ITIL® and Corporate Risk Alignment Guide

An introduction to corporate risk and ITIL, and how ITIL supports and is assisted by Management of Risk (M_o_R®)

Michael Faber and Rubina Faber

March 2010

Abstract

ITIL is the key standard for IT service management. This white paper aims to show how risk management can be of assistance in the context of service management.

Management of Risk (M_o_R) is OGC's best practice guidance on how to manage risk. There are many standards and guides that relate to risk management. M_o_R is used here for comparative purposes because, along with ITIL, it is part of OGC's portfolio of best-management practices.

The main body of this paper considers what ITIL and corporate risk are, and why they are important to business. It will align the objectives of ITIL with those of the management of corporate risk – highlighting why risk should be taken into consideration and what benefits can be realized and capitalized by aligning ITIL and M_o_R at each stage of the service lifecycle.

Contents

Introduction

In today's fast-moving world, change has become a way of life. However, alongside change we must also consider efficiency and effectiveness, which leads to the question:

How do we improve if things are always changing?

Organizations must balance management of their current service offerings with a provision for future changes. This requires an understanding of the risks to both the current business service offerings and change opportunities.

This document aims to provide an overview of risk (specifically corporate risk) and ITIL. The paper focuses on ITIL (with its service lifecycle approach), and demonstrates how and why risk should be considered within each element of the ITIL lifecycle.

Audience

This document is aimed at a broad range of communities:

- Those who understand risk and would like to understand ITIL
- Those who understand ITIL and would like to understand risk
- Those who would like a 'flavour' of risk and ITIL, and an appreciation of how risk can be integrated into the ITIL service management lifecycle and the benefits this can bring.

With such a wide readership it is not possible to cover all aspects of ITIL and risk within this document. For simplicity, we have used tables to demonstrate the alignment between ITIL and risk at each stage of the service lifecycle. Within these tables, the associated risk considerations for each activity are referenced. It is hoped that this approach makes it an easy reference guide – for all communities!

Further information can be found in the sources referenced at the end of this document.

What is corporate risk?

Risk is inherent in everything we do, at both a business and personal level.

When referring to corporate risk we are concentrating on the objectives of the business (or organization), and identifying and managing risks that could affect the outcome of those objectives.

The word 'corporate' is often thought to relate to the private sector, but here it refers to the *organization*, whether public or private sector.

What is risk?

When considering our objectives and the activities associated with the delivery of them, we need to think about what might happen. This element of uncertainty is known as risk.

Definition of risk:

'an uncertain event or set of events which, should it occur, will have an effect on the achievement of objectives. A risk consists of a combination of the *probability* of a perceived *threat* or *opportunity* occurring and the magnitude of its *impact* on objectives.'

Within this definition:

'Threat' is used to describe an uncertain event that could have a negative impact on objectives or benefits; and

'Opportunity' is used to describe an uncertain event that could have a favourable impact on objectives or benefits.

Unfortunately, when referring to risk most people think about negative outcomes – forgetting that positive things can happen as well!

BS31100 (the British Standard for risk management) recognizes these opportunities, stating in the introduction that risk management is as much about exploiting potential opportunities as preventing potential problems.

Example:

Let us consider a simple scenario where Company X has decided (as part of its strategy) to provide a service enabling customers to buy its products and services via the internet. To assist in meeting this objective, Company X will adopt an online payment system as part of its service management offering.

The organization would need to understand the impact that the new purchase order system would bring. It would be foolish for it to just say 'let's go ahead and do it' without any consideration for the business (although experience shows this does happen!). Even if the system costs nothing to buy, without some analysis of the risks this change could bring the organization may not only subject itself to a high degree of threat (negative risk) which could effectively stop the business from functioning, it may also miss out on opportunities (further benefits) simply because it didn't consider them.

The organization needs to understand the overall threats and opportunities (i.e. corporate risk) it faces and take this into consideration when making decisions.

You might come to the conclusion that this is simply good business practice, ensuring that a business is protected. In simple terms this is what is meant by corporate governance – putting things in place to protect the business.

Why is this necessary, you may ask? Well, let's take a history lesson…

Corporate governance and governance (including IT governance)

Definition of corporate governance:

'The ongoing activity of maintaining a sound system of internal control by which the directors and officers of an organization ensure that effective management systems, including financial monitoring and control systems, have been put in place to protect assets, earnings capacity and the reputation of the organization.'

History should teach us a lesson!

When things go wrong there is normally evidence of organizational practices where risk does not seem to have been taken into account.

Since the early 1990s, corporate governance has received considerable press attention with incidents such as the Robert Maxwell pensions scandal, the collapse of Barings Bank and the massive bankruptcies and criminal malpractice in the cases of, for example, Enron and WorldCom, to name but a few.

We are often left asking the question 'how could this have happened?'

To obtain the answer stakeholders have often demanded an inquiry. These inquiries frequently publish reports, which include recommendations.

We all want to learn from mistakes – to avoid them happening to us and to develop our own good practice. As a result, these recommendations have, over time, developed to become a code of good practice – in the UK this is more formally known as the Combined Code on Corporate Governance (last revised in 2006).

The Combined Code makes reference to 'corporate' governance. Companies listed on the London Stock Exchange are required to comply with the code or, where compliance is not made, they must indicate why there is variation in their internal controls.

Corporate governance applies to all organizations, big and small – and not just large shareholder ones. Essentially, it is how governance (i.e. internal controls) are adopted and adapted to protect the organization in its practices.

Governance, in a more general sense, concerns decision making and the way in which processes are implemented. When working with governance you will be involved in the analysis of processes and systems by which an organization operates.

For organizations not listed on the stock exchange the Combined Code is not mandatory. However, compliance would create confidence and assure stakeholders that things are being managed to a particular code of best practice.

Other requirements could include:

- Sarbanes-Oxley in the US requires an organization's management to report on their internal controls, and auditors to make comment on the management's assessment
- Basel II is of particular relevance to organizations in the finance sector. It aims to provide a framework which is more representative of modern risk management practices.

However, compliance with governance codes does not mean that we have completely removed all risk. As evidenced by more recent events, including the collapse of the US sub-prime market and the knock-on effect on economies around the world, we are faced with unprecedented circumstances. The closure of Woolworths on the British high street, Lehman Bros. in the city, and million (if not billion)-pound government bail-outs are recent examples of where potential weaknesses in an organization's practices could have been reduced (although not entirely removed) by better (corporate) governance practices.

Ultimately, the responsibility for corporate governance rests with a company's board members and executive management. The implementation of best practice can assist the management in exercising some form of governance and due diligence when overseeing day-to-day business activities, and setting strategy for future direction.

Corporate governance provides the high-level framework for IT governance.

IT governance is a subset of corporate governance, focusing on IT systems and their performance and internal controls.

IT governance is often referenced for compliance initiatives (e.g. Sarbanes-Oxley and Basel II) although, increasingly, projects and their associated IT elements and change impacts are being recognized as affecting the risks an organization faces. This has put IT governance on the project agenda.

Definition of IT governance:

'Ensures that policies and strategy are implemented and that requested processes are correctly followed. Governance includes roles and responsibilities, measuring and reporting and taking actions to resolve any issues identified.'

ITIL Glossary – www.best-management-practice.com/Glossaries-and-Acronyms

IT governance should include a system where all stakeholders – such as the board, internal customers and, in particular, departments such as finance – have the necessary input into the decision-making process. This should avoid deferring all key decisions to a company's IT professionals.

A collaborative approach prevents IT functions being blamed for poor decisions or design simply because others do not understand the IT infrastructure.

As a minimum, the board must ensure that management knows what information resources are held and the integrity of the information, because this is often used to assist in decision making on investments and/or revenue generation. Readers may like to consider COBiT which specifically addresses IT governance and in more depth than ITIL. A comparison of these frameworks is available in a separate paper. www.itgovernance.co.uk/files/ITIL-COBiT-ISO17799JointFramework.pdf

Governance, ITIL and M_o_R

If corporate governance is good business practice, then it follows that IT has a part to play – particularly in the context of service management where IT governance can establish clear roles and responsibilities.

ITIL can assist in supporting a governance framework for an organization's IT infrastructure.

M_o_R can assist in identifying the risks in the underlying IT infrastructure, and establishing the governance (internal controls) required to manage risks to the organization.

Both ITIL and M_o_R refer to the RACI (responsible, accountable, consulted and informed) model as a means of identifying roles and responsibilities within an organization e.g. who is involved and in what capacity, from either a service management (ITIL) perspective, or a risk management (M_o_R) one.

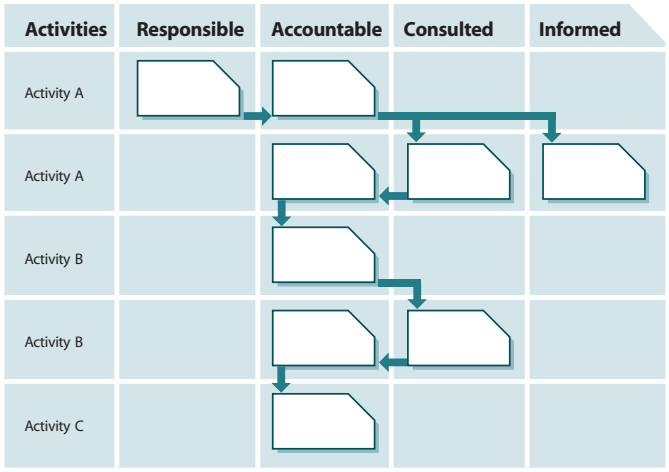

Figure 1 RACI diagram

What is ITIL?

Over time, organizations have evolved to become more dependent on technology as a means of providing an invaluable service to the business. This led to the recognition that this 'service' needs to be managed, and so the practice of service management evolved.

From as early as the 1980s, the UK government developed guidance detailing the best practice methods adopted by successful organizations, providing an approach to (IT) service management. This guidance became a series of publications collectively referred to as the IT Infrastructure Library (or ITIL).

Such is the popularity of ITIL that formal standards were developed based on its approach – initially the British Standard 15000, and more recently the ISO/IEC 20000, which provides a registration path for compliance to IT service management standards.

The use of best practice standards brings together not just the experience and knowledge of a variety of industry sectors, but provides a common language. This is part of the wider collaborative partnership approach being adopted across all sectors.

The service lifecycle contains five elements, as shown in Figure 2. It uses a hub and spoke design, with Service Strategy at the centre and Service Design, Transition and Operation as revolving lifecycle stages, anchored by Continual Service Improvement, which supports all the lifecycle stages.

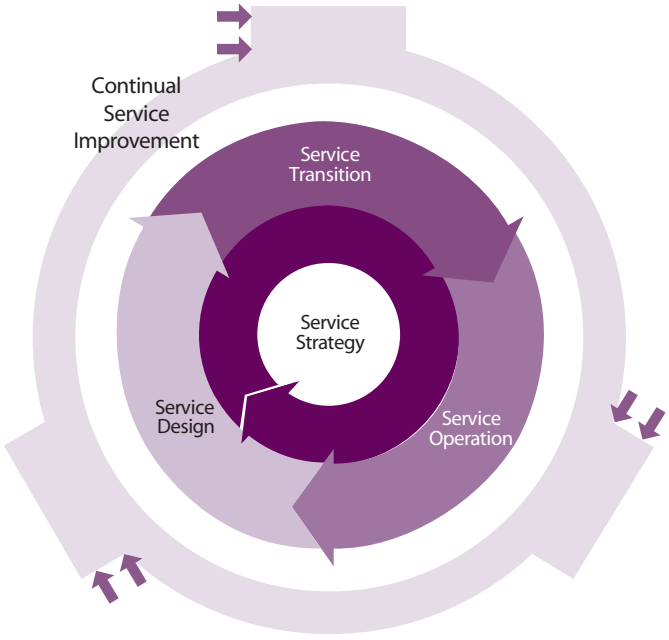

Figure 2 The ITIL Service Lifecycle

The ITIL lifecycle approach covers end-to-end services. It can assist in adopting an approach to support service management best practice within a day-to-day operations environment, while also considering continual service improvement and implementing change.

ITIL is accepted as a key framework for service management, and it provides a good foundation for considering what could be at risk within our services.

ITIL makes a number of references to risk and how it is managed in the context of service management. In this paper, we have used the risk definitions in OGC's Management of Risk (M_o_R) guidance.

This paper has been designed to provide simple guidance on the fundamentals of corporate risk and areas within ITIL that relate to it. It also looks at ways in which ITIL can further assist in managing corporate risk.

Example of how ITIL and corporate risk fit into this

The ITIL service lifecycle begins with Service Strategy (see Figure 2). Service Strategy is at the hub of the service lifecycle, it is where consideration is given to the organizations (management) strategy, markets and offerings, and associated challenges and risks. This demonstrates that, although we may not initially realize it, ITIL has risk management practice integrated throughout the service lifecycle.

In M_o_R, there is a similar concept in the process 'identify' – context. The aim of this process is to ensure that an organization and its objectives (including the environment within which it operates) are understood.

Both ITIL and M_o_R make references to the organization's strategy needing to consider both the positive and negative aspects of change. Table 1 illustrates some possible considerations.

New purchase order system	Example 1	Example 2
Positives	Speed up the purchasing process	Ability to track orders online
Negatives	Downtime whilst staff are re-trained in the new processes and procedures	Reduction in verbal communication with supplier, a change in that relationship

Table 1 Positive and negative impacts of a new purchase order system

The table above shows consideration of one possible aspect of an organization's strategy; the acquisition of a new purchase order system. However, in real terms, organizations usually have a number of change initiatives (e.g. projects) to support the achievement of their strategic objectives. Invariably, the more ambitious the organization's strategy the greater the number of change activities and the greater the risk.

To help an organization focus on activities that support its objectives, a simple control might be to ensure that there is a business need for each activity being suggested. In other words, the new purchase order system should have a business case, which helps the organization evaluate the business needs it supports while balancing the benefits, costs and risks. Within the ITIL service lifecycle, objectives are considered part of service strategy.

Why should an organization manage corporate risk?

As stated previously, there is a requirement for listed companies to comply with the Combined Code for Corporate Governance in the UK, and Sarbanes-Oxley (SOX) in the US. As part of corporate governance (and good governance generally) it is necessary to set-up, monitor and manage a range of internal controls to underpin a good business structure.

While these internal controls of practices, procedures and polices are intended to safeguard the assets of an organization it is impossible to eliminate all corporate risks within a business. To survive and create greater value within the organization we need to take risks, but the risks we take should be understood and managed. Arguably, with a well-managed corporate risk strategy, a business is able to take on more risk (but in a controlled way) resulting in greater shareholder value.

How to manage risk

Best practice approaches, including those highlighted by the M_o_R guidance

There are many published approaches, best practice guidance and standards related to managing corporate risk. For the purposes of this paper, we have chosen to use OGC's Management of Risk (M_o_R) guidance, because it sits well with ITIL and will be valuable to those looking for a consistent approach to best practice across multiple disciplines.

What is M_o_R?

The first edition of OGC's Management of Risk (M_o_R) guidance was published in 2002. It was designed to provide a generic framework for risk management across all areas of an organization.

In 2007, M_o_R was updated to reflect the changes in the world of risk management (including the update to the Sarbanes-Oxley in 2002, the Basel II Accord in 2004 and Combined Code in 2006 (UK).

Although M_o_R is produced by the Office of Government Commerce (an office of the UK government) it has been designed to help both domestic and international organizations to put into place effective frameworks for risk management.

The M_o_R framework is based on four core concepts:

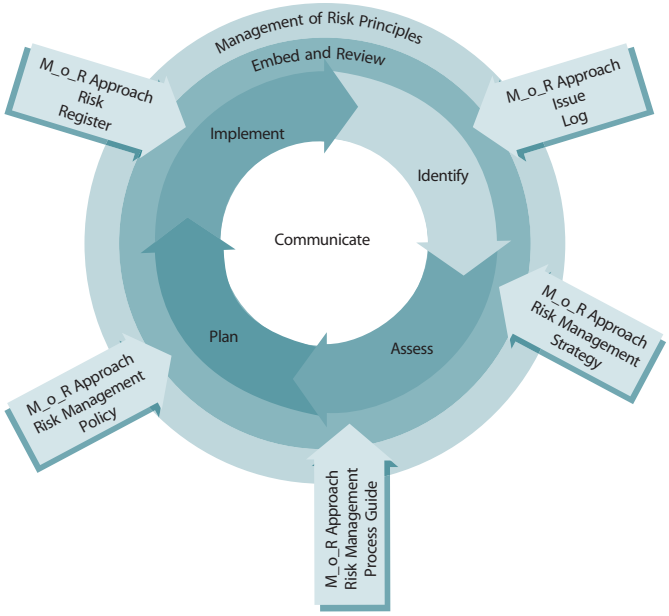

Figure 3 The M_o_R framework

- **M_o_R principles** These are essential for the development of good risk management practice and are the underlying values that determine an organization's way of working. They are derived from corporate governance principles in the recognition that risk management is a subset of any organization's internal controls.
- **M_o_R approach** To adopt and adapt these principles into its own environment, an organization would usually agree and define a risk management policy, process guide and strategies, and support these with the use of risk registers and issue logs.
- **M_o_R processes** The four main process steps describe the inputs, outputs and activities involved in ensuring that risks are identified, assessed and controlled.
- **Embedding and reviewing M_o_R** To ensure that the principles, approach and processes are consistently applied across the organization, M_o_R suggests that there should be an emphasis on continual improvement. This will help an organization establish areas of strength and weakness which, in turn, will bring greater confidence to the stakeholders of that organization.

Risk management requires a process that is designed to be visible, repeatable and consistently applied to support decision making. Ideally carried out as a series of well-defined steps, this process ensures that risk management is cost-effective and efficient.

Definition of risk management:

'The systematic application of principles, approach and processes to the tasks of identifying and assessing risks, and then planning and implementing risk responses.'

A proactive approach enables a controlled environment.

For risk management to be effective, risks must be identified, assessed and controlled.

M_o_R provides guidance on how this can be achieved via the M_o_R process steps, which consist of four primary processes and the communicate process (see Figure 3 and Table 2 on the following page).

The M_o_R processes

Collectively, these processes form a logical sequence of steps, necessary for the adoption of a robust approach to the implementation of risk management. They are carried out in sequence, as any one step cannot be undertaken until the preceding step has been completed. They are all iterative in nature and when additional information becomes available, it is often necessary to revisit earlier steps and carry them out again in order to achieve the most informative result.

The overall management of risk process is illustrated in Figure 3. The steps are represented as a circle of arrows because it is common for the entire process to be completed several times in the lifecycle of an organizational activity.

The activity 'communicate' stands alone because the findings of any individual step may be communicated to management for action prior to the completion of the overall process.

'Embed and review' embraces all of the steps in the process. This activity looks at each individual step in turn to determine its contribution to the overall effectiveness of the complete process. The management of risk principles form the foundation of all risk management activities, and permeate all risk management processes.

M_o_R process step	Objective(s) of the step
Identify (includes 2 steps):	
(i) Identify context	(i) Identify context – to obtain information about the planned activity (e.g. the environment, market etc.) including stakeholders at any perspective level.
(ii) Identify risks	(ii) Identify risks – this process identifies the risks (opportunities or threats) to an organization that would reduce or remove the likelihood of the organization reaching its objectives.
Assess (includes 2 steps):	
(i) Assess estimate	(i) Assess estimate – having identified the threats and opportunities these are now assessed in terms of their *probability* (likelihood) and impact (consequences). The risk *proximity* (timing) may also be assessed as this will provide an indicator of when the risk is likely to materialize.
(ii) Assess evaluate	(ii) Assess evaluate – to understand the net effect of the identified threats and opportunities when aggregated together (this process step enables the bigger picture of overall risk to be understood).
Plan	To consider what responses to the threats and opportunities we can adopt – ideally, minimizing the threats and maximizing the opportunities.
Implement	To ensure that the planned risk management actions are implemented and monitored as to their effectiveness, and corrective action is taken where responses do not match expectations.
Communicate	Shown at the core of the framework (see Figure 3), communicate is an activity that is carried out throughout the whole process. The aim is to ensure that the appropriate aspects of the risk management process are addressed appropriately with relevant stakeholders.

Table 2 The M_o_R processes

Based on OGC M_o_R® material. Reproduced under licence from OGC.

Perspectives

A critical factor in ensuring the success of risk management is to work within the corporate culture of the business, and as part of the maturing process, to embed it within the day-to-day operation of the business.

Viewing the business from different perspectives is a useful way of identifying and grouping risks and ensuring that risk management applies to all levels of an organization. A simple view of the varying perspectives of an organization is shown in Figure 4.

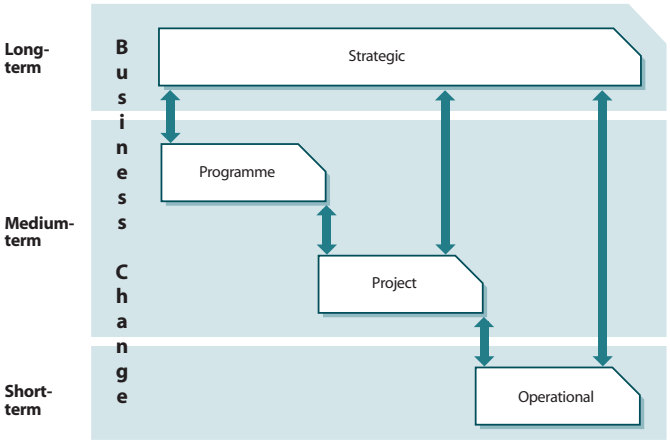

Figure 4 Organizational perspectives

Describing risks

When identifying risks it is important to be able to describe a risk clearly. M_o_R guidance suggests the following aspects are considered:

- Risk cause: the source of the risk
- Risk event: the area of uncertainty
- Risk effect: The impact the risk would have on the organization should it materialize.

It can be helpful to use the following sentence to structure your risk description:

'As a result of ……, there is a risk that…….. which may lead to ……..'

Example:

Risk cause	As a result of :	lack of funds in the company
Risk event	There is a risk that:	we may not be able to acquire the new purchasing system
Risk effect	Which may lead to:	being unable to realize the benefits of efficiency e.g. less staff required to track the purchase orders

Stakeholders

Stakeholders

Definition of a stakeholder:

'Any individual, group or organization that can affect or be affected by, or perceive itself to be affected by, an initiative (programme, project, activity or risk).'

Good governance requires that roles and responsibilities are understood, and this is particularly important for decision making. Two of the M_o_R principles are roles and responsibilities, and stakeholder involvement.

All stakeholders – including the board, internal customers and particularly departments such as finance – should be included in the decision-making process. If IT governance ensures this, then all key decisions need not be deferred to a company's IT professionals.

When dealing with corporate risk, communication is very important. To enable efficient and effective communication requires an understanding of the appropriate stakeholders to ensure they are both informed and understood. Hence it is important to identify stakeholders and their interests and to have an understanding of their roles and responsibilities to establish appropriate communication mechanisms both to and from them.

Stakeholder workshops and stakeholder maps (such as Figure 5) can be useful.

The relationship between corporate risk and ITIL

ITIL is internationally recognized best practice guidance for IT service management. Clearly, IT is a fundamental component of the modern world and is part of the infrastructure of most businesses today. In the early days of automation, it was possible to revert to manual operations if there were problems with IT service management. Today, however, reliance on technology operations and solutions is fundamental to business survival.

In May 2007, following a major refresh project, ITIL version 3 was published. The new version gives recognition to the idea that delivering IT services can be considered of strategic value to a business. ITIL Version 3 highlights the importance of managing corporate risk and the *Service Strategy* publication includes information on strategic risks across the ITIL service lifecycle.

ITIL currently supports corporate risk in the following areas:

- **Problem management** There is a good understanding within best practice that problem management needs to be proactive as well as reactive, reducing the impact of service outages
- **Change management** Good change management techniques and approaches help to reduce risks, minimize the potential negative impact of change, and reduce the risk of an undesirable outcome
- **Service delivery** Designed to ensure that service and overall service levels are maintained
- **Availability management** Focuses on reliability and putting in place alternative options to ensure the service continues

	INTEREST AREAS					
Stakeholders	**Strategic direction**	**Financial**	**Operational changes**	**Interface with customers**	**Public safety**	**Competitive position**
Business partner	●	●		●		●
Project teams			●			
Customers		●		●	●	
Press and media						●
Trade unions			●			
Staff	●		●			
Regulatory bodies		●			●	

Figure 5 Stakeholder map

- **IT service continuity** Is very much aligned to the business, assessing risk to ensure overall continuity for the business.

Looking at the organizational perspectives in Figure 4, it is clear that ITIL best practice guidance assists and supports the operational perspective through service delivery and availability etc. and also, very importantly, assists and supports the change perspective through change management.

Change is necessary for survival and one of the key challenges for modern businesses is managing the risks associated with change – adding extra pressure for new and innovative IT solutions. The benefit that best practice change management can deliver to a business is significant because change and risk span the whole ITIL lifecycle.

For simplicity, alignment between ITIL and risk is demonstrated via the use of tables. A table, which includes the associated risk considerations for each activity, is provided for each of the ITIL service lifecycle phases.

1. ITIL service lifecycle: Service Strategy

Goals:

- To consider *why* something should be done before thinking *how* it can be done.
- This approach will ensure that an organization focuses on activities which will deliver the organization's (management) strategy.

The lifecycle approach starts here, however Continual Service Improvement ensures risk is built into each stage of the lifecycle.

What is included?

- Looking at the markets, both internal and external to the organization
- Looking at the service assets – what products and services do we offer?
- Developing our strategy
- Implementing the strategy
- Ensuring business finances are managed; and demand management is handled in the context of resources being allocated to the right products and services at the right time
- Ensuring we take account of strategic risks.

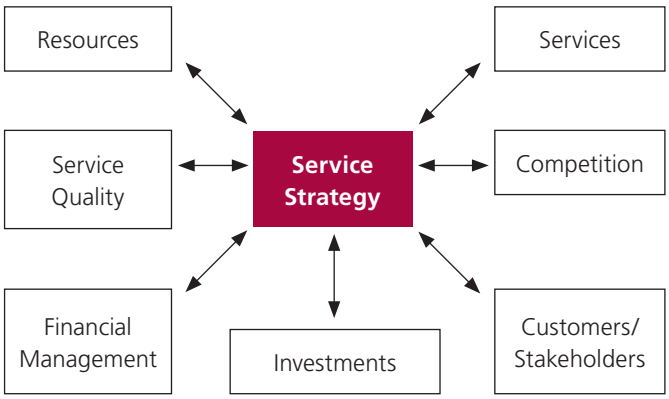

Figure 6 The objectives of Service Strategy

Objective	ITIL Service Strategy objective	Risk consideration	Why is this important?
Services	Understand what products and services we should offer in our service portfolio.	Ensure that the organization is considering both opportunities and threats when reviewing its service portfolio of products and services. This needs to take into account existing offerings as well as anything new. Risk: what happens if we do /do not enter a particular market?	We can ensure that we meet the needs of our customers and stakeholders and focus our resources appropriately.
Competitors	Understand the market place including how we may differ from our competitors.	Is the market place already saturated with competition offerings of the same products? Risk: Should we be innovative and consider something new?	If we do not consider our market place we may find that there is little or no demand for our products and services. In doing this we should also consider further opportunities, e.g. collaborative partnerships that bring a new product to market may have fewer benefits but would enable sharing of the risk.
Customers/ stakeholders	What value will we create for our customers/ stakeholders?	If there is no value there will be no market. Risk: what happens if we do not enter a particular market?	We need to ensure we meet the needs of our customers (those who need our products and services) whilst not forgetting those who may be impacted in some other way, positive or negative.
Investments	Understand why we are doing things. Is there a business case for our products and services?	Our investments should show a link to the achievements of our objectives. Risk: are we achieving benefits in the way of financial return and do we understand the risks associated with these?	There should be a business case for all investments. This should take into account the justification for the delivery of the product or service and the benefits it brings whilst also considering the threats and opportunities which may also evolve.
Financial management	What is the demand for the products/ services and are these reflected in our service portfolio?	We need to maximize our opportunities and concentrate on meeting the demand appropriately. Risk: Are our financial investments delivering the best value from these products/services?	If we do not concentrate on supply and demand we may be using our resources inefficiently.
Service quality	Define our approach to service quality.	We need to ensure products and services are fit for purpose and fit for use. Risk: are we delivering to our customers' requirements?	We could be building in too much quality at a cost which is not to the customers' requirements; e.g. customers may accept packing their own products at a discount store whilst service expectations at a higher-end store might be that the staff will pack for them. These differing approaches will have an impact on time, cost and quality considerations and need to be understood.
Resources	Use resources efficiently, particularly where there are conflicting demands for shared resources.	We need to ensure that we recognize the constraints we may have in terms of capacity and capability. Risk: are resources aligned with demand?	Managing resources efficiently will ensure that service quality expectations are delivered.

Table 3 How risk (M_o_R) can be used to help organizations achieve ITIL Service Strategy objectives

2. ITIL service lifecycle: Service Design

Goals:

- Design of a new or changed service ready for transition into the live environment
- Service Design starts with the business requirements and ends with the development of a service solution designed to meet the needs of the organization (see Figure 7). This designed solution, together with its Service Design package, will pass onto service transition where it will be evaluated, built, tested and deployed. Once transition is completed, control will finally be passed to Service Operation.

This lifecycle approach ensures that continual service improvement is built into each stage.

Figure 7 The input and output of Service Design

What is included?

- Designing the new or changed services
- Designing the service portfolio, including the service catalogue
- Design of the technology architecture and management systems
- Design of the processes, roles, responsibilities and skills required
- Design of the measurement methods and metrics.

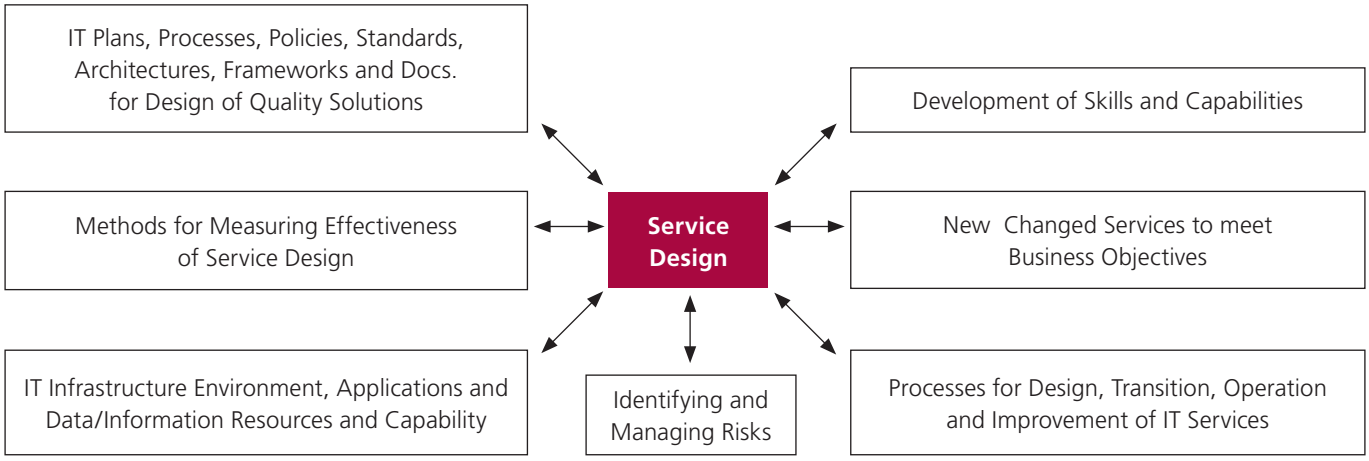

Figure 8 The objectives of Service Design

Objective	ITIL Service Design objective	Risk consideration	Why is this important?
New or changed services	Design what the new or changed services will be, and how they meet the business objectives and help with the design of our service portfolio and service catalogue.	Need to ensure that we have a design for the products and services we are to build/change and ensure that we are considering both opportunities and threats when reviewing them against our service portfolio. Risk: are we introducing/maintaining the right products and services?	With the design of the products and services we can ensure that we meet the needs of our customers and stakeholders whilst also ensuring that they align to meet our business objectives.
Process for service lifecycle	Design the processes required for design, transition, operation and continual service improvement.	Ensure we understand what is required for the whole of the lifecycle – from the business design through to the live environment. Risk: do we have existing processes in place to handle the stages of the lifecycle? If not then these need to be designed and implemented to ensure that requirements are met.	Processes are important as these are the activities we undertake to achieve delivery of the products and services. We may have existing processes in place or we may need to create new ones. If there are no clearly defined processes, resources may be wasted and/or things may not be done appropriately.

Objective	ITIL service design objective	Risk consideration	Why is this important?
Identifying risks	Throughout all of the objectives risk should be considered. However, ITIL v3 makes explicit reference to identifying and managing risks as part of the service design phase.	There is risk (both positive and negative) in all activities. A risk-based approach will ensure that we create an organization that increases its risk maturity, which will help us to implement continual service improvement. Risk: what do we need to deliver and what are the risks (threats and opportunities) to the achievement of our objectives if we do not design products and services which are fit for purpose/fit for use?	Ideally, we should be aiming for continuous improvement, which means we will achieve our business objectives and enable ourselves to deliver more value to business users/customers.
IT infrastructure, environment, applications, data/ information resources and capability	Understand the IT requirements, the interfaces and applications; what data/ information we will need to hold and the capability we will need to work within this environment.	Each of the four types of resource ((i) people, (ii) products/technology)/(iii) processes/(iv)partners/suppliers) should be prepared, planned and coordinated to achieve the optimum design for service management. Risk: do we have a clear understanding of our wider IT environment and the impact (+/-) we could have on other parts of the business?	A blueprint of our existing processes, organization structure, technology requirements, information etc. will help us to understand where we are now. From this we can align our design to our strategy of where we want to be. The gap between the present and the future will help to determine the (transition) projects required for the remaining lifecycle.
Measurement methods and metrics for assessing effectiveness and efficiency	Understand what needs to be measured and how this will be used.	If things are to be measured they are usually delivered to better standards. We need to understand what measures we need and design them so we can determine our effectiveness and efficiency. Risk: what service levels should we be delivering to; how can we capture measurements against this; and how can we interpret this information?	It is important to be able to assess our services to ensure that we are meeting service requirements. Creating measures and metrics enables this.
IT plans, processes, policies, standards, architectures, frameworks, and documents for the design of quality IT solutions	Establish what needs to be done when; where and by whom; and to what quality. This may involve the documentation of policies, standards etc.	We need to understand any governance requirements we may need to adhere to. Risk: what are the roles and responsibilities we need to adopt?	We need to establish a plan for delivery. A clearly defined approach outlined in, policy documents (with reference to appropriate standards) will ensure that we deliver to best-practice.
Develop skills and capability within IT	Ensure that we have people with the right skills and capabilities.	The service design phase will help us to understand the skills required for design and the remaining phases of the lifecycle. Risk: we may not have the capability for delivery.	Without a clear understanding of our requirements we may design products which do not deliver the best value.

Table 4 How risk (M_o_R) can be used to help organizations achieve ITIL Service Design objectives

3. ITIL service lifecycle: Service Transition

Goals:

- Enable the business/customer project to integrate a release into the business processes and services
- Reduce known errors and minimize risks from transition (going from old to new ways of working)
- Ensure that the service can be used as per the requirements.

This lifecycle approach ensures that Continual Service Improvement is built into each stage of the lifecycle.

What is included?

- Management and coordination of processes, systems and functions to build, test and deploy a release (package) into production
- Establish the service specified in the customer and stakeholder requirements.

The Service Transition stage also specifically references the following lifecycle processes (although these do support all lifecycle stages):

- Change management
- Service asset and configuration management
- Knowledge management.

Note: the following are not included in Service Transition objectives:

- Minor modifications to production services and environment
- Ongoing continual service improvements that do not significantly impact on the services or service provider's capability to deliver the services.

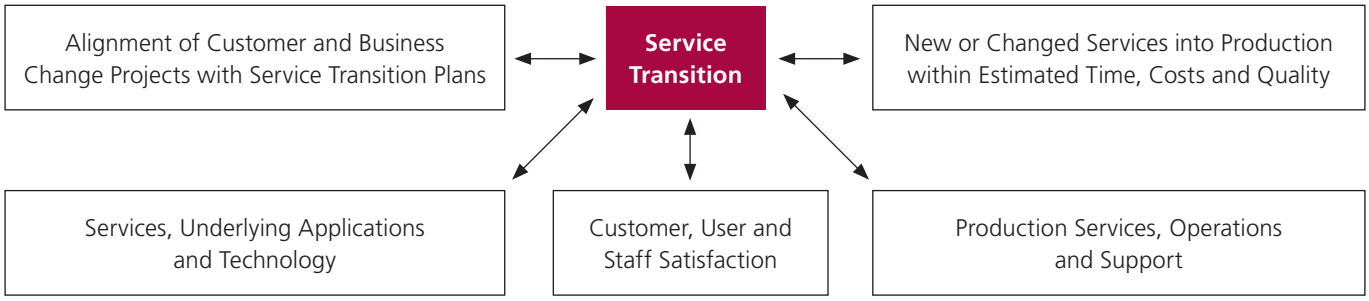

Figure 9 The objectives of Service Transistion

Objective	ITIL Service Transition objective	Risk consideration	Why is this important?
New or changed services into production within estimated time, cost and quality	Plan and manage the resources to establish a new or changed service into production within time, cost and quality.	Need to ensure that we deliver within time and budget and to the customers'/business requirements. Risk: do we have sufficient resources with the appropriate skills to deliver on time?	If we do not plan and manage the change we cannot control the impact on the business services.
Production services, operations and support	Ensure there is minimal impact on production services, operations and support.	Transition is a risky time for the organization as we move from old to new ways of working. We need to ensure we don't jeopardize the current services for services yet to come. Risk: is the business ready for the changed services to be transitioned into operation?	Availability of existing services needs to be managed as we move to the delivery of new ways of working.

Objective	ITIL Service Transition objective	Risk consideration	Why is this important?
Customer, user and staff satisfaction	Increase customer, user and service management staff satisfaction with the service transition practices.	The expectations of customers, users and staff should be assessed to ensure success. Risk: are we delivering what was required?	Customer/business confidence will need to be managed during transition as people may be affected.
Services to underlying applications and technology	Increase the proper use of the services and underlying applications and technology.	Ensuring that value is delivered from technology. Risk: lack of knowledge in the use of applications and technology means a reduction in service quality.	Capability and skills are important measures in delivering quality. Whilst IT can assist in improving efficiency and effectiveness people need to be educated in the role and use of the supporting infrastructure.
Alignment of customer and business change projects with service transition plans	As projects deliver their outputs (products) these will need to be aligned with transition plans to ensure that service management remains aligned.	Project deliverables need to be aligned to service operations to minimize disruption to the business. Risk: is the business ready for the change? Do we have support services in place?	Constant change will have a significant impact on service if project and service transition plans are not aligned.
Processes used to Support all Lifecycle Stages (specifically referenced in service transition)			
Knowledge management	Review and analyze data, to convert it into information and knowledge.	Information combined with experience, context, interpretation and reflection will assist in decision making. Risk: we cannot learn from experience if the information is available but not utilized.	Lessons can be learnt from past experience.
Service asset and configuration management	Support efficient and effective service management processes by providing accurate information about assets and configuration items.	Management of assets is essential if an organization is to remain in control of its products and services. Risk: lack of configuration management may impact quality of service.	It is essential we understand our products and their components to deliver service quality.
Change management	• Respond to customer's changing business requirements • Respond to the business and IT requests for change • Ensure that changes are recorded, evaluated, authorized, prioritized, planned, tested, implemented, documented and reviewed in a controlled manner.	Change incurs risk. Impact of changes needs to be managed. Risk: a change to requirements may result in a service which does not meet service requirements.	No matter how much we plan there will be changes. Changes will impact service quality and need to be managed.

Table 5 How risk (M_o_R) can be used to help organizations achieve ITIL Service Transition objectives

4. ITIL service lifecycle: Service Operation

Goals:

- To achieve effectiveness and efficiency in the delivery and support of services and maintain stability, while at the same time allowing for changes and improvements.

This lifecycle approach ensures that continual service improvement is built into each stage of the lifecycle.

What is included?

- The execution of all ongoing activities required to deliver and support services, including:

a. The services themselves
b. Service management processes
c. Technology
d. People.

Figure 10 The objectives of Service Operation

Objective	ITIL Service Operation	Risk consideration	Why is this important?
Delivery and management of services	Coordinate and carry out the activities and processes required to deliver and manage services to agreed levels to the business users and customers.	The activities and processes to deliver to the agreed service levels need to be managed. Risk: failure to deliver to agreed service levels may result in financial loss.	Service agreements are used to measure service quality. Failure to deliver these levels can impact the organization in a variety of ways.
Technology	Manage the technology that is used to deliver and support services.	Service management technology enables communication between service providers and customers. We need to consider the value of technology and the types of encounters being provided to deliver and support services: (i) Technology free – no technology involved in the service (ii) Technology assisted – service provider has access to technology (iii) Technology facilitated – both the customer and the service provider have access to the same technology (iv) Technology mediated – the service provider and customer are not in physical proximity (v) Technology generated – the service provider is entirely represented by technology (commonly known as self-service). Risk: does technology add value to the service or hinder it?	The use of technology should be seen as a solution to a problem, not a problem itself!

Table 6 How risk (M_o_R) can be used to help organizations achieve ITIL Service Operation objectives

5. ITIL service lifecycle: Continual Service Improvement

Goals:

- To continually align and realign IT services to the changing business needs by identifying and implementing improvements to IT services that support business processes
- CSI is about efficiency and effectiveness.

The lifecycle approach ensures that Continual Service Improvement is built into each stage.

What is included?

- Consideration of service management overall
- The continual alignment of the portfolio of services for current and future business needs
- The maturity of the processes for each service in a continual service lifecycle model.

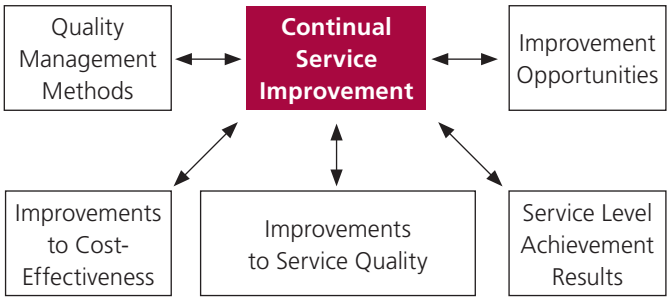

Figure 11 The objectives of Continual Service Improvement

Objective	ITIL Continual Service Improvement objective	Risk consideration	Why is this important?
Improvement opportunities	Understand what products and services we offer in our service portfolio and how we can improve them.	Ensure that the organization is considering both opportunities and threats when reviewing its service portfolio of products and services. Risk: what happens if we do /do not enter a particular market?	We can ensure that we meet the needs of our customers and stakeholders and focus our resources appropriately.
Service level achievement results	Have a measure of our service achievement levels.	Are we delivering to requirements? If not, why not? Risk: are service levels specific, measurable, achievable, realistic and timely?	If we do not agree our service levels or measure our results how will we know what we have achieved and where there is room for improvement?
Improvements to service quality	Are we delivering products which are fit for purpose and fit for use? Do they meet the requirements of our customers/stakeholders?	We should consider if there is value in further quality improvements. Risk: we improve our service quality by utilizing more resources but this is not required by the customer and we are not paid for this extra value.	Remember, we need to agree service levels. If we deliver above these levels what are the benefits? If we deliver below these levels, we need to manage the threat.
Improvements to cost-effectiveness	We need to understand why we are doing things. Is there a business case for improvements to our products and services?	Our investments should show a link to the achievements of our objectives. Risk: are we achieving benefits in the way of financial return and do we understand the risks associated with these?	There should be a business case for all investments. This should take into account the justification for the delivery of the product or service and the benefits it brings, whilst considering the threats and opportunities which may also evolve.
Quality management methods	Are there any existing quality management methods we can utilize?	We need to maximize our service management processes. Risk: utilising existing quality methods will deliver benefits whilst avoiding us reinventing the wheel.	Best-practice should be developed to become embedded into our working practices.

Table 7 How risk (M_o_R) can be used to help organizations achieve ITIL Continual Service Improvement objectives

The culture of an organization affects the way in which it operates and how well it manages IT and corporate risk. Adopting ITIL and M_o_R will deliver good practice which, if fully integrated within the corporate culture, standardized and documented across the business, will lead to significant benefits.

In the past risk management (including resilience and recovery) has often been an afterthought in new programme or project developments – sometimes only reviewed or identified post-implementation. Retrofitting resilience once a system has been implemented can be very costly and, in some cases, simply not possible. In the meantime, risks at an operational and corporate level may be taken without the realization of the business. Ensuring that risk management is embedded within the ITIL framework ensures that risks are identified as early as possible. In some cases, this may highlight unacceptable risks and the programme may be terminated at the feasibility stage, limiting cost to the business.

Everyone within an organization is involved in risk management. Risk can occur in any organization (large or small) and in any process, so everyone should be made aware of the company's risk management policies and procedures. Adopting M_o_R will enable a company to utilize risk management best-practice gathered from both public and private sector. Generally the way organizations engage with everyone in 'how they want things to be done' is via the adoption of policies. M_o_R provides guidance with examples of the composition of the risk management policy, risk management strategy, risk management process guide, risk register and issue log amongst others. Collectively these can help an organization have the confidence to develop the documents for their own environment and hence move towards having everyone engaged in risk management in a consistent way.

It is recognized that there are specific areas within an organization where a more defined and specific risk management role is involved. However, it is important that specializm silos within risk management are not created or promoted. There should be a common approach to storing and reporting risks, risk events and near misses to ensure that the board is given a consistent and consolidated view of the risks it is taking, and enable it to make informed decisions as a result. Areas of specialisms include:

- IT security
- Information security
- Business continuity
- Audit
- Compliance
- Legal
- Operational risk
- Health and safety.

And, within the finance sector:

- Credit risk
- Market risk
- Enterprise risk management.

A common platform, methods language and understanding will greatly assist in the consolidation and overall management of risk.

In conclusion, best practice should be used as a means of implementing what it says – best practice!

The authors

Michael Faber manages risk, resilience and recovery for an international finance organization based in the City of London.

Michael is also Managing Director of Regal Training and Consultancy Limited – a firm specializing in OGC products, including Management of Risk – and vice chairman of the Institute of Operational Risk, helping to develop the industry and discipline of operational risk.

Rubina Faber has worked in a number of senior management positions in industry sectors including finance, IT, marketing and retail, with over 20 years experience of implementing change.

Rubina is a director of Regal Training and Consultancy Limited and is an accredited trainer in PRINCE2, MSP, M_o_R and change management, and is ITIL qualified.

Further information

Aligning COBIT 4.1, ITIL V3 and ISO/IEC 27002 for Business Benefit.

Turnbull Report (1999). Drawn up with the London Stock Exchange (LSE). London.

BS 31100 Code of Practice for Risk Management (2008). London: BSI

Combined Code on Corporate Governance (2008). London: Financial Reporting Council (FRC).

Higgs Review (2003) *Review of the Role and Effectiveness of Non-Executive Directors*, published by the Department of Trade and Industry (now the Department for Business Innovation and Skills), UK. Printed by TSO (The Stationery Office).

HM Treasury (2004). *Management of Risk – Principles and Concepts* (the Orange Book) revised.

ISO 31000:2009 Risk Management – Principles and guidelines. Available from the International Organization for Standardization.

Office of Government Commerce (2007). *Continual Service Improvement*. London: TSO (The Stationery Office).

Office of Government Commerce (2007). *Management of Risk: Guidance for Practitioners* (2nd edition). London: TSO (The Stationery Office).

Office of Government Commerce (2007). *Service Design*. London: The Stationery Office.

Office of Government Commerce (2007). *Service Operation*. London: The Stationery Office.

Office of Government Commerce (2007). *Service Strategy*. London: The Stationery Office.

Office of Government Commerce (2007). *Service Transition*. London: The Stationery Office.

Sarbanes-Oxley (SOX) (2002). United States federal law, overseen by the Public Company Accounting Oversight Board (PCAOB). Washington.

Trademarks and Statements