and Staff	Task execution Team membership Team and Site liaison

Typical responsibilities for ITSCM in planning and dealing with disaster are similar to how First Aid Officers and Fire Wardens act in planning and operational roles.

Skill requirements for ITSCM Manager and staff:

- Knowledge of the business (help set priorities),
- Calm under pressure,
- Analytical (problem solving)
- Leadership and Team players,
- Negotiation and Communication.

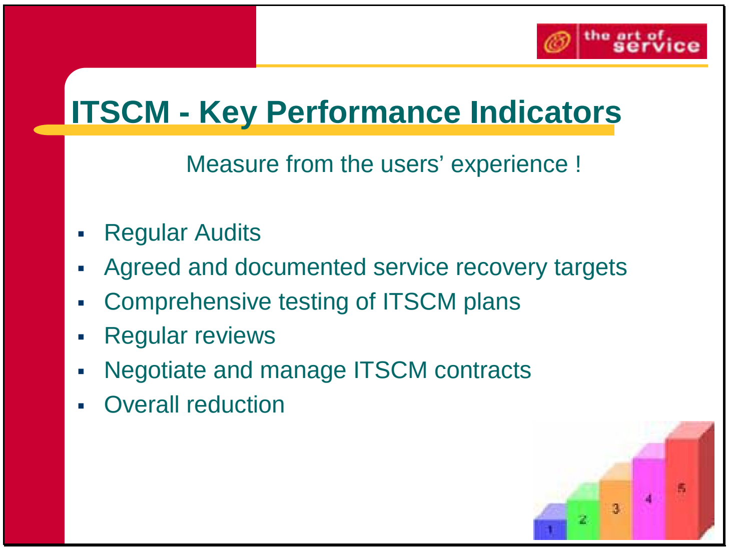
1.4.29 Slide 25: Continuous Service Improvement



Continuous Service Improvement

- Analyze test runs and implement improvements
- Analyze the market place for
  - improved alerting tools
  - products with better resilience, serviceability & maintainability
  - case studies for lessons to be learnt
- Seek independent reviews and audits
- Embed ITSCM checks into other operational processes (support automatic updating of ITSCM Plan)

1.4.30 Slide 26: Key Performance Indicators



ITSCM - Key Performance Indicators

Measure from the users' experience !

- Regular Audits
- Agreed and documented service recovery targets
- Comprehensive testing of ITSCM plans
- Regular reviews
- Negotiate and manage ITSCM contracts
- Overall reduction

the art of service
1
2
3
4
5

IT services are to be delivered and can be recovered to meet business objectives:

- Regular Audits of the ITSCM plans, to ensure that ,at all times, the agreed recovery requirements of the business can be achieved
- All service recovery targets are agreed and documented in SLA's and are achievable within the ITSCM plans.
- Regular and comprehensive testing of ITSCM plans
- Regular reviews are undertaken, at least annually, of the business and IT continuity plans with the business areas
- Negotiate and manage all necessary ITSCM contracts with third party
- Overall reduction in the risk and impact of possible failure of IT services.
- Awareness throughout the organizations of the plans:
- Ensure awareness of business impact, needs and requirements throughout IT
- Ensure that all IT service areas are prepared and able to respond to an invocation of the ITSCM plans
- Regular communication of the ISCM objectives and responsibilities within the appropriate business and IT service areas.

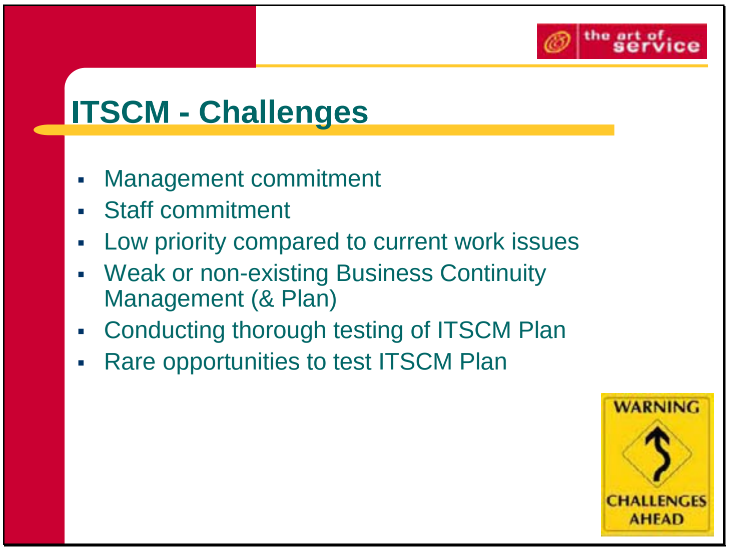
1.4.31 Slide 27: Benefits

ITSCM - Benefits

Overall better risk management

- Lower insurance premiums
- Meet regulatory requirements
- Better relationship with customers
- Competitive advantage
- Enhance organizational credibility

1.4.32 Slide 28: Challenges



the art of service

ITSCM - Challenges

- Management commitment
- Staff commitment
- Low priority compared to current work issues
- Weak or non-existing Business Continuity Management (& Plan)
- Conducting thorough testing of ITSCM Plan
- Rare opportunities to test ITSCM Plan

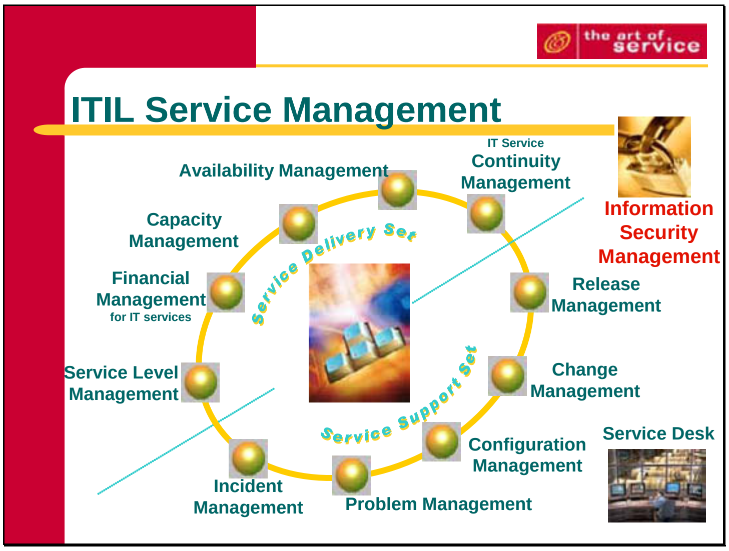
WARNING
CHALLENGES AHEAD

1.5 Risk Management ITIL V3 – ISM

1.5.1 Slide 1: Risk Management & ITIL

Risk Management and ITIL

1.5.2 Slide 2: ITIL Service Management

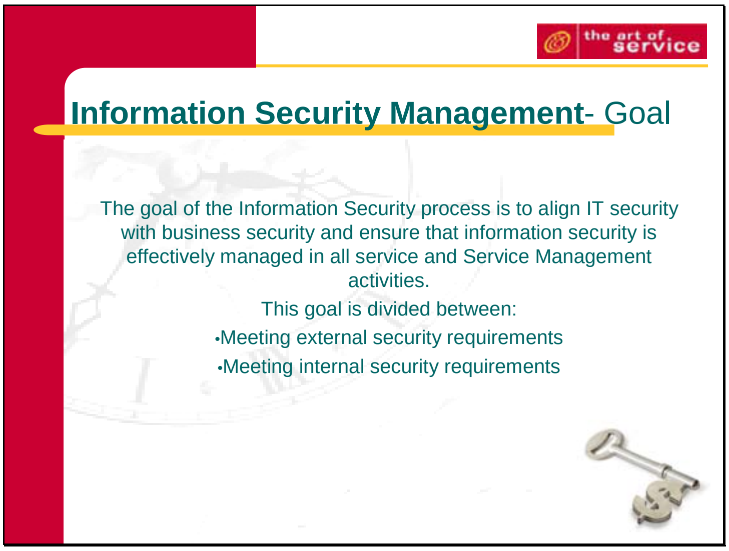


ITIL Service Management

1.5.3 Slide 3: Information Security Management (ISM)

Information Security Management

1.5.4 Slide 4: ISM – Goal



Information Security Management- Goal

The goal of the Information Security process is to align IT security with business security and ensure that information security is effectively managed in all service and Service Management activities.

This goal is divided between:

•Meeting external security requirements

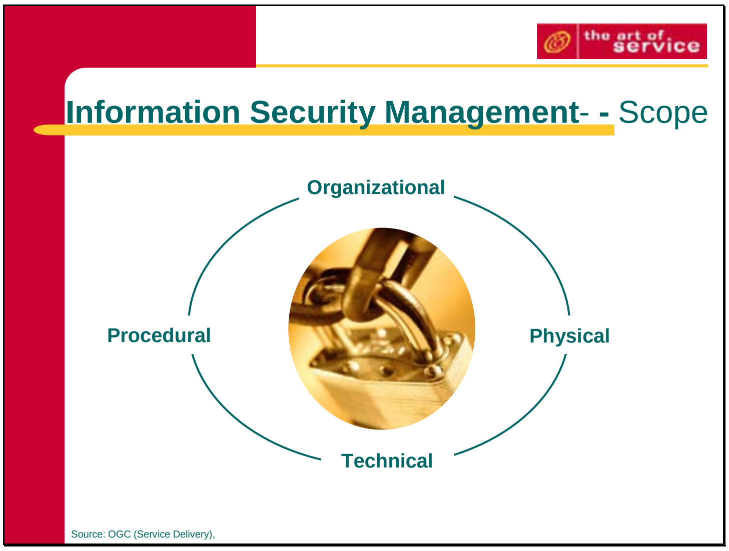
•Meeting internal security requirements

For most organizations, the security objective is met when:

- Information is available and usable when required, and the systems that provide it can appropriately resist attacks and recover from or prevent failures (availability).
- Information is observed by or disclosed to only those who have a right to know (confidently)
- Information is complete, accurate and protected against unauthorized modification (integrity)
- Business transactions, as well as information exchanges between enterprises, or with partners, can be trusted (authenticity and non-repudiation).

Prioritization of confidentiality, integrity and availability must be considered in the context of business and business processes. The primary guide to defining what must be protected and the level of protection has to come from the business. To be effective, security must address entire business processes from end to end and cover the physical and technical aspects. Only within the context of business needs and risks can management define security.

1.5.5 Slide 5: ISM – Scope



Information Security Management- - Scope

Organizational

Procedural

Physical

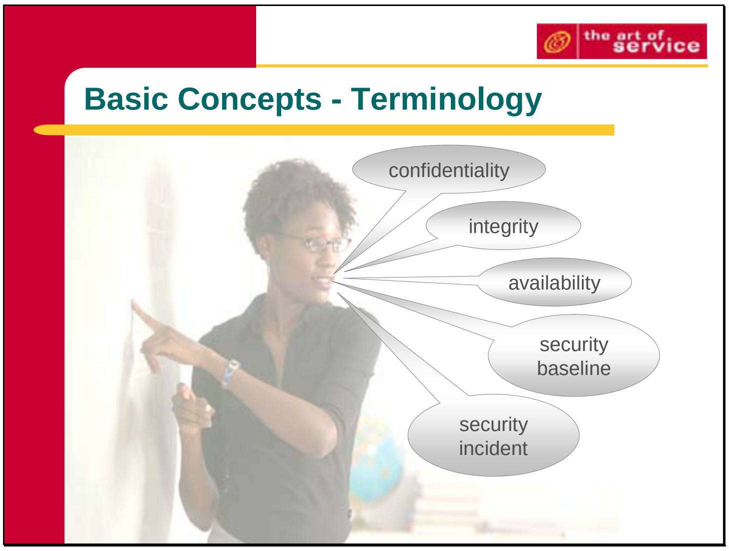
Technical

Source: OGC (Service Delivery),

The ISM process should be the focal point for all IT security issues, and must ensure that an Information Security Policy is produced, maintained and enforced that covers the use and misuse of all IT systems and services. ISM needs to understand the total IT and business security environment, including the:

- Business Security Policy and plans
- Current business operation and its security requirements
- Future business plans and requirements
- Legislative requirements
- Obligations and responsibilities with regard to security contained within SLA’s
- The business and IT risks and their management.
- Understanding all of this will enable ISM to ensure that all the current and future security aspects and risks of the business are cost effectively managed.

1.5.6 Slide 6: Basic Concepts – Terminology



Basic Concepts - Terminology

the art of service
confidentiality
integrity
availability
security baseline
security incident

Confidentiality: Protecting information against unauthorized access and use.

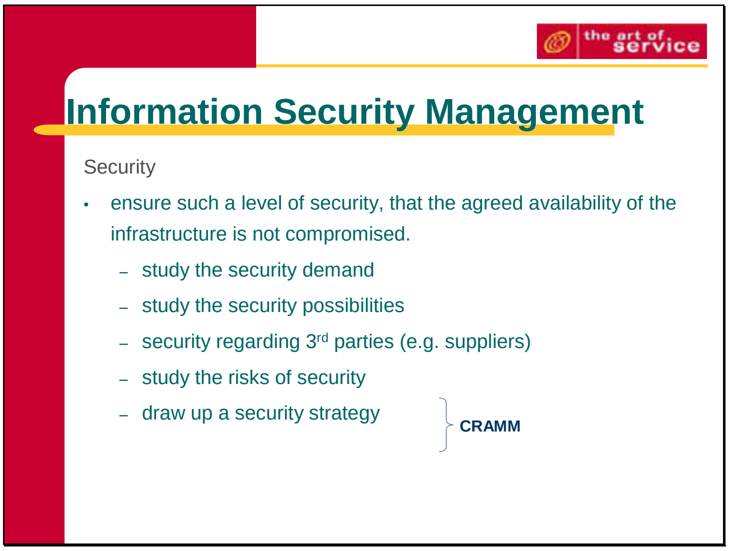
Integrity: Accuracy, completeness and timeliness of the information.

Availability: The information should be accessible for authorized users at the agreed time. This depends on the continuity provided by the information processing systems.

Security Baseline: The security level adopted by the IT organization for its own security and from the point of view of good 'due diligence'. Possible to have multiple baselines

Security Incident: Any incident that may interfere with achieving the SLA security requirements; materialisation of a threat

1.5.7 Slide 7: ISM – Security



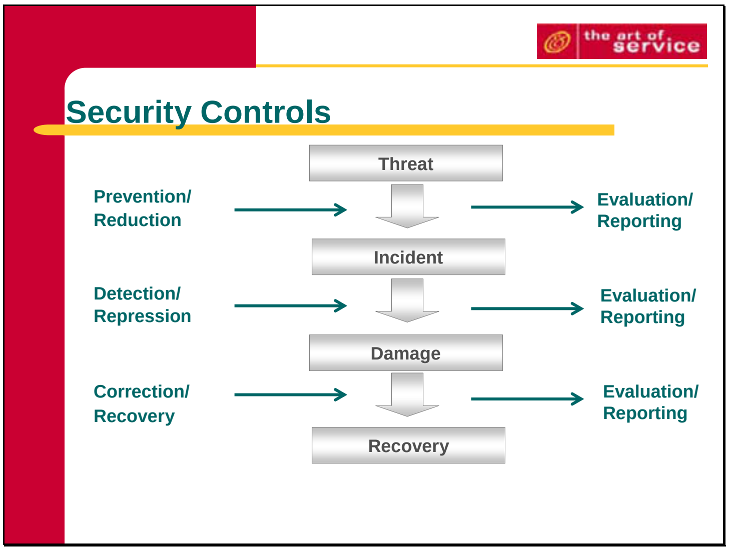
Information Security Management

Security

- ensure such a level of security, that the agreed availability of the infrastructure is not compromised.
  - study the security demand
  - study the security possibilities
  - security regarding 3rd parties (e.g. suppliers)
  - study the risks of security
  - draw up a security strategy

CRAMM

1.5.8 Slide 8: Security Controls

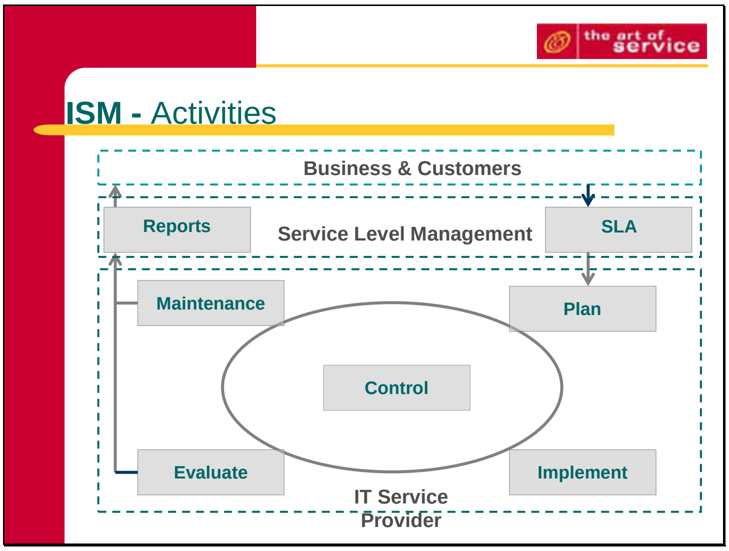


Security Controls

The Information Security Manager must understand that security is not a step in the lifecycle of services and systems and that security can not be solved through technology. Rather, information security must be an integral part off all services and systems and is an ongoing process that needs to be continuously managed using a set of security controls – as shown above.

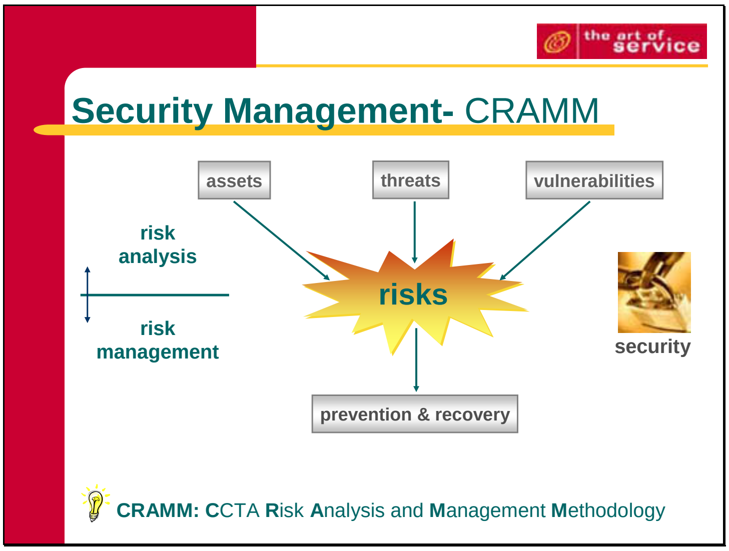
The set of security controls should be designed to support and enforce the Information Security Policy and to minimize all recognized and potential threats. The controls will be considerably more cost effective if included within the design of all services. This ensures continued protection of all existing services and that new services are accessed in line with the policy.

1.5.9 Slide 9: ISM – Activities



ISM - Activities

1.5.10 Slide 10: Security Management – CRAMM



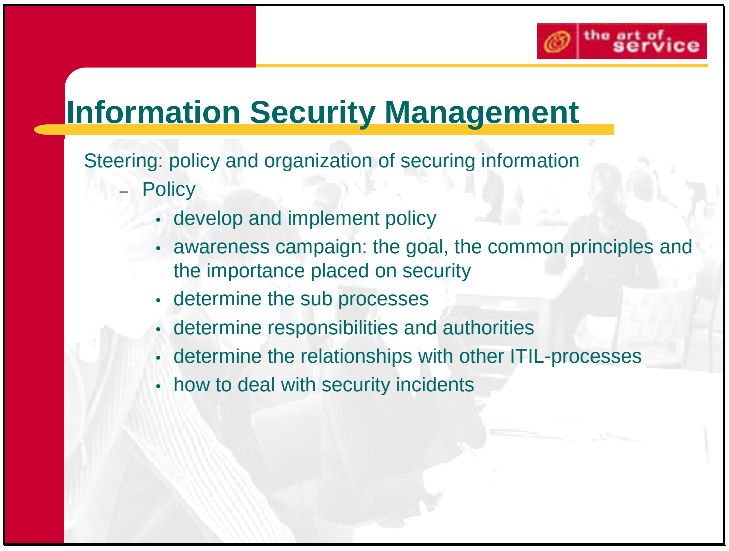
Security Management- CRAMM

CRAMM: CCTA Risk Analysis and Management Methodology

Based on the UK Government's preferred risk assessment methodology, CRAMM provides a comprehensive risk assessment method.

More information on CRAMM, can be found on page 187.

1.5.11 Slide 11: ISM – Policy

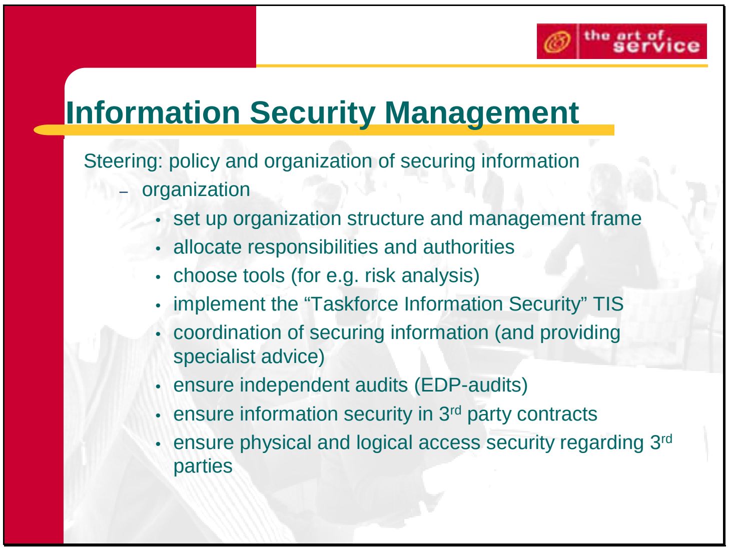


Information Security Management

Steering: policy and organization of securing information

- Policy
  - develop and implement policy
  - awareness campaign: the goal, the common principles and the importance placed on security
  - determine the sub processes
  - determine responsibilities and authorities
  - determine the relationships with other ITIL-processes
  - how to deal with security incidents

1.5.12 Slide 12: ISM – Steering

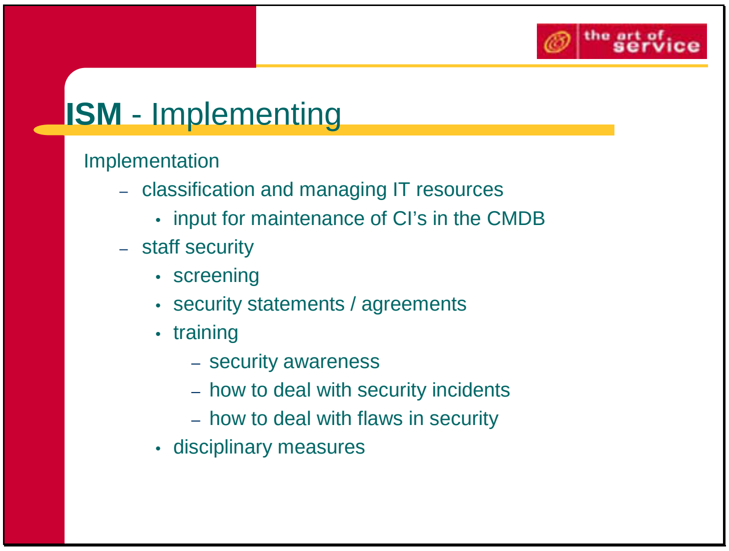


Information Security Management

Steering: policy and organization of securing information

- organization
  - set up organization structure and management frame
  - allocate responsibilities and authorities
  - choose tools (for e.g. risk analysis)
  - implement the “Taskforce Information Security” TIS
  - coordination of securing information (and providing specialist advice)
  - ensure independent audits (EDP-audits)
  - ensure information security in 3rd party contracts
  - ensure physical and logical access security regarding 3rd parties

1.5.13 Slide 13: ISM – Implementing

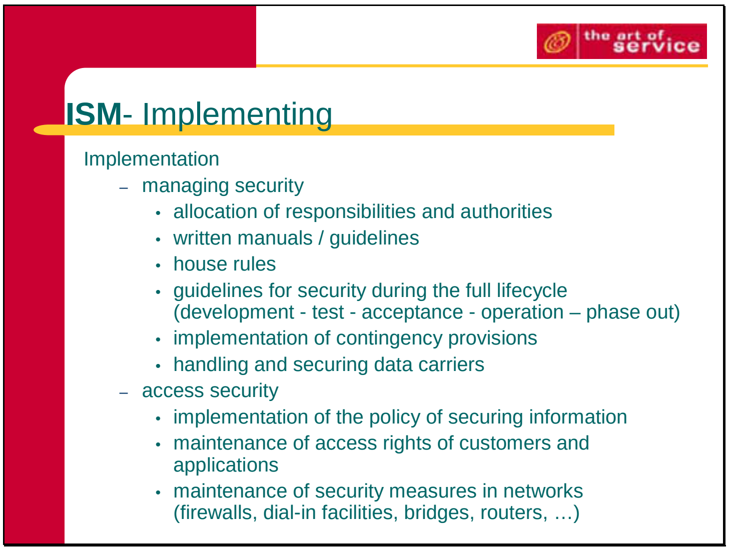


ISM - Implementing

Implementation

- classification and managing IT resources
  - input for maintenance of CI’s in the CMDB
- staff security
  - screening
  - security statements / agreements
  - training
    - security awareness
    - how to deal with security incidents
    - how to deal with flaws in security
  - disciplinary measures

1.5.14 Slide 14: ISM – Implementing

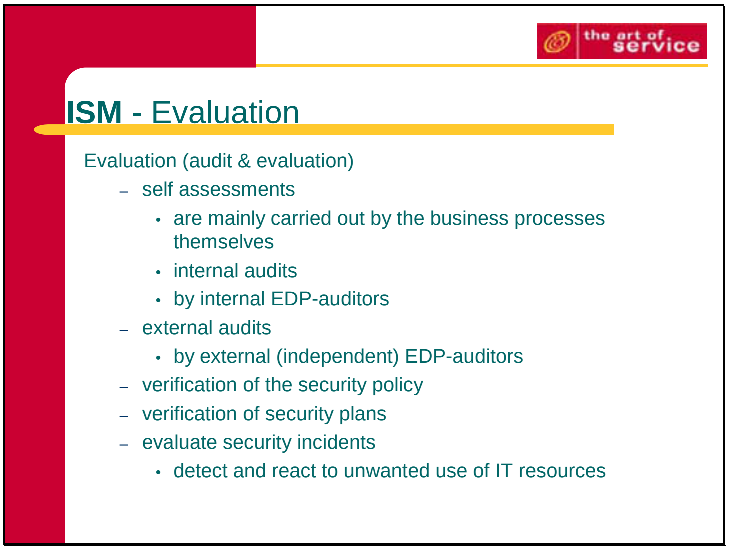


ISM- Implementing

Implementation

- managing security
  - allocation of responsibilities and authorities
  - written manuals / guidelines
  - house rules
  - guidelines for security during the full lifecycle (development - test - acceptance - operation – phase out)
  - implementation of contingency provisions
  - handling and securing data carriers
- access security
  - implementation of the policy of securing information
  - maintenance of access rights of customers and applications
  - maintenance of security measures in networks (firewalls, dial-in facilities, bridges, routers, …)

1.5.15 Slide 15: ISM – Evaluation

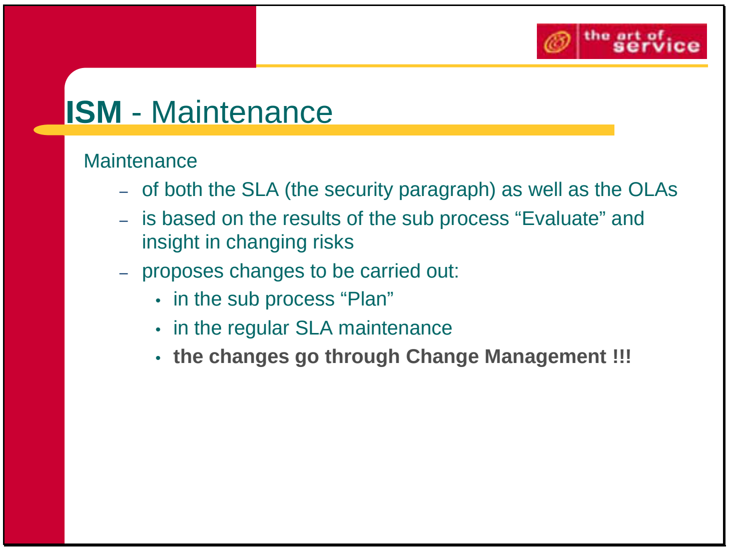


ISM - Evaluation

Evaluation (audit & evaluation)

- self assessments
  - are mainly carried out by the business processes themselves
  - internal audits
  - by internal EDP-auditors
- external audits
  - by external (independent) EDP-auditors
- verification of the security policy
- verification of security plans
- evaluate security incidents
  - detect and react to unwanted use of IT resources

1.5.16 Slide 16: ISM – Maintenance

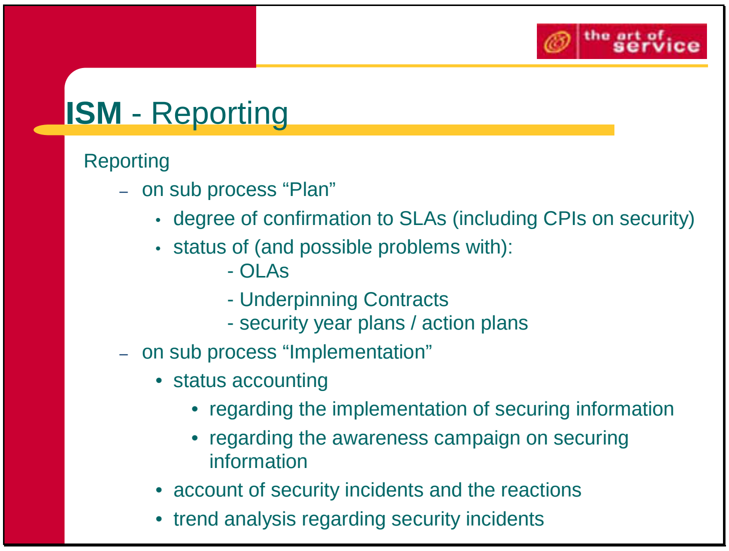


ISM - Maintenance

Maintenance

- of both the SLA (the security paragraph) as well as the OLAs
- is based on the results of the sub process “Evaluate” and insight in changing risks
- proposes changes to be carried out:
  - in the sub process “Plan”
  - in the regular SLA maintenance
  - **the changes go through Change Management !!!**

1.5.17 Slide 17: ISM – Reporting

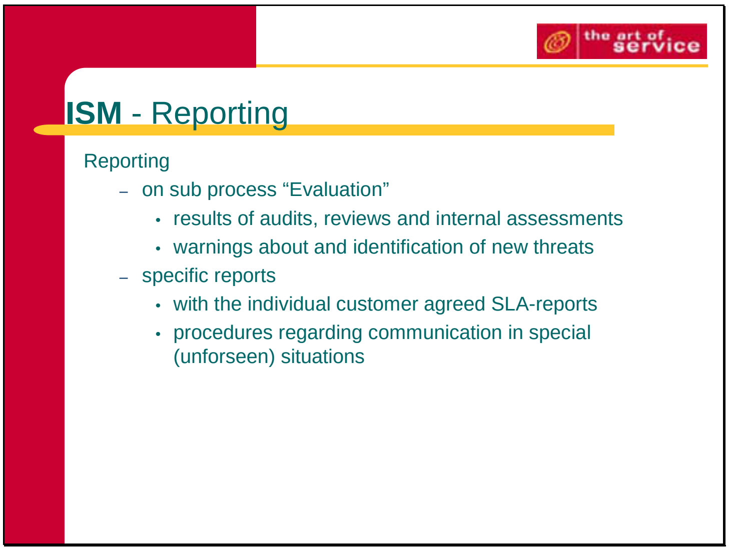


ISM - Reporting

Reporting

- on sub process “Plan”
  - degree of confirmation to SLAs (including CPIs on security)
  - status of (and possible problems with):
    - OLAs
    - Underpinning Contracts
    - security year plans / action plans
- on sub process “Implementation”
  - status accounting
    - regarding the implementation of securing information
    - regarding the awareness campaign on securing information
  - account of security incidents and the reactions
  - trend analysis regarding security incidents

1.5.18 Slide 18: ISM – Reporting

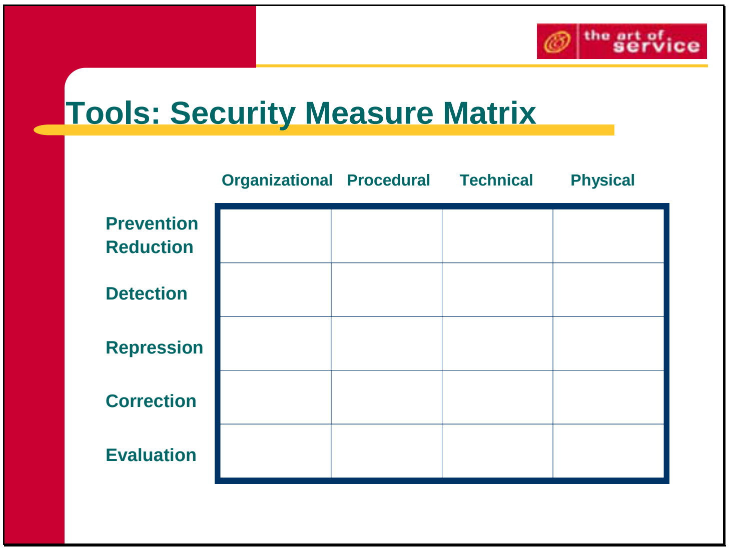


ISM - Reporting

Reporting

- on sub process “Evaluation”
  - results of audits, reviews and internal assessments
  - warnings about and identification of new threats
- specific reports
  - with the individual customer agreed SLA-reports
  - procedures regarding communication in special (unforseen) situations

1.5.19 Slide 19: Security Measure Matrix



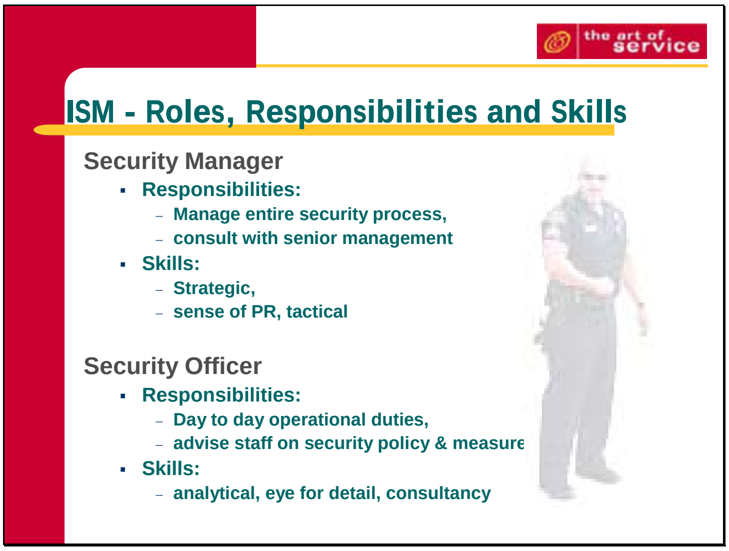
Tools: Security Measure Matrix

	Organizational	Procedural	Technical	Physical
Prevention Reduction				
Detection				
Repression				
Correction				
Evaluation				

The idea is to have a balance in measures. Avoid a concentration of measures in either a certain area (e.g. technical) or of a certain type (e.g. detection).

Remember: ultimately it’s a cost-benefit analysis that determines how much you invest in security.

1.5.20 Slide 20: Roles, Responsibilities & Skills



ISM - Roles, Responsibilities and Skills

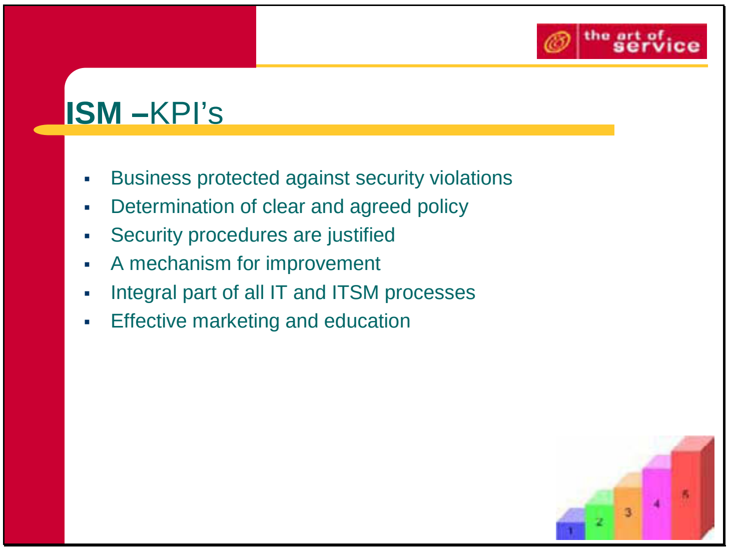
Security Manager

- Responsibilities:
  - Manage entire security process,
  - consult with senior management
- Skills:
  - Strategic,
  - sense of PR, tactical

Security Officer

- Responsibilities:
  - Day to day operational duties,
  - advise staff on security policy & measure
- Skills:
  - analytical, eye for detail, consultancy

1.5.21 Slide 21: Key Performance Indicators



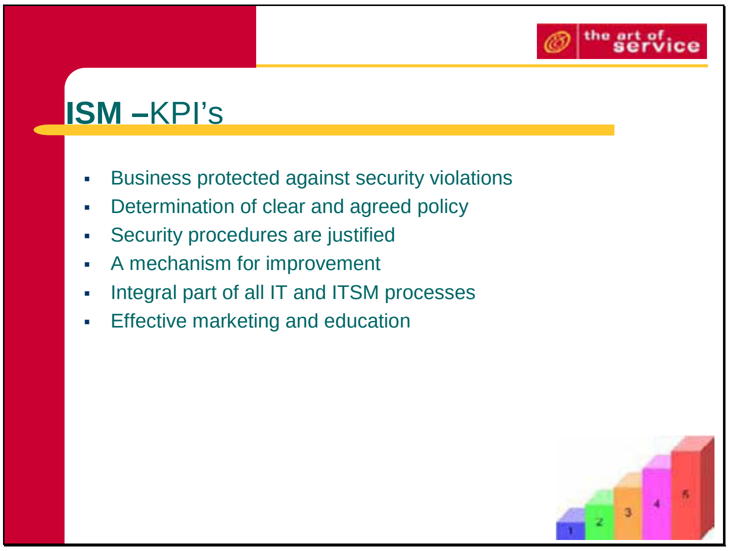
ISM –KPI's

- Business protected against security violations
- Determination of clear and agreed policy
- Security procedures are justified
- A mechanism for improvement
- Integral part of all IT and ITSM processes
- Effective marketing and education

Business protected against security violations:

- Percentage decrease in security breaches reported to the Service Desk
- Percentage decrease in the impact of security breaches and incidents
- Percentage increase in SLA conformance to security clauses.
- The determination of clear and agreed policy, integrated with the needs of the business: decrease in the number of non-conformances of the ISM process with the business security policy and process.
- Security procedures that are justified, appropriate and supported by senior management:
- Increase in the acceptance and conformance of security procedures
- Increased support and commitment of senior management.
- A mechanism for improvement:
- The number of suggested improvements to security procedures and controls

1.5.22 Slide 21 cont…

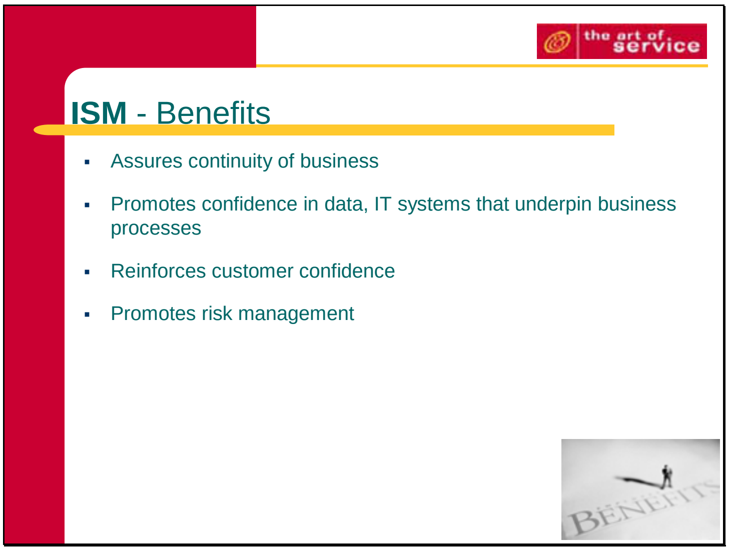


ISM –KPI's

- Business protected against security violations
- Determination of clear and agreed policy
- Security procedures are justified
- A mechanism for improvement
- Integral part of all IT and ITSM processes
- Effective marketing and education

- Decrease in the number of security non-conformance detected during audits and security testing.
- Information security is an integral part of all IT and ITSM processes: increase in the number of services and processes conformant with security procedures and controls.
- Effective marketing and education in security requirements, IT staff awareness of the technology supporting the services:
- Increased awareness of the security policy and its contents, throughout the organization
- Percentage increase in completeness of the technical Service Catalogue against IT components supporting the services.
- Service Desk supporting all services.

1.5.23 Slide 22: Benefits

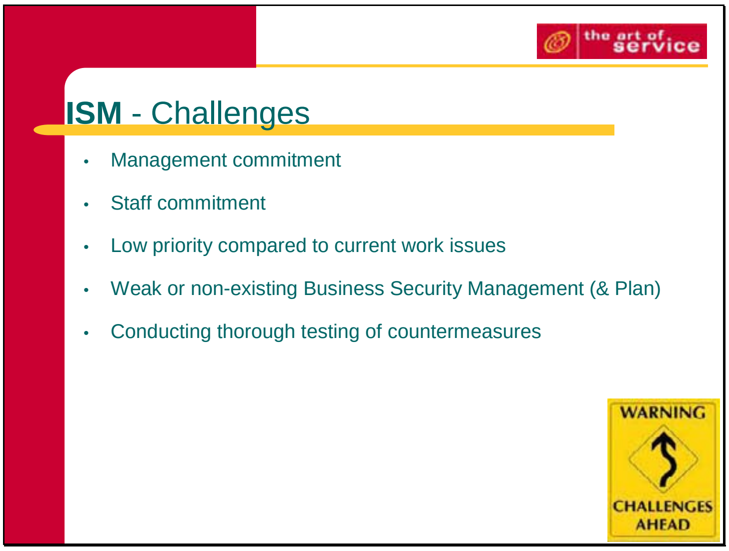


ISM - Benefits

- Assures continuity of business
- Promotes confidence in data, IT systems that underpin business processes
- Reinforces customer confidence
- Promotes risk management

the art of service
BENEFITS

1.5.24 Slide 23: Challenges



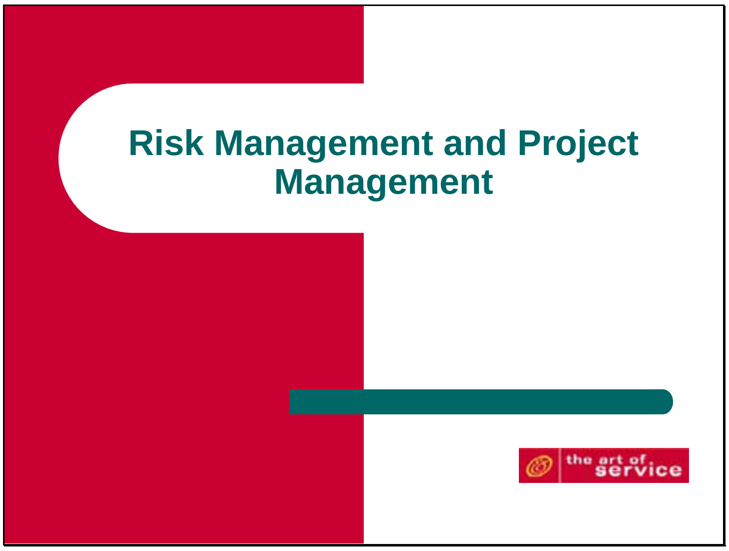
ISM - Challenges

- Management commitment
- Staff commitment
- Low priority compared to current work issues
- Weak or non-existing Business Security Management (& Plan)
- Conducting thorough testing of countermeasures

the art of service
WARNING
CHALLENGES AHEAD

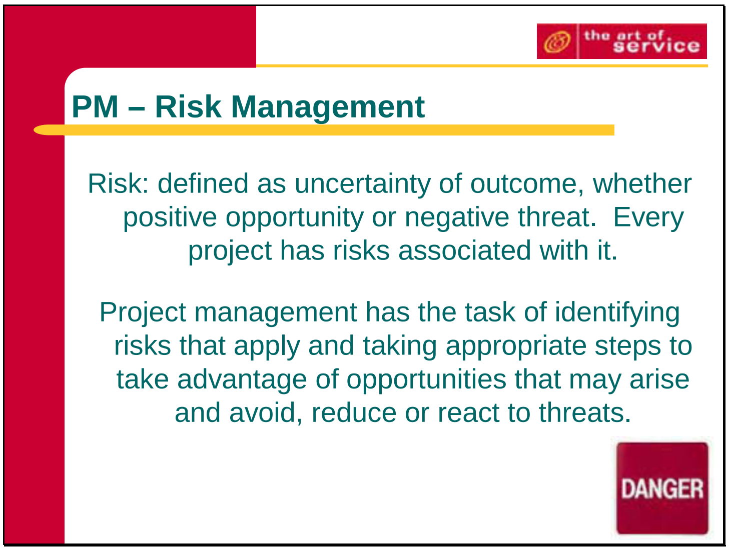
1.6 Risk Management – PROJECT MANAGEMENT

1.6.1 Slide 1: Risk Management & Project Management



Risk Management and Project Management

1.6.2 Slide 2: PM – Risk Management



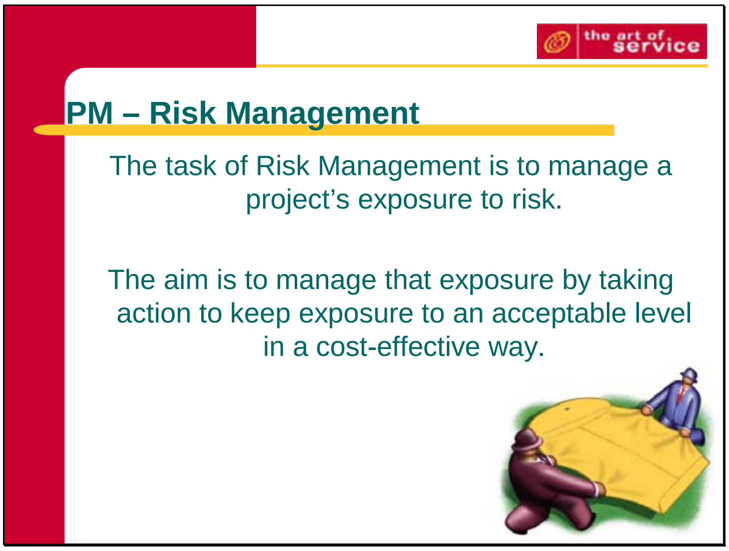
PM – Risk Management

Risk: defined as uncertainty of outcome, whether positive opportunity or negative threat. Every project has risks associated with it.

Project management has the task of identifying risks that apply and taking appropriate steps to take advantage of opportunities that may arise and avoid, reduce or react to threats.

the art of service
DANGER

1.6.3 Slide 3: PM – Risk Management



PM – Risk Management

The task of Risk Management is to manage a project's exposure to risk.

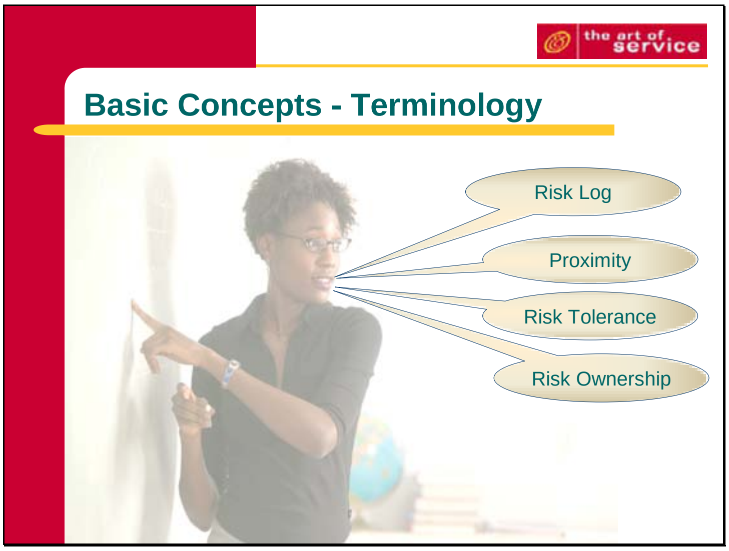
The aim is to manage that exposure by taking action to keep exposure to an acceptable level in a cost-effective way.

Risk Management involves having:

- Access to reliable, up to date information about risks
- Decision-making processes supported by a framework of risk analysis and evaluation
- Processes in place to monitor risks
- The right balance of control in place to deal with those risks.

Risk Management at the project level focuses on keeping unwanted outcomes to an acceptable minimum. Decisions about risk management at this level form an important part of the business case. Where suppliers and/or partners are involved, it is important to gain a shared view of the risks and how they will be managed.

1.6.4 Slide 4: Basic Concepts – Terminology



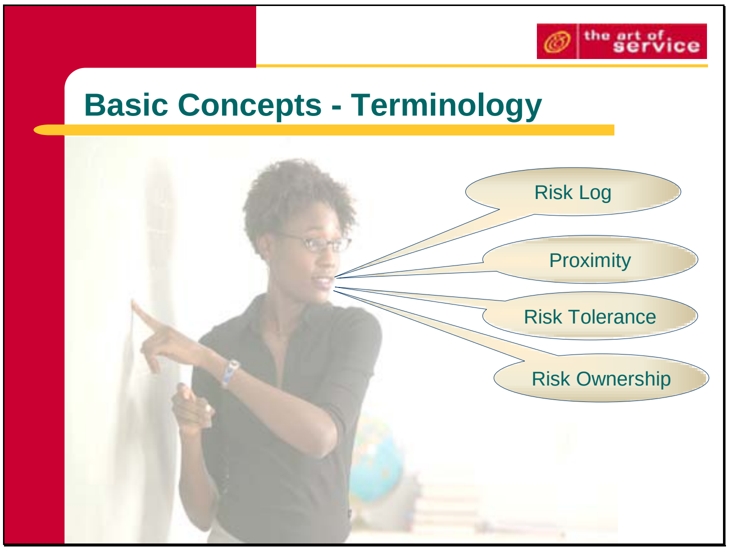
Basic Concepts - Terminology

Risk Log: Contains all information about the risks, their analysis, countermeasures and status. Also known as a Risk Register.

Proximity (of risk): Reflects the timing of the risk, i.e. is the threat (or opportunity) stronger at a particular time, does it disappear some time in the future, or does the probability or impact change over time?

Risk Tolerance: Also known as 'risk appetite'. Before determining what to do about risks, the Project Board and Project Manager must consider the amount of risk they are prepared to tolerate. This will vary according to the perceived importance of particular risks. Risk tolerance can also be related to other tolerance parameters, e.g. timescales and cost etc.

1.6.5 Slide 4 cont…



Basic Concepts - Terminology

Risk Log

Proximity

Risk Tolerance

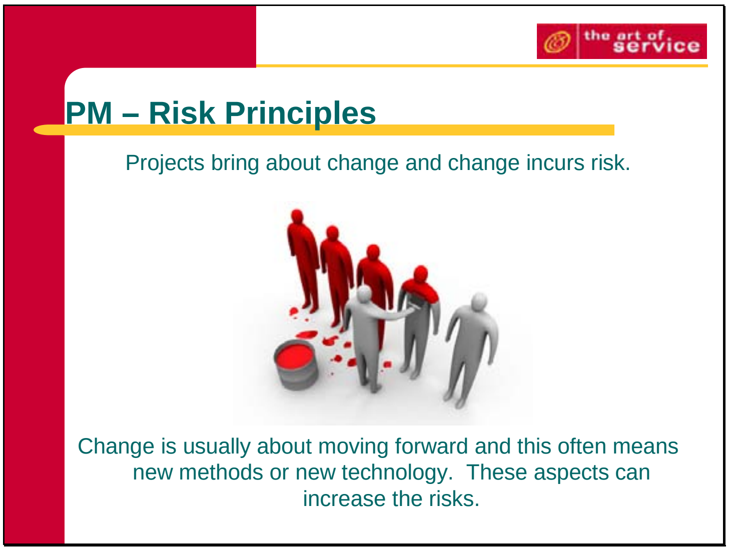
Risk Ownership

Risk Ownership: An ‘owner’ should be identified for each risk; this should be the person best situated to keep an eye on it. The Project Manager will normally suggest the ‘owner’ and the Project Board should make the final decision. When describing who owns the risk, it is important to identify the following:

- Risk framework in totality
- Setting risk policy and the project team’s willingness to take risk
- Different elements of the risk process through to producing risk response and reporting
- Implementation of the actual measures taken in response to the risk
- Interdependent risk that cross organizational boundaries.

A <u>Checklist on Assignment of Risk Ownership</u> can be found on page 191.

1.6.6 Slide 5: PM – Risk Principles



PM – Risk Principles

Projects bring about change and change incurs risk.

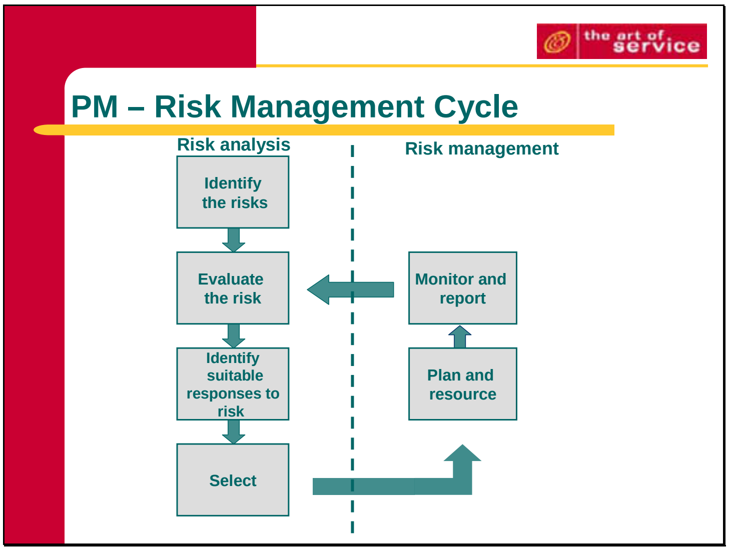
Change is usually about moving forward and this often means new methods or new technology. These aspects can increase the risks.

There are some essential elements that need to be in place in a project if risk management is to be effective and innovation encouraged, i.e. that:

- Project board supports and promotes risk management, and understands and accepts the time and resource implications of any countermeasures
- Risk management policies and the benefits of effective risk management are clearly communicated to all staff.
- A consistent approach to risk management is fully embedded in the project management processes
- Management of risks is an essential contribution to the achievement of business objectives
- Risks through working with programs and other projects are assessed and managed
- There is a clear structure to the risk process so that each element or level of risk identification fits into an overall structure.

Where the project is part of a program, changes in the state of any project risks that are also identified as program risks must be flagged to program management or the designated risk management function in the program.

1.6.7 Slide 6: PM – Risk Management Cycle



PM – Risk Management Cycle

Risk analysis

Risk management

Identify the risks

Evaluate the risk

Identify suitable responses to risk

Select

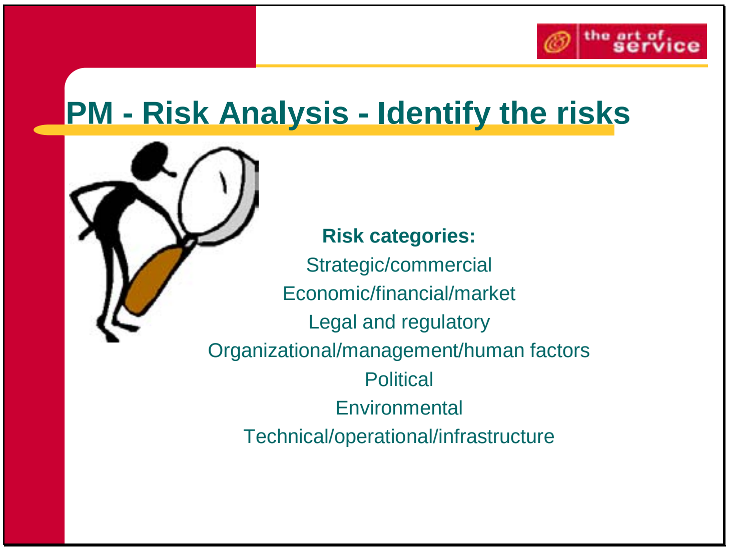
Monitor and report

Plan and resource

Every project is subject to constant change in its business and wider environment. The risk environment is constantly changing too. The project's priorities and relative importance of risks will shift and change. Assumptions about risk have to be regularly revisited and reconsidered; at a minimum, this should occur at each stage assessment.

There is more detail on each of the main steps in the following slides.

1.6.8 Slide 7: Risk Analysis – Identify the Risks



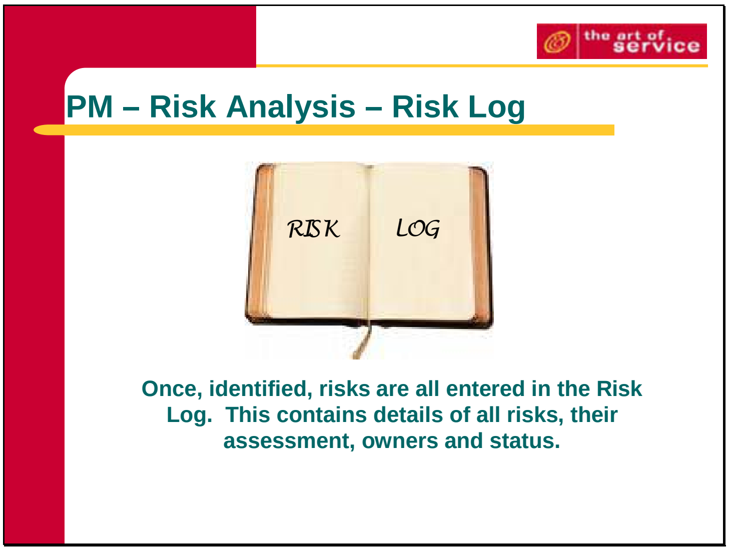
PM - Risk Analysis - Identify the risks

Risk categories:

Strategic/commercial
Economic/financial/market
Legal and regulatory
Organizational/management/human factors
Political
Environmental
Technical/operational/infrastructure

It is important not to judge the likelihood of the risk at this early stage. This is done in a controlled manner in a later step. Attempting to form judgments while identifying a list of potential risks may lead to hurried and incorrect decisions to exclude some risks.

1.6.9 Slide 8: Risk Analysis – Risk Log

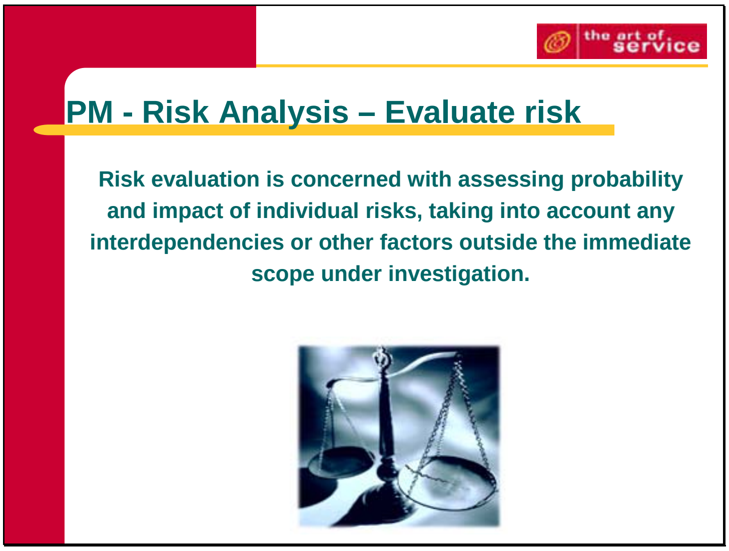


PM – Risk Analysis – Risk Log

Once, identified, risks are all entered in the Risk Log. This contains details of all risks, their assessment, owners and status.

The Risk Log is a control tool for the Project Manager, providing a quick reference to the key risks facing the project, what monitoring activities should be taking place and by whom. Reference to it can lead to entries in the Project Manager's Daily Log to check on the status of a risk or associated activities.

1.6.10 Slide 9: Risk Analysis – Evaluate Risk



PM - Risk Analysis – Evaluate risk

Risk evaluation is concerned with assessing probability and impact of individual risks, taking into account any interdependencies or other factors outside the immediate scope under investigation.

Probability is the evaluated likelihood of a particular outcome actually happening.

Impact is the evaluated effect or result of a particular outcome actually happening.

Impact should ideally be considered under the elements of:

Time

Cost

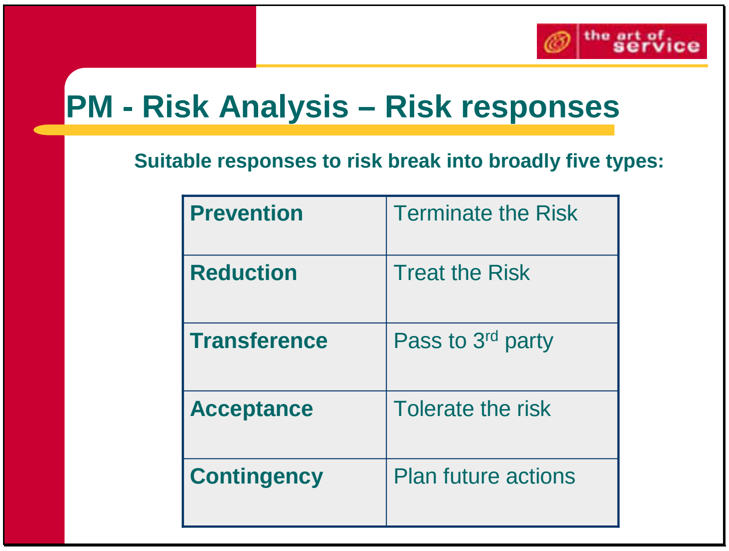
Quality

Scope

Benefit

People/resources.

1.6.11 Slide 10: Risk Analysis – Risk Responses



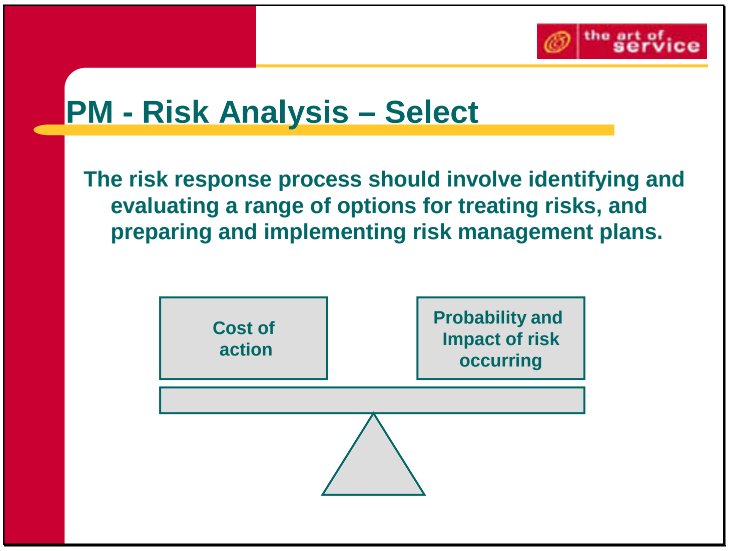
PM - Risk Analysis – Risk responses

Suitable responses to risk break into broadly five types:

Prevention	Terminate the Risk
Reduction	Treat the Risk
Transference	Pass to 3rd party
Acceptance	Tolerate the risk
Contingency	Plan future actions

Any given risk could have appropriate actions in any or all these categories. There may be no cost effective actions available to deal with a risk, in which case the risk must be accepted or the justification for the project revisited, possibly resulting in the termination of the project.

1.6.12 Slide 11: Risk Analysis – Select



PM - Risk Analysis – Select

The risk response process should involve identifying and evaluating a range of options for treating risks, and preparing and implementing risk management plans.

It is important that the control action plan put in place is proportional to the risk. Every control has an associated cost. The control action must offer value for money in relation to the risk its controlling.

Selection of the risk actions to take is a balance between a number of things. For each possible action it is, first a question of balancing cost of taking that action against the likelihood and impact of allowing the risk to occur.

1.6.13 Slide 12: Risk Management – Plan & Resource

PM - Risk Management – Plan & resource

Once the selection is made, implementation of selected actions will need to be planned and resourced. This may include plan changes and new or modified work packages.

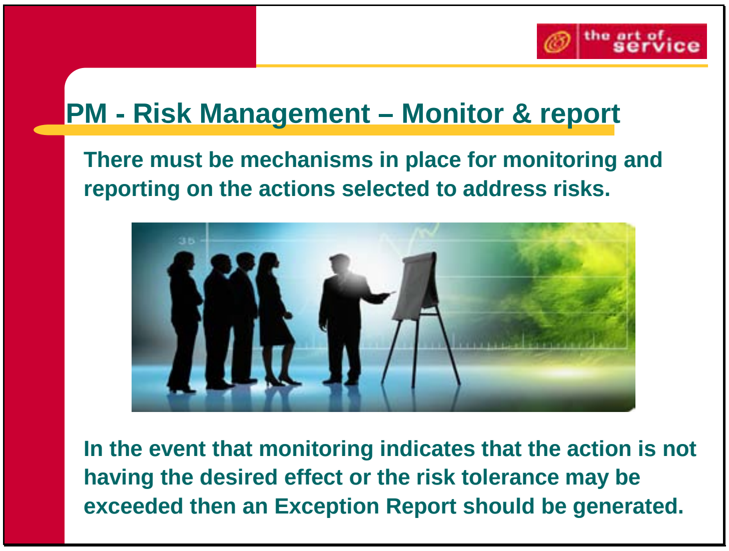
Planning:

- Identifying the quantity and type of resources required to carry out the actions.
- Developing a detailed plan of actions
- Confirming the desirability of carrying out the actions identified during risk evaluation in light of any additional information gained.
- Obtaining management approval along with all the other aspects of the plans being produced.

Resourcing:

- Assignments will be shown in project and stage plans.
- Resources required for the prevention, reduction and transference actions will have to be funded from the project budget since they are actions that we are committed to carrying out.
- Contingency actions will normally be funded from a contingency budget.

1.6.14 Slide 13: Risk Management – Monitor & Report



PM - Risk Management – Monitor & report

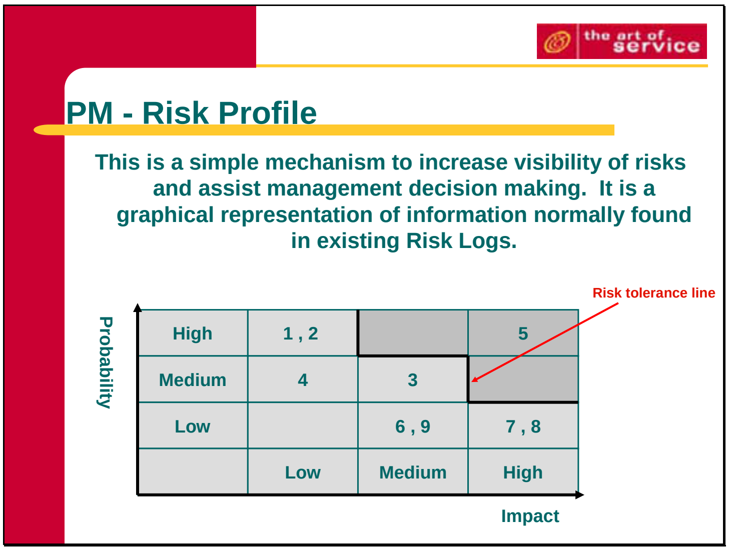
There must be mechanisms in place for monitoring and reporting on the actions selected to address risks.

In the event that monitoring indicates that the action is not having the desired effect or the risk tolerance may be exceeded then an Exception Report should be generated.

Some of the actions may have only been to monitor the identified risks for signs of a change in its status. Monitoring, however, may consist of:

- Checking that execution of the planned actions is having the desired effect
- Watching for the early warning signs that a risk is developing
- Modeling trends, predicating potential risks or opportunities
- Checking that the overall management of risks is being applied effectively.

1.6.15 Slide 14: PM – Risk Profile



PM - Risk Profile

This is a simple mechanism to increase visibility of risks and assist management decision making. It is a graphical representation of information normally found in existing Risk Logs.

Risk tolerance line

Probability

High	1 , 2		5
Medium	4	3	
Low		6 , 9	7 , 8
	Low	Medium	High

Impact

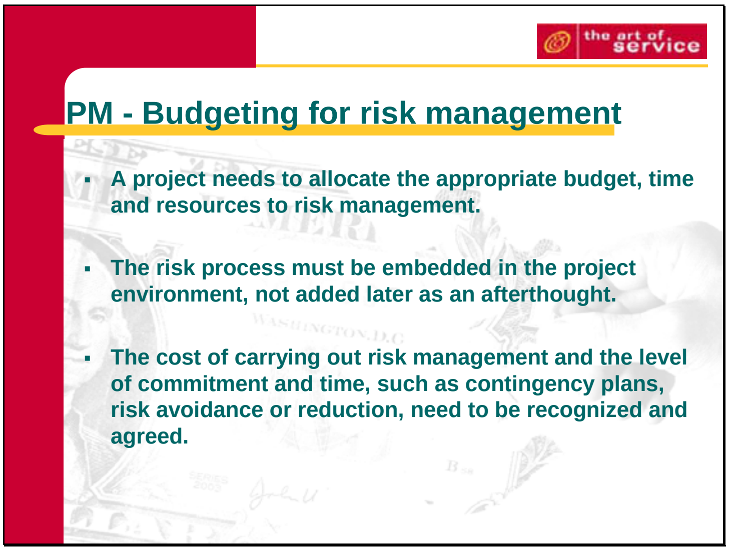
The profile shows risks, using the risk identifier, in terms of probability and impact with the effects of planned countermeasures taken into account. The project manager would update this matrix in line with the Risk Log on a regular basis.

In the above example, risk 5 is already considered to be of high probability and high impact. In particular, any risk shown above and to the right of the 'risk tolerance line' (the thick black line) should be referred upwards. The line is set for the project by agreement between the executive and the project manager.

As risks are reviewed, any changes to their impact or probability which cause them to move above and to the right of the 'risk tolerance line' need to be considered carefully and referred upwards for a management decision on the action to take.

A detailed and usable example of a Generic Project Risk Assessment is available on page 193.

1.6.16 Slide 15: Budgeting for Risk Management

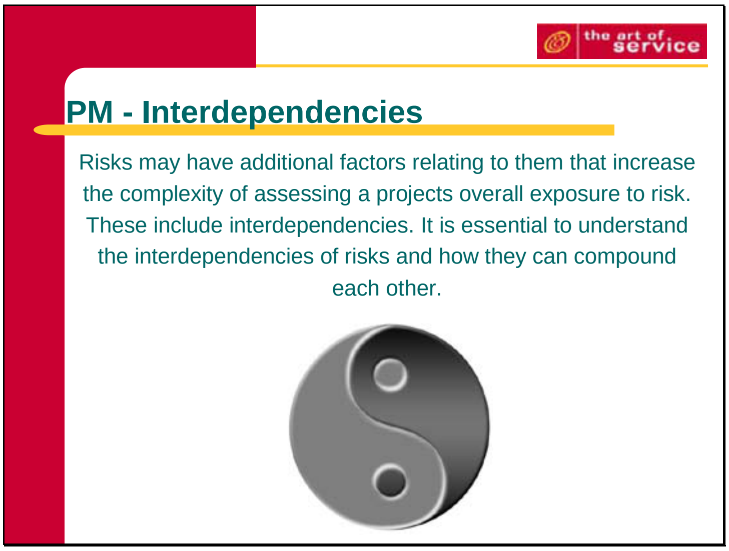


PM - Budgeting for risk management

- A project needs to allocate the appropriate budget, time and resources to risk management.
- The risk process must be embedded in the project environment, not added later as an afterthought.
- The cost of carrying out risk management and the level of commitment and time, such as contingency plans, risk avoidance or reduction, need to be recognized and agreed.

While the budget may be allocated to actions relating to risk treatment, there is often a failure to provide sufficient budget to the earlier parts of the process, such as risk assessment, which can require a diverse range of skills, tools and techniques. Experience has shown that allocating the correct budget to the risk management process early on will pay dividends later.

1.6.17 Slide 16: PM – Interdependencies



PM - Interdependencies

Risks may have additional factors relating to them that increase the complexity of assessing a projects overall exposure to risk. These include interdependencies. It is essential to understand the interdependencies of risks and how they can compound each other.

A project may have interdependencies with other projects. A project may be dependent upon a supplier delivering products or services that have a further interdependency upon another internal project delivering its objectives and so on in the supply chain. These need to be explicitly identified and assessed as part of the process of risk management.

2 SUPPORTING DOCUMENTS

2.1 *Risk Management ITIL V3 – ITSCM*

Through the documents, look for text surrounded by << and >> these are indicators for you to create some specific text.

Watch also for highlighted text which provides further guidance and instructions.

2.1.1 ITSCM Reciprocal Arrangements

IT Services

IT Service Continuity Management Reciprocal Arrangement between Client (X) And Client (Y)

Status:	Draft
Version:	0.1
Release Date:	

Document Control

Author

Prepared by <name and / or department>

Document Source

This document is located on the LAN under the path:

I:/IT Services/Service Delivery/ITSCM/

Document Approval

This document has been approved for use by the following:

- <first name, last name>, IT Services Manager
- <first name, last name>, IT Service Delivery Manager
- <first name, last name>, National IT Help Desk Manager
- <first name, last name>, ITSCM Manager

Amendment History

Issue	Date	Amendments	Completed By

Distribution List

When this procedure is updated the following copyholders must be advised through email that an updated copy is available on the intranet site:

<Company Name> Business Unit	Stakeholders
IT	

Introduction

Purpose

The purpose of this document is to provide relevant Business Units with the existing Reciprocal Arrangements for their IT Services.

Scope

This document describes the following:

- Details of Reciprocal Arrangements between << company name >> and << external company >>

Note: It is assumed for each service described in this document that the supporting back-end technology is already in place and operational.

Audience

This document is relevant to all staff in <company name>

Ownership

IT Services has ownership of this document.

Related Documentation

Include in this section any related Service Level Agreement reference numbers and other associated documentation:

- IT Service Continuity Management Policies, Guidelines and Scope Document (ITSCM2300)
- Business Impact Analysis Template (ITSCM2700)
- Risk Assessment (ITSCM2800)
- Relevant SLA and procedural documents (SLM1901, 1902, 1903)
- IT Services Catalogue (SLM2200)
- Relevant Technical Specification documentation (SLM2202)
- Relevant User Guides and Procedures

More templates and other ITIL process information available at www.itilsurvival.com

Executive Overview

Describe the purpose, scope and organization of the document.

Scope

As not all IT Services may initially be included within the Continuity Management Strategy document, it is important to set the scope for what will be included.

Scope for the Business Continuity Strategy may be determined by the business, therefore covering only a select few of the IT Services provided by the IT department that are seen as critical to the support of the business processes.

Overview

General principles

Include in this section any general principles for the reciprocal arrangement. Below are some examples of these principles.

<<

(Client 1) has agreed with **(Client 2)** to have a reciprocal arrangement for disaster recovery. A consideration of **$** has been paid in respect of this agreement.

In these notes the following terms are used:

- **Host**, to indicate the company that is providing facilities;
- **Client**, to indicate the company using these facilities; and
- **Service**, to indicate all facilities within the provision.

In essence, the plan allows for the following:

- Provision of (**Specify Location**) -based office facilities for up to **(Number of staff people)** staff for a **(Specify length of time)** period.
- Provision of access to **<< Logistics System >>** and PC facilities for **(Specify number of staff members)** staff.
- Periodic testing and checking of the plan.
- Access to facilities in **(Specify location)** including **(Specify client 2)**.

It is understood that:

- Neither firm should make a profit or a loss from this arrangement.
- Both parties will agree to confidentiality of data, clients, and business practices.
- Neither party will seek compensation from the other should any problems or difficulties arise from the service provided.

- This plan will be shown to **(Client 1's)** supplier and, although their approval of such will not be sought, their comments, the subject of the agreement of **(Client 1)** and **(Client 2)**, will be incorporated into the plan. Refer to Appendix F for **(Specify supplier)** agreement to the Plan.
- All items to be used in these plans will be maintained and kept in good working order.
- Termination can only occur within **(Specify length of time)** written notice unless otherwise mutually agreed.
- The agreement will run for **(Specify duration of agreement)** at a time, to be renewable if both parties agree.
- The insurers of each company will be made aware of these plans.
- If a service is provided for more than **(Specify a number of days)** elapsed days (including weekends), then the host will be compensated by the client by payment of agreed fees.
- The client will advise all relevant parties of these temporary arrangements (i.e., business clients, etc.) including the new address, phone number(s) and fax number(s) and will also advise reversion when the service terminates.
- Any data tapes, letter-headed stationery, or other items at the reciprocal party's office will be stored in a secure, lockable place.
- The plan will be capable of being implemented within **(Specify Time)** of a requirement arising within normal office hours. All effort will be made to ensure rapid assistance out of normal office hours.

>>

Definition of a disaster

In this section provide an agreed upon definition of disaster. This is integral to the success of the arrangement. Be very specific and provide all necessary details.

Period of service

Capture the service period for the arrangement in the event of a disaster. This will include maximum duration from the time of the disaster and will usually be provided free of charge by the host for a specified time. This time will be determined here.

Period beyond specified times may be charged at a nominal fee.

Include also the renewing of the contract, probably every year, but should never exceed the date of the contract expiration date.

Prerequisites

<<

For the arrangement to effective to both parties, there needs to be an agreement on any prerequisites. Some examples may be:

- An adequate backup of data should be lodged off-site. This will include << system name >> system data
- Any necessary documentation and appropriate systems
- Sufficient free space will be set aside on computer systems to handle any loaded data.
- Insurers for both companies will be made fully aware of these arrangements.
- Stationary concerns, i.e. adequate printing facilities etc.
- A list of main staff contacts will be distributed, including contact numbers and locations.
- A current signed agreement to this plan is in force.
- The host will only provide services if its own office is not subject to disruption at the same time as the client's.
- This is intended purely to cover both parties in the instance where one or more events disrupt both offices simultaneously.

>>

This is very important.

Well established prerequisites allow both parties to understand the upfront responsibilities. Remember that most reciprocal arrangements will be a two way street. What is meant by this is that Company A will use Company B facilities in the event of a disaster, and Company B will use Company A in the event of a disaster.

As such, it is important not to use this list in an aggressive manner.

Alignment

Specify kind of system, for example: Logistics system

<<

It is vital that the **(Specify kind of system, for example: Logistics system)** each system is transferable

Bearing in mind that the **<< Logistics system >>** has many options available within it and that the **<< Logistics system >>** programs will be used from a common source.

Provision of the **<< Logistics system >>** will be a minimum of, but not limited to:

The follow should be maintained:

- Transaction processing
- Consignment processing
- Risk Processing
- Reporting
- Document Archiving

If required and agreed at the time of need, provision may be made for **<< Logistics System >>** facilities.

>>

Include in this section how administration of the system will be performed, and what limitations or caveats will be in place for the administration of the system.

Include responsibilities pertaining to data backup, restoration and storage.

Keep in mind, that in the event of an emergency, Change and Release procedures are imperative to ensure a structure recovered operation with out causing more issues. Include things like the following:

<<

It is agreed that: Releases of the **<< Logistics System >>** will be aligned so that no more than seven days elapse between installation of like releases at each site.

This requires advance warning to the companies of planned releases. At least **(Specify time period, for example: two weeks)** written notice will be provided. If one party accepts a pre-release program/fix they should notify the other in order that alignment can be maintained, if such is required. If misalignment does occur, it is agreed that the oldest release will be upgraded to the newer release, whether this relates to the client or the host.

>>

Specific data and applications

It is important to ensure that alignment of specific data and applications is maintained. To do this, release numbering and release processes becoming integral to the arrangement. It is important that certain elements be consistent across sites. List them here.

Also list products that do not have to be replicated:

- NT Server will be used
- Microsoft software will be used

Further example of information:

<<

However, it is agreed that each site will use the following products (version/service pack is not vital:

- Microsoft Word
- Microsoft Excel
- Microsoft Access

The following will not be made available as a matter of course, although arrangements can be made as and when a need arises (and if possible):

- List systems and applications that won't be made available

>>

Also include how access to the facilities will be made available. This will be both physical and logical access.

Backup facilities

In this section, list the backup facilities that need to be kept in line with the other sites or systems.

Provisions

<<

The plan provides for provision of a service by the host to the client within two hours of notification that such is required by the client. Obviously not all facilities may be in place within this timeframe.

The service will only be provided if the office of the client is not capable of being used to provide an equivalent service. << include reasons why this could be the case, i.e. flood, fired etc >>. In addition, the service will be provided if the client's office or surrounding area is closed by the authorities.

>>

The following sections list out those necessary provisions required in the event of a disaster.

Office space

Include in this section how access to office space will be arranged. Include a table of names for staff that will require access. Make sure you inform security.

Establish if any passes are required for access or elevators. Directions to the location of the hosting client's office should also be listed here.

The following points need to be considered:

- Access hours
- Access on weekends
- Allowable office space
- Access to pertinent areas within the hosts environment – this may exclude certain server rooms or floors in the building
- Etc.

Work space

How will the work space be set up to cater for the client? Below are some example words that can be used.

<<

Workspace will be made available for up to **(number)** people. It should be assumed that **(number)** attendees will be in the office at any one time, so **(number)** desks and associated facilities will be made available. If more space is available, then this may be offered. Office space assigned will be set aside solely for this use during the required period.

Therefore the following will be made available:

- Minimum of two dedicated desks
- Minimum of two dedicated chairs

These will be located, if at all possible, in the Boardrooms of both **(Client 1)** and **(Client 2)**, although it is accepted that this may not always be possible.

>>

Meeting space

List any requirements for meeting space.

Storage space

Provide details about applicable storage space for the client.

This may include such things as:

- Store Room
- Lockable cabinet
- Etc.

Safe

Provide details about facilities for storing cash, cheque books, or other valuable items will be made available to the client as available.

Office equipment

<<

It is essential that the host provide facilities to enable the client to perform its normal business as much as is possible. Therefore it is agreed to provide:

>>

Telephone

Number of phones and reimbursement plan should be included here.

Fax

Include details about fax facilities.

E-mail

Include details about e-mail facilities.

Mail, courier, and messenger services

Include details about mail, courier and messenger services and reimbursement plans.

Stationery, photocopying, and other facilities

Include details about general office services.

Computer equipment

<<

All computer equipment will be maintained by the host. It is the responsibility of the host to ensure that computer equipment is made immediately available to the client.

>>

PC

Specify any details regarding the provision or supply of PC equipment, including setup, storage, leasing schedules etc.

Printer

Include printer information. This will be the type of printer, the number of printers, and any stationary.

Backups (initial data load)

Include any backup information. This will include:

- Procedures
- Technical Equipment
- People
- Roles and Responsibilities

.

Backups (within service provision)

<<

When the client is able to return to its own office, the host will provide the client with:

- A backup of its system data
- A backup of any data stored on the LAN
- A backup of any data stored on PCs

It is agreed that the following backup facilities will be used:

- UNIX—Normal UNIX backup facility
- LAN data

>>

Specify platform from which data should be backed up

Include platform information and responsibilities pertaining to the host and client.

Specialist requirements

Non-standard items

Record any exceptions regarding client and host requirements in this section. This could include things like nil access to specific equipment or services.

Slips, cover notes, and other documents

List any requirements covering documentation. Include how they are stored and retrieved in the event of a disaster.

Restrictions

List any restrictions that may be applicable when the arrangement is in place and being used.

<<

If it is considered that the client is hindering the host's own processing or office procedures in any way, the client must change or stop such actions immediately, if requested to do so.

>>

Termination Procedure

Of hosting service

This will normally occur when the client has restored adequate facilities in their own environment.

List the reasons for termination and also the roles and responsibilities. Include any necessary clean up.

Of the agreement

<<

This agreement can only be cancelled by one of the following:

- Written notice being given by one company to the other.
- At annual renewal, in which case one month notice should still be provided.
- If agreed between the two companies at any stage.

>>

Responsibilities

Responsibilities for the plan rest with the following:

Client 1: ______________________________
Client 2: ______________________________

The Directors concerned are:
Client 1: ______________________________
Client 2: ______________________________

Testing the Plan

<<

The plan will be tested, at most, twice a year and at least once a year. Dates will be agreed to no less than two weeks before the test date.

Testing will be restricted to the following:

- Loading of data to each other’s system
- Ensuring that access to the system is possible for the client via LAN and
- Logons
- Loading of some documents
- Testing that these documents are accessible

It is not anticipated that testing of the following will occur:

- Telephones
- Fax
- Office space (including desks, chairs, etc)
- PC- or LAN-related items
- Printing

APPENDIX A

AGREEMENT TO

DIASTER RECOVERY PLAN

BETWEEN

<u>CLIENT 1</u>

AND

<u>CLIENT 2</u>

Client 1

Name: ____________________________________
Signed: ____________________________________
Title: ____________________________________
Dated: ____________________________________

Client 2
Name: ____________________________________
Signed: ____________________________________
Title: ____________________________________
Dated: ____________________________________

APPENDIX B

Disaster Recovery Plan

SERVICE CONTACTS

Client 1

Name	Title	Phone Number	Locations / Dept

Client 2

Name	Title	Phone Number	Locations / Dept

APPENDIX C

Disaster Recovery Plan

STAFF TO BE RESIDENT

Client 1

Name	Title	Phone Number	Locations / Dept

Client 2

Name	Title	Phone Number	Locations / Dept

APPENDIX D

Disaster Recovery Plan

STAFF NEEDING TO VISIT OTHER SITE

Client 1

Name	Title	Phone Number	Locations / Dept

Client 2

Name	Title	Phone Number	Locations / Dept

APPENDIX E

Disaster Recovery Plan

Allocation of resources at Client 2

Item	Description	Comments
Desks		
Phones		
Fax		
Laptops		
PCs		
Servers		
Printers		
LAN		
WAN		
Applications		
Licences		
Logons		

APPENDIX G

Client 2 Limited - Items stored Off-Site

At CLIENT 1 under supervision of:

The list below is provided for example. Specify items to be stored and quantity of items per your individual circumstances.

Item	Qty	Location
Stationary		
PCs		
Laptops		
Backup Devices		
Desks		
Chairs		
etc		

2.1.2 ITSCM Business Impact Assessment

IT Services

IT Service Continuity Management Business Impact Assessment

Status:	Draft
Version:	0.1
Release Date:	

Document Control

Author

Prepared by <name and / or department>

Document Source

This document is located on the LAN under the path:

I:/IT Services/Service Delivery/Functional Specifications/

Document Approval

This document has been approved for use by the following:

- ♦ <first name, last name>, IT Services Manager
- ♦ <first name, last name>, IT Service Delivery Manager
- ♦ <first name, last name>, IT Service Continuity Process Manager
- ♦ <first name, last name>, Customer representative or Service Level Manager

Amendment History

Issue	Date	Amendments	Completed By

Distribution List

When this procedure is updated the following copyholders must be advised through email that an updated copy is available on the intranet site:

<Company Name> Business Unit	Stakeholders
IT	

Introduction

Purpose

The Business Impact Analysis allows an analysis and then an identification of the basic critical IT requirements needed to support the business. The purpose of this document is to provide an overview of findings in this analysis.

Scope

This document describes the following:

- Summary of each service provided by IT Services including
- Summary of the Continuity Strategy for each applicable service
- Detailed list of Continuity Strategy for each applicable service

Note: It is assumed for each service described in this document that the supporting back-end technology is already in place and operational.

Audience

This document is relevant to all staff in <company name>

Ownership

IT Services has ownership of this document.

Related Documentation

Include in this section any related Service Level Agreement reference numbers and other associated documentation:

- IT Service Continuity Management Policies, Guidelines and Scope Document (ITSCM2300)
- Business Continuity Strategy Template (ITSCM2900)
- Risk Assessment (ITSCM2800)
- Reciprocal Arrangements (ITSCM3000)
- Relevant SLA and procedural documents (SLM1901, 1902, 1903)
- IT Services Catalogue (SLM2200)
- Relevant Technical Specification documentation (SLM2202)
- Relevant User Guides and Procedures

More templates and other ITIL process information available at www.itilsurvival.com

Executive Overview

Describe the purpose, scope and organization of the Continuity Management Strategy document.

Scope

As not all IT Services may initially be included within the Business Impact Analysis. Use this section to outline what will be included and the timetable for other services to be included.

Scope for the BIA may be determined by the business, therefore covering only a select few of the IT Services provided by the IT department that are seen as critical to the support of the business processes.

IT Service Definition

This section is where you will document the Service Descriptions for the services or applications used by the Business people. This information should be x-referenced to your Service Catalog (SLM2200) and/or related Service Level Agreements. You need to list all the Services here that the BIA is required on.

IT Service	Owner	Business Process	Business Owners	SLA #/Service Catalog Reference	BIA Score (from Details below)	Notes/Comments
Service A	J. Ned	Billing	T. Smith	SLA001	Form + escalation + resource + time	
Email	A. Boon	Communication	R. Jones	SLA234		
SAP	C. Jones	Invoice and Payroll	P. Boon	SLA123		
Service B	L. Smith	Marketing	R. Reagan	SLA009		
Service C	R. Smith	Manufacturing	R. Smith	SLA007		

Note: a high score here indicates a service area that has a potentially high Business impact of lost. The Score can also be used as a guide for the types of service recovery (intermediate, immediate, etc.) that would be acceptable to the business. This score is a starting point for recovery options and considerations.

Service A

(This section needs to be duplicated for each service listed in the table above)

Form of Loss

In this table for this service describe how a disruption to this service will be seen within the business. For example, will the loss of service invoke a contract that has set costs associated with it? If we lose this service can we expect to lose customers/clients/market share. Define each form that the loss of the service may take and give each a score for magnitude.

Form	Description	Magnitude Score (1 is negligible, 10 Severe)
Reputation	Our industry is reputation sensitive	9
Third party support	Contract is invoked to provide 24 hour recovery	7
Frustration of end users	Not high, as end users have other tasks to perform.	4
Etc.	Etc.	Etc.
Total Form of Loss Score		**56**

Other triggers to identify forms of loss:

- Breach of contract, Breach of law or industry imposed standards
- Safety issues
- Confidence drop in skills of Service Providers

Escalation

Use this section to specify for this Service/application the speed at which it is likely that the situation regarding the loss of this service will degrade overall performance.

That is, provide a score of 1 (low) to 10 (highest) that indicates how the service loss will grow in severity.

Escalation Score (1 is slow/barely noticeable, 10 Rapid pace of overall deterioration)
9

Resources Factor

Use this section to specify for this Service/application the combination of the complexity of facilities and the level of skills required in the people that will permit this service to stay operating, in the event of a failure.

That is, provide a score of 1 (low resource requirement) to 10 (maximum resources and skills required).

Resources Score **(1 is minimal skills and resources required to maintain service, 10 Expert level of skills and extensive resources)**
3

Time Considerations

There are two time considerations to factor in to your decision on a score in this area. The first time issue relates to how quickly/slowly the business requires just bare levels of service restored. The second time issue relates to how quickly/slowly the entire service and all associated systems should be fully operational.

That is, provide a score of 1 (slow return to service is acceptable) to 10 (where any real delay in service restoration could have a dire impact upon the business)

Time Factor Score **(1 is non-urgent, 10 is business critical)**
5

Conclusion (not part of the repetitive process)

This template has given you a concise and simple way to look at the impact that the loss of particular IT Services will have on an organization.

We must however remember that the impact of loss will change over time. A BIA should be performed on a regular time basis (to coincide with reviews of the Service Level Management – Service Catalog or Service Level Agreement reviews).

Appendices

Include any applicable appendixes that are needed.

E.g. mission statement and/or business objectives, which drove this BIA.
Relevant details of people who provided input

Terminology

Make sure that all terminology is captured and documented correctly.

E.g.

CMDB	Configuration Management Data Base (www.itilsurvival.com CONMGT stream)
ITSCM	Information Technology Services Continuity Management
SLA	Service Level Agreement (template example at www.itilsurvival.com SLM1901, 1902, 1903)
UC	Underpinning Contract (template example at www.itilsurvival.com SLM2000)

2.1.3 Management of Risk Framework M_O_R

A standard methodology, such as the Management of Risk (M_o_R), should be used to assess and manage risks within an organization. The M_o_R framework is illustrated below in Figure 1.

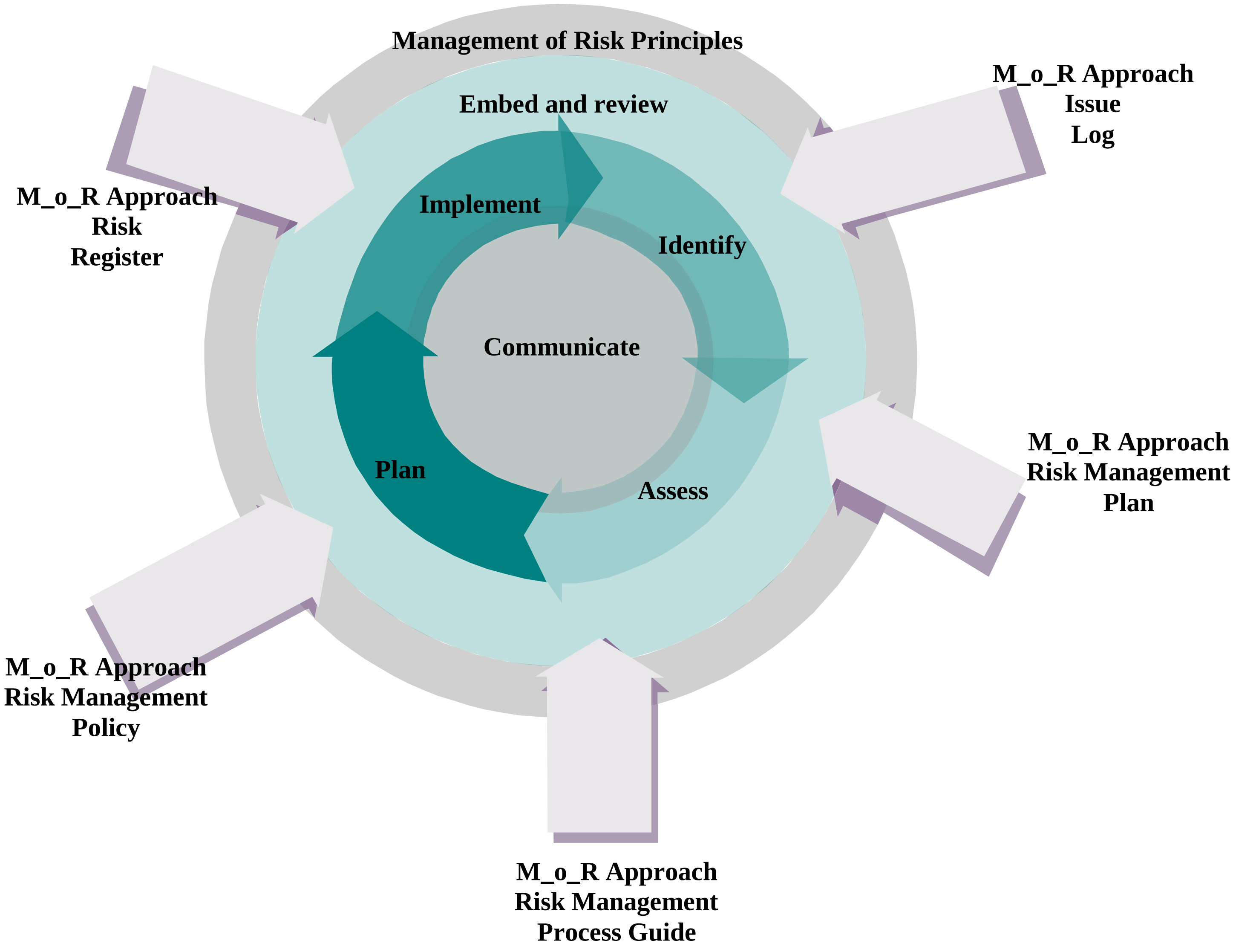


Figure 1.

The M_o_R approach is based around the above framework, which consists of the following:

- **M_o_R principles**: these principles are essential for the development of good risk management practice and are derived from corporate governance principles.
- **M_o_R approach**: an organization's approach to these principles needs to be agreed and defined within the following living documents:
    - Risk Management Policy
    - Process Guide
    - Plans
    - Risk registers
    - Issue Logs.
- **M_o_R Processes**: the following four main steps describe the inputs, outputs and activities that ensure that risk are controlled:
    - **Identify**: the threats and opportunities within an activity that could impact the ability to reach its objective.
    - **Assess:** the understanding of the net effect of the identified threats and opportunities associated with an activity when aggregated together
    - **Plan**: to prepare a specific management response that will reduce the threats and maximize the opportunities.
    - **Implement**: the planned risk management actions monitor their effectiveness and take corrective action where responses do not match expectations.
- **Embedding and reviewing M_o_R**: having put the principles, approach and processes in place, they need to be continually reviewed and improved to ensure they remain effective.
- **Communication**: having the appropriate communication activities in place to ensure that everyone is kept up-to-date with changes in threats, opportunities and any other aspects of risk management.

The M_o_R method requires the evaluation of risks and the development of a risk profile, see example shown in Figure 2.

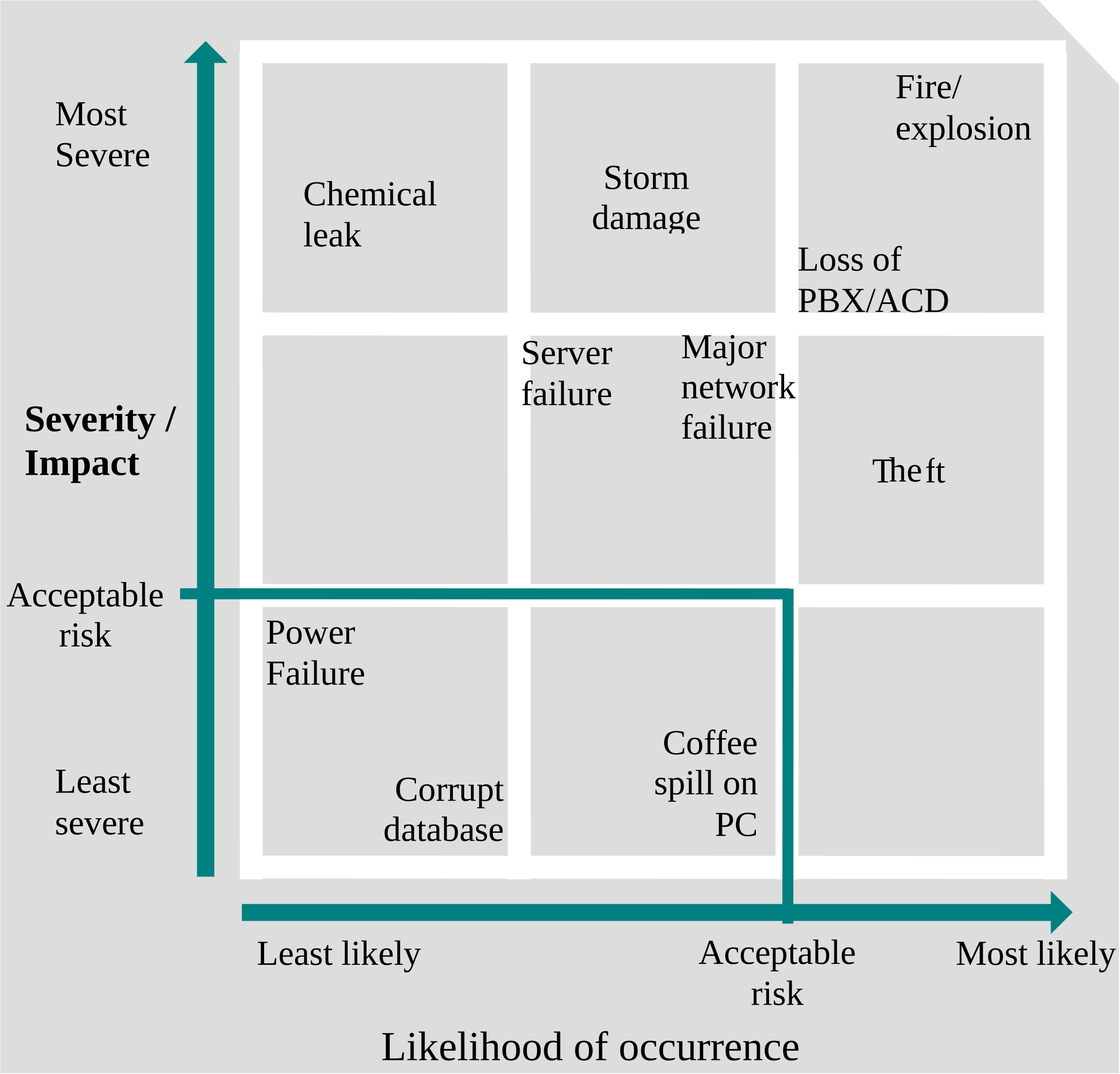


Figure 2.

Figure 2 shows an example risk profile, containing many risks that are outside the defined level of 'acceptable risk'. Following the Risk Analysis it is possible to determine appropriate risk responses or risk reduction measures (ITSCM mechanisms) to manage the risks i.e. reduce the risk to an acceptable level or mitigate the risk. Wherever, possible, appropriate risk responses should be implemented to reduce either the impact or the likelihood, or both, of these risks from manifesting themselves.

2.1.4 IT Risk Assessment Planning

This document describes the major considerations which go into planning the IT Risk Assessment.

OBJECTIVE: Prepare a Risk Assessment Audit of System IT to comply with ACME requirements.

Safeguarding Objectives of ACME

a. Ensure security and confidentiality of customer information.
b. Protect against anticipated threats to the security or integrity of such information
c. Guard against the unauthorized access or use that could result in substantial harm or inconvenience

Basic requirements to be in compliance

Restrict access to those who have a need for the information through logon ID's and passwords. Insure the security of the data during processing and the destruction when no longer needed.

Scope of this Risk Assessment:

d. System IT
e. Hardware and support which serves the entire system.
f. Records containing:
    i. Name
    ii. Address
    iii. Phone number
    iv. Bank account numbers
    v. Credit card account numbers
    vi. Income history
    vii. Credit history
    viii. Social security number
    ix. Medical Records
    x. Financial Records
    xi. Driver's license numbers
    xii. Sex
    xiii. Financial status
    xiv. Salary History
    xv. Personal Check Information (payroll direct deposit)
    xvi. Ethnicity
    xvii. PeopleSoft ID (Employee ID) Number

g. User and Hardware Considerations
    i. Storage protection (fire, disk destruction, system malfunction)
    ii. Disaster recovery and back-up based security issues
        1. loss or corruption of backed-up data
        2. unauthorized use of back-up data
        3. security of back-up data
    iii. Unauthorized access or changes to data by IT staff during maintenance or development activity.
    iv. Security of Inter-campus or UNET transmission of data from unauthorized read or alternation.
    v. Unauthorized access to systems (ex: hacking or casual entry to otherwise secured platforms)
    vi. Maintenance of firewalls, appropriate containment and anti-virus software
    vii. Database intrusion detection and control
    viii. Maintaining the system in accordance with manufacturer's recommendations as to hardware and software maintenance of the platform, operating system and applications software.
    ix. Awareness that email and attachments cannot be prevented from being forwarded.
    x. Awareness that data on unsecured machines and diskettes not under direct control can be used to access the information contained thereon.
    xi. Data transmitted on wireless networks at home and in the community is not secure from read access.
    xii. Theft of computers, laptops, personal organizers etc…will allow data to be distributed to unknown persons.
    xiii. Changing passwords regularly and not sharing them
    xiv. Erasing all data when disposing of or transferring hardware between users.
    xv. Business risks if ID's are shared or if terminals are left unattended.

Risks out of scope

h. Non-IT Risks
    i. Inappropriate use of the information gained from a legitimate IT source or process. i.e. What an individual may do with the information once they have read it from an IT source

Risks in scope

i. IT scope should include from data entry through file destruction including any downstream or related systems.
j. Limit analysis to that data which is gathered, processed or stored in an IT system.
k. INPUT – destruction/safeguarding of source documents not otherwise covered in the review
l. DATA STORAGE
    i. How stored?
    ii. Direct access by an individual
    iii. Access by jobs during processing (imbedded id's and passwords)
    iv. Authorization/validation if data is changed
    v. Verification of data changed by the system from before to after job is run.
    vi. Deletion of data when no longer needed
    vii. Data back-up and recovery procedures

m. Data processing
    i. Disposition of Output from jobs which use the data
        1. paper
        2. files
        3. transmission to other systems
        4. Manual Copying and downstream use.
    ii. Inadvertent change to data during processing
    iii. Known changes to data during processing
    iv. Deletion of data during processing

n. Data Disposal
    i. Retention policy of data of interest

o. Controls:
    i. Where is the data stored
    ii. Is the data copied during any processing to other files that are not purged at the completion of the job?
    iii. What changes have been made to the programs that access the data since the last audit/evaluation
    iv. Which jobs have access to the database
    v. Which users have access to the database
    vi. What is done with the data downstream of any processing?
    vii. Is the data transmitted to another system within or outside the system

2.1.5 IT Risk Assessment Score Sheet

INTERNAL AUDIT DEPARTMENT

IT RISK ASSESSMENT SCORESHEET

Department _________________

System/Application ____________

Risk Score for Criteria	Initial Risk Factors/Criteria	Risk Rating (H, M, L)	Risk Score

H = 5
M = 3
L = 0
	Reputation Risk
	e.g. if the Bank were to be without the system/application for more than a day, it would cause:
	High: a significant disruption in customer service and operations, negative publicity.
	Medium: some disruption in customer service and operations, no negative publicity.
	Low: little or no customer impact, no negative publicity.		

H = 5
M = 3
L = 0
	Regulatory/Compliance Risk
	High: System/application is a key control in ensuring compliance with regulations. Manual intervention for a prolonged period of time is not possible. Problems would cause regulatory violations and possibly fines.
	Medium: System/application, along with other processes, policies and procedures, ensure compliance. Manual intervention is possible and would be required to avoid regulatory violations.
	Low: System/application is not a key control in ensuring compliance with regulations.		

H = 5
M = 3
L = 1
	Customer Data
	High: e.g. system/application stores/processes customer public and/or non-public information.
	Medium: e.g. system/application stores/processes customer public information.
	Low: e.g. system/application stores/processes other 'non-customer' information.		

H = 5	**Financial Statement Impact** *High*: e.g. system/application processes data that comprises a significant percentage (>50%) of the Bank's assets, liabilities, income and/or expense.		

Risk Score for Criteria	Initial Risk Factors/Criteria	Risk Rating (H, M, L)	Risk Score

M = 3
L = 1
	Medium: e.g. system/application process data that comprises between 20% and 49% of the Bank's assets, liabilities, income and/or expense.
	Low: e.g. system/application processes data that comprises less than 20% of the Bank's assets, liabilities, income and/or expense.		

H = 5
M = 3
L = 1
	System/Application Maturity & Stability
	High: e.g. Start-up company and/or brand new product (i.e. less than 1 year old) or installed more than 1 year but system is still evolving and changing.
	Medium: e.g. Mature company/product but new to the Bank (i.e. has been installed for less than 2 years).
	Low: e.g. Mature company/product and has been installed at the Bank for more than 2 years and there are no known problems		

H = 7
M = 3
L = 1
	Complexity of the System/Application
	High: e.g. Complex - LAN, many (>10) users, complex logical security administration, remote access, multiple applications, etc.
	Medium: e.g. LAN or standalone with <10 users, no remote access, one or a few applications, etc.
	Low: e.g. single application, few users, no remote access.		

H = 7
M = 3
L = 1
	Security Risk
	High: e.g. Remote access, access to system/application via internet (e.g. Online Banking), multiple points of entry (servers, workstations, network drops, ports, etc.)
	Medium: e.g. System administered outside of Information Systems Department, no remote access, limited points of entry.
	Low: e.g. No remote access, no internet access, standalone PC.		

H = 5
M = 3
L = 1
	Vendor Risk
	High: e.g. Vendor was rated "High" in the Vendor Final Risk Assessment.
	Medium: e.g. Vendor was rated "Medium in the Vendor Final Risk Assessment.
	Low: e.g. Vendor was rated "Low" in the Vendor Final Risk Assessment.		

H = 10
M = 5
L = 1
	Management, Audit Committee, External Auditor Concern
	High: Direct request for current cycle review.
	Medium: Concern Expressed or requested for future review.
	Low: No known concern.		

	Prior Audit Results: Nature and criticality of findings/conditions noted in external audit management letter,		

Risk Score for Criteria	Initial Risk Factors/Criteria	Risk Rating (H, M, L)	Risk Score

H = 3
L = 1
	internal audit reports/follow-ups or regulatory reviews.
	High: Continuing lack of implementation of corrective action to key control problems, etc...
	Low: Minor or no findings, or strong implementation of a corrective action.		

		TOTAL	

IT RISK ASSIGNMENT (Check One)

___ **High** = Total Score 31 - 57 ______ **Medium** = Total Score 12 - 30 ______ **Low** = Total Score = 0 - 11

Completed by (please print): ____ Date: __________________________

2.1.6 Risk Assessment and Control Form

Risk Assessment and Control Form	

Division:	Unit:

Documents Number:	Initial Issue Date:	Current Version:	Current Version Issue Date:	Next Review Date:

Step 1: Identify the Activity

Unit:

Describe the Activity:

Describe the Location:

Step 2: Identify who may be at risk by the activity

A number of people may be at risk from any activity. This may affect the risk controls needed. These people may include fellow workers, visitors, contractors and the public. The location of the activity may affect the number of people at risk.

Steps 3 to 7: Identify the hazards, risks, and rate the risks

1. An activity may be divided into tasks. For each task identify the hazards and associated risks.
2. List existing risk controls and determine a risk rating using the ACME Risk Rating Procedure.
3. Additional risk controls may be required to achieve an acceptable level of risk. Re-rate the risk if additional risk controls used.

Tasks	Hazards (Step 3)	Associated Risks (Step 4)	Existing Risk Controls	Risk rating with existing controls *			Additional risk controls required (Step 6) (Apply the hierarchy of risk controls)	Risk rating with additional controls * (Step 7)		
				C	L	R		C	L	R

C = Consequence   L = Likelihood   R = Risk Rating

Step 8: Documentation and Initial Approval

Completed by: (name) (signature)

Authorized by: (name) (signature) Date:

Step 9: Implement the additional risk controls identified

Indicate briefly what additional risk controls from Step 6 above were implemented, when and by whom.

Risk control: Date: Implemented by:

Risk control: Date: Implemented by:

Risk control: Date: Implemented by:

Risk control: Date: Implemented by:

Risk control: Date: Implemented by:

Step 10: Monitor and review the risk controls

It is important to monitor risk controls and review risk assessments regularly. Review is required when there is a change in the process, relevant legal changes, and where a cause for concern has arisen. Reviews could be scheduled on an annual basis. If the risk assessment has substantially changed a new risk assessment is warranted.

Risk control:	Reviewed by:	Authorized by:
Risk control:	Reviewed by:	Authorized by:
Risk control:	Reviewed by:	Authorized by:
Risk control:	Reviewed by:	Authorized by:
Risk control:	Reviewed by:	Authorized by:

Documentation

It is a requirement that legal and advisory documentation that supports this risk assessment be listed. Such documentation includes Acts, Regulations, Australian Standards and Codes of Practice, where applicable.

2.1.7 Risk Assessment Questionnaire

Instructions for Completing the Risk Assessment Questionnaire

Please answer the following information security program questions as of the examination date pre-determined by the ACME. The majority of the questions require only a “Yes” or “No” response; however, you are encouraged to expand or clarify any response as needed directly below each question, or at the end of this document under the heading “Clarifying or Additional Comments”. For any question deemed non-applicable to your institution or if the answer is “None”, please respond accordingly (“NA” or “None”). Please do not leave responses blank. At the bottom of this document is a signature block, which must be signed by an executive officer attesting to the accuracy and completeness of all provided information.

I hereby certify that the following statements are true and correct to the best of my knowledge and belief.		
Officer’s Name and Title	**Institution’s Name and Location**	
Officer’s Signature	**Date Signed**	**As of Date**
This is an official document. Any false information contained in it may be grounds for prosecution and may be punishable by fine or imprisonment.		

PART 1 – RISK ASSESSMENT

An IT risk assessment is a multi-step process of identifying and quantifying threats to information assets in an effort to determine cost effective risk management solutions. To help us assess your risk management practices and the actions taken as a result of your risk assessment, please answer the following questions:

a. Name and title of individual(s) responsible for managing the IT risk assessment process:

b. Names and titles of individuals, committees, departments or others participating in the risk assessment process. If third-party assistance was utilized during this process, please provide the name and address of the firm providing the assistance and a brief description of the services provided:

c. Completion date of your most recent risk assessment:

d. Is your risk assessment process governed by a formal framework/policy (Y/N)?

e. Does the scope of your risk assessment include an analysis of internal and external threats to confidential customer and consumer information as described in ... of the ACME's Rules and Regulations (Y/N)?

f. Do you have procedures for maintaining asset inventories (Y/N)?

g. Do risk assessment findings clearly identify the assets requiring risk reduction strategies (Y/N)?

h. Do written information security policies and procedures reflect risk reduction strategies identified in "g" above (Y/N)?

i. Is your risk assessment *program* formally approved by the Board of Directors at least annually (Y/N)?

   If yes, please provide the date that the risk assessment program was last approved by the Board of Directors:

j. Are risk assessment *findings* presented to the Board of Directors for review and acceptance (Y/N)?
   If yes, please provide the date that the risk assessment findings were last approved by the Board of Directors:

PART 2 – OPERATIONS SECURITY AND RISK MANAGEMENT

To help us assess how you manage risk through your information security program, please answer the following questions for your environment. If any of the following questions are not applicable to your environment, simply answer “N/A.”

a. Please provide the name and title of your formally designated IT security officer:

b. Please provide the name and title of personnel in charge of operations:

c. Do you maintain topologies, diagrams, or schematics depicting your physical and logical operating environment(s) (Y/N)?

d. Does your information security program contain written policies, procedures, and guidelines for securing, maintaining, and monitoring the following systems or platforms:

1. Core banking system (Y/N)?
2. Imaging (Y/N)?
3. Fed Line and/or wire transfer (Y/N)?
4. Local area networking (Y/N)?
5. Wide-area networking (Y/N)?
6. Wireless networking – LAN or WAN (Y/N)?
7. Virtual private networking (Y/N)?
8. Voice over IP telephony (Y/N)?
9. Instant messaging (Y/N)?
10. Portable devices such as PDAs, laptops, cell phones, etc. (Y/N)?
11. Routers (Y/N)?
12. Modems or modem pools (Y/N)?
13. Security devices such as firewall(s) and proxy devices. (Y/N)?
14. Other remote access connectivity such as GoToMyPC, PcAnyWhere, etc. (Y/N)?
15. Other – please list:

e. Do you have formal logging/monitoring requirements for 1-15 above (Y/N)?

f. Do you have formal configuration, change management, and patch management procedures for all applicable platforms identified in “d.” above (Y/N)?

g. Do you have an antivirus management program to protect systems from malicious content (Y/N)?

h. Do you have an anti-spyware management program to protect end-user systems (Y/N)?

i. Do you have a formal intrusion detection program, other than basic logging, for monitoring host and/or network activity (Y/N)?

j. Has vulnerability testing been performed on internal systems (Y/N)?

   If yes, please provide date performed and by whom:

k. Has penetration testing of your public or Internet-facing connection(s) been performed (Y/N)?

   If yes, please provide date performed and by whom:

l. Do you have an incident response plan defining responsibilities and duties for containing damage and minimizing risks to the institution (Y/N)?

   If yes, does the plan include customer notification procedures (Y/N)?

m. Do you have a physical security program defining and restricting access to information assets (Y/N)?

n. Do you have a vendor management program (Y/N)?

o. Are all of your service providers located within the United States (Y/N)?

p. Do you have an employee acceptable use policy (Y/N)?

   If yes, please provide how often employees must attest to the policy contents:

q. Do you have an employee security awareness training program (Y/N)?

   If yes, please indicate the last date training was provided:

r. Are you planning to deploy new technology within the next 12 months (Y/N)?

   If you answered “Yes”, were the risks associated with this new technology reviewed during
   your most recent risk assessment (Y/N)?

s. Have you deployed new technology since the last ACME examination that was not included in your last risk assessment (Y/N)?

t. Is security incorporated into your overall strategic planning process (Y/N)?

u. Do you have policies/procedures for the proper disposal of information assets (Y/N)?

PART 3 – AUDIT/INDEPENDENT REVIEW PROGRAM

To help us assess how you monitor operations and compliance with your written information security program, please answer the following questions:

a. Please provide the name and title of your IT auditor or employee performing internal IT audit functions. Include who this person reports to, and a brief description of their education and experience conducting IT audits.

b. Do you have a written IT audit/independent review program (Y/N)?

c. Please provide the following information regarding your most recent IT audit/independent review:

   1. Audit Date:
   2. Firm name (if external):
   3. Was an audit report produced (Y/N)?
   4. Date audit report was reviewed and approved by the Board:
   5. Audit scope and objectives:

d. Does audit coverage include a comparison of actual system configurations to documented/baseline configuration standards (Y/N)?

e. Does audit coverage include assessing compliance with the information security program requirements (Y/N)?

f. Does audit coverage include assessing users and system services access rights (Y/N)?

g Is audit involved in your risk assessment process (Y/N)?

h. Briefly describe any security incidents (internal or external) affecting the bank or bank customers occurring since the last ACME IT examination.

Briefly describe any known conflicts or concentrations of duties.

PART 4 - DISASTER RECOVERY AND BUSINESS CONTINUITY

To help us assess your preparedness for responding to and recovering from an unexpected event, please answer the following:

a. Do you have an organization-wide disaster recovery and business continuity program (Y/N)?

If yes, please provide the name of your coordinator:

b. Are disaster recovery and business continuity plans based upon a business impact analyses (Y/N)?

If yes, do the plans identify recovery and processing priorities (Y/N)?

c. Is disaster recovery and business continuity included in your risk assessment (Y/N)?

d. Do you have formal agreements for an alternate processing site and equipment should the need arise to relocate operations (Y/N)?

e. Do business continuity plans address procedures and priorities for returning to permanent and normal operations (Y/N)?

f. Do you maintain offsite backups of critical information (Y/N)?

If "Yes," is the process formally documented and audited (Y/N)?

g. Do you have procedures for testing backup media at an offsite location (Y/N)?

h. Have disaster recovery/business continuity plans been tested (Y/N)?

If "Yes", please identify the system(s) tested, the corresponding test date, and the date reported to the Board:

Clarifying or Additional Comments:

2.1.8 ITSCM Business Continuity Strategy

IT Services

IT Service Continuity Management Business Continuity Strategy

Status:	Draft
Version:	0.1
Release Date:	

Document Control

Author

Prepared by <name and / or department>

Document Source

This document is located on the LAN under the path:

I:/IT Services/Service Delivery/Functional Specifications/

Document Approval

This document has been approved for use by the following:

- <first name, last name>, IT Services Manager
- <first name, last name>, IT Service Delivery Manager
- <first name, last name>, National IT Help Desk Manager

Amendment History

Issue	Date	Amendments	Completed By

Distribution List

When this procedure is updated the following copyholders must be advised through email that an updated copy is available on the intranet site:

<Company Name> Business Unit	Stakeholders
IT	

Introduction

Purpose

The purpose of this document is to provide relevant Business Units with the Business Continuity Strategies for the range of services provided by IT Services to the <company name> community.

Scope

This document describes the following:

- Summary of each service provided by IT Services including
- Summary of the Continuity Strategy for each applicable service
- Detailed list of Continuity Strategy for each applicable service

Note: It is assumed for each service described in this document that the supporting back-end technology is already in place and operational.

Audience

This document is relevant to all staff in <company name>

Ownership

IT Services has ownership of this document.

Related Documentation

Include in this section any related Service Level Agreement reference numbers and other associated documentation:

- IT Service Continuity Management Policies, Guidelines and Scope Document (ITSCM2300)
- Business Impact Analysis Template (ITSCM2700)
- Risk Assessment (ITSCM2800)
- Reciprocal Arrangements (ITSCM3000)
- Relevant SLA and procedural documents (SLM1901, 1902, 1903)
- IT Services Catalogue (SLM2200)
- Relevant Technical Specification documentation (SLM2202)
- Relevant User Guides and Procedures

More templates and other ITIL process information available at www.itilsurvival.com

Executive Overview

Describe the purpose, scope and organization of the Continuity Management Strategy document.

Scope

As not all IT Services may initially be included within the Continuity Management Strategy document, it is important to set the scope for what will be included.

Scope for the Business Continuity Strategy may be determined by the business, therefore covering only a select few of the IT Services provided by the IT department that are seen as critical to the support of the business processes.

IT Service Continuity Strategy Summary

This section provides a summary of all the IT Services covered within the Business Continuity Strategy. It provides a break down of all the IT Services, the Recovery Options, Owners of IT Service, Affected Business Processes, and Threat to Business Operations, Service Level Agreements, and associated procedures.

IT Service		Service A	Email	SAP	Service B	Service C
Owner		J. Ned	A. Boon	C. Jones	L. Smith	R. Smith
Recovery Options	Work Around	Yes	No	No	Yes	Yes
	Gradual	Backup Tapes	Backup CD	Backup Tapes	Rebuild	Rebuild
	Intermediate	Reciprocal Arrangement	Reciprocal Arrangement	No	No	No
	Immediate	No	Replicated Server	Replicated Service	No	No
Business Process		Billing	Communication	Invoice and Payroll	Marketing	Manufacturing
Threat to Business		High	Low	Very High	Medium	High
Business Owners		T. Smith	R. Jones	P. Boon	R. Reagan	R. Smith
Service Level Agreements	SLA#	SLA001	SLA234	SLA123	SLA009	SLA007
	Response Time	4 Hours	2 Hours	30 mins	1 Hour	30 mins
	Recovery Time	8 Hours	4 Hours	2 Hours	3 hours	2 Hours
Applicable Procedures		IncMgt101	ComRec231	N/A	N/A	N/A

Service A

Please Note. Some of the sub-headings here may not be applicable for the IT Service. For example, in some instance where you have an Immediate Recovery Option for a Service it may not be applicable to have spent money on Gradual Recovery Options, and vice versa.

Description

Provide a description of the IT Services. Include all relevant SLA and Ownership Details.

Service	Owner	Service Level Agreements			Procedures	Business Process	Business Impact
		SLA #	Response Times	Recovery Times			

Risk Summary

In this section provide a brief description of any know and major risks to the IT Service. Risks are determined by understanding the assets that are involved in the service, the threats to those assets and any identified threats.

A risk summary table, below, provides a summary of risks to the IT Service.

Assets/Service	Threats	Vulnerabilities	Risk Level

Definitions:

A **threat** is 'how likely is it that a particular service will be disrupted.
Vulnerability assesses what the impact will be upon the organization if the threat manifests.
The **risk level** is then the combination of the threat and the vulnerability. It can be reached through a quantitative analysis or simply a subjective feel.

After completing the above table, summaries the overall risk to the service and the impact on the business.

Manual Work Around

As it is not possible to always provide an immediate IT solution to every disaster, it is therefore imperative to capture any manual work around options that may be available.

A manual work around can be seen as an effective interim measure until the IT Service has been restored.

The manual workarounds will be for both IT departments and the Business. List all Manual Work Around options in this section.

IT Procedure	Owner	Business Procedure	Business Owner

Reciprocal Arrangements

In some situations, organizations will rely on like minded businesses to provide services in the event that they experience some sort of loss of service. This is called a reciprocal Arrangement.

Reciprocal Arrangements may be made with several organizations for the one service.

Reciprocal Arrangement - <<Company Name>>

Contract or Agreement	Agreed Services (Underpinning Contract or Service Level Agreement)			Business Contact	IT Service Contact
	Response Time	Recovery Time	Durations		

Reciprocal Arrangement - <<Company Name>>

Contract or Agreement	Agreed Services (Underpinning Contract or Service Level Agreement)			Business Contact	IT Service Contact
	Response Time	Recovery Time	Durations		

Gradual Recovery

This recovery options is used for services where immediate restoration of business processes is **not** needed and can function for up to a period of 24 to 72 hours as defined in a service agreement.

Agreements

Agreements will include those with the business for Gradual Recovery. They will also include any additional accommodation and services plans.

Technology

This section will provide details about the computer systems and network plans, as well as any telecommunications plans.

Security

In the event of a disaster, there may be some impact on the security of the IT Department and the business as a whole. In this section include any security issues, appropriate security plans, and security to be tested and revisited after recovery.

Finance

Include in this section any required finance for the recovery options. This information will be used in the budgeting process for subsequent years.

Personnel

List all responsible personnel for the recovery of this service.

Summary

Provide a summary for the Gradual Recovery of Service << Service Name >>

Intermediate Recovery

This recovery options is used for services that are important enough to the business that a 4 to 24 hour restoration period is required.

Agreements

> Agreements will include those with the business for Gradual Recovery. They will also include any additional accommodation and services plans.

Technology

> This section will provide details about the computer systems and network plans, as well as any telecommunications plans.

Security

> In the event of a disaster, there may be some impact on the security of the IT Department and the business as a whole. In this section include any security issues, appropriate security plans, and security to be tested and revisited after recovery.

Finance

> Include in this section any required finance for the recovery options. This information will be used in the budgeting process for subsequent years.

Personnel

> List all responsible personnel for the recovery of this service.

Summary

> Provide a summary for the Gradual Recovery of Service << Service Name >>

Immediate Recovery

This recovery options is used for services where immediate restoration of business processes is needed and the business will suffer severe consequences if restoration is not within 2 to 4 hours.

Agreements

Agreements will include those with the business for Gradual Recovery. They will also include any additional accommodation and services plans.

Technology

This section will provide details about the computer systems and network plans, as well as any telecommunications plans.

Security

In the event of a disaster, there may be some impact on the security of the IT Department and the business as a whole. In this section include any security issues, appropriate security plans, and security to be tested and revisited after recovery.

Finance

Include in this section any required finance for the recovery options. This information will be used in the budgeting process for subsequent years.

Personnel

List all responsible personnel for the recovery of this service.

Summary

Provide a summary for the Gradual Recovery of Service << Service Name >>

Appendices

Include any applicable appendixes that are needed.

E.g. Logical Schematic of the IT environment.
Contact details

Terminology

Make sure that all terminology is captured and documented correctly.

E.g.

CMDB	Configuration Management Data Base (www.itilsurvival.com CONMGT stream)
ITSCM	Information Technology Services Continuity Management
SLA	Service Level Agreement (template example at www.itilsurvival.com SLM1901, 1902, 1903)
UC	Underpinning Contract (template example at www.itilsurvival.com SLM2000)

2.1.9 Typical Contents of a Recovery Plan

The typical contents of an ITSCM recovery plan are as follows.

Generic Recovery Plan

Document Control

This document must be maintained to ensure that systems, Infrastructure and facilities included, appropriately support business recovery requirements.

Document Distribution

Copy	Issued to	Date	Position
1.			
2.			
3.			
4.			

Document Revision

This document will be reviewed every X months.

Current Revision: *date*
Next Revision: *date*

Revision Date	Version No	Summary of Changes

Document Approval

This document must be approved by the following personnel:

Name	Title	Signature

Supporting Information

Introduction

This document details the instructions and procedures that are required to be followed to recover or continue the operation of systems, Infrastructure, services or facilities to maintain service continuity to the level defined and agreed with the business.

Recovery Strategy

The systems, Infrastructure, services or facilities will be recovered to alternative systems, infrastructure, services or facilities.

It will take approximately X hours to recover the systems, infrastructure, services or facilities. The system will be recovered to the last known point of stability/data integrity, which is point in day/timing.

The required recovery time for this system, infrastructure, service or facility is:

The required time and procedures for this system infrastructure, service or facility was last tested on:

Invocation

The following personnel are authorized to invoke this plan:
1
2

Interfaces and dependencies on other plans

Details of the inter-relationships and references with all other continuity and recovery plans and how the interfaces are activated.

General Guidance

All requests for information from the media or other sources should be referred to the company procedure.

When notifying personnel of a potential or actual disaster, follow the defined operational escalation procedures, an in particular:

- Be calm and avoid lengthy conversation
- Advise them of the need to refer information requests to escalation point
- Advise them of expectations and actions (avoid giving them details of the incident unless absolutely necessary)
- If the call is answered by somebody else:
    - Ask if the contact is available elsewhere
    - If they cannot is available elsewhere
    - If they cannot be contacted, leave a message to contact you on a given number
    - Don not provide details of the incident
    - Always document call time details, responses and actions.

All activities and contact/escalation should be clearly and accurately recorded. To facilitate this, actions should be in a checklist format and there should be space to record the date and time the activity was started and completed, and who carried out the activity.

Dependencies

System, infrastructure, service, facility or interface dependencies should be documented (in priority order) so that related recovery plans and procedures that will need to be invoked in conjunction with this recovery plan can be identified and actioned. The person responsible for invocation should ensure recovery activities are coordinated with these other plans.

System	Document Reference	Contact

Contact List

Lists of all contact names, organizations and contact details and mechanisms:

Name	Organization/Role	Title	Contact Details

Recovery Team

The following staff/functions are responsible for actioning these procedures or ensuring the procedures are actioned and recording any issues or problems encountered. Contact will be made via the normal escalation procedures.

Name	Title	Contact Details

Recovery Team Checklist

To facilitate the execution of key activities in a timely manner, a checklist similar to the following example should be used.

Task	Target Completion	Actual Completion
Confirm invocation		
Initiate call tree and escalation procedures		
Instigate and interface with any other recovery plans (e.g. BCP, Emergency Response Plan)		
Arrange for backup media and documentation to be shipped to recovery site		
Establish recovery teams		
Initiate recovery actions		
Confirm progress reporting		
Inform recovery team of reporting requirements		
Confirm liaison requirements with all recovery teams		
Advise customers and management of estimated recovery completion		

Recovery Procedure

Enter recovery instructions/procedures or references to all recovery procedures here.

Content/format should be in line with company standards for procedures. If there a re none, guidance should be issued by the Manager or Team Leader for the area responsible for the system, infrastructure, services or facility. The only guideline is that the instructions should be capable of being executed by an experienced professional without undue reliance on local knowledge.

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.

2.1.10 ITSCM Communication Plan

IT Services

IT Service Continuity Management Communication Plan

Status:	In draft Under Review Sent for Approval Approved Rejected
Version:	<<your version>>
Release Date:	

The document is not to be considered an extensive statement as its topics have to be generic enough to suit any reader for any organization.

However, the reader will certainly be reminded of the key topics that have to be considered.

This document serves as a GUIDE FOR COMMUNICATIONS REQUIRED for the IT Service Continuity Management process. This document provides a basis for completion within your own organization.

This document contains suggestions regarding information to share with others. The document is deliberately concise and broken into communication modules. This will allow the reader to pick and choose information for e-mails, flyers, etc. from one or more modules if and when appropriate.

This document was;

Prepared by: ______________________________
On: <<date>>

And accepted by: ______________________________
On: <<date>>

Initial Communication

Sell the Benefits

First steps in communication require the need to answer the question that most people (quite rightly) ask when the IT department suggests a new system, a new way of working. WHY?

It is here that we need to promote and sell the benefits. However, be cautious of using generic words. Cite specific examples from your own organization that the reader will be able to relate to (to help develop specific examples contact service@itilsurvival.com for competitive quotation).

Generic Benefit statements	Specific Organizational example
Improved Customer Service	This is important because…
Reduction in the number of Incidents	In recent times our incidents within IT have…
Provides quicker resolution of Incidents	Apart from the obvious benefits, the IT department in recent times has…
Improved Organizational learning	A recent example of … saw the individual and others in the company start to…

The above Communication module (or elements of) was/were distributed;

To: ______________________________
On: <<date>>

By: ______________________________
On: <<date>>

IT Service Continuity Management Goal

The Goal of IT Service Continuity Management

The Goal of IT Service Continuity Management can be promoted in the following manner.

Official Goal Statement: To support the overall business continuity management process by ensuring that the required IT technical and service facilities(including computer systems, networks, applications, data, repositories, telecommunications, environment, technical support and Service Desk) can be resumed within required, and agreed, business timescales.

- High visibility and wide channels of communication are essential in this process. Gather specific requirements from nominated personnel

(Special Tip: Beware of using only Managers to gain information from, as the resistance factor will be high)

- Oversee the monitoring of process to ensure that the business needs of IT are not impacted, but taking into account that changes are required to ensure continued high levels of IT Service Delivery and Support.

- Provide relevant reports to nominated personnel.

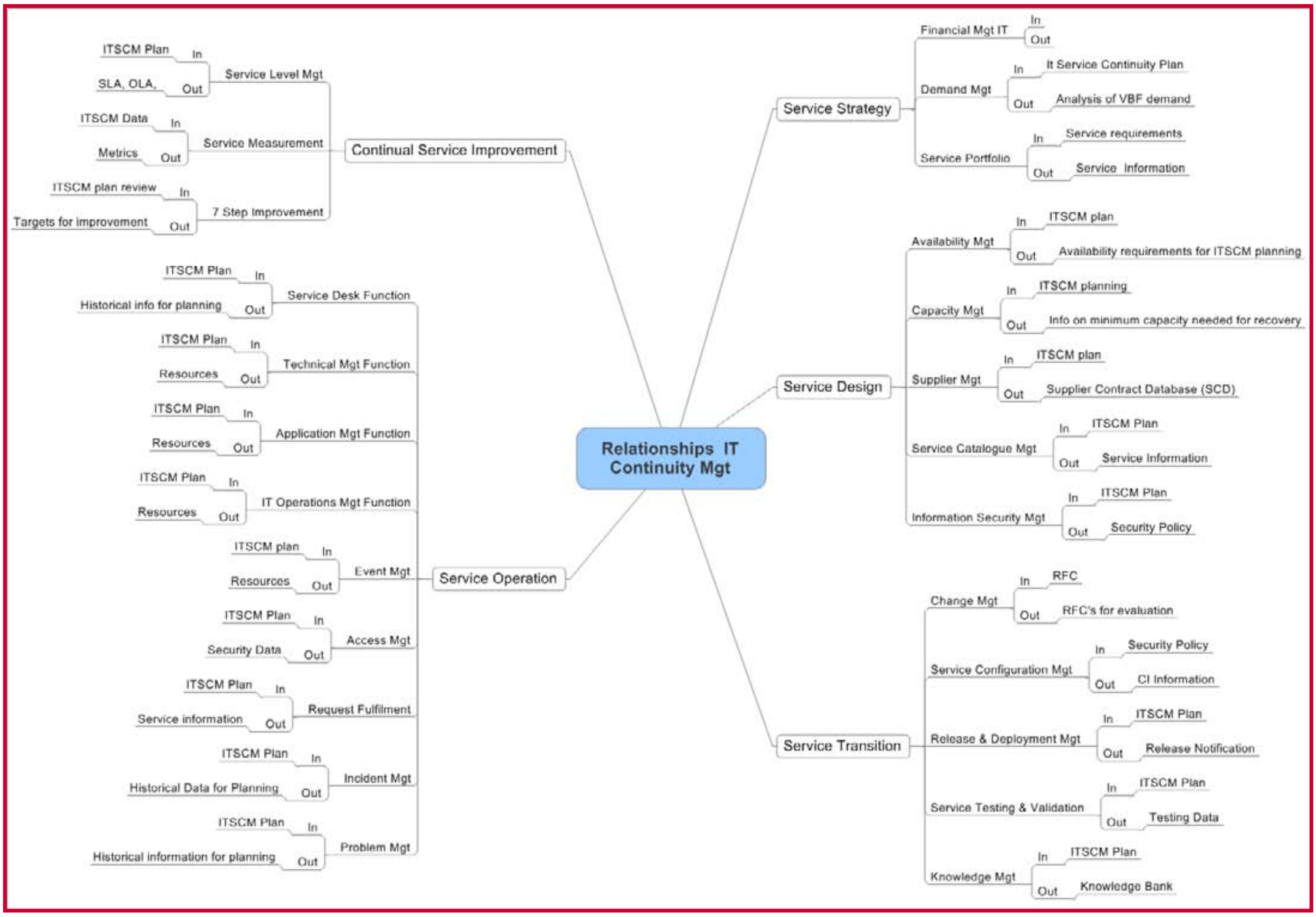
Always bear in mind the “so what” factor when discussing areas like goals and objectives. If you cannot honestly and sensibly answer the question “so what” – then you are not selling the message in a way that is personal to the listener and gets their “buy-in”.

The above IT Service Continuity Management Goals module was distributed;

To: ______________________________
On: <<date>>

By: ______________________________
On: <<date>>

IT Service Continuity Management Relationships



IT Service Continuity Management Planning

Costs

Information relating to costs may be a topic that would be held back from general communication. Failure to convince people of the benefits will mean total rejection of associated costs. If required, costs fall under several categories:

- Personnel – IT Service Continuity Management staff, technical management team (Set-up and ongoing of the technical infrastructure)
- Accommodation – Physical location (Set-up and ongoing)
- Software – Tools (Set-up and ongoing)
- Hardware – Infrastructure (Set-up)
  Provide options for replacement
- Education – Training (Set-up and ongoing)
- Procedures – external consultants etc (Set-up)
  Risk analysis and execution of continuity planning
  Production of the evacuation plan
  Testing and reviewing the plan
  Maintain the plan

The costs of implementing IT Service Continuity Management will be outweighed by the benefits. For example, many organizations have a negative perception of the IT Service Continuity Management process as it doesn't seem to offer any visible services. To alleviate this, customers and end-users need to be constantly informed of the service being provided. This provides good customer service and adds a level of comfort to the users in the sense that they can "see" action taking place.

A well run IT Service Continuity Management process will make major inroads into altering the perception of the IT Organization.

2.1.11 ITSCM E-Mail Text

IT Services

IT Service Continuity Management Communication Plan

Status:	In draft Under Review Sent for Approval Approved Rejected
Version:	<<your version>>
Release Date:	

Introduction

In the next section of this document is an example email text that can be distributed across your organization.

Note, that this is just one piece of text for one email.

However, it is advisable to create a few different versions of the below text, which you can store in this document, for future use.

This is very important, as each time you send an email regarding your IT Service Continuity Management process it should be different and targeted to the correct audience.

This document provides a method for also keeping track of your communication that you have made to the rest of the organization, and to keep in focus the promises that have been made regarding this process.

Note: SEARCH AND REPLACE
<<organization name>>

Search for any << or >> as your input will be required
Also review any yellow highlighted text

Dear << insert audience here, for example, Customer, IT Staff, Marketing Dept etc >>

IT Service Continuity Management Program

The IT Department <<give a specific name here if appropriate>> is embarking on a programme to ensure that – in the event of an unplanned and major service outage, we are able to respond and restore IT services.

What does this mean to you?

The IT Department continually strives to improve the service it delivers to its customers. The IT Services department provides internal support for <<e.g. Business applications and equipment: Enter any appropriate details here>>.

In order to improve the IT Services and ensure that they are aligned with the needs of the organization, we have decided to embark on a service improvement programme. This programme will result in the implementation of a process called IT Service Continuity Management.

Why the need for IT Service Continuity Management?

Organizations are required to operate and provide a service at all times. It's that simple. Increasing competition and a growth in the requirement by consumers for instant or near real time response has fuelled the necessity for an agreed level of IT services to be provided following an interruption to the business. Such "interruptions" can be a loss of a single application or a complex system failure – all the way through to the loss of a building (e.g. through fire, flood, etc.)

We have defined the Goal for IT Service Continuity Management as follows:

The goal for IT Service Continuity is to support the Business Continuity Management process (following pre-defined losses in organizational ability), through the delivery of IT services, within agreed times and costs.

<< INSERT YOUR OWN GOAL FOR IT SERVICE CONTINUITY MANAGEMENT HERE >>

What is your involvement?

The IT Department will be creating a list of IT Services that it delivers. This will be captured in a Service Catalogue (SC). The list of services will then be presented to the different departments within <<organization name>>. From this list, each department will be able to pick the service that they use, and through our requirements gathering, make comments about the requirements for that service during times of major outage or loss.

From this, we will be able to then formulate agreements on the services being provided. These agreements are called Service Level Agreements and they include the requirements for continuity.

This will help ensure that the IT Department is aligning it's Services with the business needs, provide a way to measure the services, set expectations of the services being delivered, and more importantly provide an avenue for discovery in service improvement.

We have appointed an IT Service Continuity Manager to help drive this process. The IT Service Continuity Manager will be the interface between the IT Department and the Department heads within the organization.

The IT Service Continuity Manager will work closely with the business in defining the necessary services and agreeing their level of availability.

The following can be considered a list of benefits to be derived from the process:

<<

- List benefits applicable to your audience.
- For example: Benefits to the Business:
    - o Improved relationship with customers
    - o IT and Customers have a clear and consistent expectation of service
- For example: Benefits to the IT Department
    - o Better understanding of the level of service to be provided
    - o Reacting appropriately due to IT Service Continuity Agreements
    - o Operation Level Agreements reinforce communications

>>

The commencement date of the new process is scheduled for: << insert date >>

OR

Completion of the process will be: << insert date >>

This is a detailed process and there may be some operational difficulties to overcome, but with your support, I am sure we can provide an extremely beneficial process to both the Business / <<organization name>> and IT.

If you have any questions regarding this, please do not hesitate to contact me on << phone number >>

<< Your Name and Titles >>

2.1.12 ITSCM Emergency Response Plan

IT Services

IT Service Continuity Management Emergency Response Template

Status:	Draft
Version:	0.1
Release Date:	

Document Control

Author

Prepared by <name and / or department>

Document Source

This document is located on the LAN under the path:

I:/IT Services/Service Delivery/Emergency Response Plan/

Document Approval

This document has been approved for use by the following:

- <first name, last name>, IT Services Manager
- <first name, last name>, IT Service Delivery Manager
- <first name, last name>, IT Service Continuity Process Manager
- <first name, last name>, Customer representative or Service Level Manager

Amendment History

Issue	Date	Amendments	Completed By

Distribution List

When this procedure is updated the following copyholders must be advised through email that an updated copy is available on the intranet site:

<Company Name> Business Unit	Stakeholders
IT	

Introduction

Purpose

The purpose of this document is to provide an emergency response template.

Scope

This document describes the following:

- An emergency response template

Note: It is assumed for each service described in this document that the supporting back-end technology is already in place and operational.

Audience

This document is relevant to all staff in <company name>

Ownership

IT Services has ownership of this document.

Related Documentation

Include in this section any related Service Level Agreement reference numbers and other associated documentation:

- IT Service Continuity Management Policies, Guidelines and Scope Document (ITSCM2300)
- Business Continuity Strategy Template (ITSCM2900)
- Risk Assessment (ITSCM2800)
- Reciprocal Arrangements (ITSCM3000)
- Relevant SLA and procedural documents (SLM1901, 1902, 1903)
- IT Services Catalogue (SLM2200)
- Relevant Technical Specification documentation (SLM2202)
- Relevant User Guides and Procedures

More templates and other ITIL process information available at www.itilsurvival.com

Executive Overview

Describe the purpose, scope and organization of the document.

Scope

Not all IT Services may initially be included within the Emergency Response Plan. Use this section to outline what will be included and the timetable for other services to be included.

Scope for the assessment may be determined by the business, therefore covering only a select few of the IT Services provided by the IT department that are seen as critical to the support of the business processes.

The emergency response plan is fairly simple in concept and should be used in conjunction with the ITSCM3200 Salvage Plan Template.

IT Service Emergency Response Summary

This section is to provide a brief summary of the information contained in the next sections of the document.

The below table provides an example of information that can be captured to create a summary of the Emergency Response plans for the IT Services listed in this document.

Service	Customer	Description	Response Times	Recovery Options	IT Owner	Contact Number	Procedures

This template can be distributed to the business as it helps in setting the expectation of the level of service they will receive in the event a disaster is experienced.

There should be no use of technical terms in the above table**.**

Emergency Response Plan (ERP) – Service A

This section should be repeated for each Service.

Introduction

In this section provide some detail about the ERP. Include things like which aspects of the infrastructure are included, which services, why it is necessary etc.

<<

This document provides the necessary details and procedures that are required in the event of disaster

>>

Response Strategy

In this section detail the strategy being used to respond to the IT Disaster.

Important things to cover are:

- Service Agreements to Respond
- Process of Response
- Escalation Strategies
- Key Personnel for the Service
- Priorities for restoration

Invocation

The following personnel are authorised to invoke this plan:

Business Sponsors		IT Sponsors	
<< first name, last name >>	<< department >>	<< first name, last name >>	<< department >>
<< first name, last name >>	<< department >>	<< first name, last name >>	<< department >>
<< first name, last name >>	<< department >>	<< first name, last name >>	<< department >>

Dependencies

In this section list dependencies for this IT Service. Dependencies will be other systems, infrastructure, facilities, documentation etc.

The below table provides a template for capturing this information:

Dependant Service	Dependant Components	Impact on Service A	Service Level Agreement #	Operational Level Agreement #	Underpinning Contracts
		Dependant or contributor			

Response Team

The following listed people are responsible for performing the actions listed in the Response Plan. They are to ensure that the procedures are carried out in the most efficient and effective manner possible.

Name	Title	Phone Number	Locations / Dept

Response Plan

Listed Procedures for Response for Service - A:

Procedure Name	Description	Owner	Location

Response Plan for Service - A:

Step	Action	Responsibility	Target Completion	Actual Completion
1	Record disasters	Service Desk		
2	Provide disaster report	Avail. Mgt, Inc Mgt, Problem Mgt		
3	Alert Business	Service Delivery Manager		
4	Alert Salvage Team	Network Manager		
5	Perform initial investigation	Salvage Team		
6	Implement Salvage Procedures	Salvage Team, Service Delivery Manager		

Equipment Needed:

IT Components (Configuration Items (CI))				
CI #	Serial #	CI Name	Type	Sub-Type
SER345	15434563	EMERO	Hardware	Server
RT5700	54444443	CISCO-002	Hardware	Router
RT4567	76547457	CISCO-001	Hardware	Router
MS001	N/A	MS Office	Software	Microsoft

Appendices

Include any applicable appendixes that are needed.

Terminology

Make sure that all terminology is captured and documented correctly.

2.1.13 ITSCM Salvage Plan Template

IT Services

IT Service Continuity Management Salvage Plan Template

Status:	Draft
Version:	0.1
Release Date:	

Document Control

Author

Prepared by <name and / or department>

Document Source

This document is located on the LAN under the path:

I:/IT Services/Service Delivery/Salvage Plan/

Document Approval

This document has been approved for use by the following:

- <first name, last name>, IT Services Manager
- <first name, last name>, IT Service Delivery Manager
- <first name, last name>, IT Service Continuity Process Manager
- <first name, last name>, Customer representative or Service Level Manager

Amendment History

Issue	Date	Amendments	Completed By

Distribution List

When this procedure is updated the following copyholders must be advised through email that an updated copy is available on the intranet site:

<Company Name> Business Unit	Stakeholders
IT	

Introduction

Purpose

The purpose of this document is to provide a salvage plan template.

Scope

This document describes the following:

- A salvage plan template

Note: It is assumed for each service described in this document that the supporting back-end technology is already in place and operational.

Audience

This document is relevant to all staff in <company name>

Ownership

IT Services has ownership of this document.

Related Documentation

Include in this section any related Service Level Agreement reference numbers and other associated documentation:

- IT Service Continuity Management Policies, Guidelines and Scope Document (ITSCM2300)
- Business Continuity Strategy Template (ITSCM2900)
- Risk Assessment (ITSCM2800)
- Reciprocal Arrangements (ITSCM3000)
- Relevant SLA and procedural documents (SLM1901, 1902, 1903)
- IT Services Catalogue (SLM2200)
- Relevant Technical Specification documentation (SLM2202)
- Relevant User Guides and Procedures

More templates and other ITIL process information available at www.itilsurvival.com

Executive Overview

Describe the purpose, scope and organization of the document.

Scope

Not all IT Services may initially be included within the Salvage Plan. Use this section to outline what will be included and the timetable for other services to be included.

Scope for the assessment may be determined by the business, therefore covering only a select few of the IT Services provided by the IT department that are seen as critical to the support of the business processes.

The salvage plan is fairly simple in concept and should be used in conjunction with the ITSCM3100 Emergency Response Template.

Sample Salvage Plan

DISASTER PLANNING

EXAMPLE SALVAGE ASSESSMENT WORKSHEET

IT Service Description: ______________________________
IT Service Owner: ______________________________

Business Process: ______________________________
Business Process Owner: ______________________________

Records Series Title ______________________________
Note: This is the title for this salvage plan for this service

Storage of Plan:
Hardcopy ( )
Microfilm ( )
Electronic ( )
Other (specify)
____

Salvage of Service Needed:

Yes ( )
No ( )

If Yes, By What Method:

Commercial Provider ( )
Backup ( )
Rebuild ( )
System Restore ( )

Listed Procedures for Service Salvage:

Procedure Name	Description	Owner	Location

Service Salvage Plan:

Step	Action	Responsibility
1	Record disasters	Service Desk
2	Provide disaster report	Avail. Mgt, Inc Mgt, Problem Mgt
3	Alert Business	Service Delivery Manager
4	Alert Salvage Team	Network Manager
5	Perform initial investigation	Salvage Team
6	Implement Salvage Procedures	Salvage Team, Service Delivery Manager

Equipment Needed:

IT Components (Configuration Items (CI))				
CI #	**Serial #**	**CI Name**	**Type**	**Sub-Type**
SER345	15434563	EMERO	Hardware	Server
RT5700	54444443	CISCO-002	Hardware	Router
RT4567	76547457	CISCO-001	Hardware	Router
MS001	N/A	MS Office	Software	Microsoft

2.2 Risk Management ITIL V3 – ISM

Through the documents, look for text surrounded by << and >> these are indicators for you to create some specific text.

Watch also for highlighted text which provides further guidance and instructions.

2.2.1 CRAMM

CRAMM: CCTA **R**isk **A**nalysis and **M**anagement **M**ethodology

In the Information Systems environment, new business practices – such as outsourcing, partnerships and consortiums – and new technologies, such as remote working, wireless LAN's and PDA's, mean that we are constantly facing new threats and risks, and the need for additional controls.
These complexities make it practically impossible for an Information Security Officer to keep up to date without automated support and CRAMM has, for many years, been the UK Government's preferred approach to risk assessment.

CRAMM is applicable to all types of information systems and networks and can be applied at all stages in the information lifecycle, from planning and feasibility, through development and implementation to live operation. CRAMM can be used whenever it is necessary to identify the security and/or contingency requirements for an information system or network. This may include:

- During strategy planning, where a high level risk analysis may be required to identify broad security or contingency requirements for the organization and the relative costs and implications of their implementation.
- At feasibility study stage, where a high level risk analysis may be required of potential solutions to identify the broad security or contingency requirements and associated costs of the different options.
- During analysis of the detailed business and technical environments, where the security or contingency issues associated with the chosen option can be investigated or refined.
- Prior to live running, to ensure that all required physical, procedural, personnel and technical security countermeasures have been identified and implemented.
- At any point during live running, where there are concerns about security or contingency issues, e.g. in response to a new or increased threat or following a security breach.
- As part of a regular security management, audit and change management programs to monitor both compliance and new requirements.

How does CRAMM work?
Using the CRAMM methodology helps to answer the many questions that arise each day in respect of information security, such as:

- What security requirements should we include in this managed service agreement?
- Are there implications from allowing our users to connect to the internet?
- How can we demonstrate to the BS7799 auditors that our risks have been managed properly?

Managing risk is a matter of 'Risk Treatment' under which risks are reduced to an acceptable level and not 'avoided' by either ignoring or trying to remove them altogether. Risk Management processes include activities such as:

- Identifying requirements for specific controls such as Smart Cards
- Demonstrating compliance with legislation
- Developing a business continuity strategy
- Developing a security policy for a new system
- Auditing the status of security controls on an existing system.

As the pace of change accelerates ever faster, the key challenge is to be able to build security into new systems as they arise. This requires a fast and effective approach and the capability to interrogate results, as well as adapt the risk assessment as new details become available.

CRAMM is a widely adopted method for information security, risk analysis and management. It is the 'benchmark' against which all other methods are evaluated, reflecting the significant development investments made by such organizations as the UK Government and NATO.

CRAMM provides a staged and disciplined approach embracing both technical (e.g. IT hardware and software) and non-technical (e.g. physical and human) aspects of security. In order to assess these components, CRAMM is divided into three stages:

- Asset identification and valuation
- Threat and vulnerability assessment
- Countermeasure selection and recommendation.

Asset identification and valuation

CRAMM enables the reviewer to identify the physical (e.g. IT hardware), software (e.g. application package), data (e.g. the information held on the IT system) and location assets that make up the information system. Each of these assets can be valued.

Physical assets are valued in terms of the replacement cost. Data and software assets are valued in terms of the impact that would result if the information were to be unavailable, destroyed, disclosed or modified.

Threat and Vulnerability assessment

Having understood the extent of potential problems, the next stage is to identify just how likely such problems are to occur. CRAMM covers the full range of deliberate and accidental threats that may affect information systems including:

- Hacking
- Viruses
- Failures of equipment or software
- Wilful damage or terrorism
- Human error

This stage concludes by calculating the level of the underlying or actual risk.

Countermeasures selection and recommendation

CRAMM contains a very large countermeasure library consisting of over 3000 detailed countermeasures organized into over 70 logical groupings. The CRAMM software uses the measures of risk determined during the previous stage and compares them against the security level (a threshold level associated with each countermeasure) in order to identify if the risks are sufficiently great to justify the installation of a particular countermeasure. CRAMM provides a series of help facilities including backtracking, What If?, prioritization functions and reporting tools to assist with the implementation of countermeasures and the active management of the identified risks.

Risk assessments should identify, quantify, and prioritize risks against criteria for risk acceptance and objectives relevant to the organization. The results should guide and determine the appropriate management action and priorities for managing information security risks and for implementing controls selected to protect against these risks.

BS7799:2005

2.3 Risk Management – Project Management

Through the documents, look for text surrounded by << and >> these are indicators for you to create some specific text.

Watch also for highlighted text which provides further guidance and instructions.

2.3.1 Checklist on Assignment of Risk Ownership

☑ Have owners been allocated to all the various parts of the complete risk process and the full scope of the risks being catered for? For example, suppliers may be tasked with ownership of assessing and evaluating risk as part of their contracts.

☑ Are the various roles and responsibilities associated with ownership well defined?

☑ Do the individuals who have been allocated ownership actually have the authority in practice to fulfill their responsibilities?

☑ Have the various roles and responsibilities been communicated and understood?

☑ Are the nominated owners appropriate?

☑ In the event of a change, can ownership be quickly and effectively reallocated?

☑ Are the differences between benefit and delivery risks clearly understood? and, if required, do they have different owners?

The Project Manager's Daily Log can be very useful in monitoring risks. Entries can be made in it for the Project Manager to check on the status of any risks where he/she is the owner. Other entries can be made to remind the Project Manager to check that the owners are monitoring and controlling their risks and feeding the information back.

Where the project is part of a program:

- ✓ Program Management is responsible for ensuring the management of those risks with interdependencies between projects and program.

- ✓ Where appropriate, the program should take part in the risk management activities at the project level. This can normally be done by attendance at end stage assessments by either a member of the program management or a designated risk management function.

- ✓ Risks are frequently common across projects and would benefit from being centralized at program level. The cost of corrective action can be reduced if it is planned, agreed and actioned only once. Also, problems can result form an inconsistent approach being taken by projects.

2.3.2 Generic Project Risk Assessment

This Project Risk Assessment has been designed for business projects, IT infrastructure projects and general [i.e.] non-software development projects.

> Three main categories of risk factors have been identified as contributing to the risk of a project or, the probability of project failure. These are the client environment, the team environment and the product or service complexity. Each of these categories has a number of related factors, which have been allocated a low, medium or high score. The sum of the factor scores provides an indication of the degree of risk in the total project.

A guide to the value for each factor is shown against each question but any value within the specified range may be used.

Risk Assessment Weights

The weighting factors included are based on the ACME companies many years of experience in the field of IT Risk Assessment.

The results of the questionnaire should be compared against the following table:

Risk Category	**Low**	*Low/ Medium*	**Medium**	**Medium/High**	**High**
Client Environment	44-96	97-149	150-202	203-255	256-313
Team Environment	55-86	87-118	119-150	151-182	183-209
Product	51-77	78-104	105-131	132-158	159-184
Total Project	**150-260**	**261-372**	**373-484**	**485-596**	**597-706**

Given the subjective nature of the process, the use of scores to compare projects is not valid. For example, a project with a Total Risk score of 490 is still a Medium/High risk project as is one with a Total Risk score of 596. The use of the broad categories of Low, Low/Medium, Medium, Medium/High and High is the acceptable approach.

Risk Situation	Impact	Score	Weight	Weighted Score
Risk Category : Client Environment				
1. Will clients commit to a standardized product development approach?				
Yes	Low	0	2	0
No	High	2		4
2. Have clients been briefed and are prepared to commit to change control procedures?				
Yes	Low	0	4	0
No	High	4		16
3. How committed is senior client management to product?				
Extremely Enthusiastic	Low	1	4	4
Supportive	High	2		8
Neutral	High	3		12
Negative	Very High	4		16
4. Is there a Project Sponsor?				
Yes	Low	0	4	0
No	High	4		16
5. Priority for project within client group?				
High	Low	0	3	0
Average	Medium	2		6
Varied	Medium	3		9
Low	High	4		12
6. How critical will product be to the client group continuing operations when completed?				
Minor impact	Low	1	3	3
Some impact	Medium	2		6
Significant impact	Medium	3		9
Critical - showstopper	High	4		12
7. Number of outside organizations involved in concurrence, approvals and other decisions relating to the product?				
None	Low	0	4	0
1	High	3		12

Greater than 1	Very High	4		16

8. Number of different client Branches or groups involved in concurrence, approvals and other
decisions relating to the product?

1	Low	1	4	4
2	Medium	2		8
Greater than 2	High	4		16

9. Number of individual clients/direct product users?

Less than 10	Low	1	3	3
11-100	Medium	2		6
101-1000	High	3		9
Greater than 1000	Very High	4		12

10. Number of unions and/or staff associations involved in the product?

None	Low	0	4	0
1	Medium	2		8
Greater than 1	High	4		16

11. Attitude of unions/staff associations towards project?

Extremely Enthusiastic	Low	1	4	4
Supportive	High	2		8
Neutral	High	3		12
Negative	Very High	4		16

12. Number of client sites/installations involved with the product?

1	Low	1	3	3
2-10	Medium	2		6
11-101	High	3		9
Greater than 100	Very High	4		12

13. What is the severity of procedural changes/disruption in client department/area caused by
proposed product?

Minor	Low	1	3	3
Some	Medium	2		6
Significant	High	4		12

14. Does client organization have to change structurally for proposed product?

No	Low	1	3	3
Minor	Medium	2		6

Significantly	High	4		12

15. Organizational attitude towards change?

Extremely Enthusiastic	Low	1	4	4
Supportive	High	2		8
Neutral	High	3		12
Negative/Resistance	Very High	4		16

16. Critical stakeholder participation?

Full-time expert	Low	1	4	4
Part-time expert	Medium	2		8
Ad-hoc participation	High	3		12
None	Very High	4		16

17. How knowledgeable is client representative in proposed product type or class?

Expert – previous implementation experience	Low	1	3	3
Knowledgeable – some previous experience	Medium	2		6
Novice – no previous experience	High	4		12

18. How knowledgeable is client in product development process?

Expert – previous implementation experience	Low	1	3	3
Knowledgeable – some previous experience	Medium	2		6
Novice – no previous experience	High	4		12

19. What are communications between client group/s and product development group like?

Good	Low	1	3	3
Fair	Medium	2		6
Poor	High	4		12

20. Is new client - controlled technology/techniques (e.g. monitoring equipment, graphics terminals, CAD/CAM, etc) required for the product?

None	Low	0	3	0
Some	Medium	1		3
Significant	High	3		9

21. Is the project dependent on a single client expert?

No	Low	0	4	0
Yes	High	4		16

22. Is there government legislation that the project is dependent on to meet deadlines?

No	Low	0	4	0
Yes	High	4		16

23. Is the project dependent on vendors and outside consultants/experts to meet deadlines?

No	Low	0	4	0
Partially	Medium	2		8
Completely	High	4		16

Risk Criterion: Team Environment

1. Priority of project within product development group is?

High	Low	1	3	3
Medium	Medium	2		6
Low	High	4		12

2. How committed is senior product development group management to product?

Enthusiastic	Low	1	4	4
Supportive	Medium	2		8
Neutral	High	3		12
Negative	Very High	4		16

3. Project team size (including full-time business professionals)?

Less than 5	Low	1	4	4
5-10	Medium	2		8
Greater than 10	High	4		16

4. Total estimated development time in calendar months for product?

Less than 3 months	Low	1	4	4
3-6 months	Medium	2		8
7-12 months	High	3		12
Greater than 12 months	Very High	4		16

5. Project Manager (PM) availability, experience and training?

PM with successful recent experience in similar project	Low	1	4	4
PM with successful recent experience	Low	2		8
PM with knowledge but little experience	High	3		12
Inexperienced PM with limited PM knowledge	Very High	4		16

6. Key project skill and staffing level requirements can be met by?

Team members full-time	Low	1	4	4
Mix of full-time and part-time members	Medium	2		8
Part-time members	High	3		12
Ad-hoc membership	Very High	4		16

7. What proportion of project team will be brought in from an outside company/group?

Less than 25%	Low	1	4	4
26-50%	Medium	2		8
51-99%	High	3		12
All	Very High	4		16

8. Number of team members who have worked successfully together on previous projects?

All	Low	1	3	3
Some	Medium	2		6
None	High	3		9

9. How knowledgeable is product development group project team in proposed product client's area?

Have been involved in prior implementations	Low	1	2	2
Understands client’s area - no previous implementation experience	Medium	2		4
Mixed	High	3		6
Limited	Very High	4		8

10. What experience does the project team have with the product technology/techniques to be used?

Significant	Low	1	4	4
Somewhat	Medium	2		8
Limited	High	3		12
None	Very High	4		16

11. Relevant support tools and technology available to the team?

Extensive	Low	1	3	3
Available	Medium	2		6
Limited	High	3		9
None	Very High	4		12

12. Project deadlines are?

Flexible – may be established in conjunction with team	Low	1	4	4
Firm - established internally but missed dates may impact client operations	Medium	2		8

Fixed - established by specific operations, legal requirements, direction beyond organization’s control	High	4		16

13. The team will be located in?

Single office (co-located)	Low	1	4	4
Multiple offices (single building)	Medium	2		8
Multiple buildings (same city)	High	3		12
Different cities	Very High	4		16

14. The physical working environments/offices that the team occupy?

Excellent	Low	1	4	4
Average	Medium	2		8
Poor	High	3		12

15. The morale of people working in the project/group?

Excellent	Low	1	4	4
Average	Medium	2		8
Poor	High	3		12

Risk Criterion: Product/Service Complexity

1. Proposal document from clients/Business Analyst?

Complete	Low	1	2	2
Acceptable but incomplete	Medium	2		4
None	High	3		6

3. Product/service performance expectation is?

Throw-away	Low	1	4	4
Average (1-3 years)	Medium	2		8
Critical (> 3 years)	High	4		16

4. Current documentation for existing similar products?

Complete	Low	1	2	2
Acceptable but incomplete	Medium	2		4
None	High	3		6

5. Available prototype or model?

Similar product/service in existence	Low	1	3	3
Some functionality exists within organization	Medium	2		6
Some functionality exists in other organizations	High	3		9
None	High	4		12

6. Overall size of product/service?

Small	Low	1	4	4
Medium	Medium	2		8
Large	High	3		12
Super Large	Very High	4		16

7. Intrinsic complexity of product is?

Simple	Low	1	4	4
Average	Medium	2		8
High	High	3		12
Extensive	Very High	4		16

8. The product developed must interface with?

Stand alone	Low	1	4	4
Products within teams control	Medium	2		8
Products under others control	High	3		12
Complex products under others control	Very High	4		16

9. Stability of product requirements ?

Requirements are stable	Low	1	4	4
Requirements are firm but exposed to change	Medium	2		8
Requirements are firm but likely to change	High	3		12
Requirements are completely unstable	Very High	4		16

10. Level of innovation required by the product is?

Simple	Low	1	4	4
Average	Medium	2		8
Extensive	High	3		12
Very Innovative	Very High	4		16

11. Product technology availability is?

Currently available	Low	1	4	4
Limited	Medium	2		8
Not currently available	High	3		12

12. Client expectations of product quality is?

Simple	Low	1	4	4
Average	Medium	2		8
High	High	3		12
Very High	Very High	4		16

13. The degree of policy/legislation change required for successful product implementation is?

None	Low	1	4	4
Some	Medium	2		8
Extensive	High	3		12

14. The degree of new or unproven technology/techniques required for successful implementation are?

None	Low	1	4	4
Some	Medium	2		8
Extensive	High	3		12

3 RISK MANAGEMENT FRAMEWORK

3.1 Introduction

There is risk and opportunity in everything we do. As the environment in which we operate changes, risks and opportunities change. Effective risk management is a means of monitoring those changes.

This document outlines the process involved in conducting a risk assessment and has been designed to better assist managers achieve their objectives, and to contribute to the continuous improvement of performance throughout the Organization.

Risk Management Policy Statement

ACME's objective is to manage risks to minimize the exposure of itself and its stakeholders to any event, or set of occurrences able to cause adverse effects, while concurrently maximizing the efficiency and effectiveness of its operations in accordance with best practice. The Organization is committed to the management of risk to ensure the protection of it's:

- *Clients and stakeholders;*
- *Employees and associated intellectual capital;*
- *Business objectives;*
- *Environment;*
- *Quality of service;*
- *Assets and intellectual property;*
- *Contractual and statutory obligations;*
- *Image and reputation.*

Risk management is regarded as an integral part of sound management practices and must be fully integrated into the Organization's policies and procedures and business plans. It should not be seen, or practiced, as a separate program.

This approach is directed to achieving best practice in balancing the control of risks and maximisation of opportunities to which the Organization may be exposed.

Risk Management in the Organization

The organization has developed and implemented a framework to systematically identify, measure and manage risk.

All personnel are responsible for managing risks in their area of control. The Risk Management and Audit unit will facilitate the process and provide assistance and guidance, but responsibility resides with the personnel in each area concerned. The Risk Management and Audit unit will provide training in risk management and facilitate workshops for any areas requiring assistance. Risk management is applied at several levels:

1. Organization wide.
2. Network.
3. Procurement and Contract.
4. Information Technology.

Organizational

Organisation wide annual strategic risk assessments will be conducted to develop an overarching Risk Management and Audit Plan (RMAP) endorsed by the Audit Committee.

Network

It is the responsibility of each network to undertake risk assessments on a regular basis. These are often incorporated into the annual RMAP. A risk assessment is required for:

1. Any new business system, application or major upgrade at the project concept stage and prior to commencement of the project.
2. Whenever a significant policy change is envisaged or imposed on the organization.
3. Any significant mechanism of government change.

Procurement / Contract

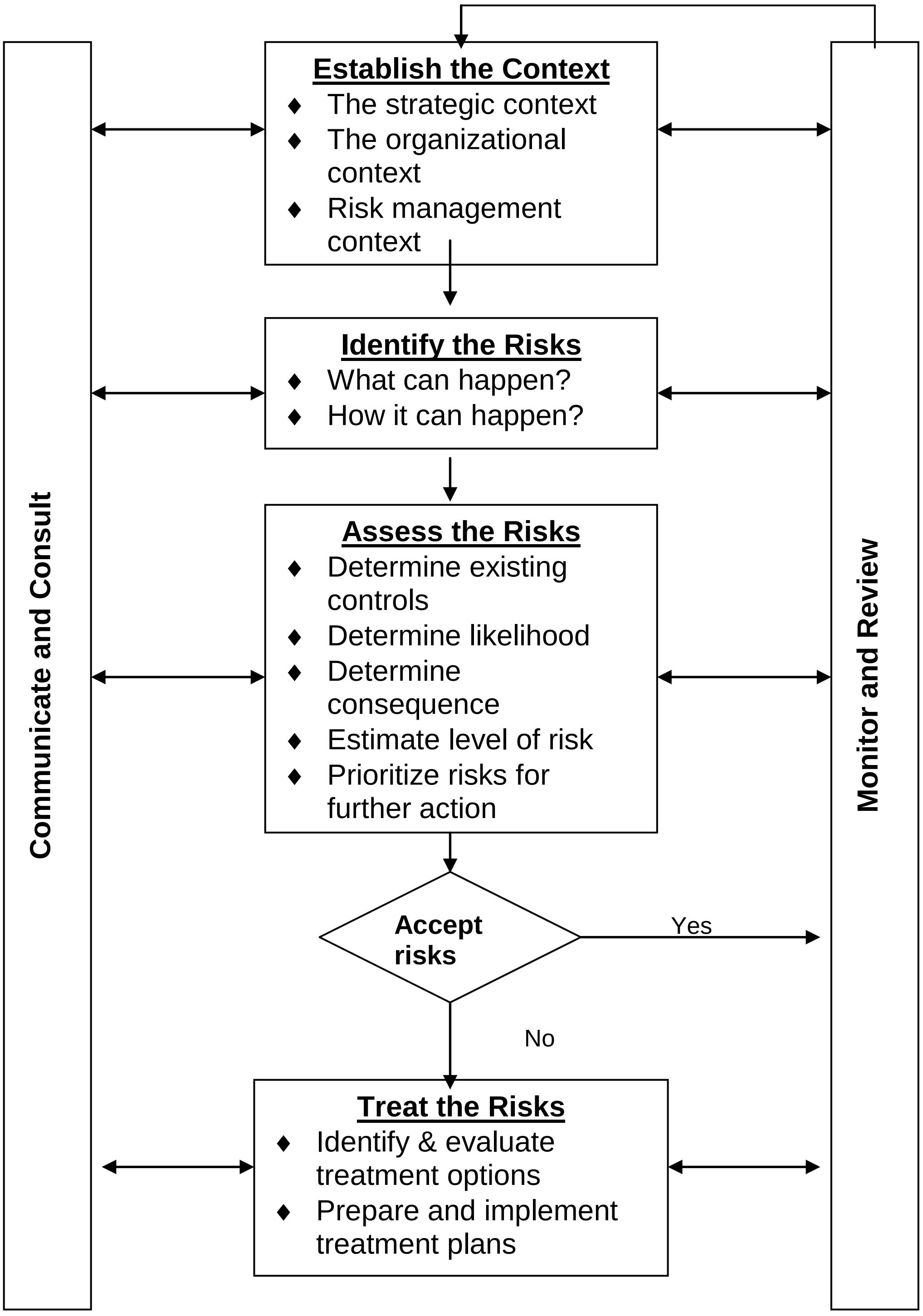
Networks are required to complete a formal risk assessment for any procurement or contract in excess of $100,000, prior to its approval and ratification.

IT risk assessments

Information technology risk assessments are regarded as special reviews. These will be identified in the RMAP and conducted as necessary and separately from the other updates.

3.1.1 Risk Management Guidelines

The following diagram illustrates the risk management framework for ACME.



3.1.2 Glossary of Terms

Control

An existing process, policy, device or practice that acts to minimise negative risk or enhance positive opportunities.

Control assessment

Systematic review of processes to ensure that controls are still effective and appropriate.

Event

Occurrence of a particular set of circumstances.

Frequency

A measure of the number of occurrrences per unit of time.

Hazard

A source of potential harm or a situation with a potential to cause loss.

Consequence

Outcome or impact of an event.

Likelihood

A general description of probability or frequency.

Loss

Any negative consequence or adverse effect, financial or otherwise.

Monitor

To check, supervise, or record the progress of an activity or system on a regular basis to identify change.

Residual risk

The remaining level of risk after risk treatment measures have been taken.

Risk

The chance of something happening that will have an impact upon the Organization's objectives. It is measured in terms of likelihood and consequence.

Risk analysis

A systematic process to understand the nature of and to deduce the level of risk.

Risk Criteria

Terms of reference by which significance of risk is assessed.

Risk evaluation

Process of comparing the level of risk agaiinst the risk criteria.

Risk Identification

The process of determining what, where, when,why and how something could happen.

Risk Management

The culture, processes and structures that are directed towards realizing potential opportunities whilst managing adverse effects.

Risk Management Process

The systematic application of management policies, procedures and practices to the tasks of communicating, establishing the context, identifying, analysing, evaluating, treating, monitoring and reviewing risk.

Risk reduction

Actions taken to lessen the likelihood, negative consequence, or both, associated with a risk.

Risk retention

Acceptance of the burden of loss, or benefit of gain from a particular risk.

Risk transfer

Shifting the responsibility or burden for loss to another party through legislation, contract, insurance or other means. Risk transfer can also refer to shifting a physical risk or part thereof elsewhere.

Risk treatment

Process of selection and implementation of measures to modify risk.

Stakeholders

Those people and organisations who may affect, be affected by, or percieve themselves to be affected by a decision, activity or risk.

SWOT analysis

Provides an assessment of an organisation’s Strengths, Weaknesses, Opportunities, and Threats to provide a snapshot of the present and a view of what the future may hold.

3.2 Basic Steps

3.2.1 Step 1: Establish the Context

Establish the strategic, organizational and risk management context in which the rest of the process will take place. Internal and external stakeholders and their objectives are defined at this stage of the process. The overall objectives of the project or activity are determined along with the scope, resources and timeline. Criteria against which risk will be evaluated should be established and the structure of the analysis defined.

a. Strategic and Organizational Context:

Define the relationship between the Organization and its environment, identifying the Organization's strengths, weaknesses, opportunities and threats. This could include Government, the economy, financial markets, employer groups, unions, the physical environment, technology, media, customers and providers.

Identify the internal and external stakeholders, and consider their objectives, taking into account their perceptions, and establish communication policies with these parties. The Organization should seek to determine the crucial elements, which might support or impair its ability to manage the risks it faces.

The organizational context takes into account the Organization's goals and objectives and the strategies that are in place to achieve them.

There should be a close relationship between the Organization's mission and strategic objectives and its management of all risks to which it is exposed. Strategic risk management involves the evaluation and prioritization that links the strategic planning process to operational planning.

b. Risk Management Context:

The goals, objectives, strategies, scope and parameters of the activity, or part of the Organization, to which the risk management process is being applied, should be established. The following should be undertaken:

- Define the project and set objectives.
- Define the extent of project in time and location.
- Identify any studies and resources required.

c. Risk Evaluation Criteria:

Decide the criteria against which risk is to be evaluated. These criteria will be used during the risk evaluation phase. It is not necessary that all facets be articulated at this stage, however the major issues should be acknowledged.

d. Stakeholder identification:

When identifying the stakeholders you should consider the following:

- Decision-makers.
- Individual who are, or perceive themselves to be, directly affected by a decision or activity.
- Individuals inside the organization, such as employees, management, senior management, and contractors.
- Union or staff representative groups.
- Partners in the decision, such as financial institutions or insurance agencies.
- Regulators and other government organizations that have authority over activities.
- Politicians with an electoral or portfolio interest.
- Business partners.
- Clients and customers.
- Suppliers and service providers.
- Media, who may either be stakeholders or conduits of information to other stakeholders.
- Individuals or groups interested in issues related to the proposal.

e. Some questions to ask when establishing the context:

- What is the policy, program, process or activity?
- Who are the key stakeholders?
- What are the major outcomes expected?
- What are the dollar values?
- What are the strengths and weaknesses?
- What are the major threats and opportunities the program presents?
- What are the significant factors in the internal and external environment? (This should include the geographic, economic, political, environmental, social and technological factors that could affect the process.)
- What is the best way to structure the risk identification phase?
- What problems were identified in previous reviews?
- What risk criteria should be established?

3.2.2 Step 2: Identify the Risks

Identify what, why and how things can arise as the basis for further analysis. This step should identify any risks arising from the operating environment identified in the previous step and generate a comprehensive list of risks that could impact on those objectives.

This step should be documented using the Risk Identification and Analysis Worksheet at Annex A.

Risk Areas

Nine key risk areas should be addressed when conducting any risk identification process.

These areas are:

1. Commercial and legal risks;
2. Economic / Financial risks;
3. Technology risks;
4. Operational risks;
5. Political risks;
6. Management activities / control risks;
7. Human resource risks;
8. Occupational Health & Safety / Environmental / Disability access risks; and
9. Natural events.

To reduce the probability of inadvertently missing a potential risk, it is recommended to systematically identify risks under each of the above headings for your activity or project.

Some recommended methods for identifying risks include:

- Audits or physical inspections.
- Accident / Incident reports.
- Brainstorming.
- Decision trees.
- History.
- Interview / focus groups.
- Personal or organisational experience.
- Scenario analysis.
- Strengths, weaknesses, opportunities and threats (SWOT) analysis.
- Survey or questionnaires.

Some questions to ask when identifying risks:

- When, where, why, and how are the risks likely to occur?
- What is the source of each risk?
- What are the stakeholder's expectations?
- What is the potential cost in time, money and disruption to customers of each risk?

Some general examples of potential sources of risk by risk area include:

		1	2	3	4	5	6
RISK AREAS	**Commercial and Legal**	Fraud	Outsourcing	Negligence	Breach of contract	Breach of statute	
	Economic / Financial	Regional instability	Delegations	Devolved responsibilities	Misuse of funds	Currency fluctuations	Misappropriation of funds
	Technology	E-commerce	IT infrastructure	Information security	Innovation	Obsolescence	
	Operational	Inappropriate client advice	Security of personnel	Reduction in client service	Commercial espionage		
	Political	Political decisions effecting business activity	On-going scrutiny by media	Terrorist activity	Community perceptions		
	Management Controls	Inappropriate project objectives	Breach of procedure	Inappropriate use of resources	Mismanagement		
	Human Resources	Loss of key staff	Employee relations	Performance management	Violence		
	Natural Events	Earthquake	Storm / tempest	Flood	Bushfires		
	OH&S / Environmental / Disability Access	Inadequate safety measures	Poor safety management	Inadequate equipment / facilities	Contamination	Pollution	Noise

3.2.3 Step 3: Assess the Risks

The objective of this Step is to separate the minor acceptable risks from the major risks and provide data for the subsequent treatment of those risks.

For each risk identified in Step 2 determine the existing controls and analyze the risk in terms of consequence and likelihood in the context of those controls. The analysis should consider the range of potential consequences and how likely they are to occur. Consequence and likelihood are combined to produce an estimated level of risk.

The estimated levels of risk are compared against the criteria established in Step 1 and a prioritized list of the risks requiring further action is prepared.

The following table can be used for assessing the consequence and likelihood. Whilst the numeric rating scale should be applied consistently for each activity or project evaluated, the detailed descriptions contained in the table is provided as an example only and will need to be altered to suit the specific activity being assessed.

	→ Consequence →				
People	Injuries or ailments not requiring medical treatment.	Minor injury or First Aid Treatment Case.	Serious injury causing hospitalization or multiple medical treatment cases.	Life threatening injury or multiple serious injuries causing hospitalization.	Death or multiple life threatening injuries.
Reputation	Internal review.	Scrutiny required by internal committees or internal audit to prevent escalation.	Scrutiny required by external committees or ACT Auditor General's Office, or inquest, etc.	Intense public political and media scrutiny e.g. front page headlines, TV, etc.	Assembly inquiry or Commission or inquiry or adverse national media.
Business Process & Systems	Minor errors in systems or processes requiring corrective action, or minor delay without impact on overall schedule.	Policy procedural rule occasionally not met or services do not fully meet needs.	One or more key accountability requirements not met, inconvenience but not client welfare threatening.	Strategies not consistent with Government's agenda. Trends show service is degraded.	Critical system failure, bad policy advice or ongoing non-compliance. Business severely affected.
Financial	1% of Budget or <$5k	2.5% of Budget or <$50K	>5% of Budget or <$500K	>10% of Budget or <$5M	>25% of Budget or >$5M

	Numerical:	Historical:
Likelihood	>1 in 10	Is expected to occur in most circumstances
	1 in 10 - 100	Will probably occur
	1 in 100 – 1,000	Might occur at some time in the future

>7: Extreme Risk

- detailed action plan required

6,7: High Risk

- needs senior management attention

5: Medium risk

- specify management responsibility

<5: Low Risk

- manage by routine procedures

High or **Extreme** risks must be reported to Senior Management and require detailed treatment plans to reduce the risk to **Low** or **Medium**

		Insignificant	Minor	Moderate	Major	Catastrophic
		1	2	3	4	5
Almost Certain	5	6	7	8	9	10
Likely	4	5	6	7	8	9
Possible	3	4	5	6	7	8
Unlikely	2	3	4	5	6	7
Rare	1	2	3	4	5	6

An evaluation of each risk is now undertaken to determine those risks that are acceptable and those that require further treatment.   This step should evaluate the level of risk found with the criteria established in Step 1 (Establish the Context).

Some reasons why a risk may be acceptable include:

- The level of risk is so low that specific treatment in not suitable given the available resources.
- There is no treatment available.
- The costs of treatment outweigh the benefit.
- Opportunities presented outweigh the threats to such an extent that the risk is acceptable.

Those risks requiring further action are prioritized for treatment in Step 4. Those risks accepted, are noted and monitored in accordance with Step 5.

3.2.4 Step 4: Treat the Risks

Accept and monitor low priority risks. For other risks, that is, those rated a 6 or higher develop and implement a specific management action plan that includes consideration of funding. The plan should use the Risk Treatment and Action Plan at Annex B
The treatment options include:

- **Avoid** the risk by deciding not to proceed with the project or activity. This may only occur within legislative requirements and business agreements.

- **Reduce the likelihood** of the occurrence. e.g. contract conditions, supervision, technical controls, compliance programs, procedure manuals, quality control manuals, training, etc.

- **Reduce the consequence** of the occurrence. e.g. contingency planning, fraud control planning, relocation of an activity or operation, etc.

- **Transfer the risk** to another party. e.g. use of contracts, insurance, partnerships, etc.

OH&S Treatment

For occupational, health and safety risks, the following prioritized treatment measures are to be followed:

1. **Elimination** - remove the hazard or risk of exposure.
2. **Substitution/isolation** - use something less hazardous or provide a barrier between hazard and person.
3. **Engineering** – new or modify equipment - e.g. using trolleys or other equipment for carrying or lifting, guarding on machinery.
4. **Administrative** - provide training, policies and procedures for safe work practices, rest breaks, job rotation.
5. **Personal protective equipment** (used as a last resort and in conjunction with one of the above) - e.g. goggles, gloves, respirator.

Risk Transfer

Where the Organization seeks to transfer risk to another party, this will be undertaken in the following order of priority:

- Obtaining indemnities from other parties for loss suffered by the Organization.
- Obtaining releases from other parties for loss suffered by them as a result of dealing with the Organization.
- Requiring other parties to insure the Organization’s exposure and their own exposure to the Organization, complete with insurer’s agreement to waive rights of recovery against the Organization.

3.2.5 Step 5: Monitor and Review

Monitor and review the effectiveness and performance of the risk treatment options, strategies, and the management system and changes which might affect it.

- Each step undertaken should be documented to enable effective monitoring and review.
- Risks and the effectiveness of treatment measures need to be monitored to ensure changing circumstances do not alter the risk priorities.
- Identification, assessment, and treatments must be reviewed to ensure the risks remain relevant and continue to be managed and that any new or emerging risks are identified and managed.

In order to understand risk and monitor performance, managers will be

required to maintain records and undertake regular reporting.

♦ **Business Records** to be retained by all Managers should include Asset Schedules, Valuations, OH & S recommendations, etc.

Additionally, management will progressively develop, implement and document safe practice procedures and guidelines, dealing with all aspects of the business including office layouts, staff appointments and dismissals, contract negotiations, setting of consultancy briefs, limitations to authority, insurance and claims management, vetting third party contracts, etc.

♦ **Standard Contracts**

The Organization uses Standard Contracts for purchasing services. The Manager Approved Procurement Unit is responsible for the clearance of all contracts prior to signing.

♦ **On-going Risk Management Education**

Including regular documentary updates (e.g. new procedures, legislation etc), seminars and workshops.

♦ **Risk Audits**

A rolling series of continuous self and third party audits and safety inspections, using checklists, analysis and positive feedback.

3.2.6 Step 6: Communicate and Consult

Communicate and consult with internal and external stakeholders as appropriate at each stage of the risk management process and concerning the process as a whole.

- A communication plan should be developed for internal and external stakeholders early in the planning process.
- Communication should be a two-way process involving consultation.

Management is responsible for identifying the existence of risk and undertaking the business of the Organization in a manner, which ensures appropriate management of those risks.

3.2.7 Step 7: Performance Indicators

i) No severe insurable loss to disrupt the Organization’s financial position.

ii) Risk management to be included in the business planning function.

iii) All new projects (in excess of $100,000 or where a significant risk to the Organization exists) to be assessed for risk in accordance with these guidelines prior to initiation.

iv) Annual assessment of risks to be recorded and acted upon as detailed in the annual Risk Management and Audit Plan.

v) No revenue loss or significant event to disrupt the Organization through improper conduct by staff.

vi) No diminishing of the Organization’s reputation or standing in the community.

Annex A

Identifying and analyzing RISK WORKSHEET

Activity/Project: ____________ Division/Unit: ____________

Completed by: ____________ Date: ____________

Reviewed by:: .... Date: ....

Risk No.	The Risk What can happen and How it can happen	The Consequence from an event happening	Description and Adequacy of Existing Controls	Likelihood Rating (a)	Consequence Rating (b)	Overall Risk Level (a+b)	Risk Priority

Annex B

Risk treatment and action plan WORKSHEET

Activity/Project: ____________ Division/Unit: ....

Completed by: ____________ Date: ....

Reviewed by:: .... Date: ____________

Correlating Ref from Risk worksheet	Treatment/Controls to be implemented	Risk rating after treatment/ controls	Person responsible for implementing treatment/controls	Timeframe	Date Completed	Risk and treatment/controls monitored/reviewed		Date completed
						How	When	

4 CONDUCTING A RISK MANAGEMENT REVIEW

4.1 Introduction

Risk management is one of the specialties within the general field of management. It is the process of making and carrying out decisions that will minimize the adverse effects of accidental losses upon an organization. An organization has one or more of a variety of objectives: profit, growth, stable earnings, public service, or the performance of a governmental function, to name a few. To achieve these objectives, an organization must first reach a more fundamental goal: survival in the face of potentially crippling accidental losses. Beyond survival, the top management of an organization also may wish to prevent any accidental losses from interrupting the organization's operations, slowing its growth, or reducing its profits or cash flows by more than a specified amount.

4.2 Basic Steps – Risk Management Flow Chart

The only losses which are significant to an organization are those that, as isolated events or as a series of accumulated losses, may interfere with the organization's achieving its objectives.

The function of risk management is to reduce the risk of loss and minimize its effects through:

a. identification of sources of Property, Net Income, Liability, and Personnel risks from which losses may arise;

b. evaluation of the financial risk involved in each exposure in terms of expected frequency, severity and impact;

c. treatment of risks by:

- Elimination or avoidance
- Reduction or control
- Transfer to others
- Funding

d. monitoring of results continuously and systematically.

4.2.1 Step 1: Identifying Exposure to Loss

A loss exposure is a possibility of loss, more specifically, the possibility of financial loss that a particular entity faces as a result of a particular peril striking a particular thing of value. Probably the most important step in the risk management process is the identification or finding of risks that need to be treated. For, if you are not aware of the existence of a risk, you certainly cannot make plans for handling it.

In order to consider the identification of risks, it is necessary to classify them in some sort of orderly manner. Although various methods for classifying risk can be devised, it is common to classify risks in a manner similar to that used by the insurance industry. This system has the advantage of making it easier to relate risks to insurance coverages.

Property risks of several types are created by the possibility of property being damaged or destroyed. Our first task involves identifying that property and then determining what perils might damage it. First party losses can be divided into three categories. A direct loss is incurred by the owner of property or the party responsible for property when it is damaged by a peril. The property may be real property or personal property. A loss is sustained if expenditure must be made to repair or replace the damaged or destroyed property.

Damage to real or personal property may cause indirect or consequential losses. These are losses which occur when, as a result of damage to real or personal property, income is reduced or additional expenses are incurred other than for the repair or replacement of damaged property.

A contingent loss may be suffered by a party who is dependent upon the activities of another party owning or operating the property that is damaged. For example, if a major supplier's facility is damaged, or access to your facilities is not possible because of a storm or other catastrophe, you may lose income, or incur additional expenses as a result of the storm.

Crime losses fall into a number of categories. They can result from employee dishonesty (infidelity) or from losses such as burglary, robbery, or forgery by outsiders. Crime losses may involve money, securities or similar types of property or merchandise. They may involve violence or the threat of violence, or they may take place unnoticed until it is discovered sometime after its having occurred. Often, the most serious losses occur when there is collusion between an employee and an outsider.

Casualty losses are of many types. The term "casualty" originally implied a sudden and accidental occurrence involving loss of life or at least serious injury. However, the term is used rather freely today to indicate losses caused by injuries to persons or liability for injuries to persons or damage to property of others. Workers Compensation, General Liability, Auto, Aircraft, Watercraft and similar losses are considered casualty losses.

4.2.2 Step 2: Evaluation of Risks

Once identified, the next step in the risk management process is to evaluate risks. For the risk manager of a large organization, this may be a complex mathematical process involving statistical analysis and theories of probability. In order to evaluate a risk, one must determine the probability of loss by considering the following:

a. frequency
b. severity
c. variation
d. impact

Frequency is merely a measure of how often a particular type of loss will occur. Generally, smaller losses are apt to occur more frequently and larger losses less frequently. Therefore, when considering the degree of risk involved, we must also consider severity--the amount of loss that is apt to be sustained. To predict future losses, prior occurrences should be reviewed to determine how often losses of a certain type have taken place, and the range in cost of those losses. Various "trending factors" are applied to recognize such things as inflation, changes in laws, delay in
reporting claims, increased activity, etc.

The need for most businesses to be cautious when surveying exposures to risk and considering prior loss experience as an indication of probable future loss experience cannot be emphasized too strongly. The fact that you have not had a fire at a location during the last five years does not mean that you will not have a fire next year. However, a high frequency of small losses may be an indication of carelessness or poor management. Frequency generally will breed severity.

While risks are commonly evaluated in terms of frequency, severity and variation, the possible impact of a loss is also an important consideration. When dealing with risks involving damage or destruction of property, it is common to consider severity and impact in terms of maximum possible loss (the worst that could happen) or maximum probable loss (the worst that is likely to happen).

Usually, maximum probable loss is a more realistic measure, but this can be very difficult to determine when large, highly valued properties are involved. Not only is it sometimes difficult to determine the extent to which a particular property would be damaged by a peril, but it can also be extremely difficult to determine the extent to which business will be interrupted or the extra expenditures that would be required to conduct operations at another location and expedite reconstruction of the damaged facility.

Evaluation of liability risks is much more difficult. for the most part, the amount of a liability claim is a matter of pure chance, although smaller losses do occur more frequently than large losses.

4.2.3 Step 3: Alternative Risk Management Techniques

After risks have been identified and evaluated, the next step in the risk management process is a determination of what to do about them. Risk management involves either stopping losses from happening (risk control) or paying for those losses that inevitably do occur (risk financing).

Risk Control Techniques

Certainly, controlling a risk is preferable to merely accepting or transferring the possible financial consequences, but complete control is seldom possible. Therefore, the treatment of risks usually involves an intermixing of controlling, transferring and funding. Risk control includes those risk management techniques designed to minimize the frequency or severity of accidental losses or to make losses more predictable. Risk control techniques include exposure avoidance, loss prevention, loss reduction, segregation of loss exposures, and contractual transfers designed to protect an organization from legal obligations to pay for others' losses.

Whether a risk is insured or self-insured, the services provided by an insurer or a service organization will play an extremely important part in determining long range costs. Although safety engineering can assist in reducing the number of losses, the prime responsibility for these functions has to lie within one's own organization. Reducing the amount or severity of claims requires the joint effort of an insured and the claims department of an insurer. A major factor to be considered when purchasing insurance is the manner in which claims are going to be investigated, defended and settled.

Risk Financing Techniques

Risk financing techniques encompass all the ways of generating funds to pay for losses that risk control techniques do not entirely stop from happening. These sources of funds, or risk financing techniques, can be classified into two large groups: retention (the funds for paying losses originate within the organization), and transfer (the funds originate from a source outside the organization). While this distinction between retention and transfer is useful in analyzing and planning to meet an organization's risk financing needs, some risk financing arrangements may involve elements of both retention and transfer.

Selection of Alternatives

After systematically considering how various risk control and risk financing options might be applied to particular loss exposures, the next step is to establish and apply criteria to determine what combination of risk control and risk financing techniques is best in serving that organization's objectives.

Selecting the best risk management technique, or more often combinations of risk control and risk financing techniques, is a two-step activity. The first requires forecasting the effects the available risk management options are likely to have on the organization's ability to fulfill its goals. The second is defining and applying criteria that measure how well each alternative risk management technique contributes to each organizational objective in cost-effective ways.

Risk management techniques are chosen on the basis of effectiveness and economy. Effective means capable of achieving the desired goals, such as organizational survival, minimum profit level, growth, and legality. Economic means least expensive of the possible effective ways.

Most organizations choose risk management techniques by financial criteria, that is, choose those techniques which have the greatest positive (or least negative) effect on rate of return.

4.2.4 Step 4: Monitoring the Risk Management Program

Once implemented, a risk management program needs to be monitored to assure that it is achieving the results expected of it and to adjust the program for changes in loss exposures and the availability and/or costs of alternative risk management techniques. The monitoring and adjusting process requires each of the elements of the general management function classically labeled "control:" (1) standards of what constitutes acceptable performance, (2) comparison of actual results with these standards, and (3) correction of substandard performance (or, if necessary, alteration of unrealistic standards).

Benefits and Costs of Risk Management

Exposures to accidental loss, both actual and potential, impose costs on particular organizations and on the entire economy. These costs fall into three broad categories: (1) property, income, lives, and other things of value damaged or destroyed in accidents; (2) the deterrence effects of potential accidental losses (the net benefits that could have been gained from activities no one undertook because they were judged to "risky"), and (3) the resources devoted to managing accidental losses (resources that could have been put to alternative uses had there been no possibility of any accidental losses, no loss exposures).

For an individual organization and for the entire economy, the third category of costs constitutes the "cost of risk management"' the reduction in either of the first two categories of costs constitutes the "benefits of risk management." For an organization as for an economy, a proper risk management program minimizes the total of all three categories of these costs.

5 FURTHER READING

For more information on other products available from The Art of Service, you can visit our website: http://www.theartofservice.com

If you found this guide helpful, you can find more publications from The Art of Service at: http://www.amazon.com