IA 315: Information Security Auditing and Assurance

Lecture 4: Risk Management and Business Continuity Planning

Presented by:
Dr. Jabhera Matogoro
E-mail: jabhera.Matogoro@udom.ac.tz

Introduction to Risk Management

- Risk:
  - It is the probability that something bad might happen
- Risk Management:
  - It is concerned with the potential loss, including economic loss, human suffering or that which may prevent the organization from being able to achieve its goals
  - It is a conscious effort of planning, organizing, directing and controlling resources and activities.
  - It is used to minimize the adverse effects of accidental loss at the least acceptable cost.

Critical Elements of Risk

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

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.

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.

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.

Risk Management Decision Process...

- Select:
  - Appropriate techniques
- Implement:
  - Chose and use techniques

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
- Hardware & Software
- Vehicle

Evaluate Loss Potential

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

Challenges to Risk Management - 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

Challenges to Risk Management - External

- Insurance market
- Vendors
- Unions
- Auxiliary organizations

Risk Management and Information Technology Infrastructure Library (ITIL)

- 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

IT Service Continuity Management

- 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.

Business Continuity Management and Risk Assessment

- Business Continuity Management (BCM):
  - It 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.
  - Analyzing 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

Business Continuity Management and Risk Assessment…

- 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

Business Continuity Management and Risk Assessment: 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.

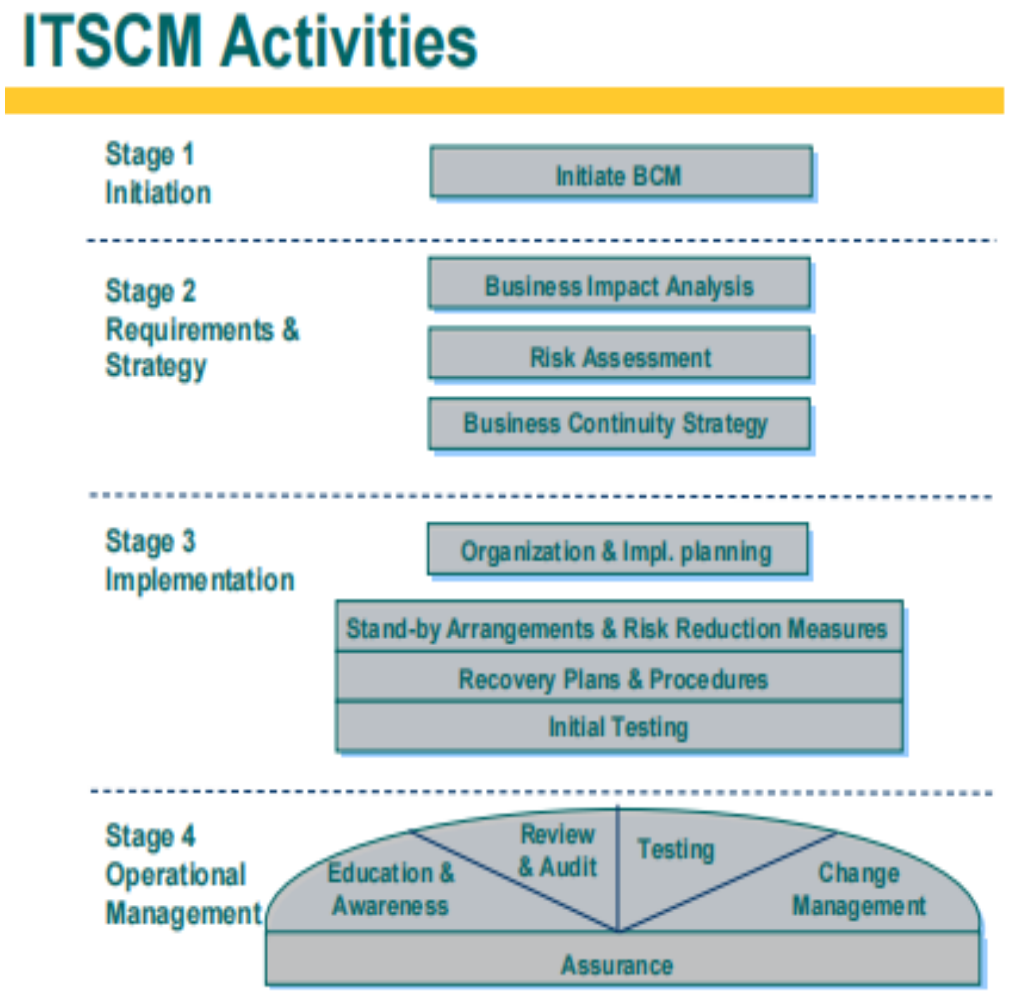
The IT Service Continuity Management (ITSCM) process:

- 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

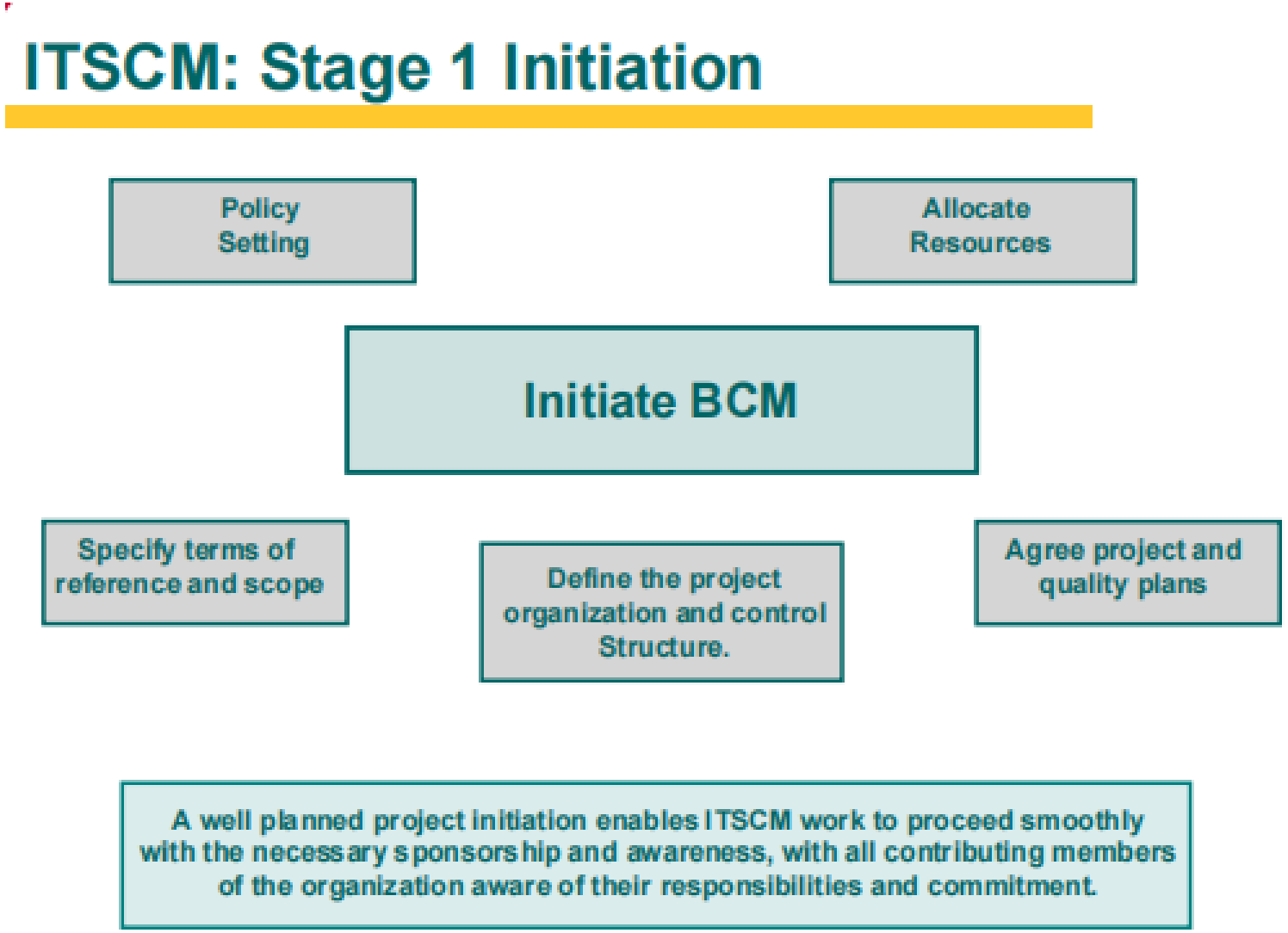
The IT Service Continuity Management (ITSCM) process...

- 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.

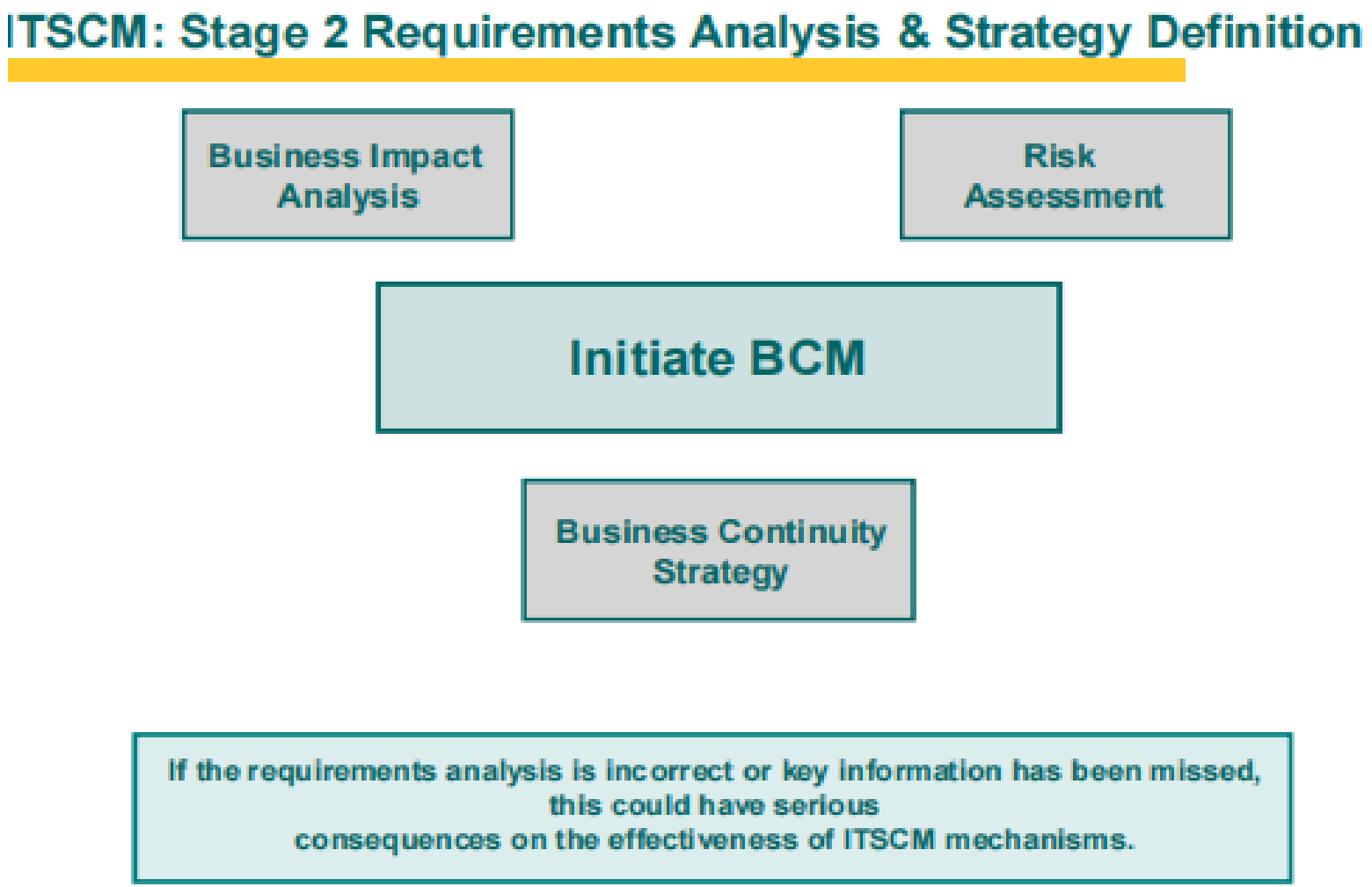
IT Service Continuity Management Activities



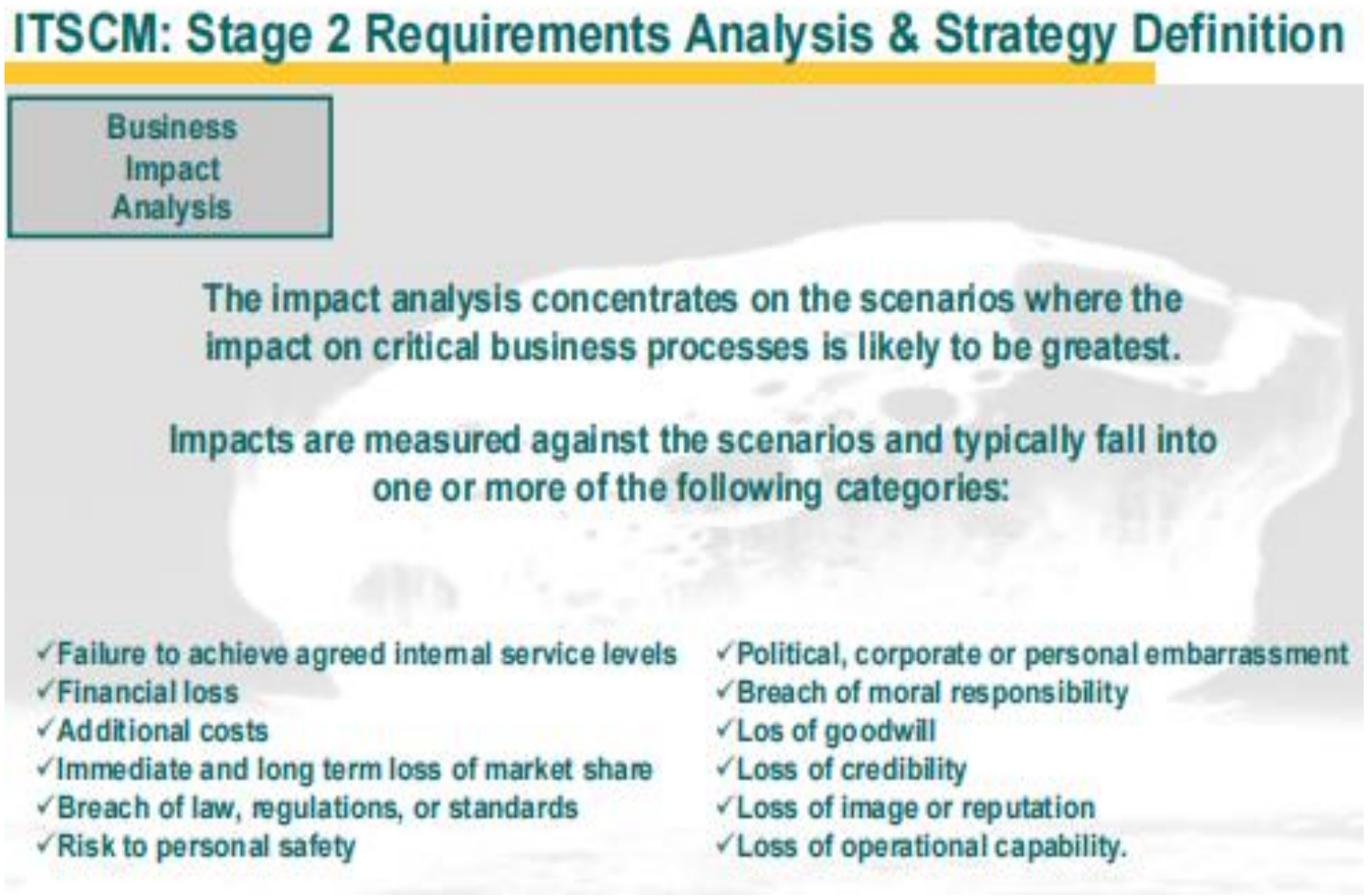
IT Service Continuity Management…



IT Service Continuity Management…



IT Service Continuity Management…



IT Service Continuity Management…

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

IT Service Continuity Management…



IT Service Continuity Management…

ITSCM: Stage 2 Requirements Analysis & Strategy Definition

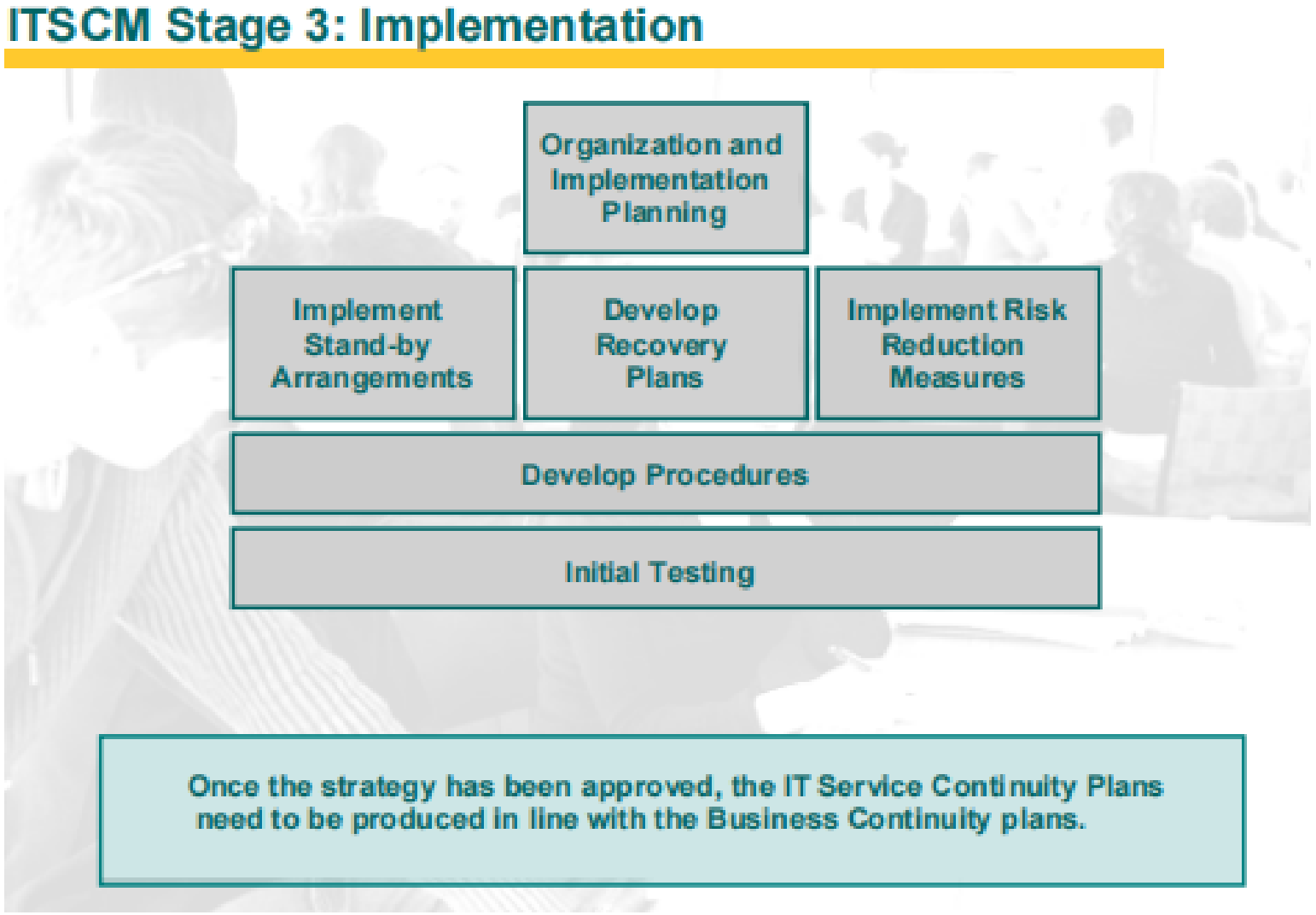
Business Continuity Strategy

Recovery Options

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



IT Service Continuity Management…



IT Service Continuity Management…



IT Service Continuity Management…



IT Service Continuity Management…

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.

IT Service Continuity Management…

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.

IT Service Continuity Management…

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.

IT Service Continuity Management…

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:

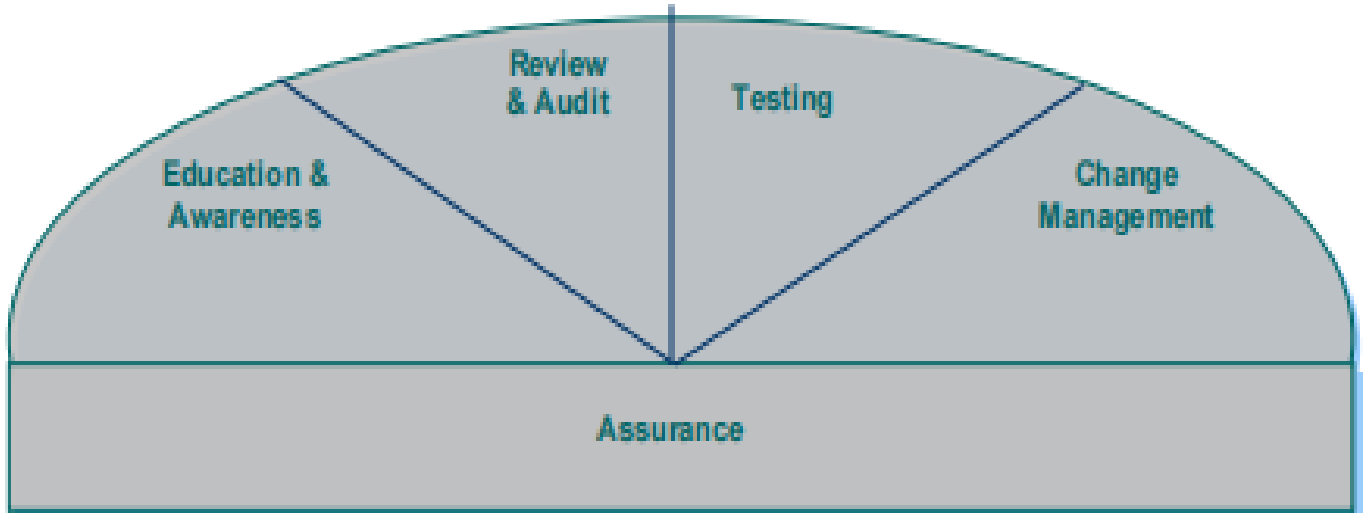
- Installation and testing of replacement hardware and networks
- Restoration of software and data to a common reference point which is consistent across all business processes
- Different times zones in a multinational organization
- Business cut-off points.

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.

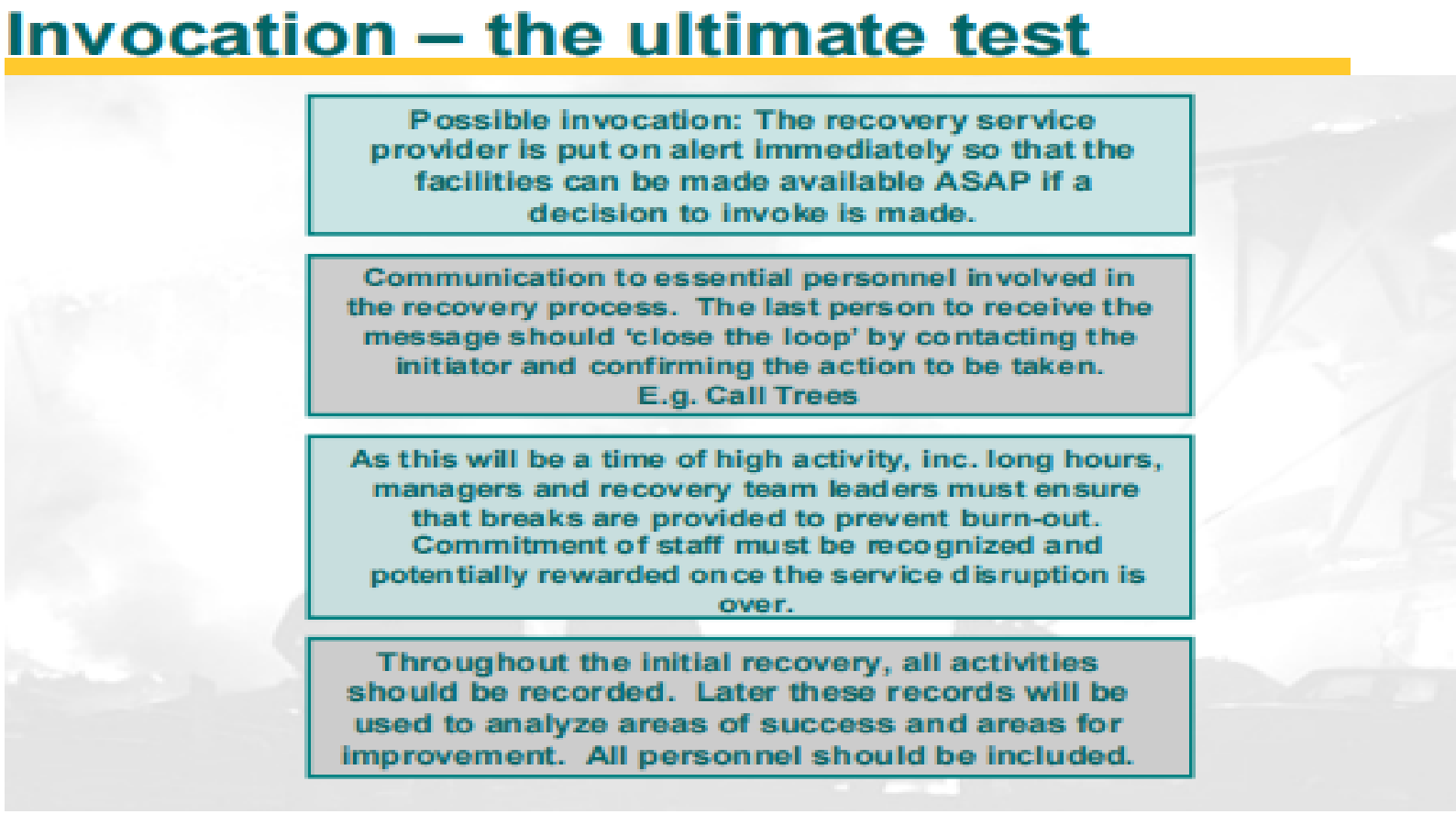
IT Service Continuity Management…

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:



IT Service Continuity Management…



IT Service Continuity Management…

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

IT Service Continuity Management…

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)

IT Service Continuity Management…

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

IT Service Continuity Management…

ITSCM - Benefits

Overall better risk management

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

IT Service Continuity Management…

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

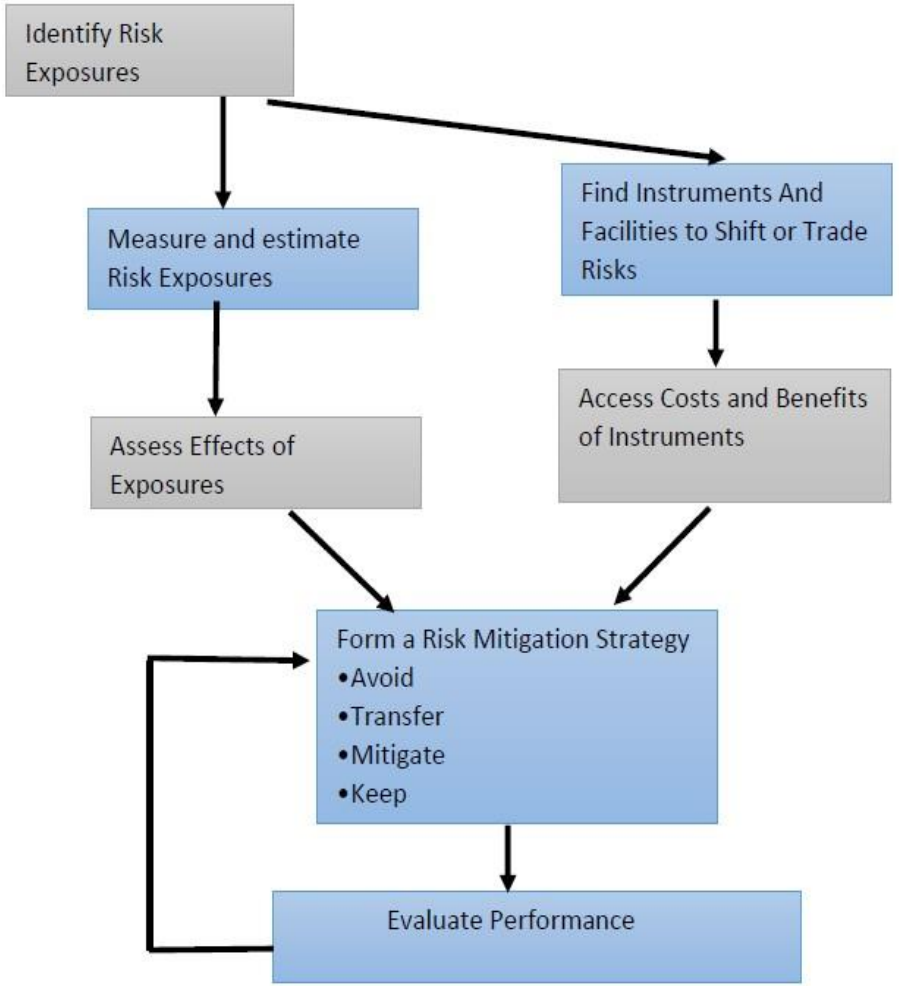
Risk Management

- ITIL V3
- ITSCM
- Management of Risk (M_o_R)

INTRODUCTION

- Risk management is a vital part of business nowadays.
- Some readers think that only innovative businesses need risk management, and that there is no risk in a conservative business. However, this is not true.
- There is risk in all organizations since its creation until its dissolution.
- Before delving into the details of risk management, it is important to define what risk is.

The risk management process diagram



The risk management process continue…

- The identification of risks is the process of identifying threats, vulnerabilities, or events that may have an impact on the set of assets owned by the organization.
- This identification can also be about opportunities, but not all risk management frameworks explore this.
- For risk identification, experience is important because it is common for the risk source to derive from a non-deterministic cause.
- After identification comes the analysis of the identified risk.

The risk management process continue…

- Risk analysis is concerned with the gathering and measuring of information about risk exposure, so that the organization can make suitable decisions and manage risk appropriately.
- Finally, risk control involves monitoring the environment for improved effectiveness against the previous set of threats, vulnerabilities, or events and make decisions about them.
- These decisions can be to avoid, mitigate, transfer or keep the risk.

The risk management process continue…

- The actual process can vary according the framework used.
- Every organization has a kind of risk management that is not always explicit, well-structured or consistently applied to support decision making.
- The task aim of risk management is to ensure that the organization makes a cost-effective use of a risk framework that has a set of well-defined steps.
- The aim is to better support more critical decision making through a good understanding of risks and their likely impact in order to achieve competitive advantage.
- IT risk management has the same goals and steps of risk management in general.

Why IT Risk Management Matters?

- Nowadays all organizations have a very strong relationship with IT, most of them are completely dependent on it and it would not be possible to maintain large scale business without IT.
- To achieve the best return of investment, avoid instability and add value to an organization, a good risk management is essential.
- So the risk management on IT Service Management is an indispensable component.
- We have uncountable guidelines, frameworks and tools designed to support risk management and IT Service Management.
- To implement an IT Service Management framework, ITIL is usually the option

IT Infrastructure Library (ITIL)

- ITIL is considered a framework of best practice guidance for IT Service Management and it is widely used in the business world.
- ITIL It was developed by CCTA, in Norwich, England, on behalf of the British government.
- The CCTA is currently the Office of Governance Commerce (OGC).
- As said by the ITIL Foundation in IT Service Management, ITIL is accepted as the Best Practices for lowering process costs while improving the quality of IT services delivered to users.
- It is derived from the practices of the most successful and effective people in the field.
- Therefore, it would be useful to explore risk management in the context of this framework.

IT Infrastructure Library continue….

- However, the information about risk management in the ITIL is generalist and unsatisfactory.
- Compared with other IT service management frameworks, ITIL is weak in the risk management field.
- This forces organizations to the implementation of a risk management framework parallel to IT Service Management which leads to a loss of efficiency and detail.
- ITIL V3 has as a base for risk management with the concept of **“coordinated risk assessment exercises**

ITIL V3

- This framework consists of five stages of the service lifecycle, with each stage consisting of processes or functions aligned with the IT organizational structure.
- These processes can be adopted based on suitability for the team, which gives ITIL some flexibility.

Stages of ITIL V3

- Strategy
- Design
- Transition
- Operation
- Continual Improvement

Stages of ITIL V3 continue…

- **Service Strategy,** the service strategy facilitates organizations to strategize and set business goals to meet customer demands and needs.
- **Service Design,** this stage in lifecycle includes design of service management processes, technology, infrastructure, products, processes, and functions.
- **Service Transition,** risk and impact of any change must be taken into consideration, which is where this stage begins. Transition planning and support is focused on maintaining current functionality while deploying new organizational changes with minimal risks.

Stages of ITIL V3 continue…

- **Service Operation,** Service operation is the stage where day-to-day operational tasks would fall. This stage is responsible for monitoring infrastructure and application related services and enables business to meet the needs of their customers and staff.
- **Continual Service Improvement,** the quality check of continual service improvement ensures that throughout the lifecycle, improvement is the end goal. This is also part of service continuity management.

Stages of ITIL V3 continue…

- Uniquely to ITIL V3 is also the four P's of service design (which is the part of service design phase in the service lifecycle), the four P's are:
  - **People:** Considering the people in charge of providing IT services as well as the people who will be using them.
  - **Processes:** Measurable processes and support needed
  - **Partners:** Which involves vendors, manufacturers, or suppliers should be considered.
  - **Products:** Tools, services, and technology used for the support and delivery of the service.

Benefits of ITIL

- Strong alignment between IT and organization as a whole
- Clearer expectations for both the IT service desk and their customers
- Reduce costs
- Improved resource utilization
- Greater visibility of assets
- Better management of risks, system failures, and service disruptions
- Improved service level and testing

Limitations of ITIL

- ITIL is considered a framework of best practice guidance for IT Service Management and it is widely used in the business world.
- In spite of this, ITIL has some gaps in Risk Management specification.
- There is just a coordination of exercises instead of a clear and owned process, what can limit the efficiency of ITIL implementation in organizations.
- Our work approaches this problem and compares IT risk management in ITIL to other IT Governance Frameworks.
- Despite ITIL stating that risk should be identified, measured and mitigated, it is not clear how to proceed (no concrete process is defined on how to deal with risk).

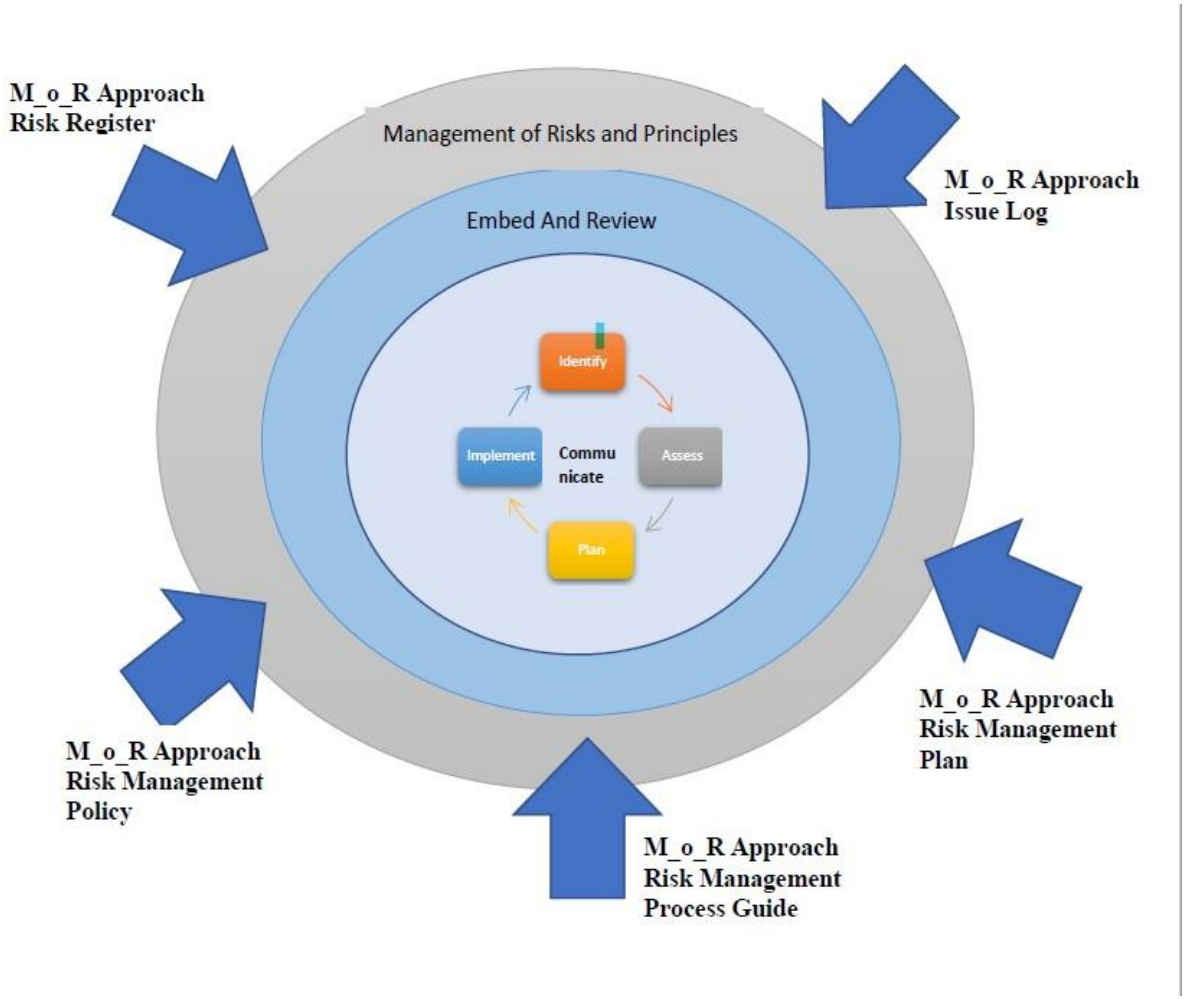
Limitations of ITIL continue…

- To solve this, we propose to map the M_o_R risk management framework in ITIL, mapping every M_o_R process in ITIL, and therefore adopt a strong risk management in ITIL, based on specific guidelines, without changing the framework.
- Besides this, we propose the introduction of new elements in the risk management ITIL process such as KRIs and a new process responsible for define risk management and guide risk management implementation in the other processes.
- With this model we present its theoretical application and evaluation by experts.

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.
- Risk Management is an enabling function that adds value to the activities of the organization and increases the probability of success in achieving our strategic objectives.
- It’s about managing uncertainty and creating an environment where surprises are minimized.

Management of Risk(M_o_R) Principles



(M_o_R) Principles continue…

- **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) Principles continue…

- **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.

(M_o_R) Principles continue…

- **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.

Benefits of M_o_R

- The benefits of creating a practical Risk Management Framework that can be applied across all part of the University include:
  - A consistent, structured approach to identifying and managing risk.
  - Supports the achievement of the University's strategic and operational goals by managing risks that may otherwise impede success.
  - Encourages an open and transparent culture where risk discussion and awareness are supported.
  - Better decision making practices that support risk informed choices, prioritize actions and distinguish between alternative courses of action.
  - Encourages an understanding of the risk environment within which the University operates.
  - Provides assurance to the Vice Chancellor and Council that critical risks are being identified and managed effectively.

Risk Assessment and control

- **Risk assessment:**
  - It is a term used to describe the overall process or method where you identify hazards and risk factors that have the potential to cause harm (hazard identification).
  - Analyze and evaluate the risk associated with that hazard (risk analysis, and risk evaluation).
- **Risk control:**
  - It is the set of methods by which firms evaluate potential losses and take action to reduce or eliminate such threats.
  - Risk control also implements proactive changes to reduce risk in these areas.
  - Risk control thus helps companies limit lost assets and income.

Risk Assessment and Control steps

- Identify the Activity
- Identify who may be at risk by the activity
- Identify the hazards
- Identify Associated Risks
- Identify Risk rating with existing controls
- Identify Additional risk controls required
- Identify Risk rating with additional controls
- Documentation and Initial Approval
- Implement the additional risk controls identified
- Monitor and review the risk controls

Conclusion

- In order to address IT Risk in an organization:
  - Ensure security and confidentiality of customer information.
  - Protect against anticipated threats to the security or integrity of such information.
  - Guard against the unauthorized access or use that could result in substantial harm or inconvenience.
  - 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.