



# Modern Risk Management Remarks

Roman Lindauer

ROMAN LINDAUER

---

# **MODERN RISK MANAGEMENT REMARKS**

Modern Risk Management Remarks

1<sup>st</sup> edition

© 2017 Roman Lindauer & [bookboon.com](http://bookboon.com)

ISBN 978-87-403-1712-1

Peer review by Ing. Jan Havlík, Ph.D. & PhDr. Ing. Antonín Pavlíček, Ph.D.

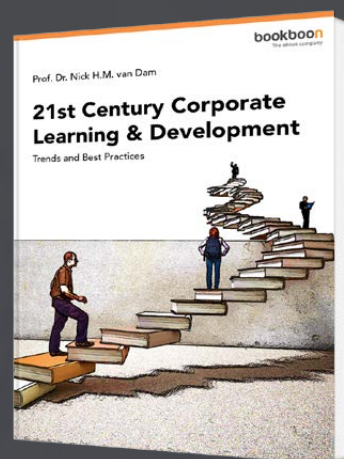
# CONTENTS

	<b>Annotation</b>	<b>7</b>
<b>1</b>	<b>Personal Remark</b>	<b>8</b>
<b>2</b>	<b>Introduction</b>	<b>9</b>
<b>3</b>	<b>Brief History of Risk Management</b>	<b>10</b>
<b>4</b>	<b>What Is Risk</b>	<b>11</b>
4.1	What Is Risk Management?	11
4.2	What Is Risk Assessment?	12
4.3	Who Makes Risk Management Decisions?	12
4.4	Understand the Key Components of Risk	17
4.5	Communicate Risk Consistently	20
4.6	Make Informed Risk Management Decisions	22
4.7	Summary of Risk Management	28

## Free eBook on Learning & Development

By the Chief Learning Officer of McKinsey

**Download Now**



Download free eBooks at [bookboon.com](http://bookboon.com)

**Click on the ad to read more**

<b>5</b>	<b>What is Quality</b>	<b>33</b>
5.1	Brief Look at Quality Systems	36
5.2	ISO	37
5.3	Kaizen	38
5.4	Lean	40
5.5	Six Sigma	41
5.6	Hamburger University	43
5.7	How Do We Differentiate Between Professional and Amateur?	44
<b>6</b>	<b>Sarbanes-Oxley Act and Its Implications</b>	<b>46</b>
6.1	Preface	46
6.2	U.S. Capital Market	46
6.3	The ENRON Story	47
6.4	The MCI WorldCom Story	49
6.5	Lessons Learnt	52
6.6	Sarbanes-Oxley Act	52
6.7	Evolution of SOX	55
6.8	COSO	56
<b>7</b>	<b>Compliance</b>	<b>60</b>
7.1	Definition of Compliance	60
7.2	Definition of Risk Compliance	61
7.3	Definition of Corporate Compliance	61
7.4	What Is Compliance	61
7.5	What Is Non-Compliance	62
7.6	Who Is an Auditor	63
7.7	Audit Run	64
7.8	Audit Statements	65
7.9	How to Deal with Auditors	67
<b>8</b>	<b>Process Driven Organizations and Operation Excellence principles</b>	<b>68</b>
8.1	Process Definition	70
8.2	Organization and Processes	70
8.3	Executive Processes	71
8.4	Managerial Processes	71
8.5	Supportive Processes	71
8.6	Operational Excellence	72
8.7	Key Performance Indicators (KPIs)	76
8.8	Key Risk Indicators (KRI)	79

<b>9</b>	<b>Internal Controls and Risk Mitigation</b>	<b>80</b>
9.1	Definition	82
9.2	Suggestions for Effective Control Environment	85
9.3	Internal Controls Principles	91
9.4	Implementation of Internal Controls	92
9.5	Examples of Internal Control Wording	92
9.6	Recommendations	93
<b>10</b>	<b>Process Maps</b>	<b>102</b>
10.1	Definition	102
10.2	Process Management	105
10.3	Process Risks	106
<b>11</b>	<b>Final Recommendations and Remarks</b>	<b>109</b>
<b>12</b>	<b>Closing Note</b>	<b>111</b>
	<b>References</b>	<b>113</b>
	<b>List of Figures</b>	<b>114</b>

# ANNOTATION

The aim of the book is to introduce the readers to key modern trends in risk management. In each chapter, the author focuses on a particular segment of the risk management knowledge and best practices based on theoretical principles supplemented by practical tips and hints. All readers have the opportunity to become familiar with quality management systems, the key features of the Sarbanes-Oxley Act (SOX), compliance principles, the description of process driven organizations, the operational excellence concept, the definition and design of internal controls and process map theory and practice. It was the author's ambition to prepare a text summarizing the risk management knowledge in a very user-friendly format. This book may be used as a study material for guidance by those who want to start mitigating risks in their business.



# 1 PERSONAL REMARK

The decision to create a document capturing the content of my lectures in writing was based on the idea that students should have some kind of support to help them refresh their memories while preparing for the final exam in the Modern Risk Management course taught at the University of Economics in Prague.

My own ambition was not to deliver the full review of risk management in the broad form of a typical textbook. I did not aim so high. My aim was to create an easy-to-read summary of key points and information I had presented during my lectures.

I tried to prepare a concentrated summary of my lectures for future reference which might be used by students when preparing for their professional roles in the field of risk management. I personally strongly believe that the future of many businesses will depend on the level of mature risk management. The field of risk management may be seen as one of the last free zones where company management can present their creativity, invention and evaluation skills.

Risk management is a very complex field which may differ by industry, type of business and economical and regional dependencies. In my opinion, risks are definitely part of every business and every economic activity. If all managers were able to understand the negative potential of risks, their importance for business development and their complexity, it would be beneficial to them. The risk management community uses a common approach to risk. This approach may sometimes depend on legal enforcement, sometimes on the business industry standards or required norms. Such a scope might be very extensive and I had no ambition to present my viewpoint as the only correct and right one.

In this publication, I would like to simply present the facts and knowledge based on my professional experience supplemented by information available on the Internet. My intention was not to infringe any intellectual property law worldwide.

Let me wish you pleasant reading.



## 2 INTRODUCTION

This text has been prepared with the aim to summarize all fundamentals of modern risk management principles and related issues. I would like to present to all readers and other wide audiences the rather complex picture of risk management methods, including the Sarbanes-Oxley Act, important details of the compliance process, the theory of Operational Excellence (OpEx), fundamentals of internal control design and implementation, processes and flow charts. The final part of the book focuses on the fundamentals of quality systems and their overlap to risk management theory.

The content of the book was enhanced by many practical recommendations and I believe my own practical experience will help all readers get a better understanding of the practical application of the presented topics.

My ambition was to create a packed text which might be used for guidance and enrichment of students and all other readers who are interested in the risk mitigation management knowledge.

The modern business world is much more effective in the battle against residual and content-related risks because we can use IT technology which can be very helpful. On the other hand, IT equipment may be another source of potential risks. In my book, I would like to present the overall picture of risk management and the current legal framework which enables us in our efforts to mitigate business risks. Not all IT-related risks are specifically mentioned because I believe that it would require a high-caliber specialist to write a publication on IT risks. The text slightly touches on some IT examples in a few cases where such examples are relevant.

Modern times brought high sensitivity to financial scandals, white collar crime and other issues associated with business ethics. Since 2002, the business world has been armed with tools, methods and principles, which might help understand how to effectively tackle business risk, like never before.

In the following chapters, I would like to present the most important information which might help all readers explore this relatively unknown area of modern risk management.

### 3 BRIEF HISTORY OF RISK MANAGEMENT

If you went to work this morning, you took a risk. If you rode your bicycle, walked, or drove your car, you took a risk. If you put your money in a bank, or in stocks, or under a mattress, you took other types of risks. If you bought a lottery ticket at a newsstand or gambled at a casino over the weekend, you were engaging in activities that involve an element of chance – something closely related to risk.

The cradle of risk management may be traced back to the times of the industrial revolution. The main invention was the general understanding that technology may be associated with risks. All the steam powered machines and engines changed the way how the society was looking at risks. Since the days the industrial revolution, risks have become a constant part of the modern human society. For example, the United Kingdom government and the U.S. Congress introduced several laws with the intention of reducing the number of people killed by the steam machine industry.

The response to the risk initiative was in the form of first regulation norms and laws affecting individuals, the society, the environment and the industry itself. Since then, the nature of risks has been broadened by railroads, bridges, airplanes, oil tankers, and even skyscrapers. Humans simply started to observe more and more areas where risks may be spotted. Today, we recognize many practical risk management tools used to identify, control and monitor potential risk factors and industries.

Transforming the risk management approach into quality management systems is how I see the future of risk mitigating initiatives. The plan is to move away from the strict rules and to start to communicate the basic objective of common interest. I am referring to delivering high-quality products in a business environment where risks would be minimized and quality aspects prevail. Such an approach would affect all managerial and communication practices currently applied worldwide.

At first, this will be undoubtedly uncomfortable for the industry and regulatory bodies, but such a different way of doing business has significant potential benefits for everyone involved.

I think the war against risk is a war that humans will not win but they should never surrender.

## 4 WHAT IS RISK

What a risk is and how it is described depends entirely on the context of the organization facing that risk and on the biases of the individual assessing it.

In the context of wider business risk management, a risk is the potential for either harmful or positive outcomes to impact upon business objectives, including reputation. Organizations cannot develop without taking risks. Technology and information risk is not just about avoidance and mitigation; the pursuit and acceptance of risk creates opportunities and can help deliver business objectives.

Having recognized this wider meaning, this publication uses the word ‘risk’ to describe the potential for security harm to occur as a result of using technology and information to achieve business objectives.

It is important not to just think about risk in the context of the confidentiality, integrity and availability of technology and information. In addition to these, other things that the organization cares about (e.g. its reputation) may be at risk and should also be taken into account [1].

### 4.1 WHAT IS RISK MANAGEMENT?

Risk management describes the decisions an organization makes and the actions it takes in response to risks that have been identified.

The purpose of risk management is to help the organization protect itself, and provide it with confidence that the technology and information it uses is secure enough to meet its needs.

Where risk management decisions and actions affect multiple organizations (or multiple parts of an organization) in an enterprise context, then some level of risk management co-ordination is likely to be required.

Risk management needs to happen throughout the lifecycle of a system or service, informed by a realistic view of risk and a clear understanding of the organization and its objectives.

Technology and information risk is just one area of business risk that organizations need to manage. As such it should fit in with the existing business risk management activities undertaken by an organization. [1]

## 4.2 WHAT IS RISK ASSESSMENT?

Risk assessment is a key risk management activity that identifies, assesses and articulates risks to the organization. Risk assessment is needed to inform risk management decision making, and it requires technical, security and business skills and knowledge.

Organizations may use different risk assessment methods to assess the risks associated with particular areas of their business (e.g. financial, legal, health and safety, etc.). The choice of risk assessment method rests with the organization and these choices are often based on the type of risk or business area under consideration. Achieving a consistent approach to describing and presenting risks from different areas of the organization will help it to consume assessment output, and make informed risk management decisions. [1]

## 4.3 WHO MAKES RISK MANAGEMENT DECISIONS?

The decisions made to manage technology and information risk are the responsibility of the organization. They are not the sole responsibility of security or IT departments. Risk management decisions should be objective and informed by an understanding of risk. They should not be made in isolation but on a basis of understanding how individual decisions affect the wider business, and what it is trying to achieve.



www.sylvania.com

We do not reinvent  
the wheel we reinvent  
light.

Fascinating lighting offers an infinite spectrum of possibilities: Innovative technologies and new markets provide both opportunities and challenges. An environment in which your expertise is in high demand. Enjoy the supportive working atmosphere within our global group and benefit from international career paths. Implement sustainable ideas in close cooperation with other specialists and contribute to influencing our future. Come and join us in reinventing light every day.

Light is OSRAM

OSRAM  
SYLVANIA

Organizations should decide for themselves what risk management decisions need to be made to support the delivery and operation of a system or service, and could include:

- the authorization of expenditure to design a system or service,
- the authorization of expenditure to build, test, install, run, and decommission a system or service,
- the approval to use information, a system or a service during the test, install, run, and decommission stages of a system or service lifecycle.

The right people need to make decisions at the right time, with the right advice and support. They need to be empowered by the organization and have the right business, technology, security knowledge and skills to enable informed and objective decisions. [1]

### **Understand the Business Context**

Taking risks is a necessary part of doing business in order to create opportunities and help deliver business objectives. Organizations should always be aware of the risks they are taking to achieve their aims.

To ensure meaningful outcomes, organizations need to provide a context in which risk management and risk assessment is conducted. This context can be set by answering the following questions:

- What is the organization trying to achieve, and what does it really care about?
- What business assets are involved (for example systems, services, information and other business assets such as reputation), and what are they worth to the organization?
- What risks is the organization prepared/not prepared to take with those assets to achieve its objectives?
- Are there any external legal and regulatory requirements that need to be considered?
- Are there any third party risk management or contractual considerations to take into account?
- What rewards may be realized by taking risks?
- What governance structure will the organization have in place to support risk management decision making?

Those responsible for making risk management decisions should contribute to, and agree with, the formulation of this context. [1]

## Decide on the Risk Management Approach

Before taking any action, the organization must understand and communicate what risk management approach the business is going to take to provide confidence that the technology and information used is sufficiently secure. This is an important business decision because the security of the organization and its assets depend on it.

Risk assessment and other risk management activities require technical, security and business skills and knowledge and resources. Choosing the wrong approach could be costly in terms of resource use and security compromise. [1]

Rely on the security provided by commercial products and services

In this approach, the organization relies on the security provided by a commercial product or service, without conducting further security analysis. If the organization adopts this approach, then there is no need to conduct customized technology and information risk assessments to help specify additional security controls. However, the organization must accept that:

- It is completely reliant on the security claimed to be provided by commercial products and services, which can vary from ‘very robust’ to ‘almost none at all’.
- Security won’t be tailored to any specific needs the organization might have.

From a security perspective, this approach does not mean ‘do nothing’. Organizations that choose to take this approach still need to:

- have in place organizational controls (for example personnel security, physical security and security training for users),
- seek confidence and assurance that the commercial products and services they use are appropriate in the context of what they are doing and the threats they face,
- make best use of the security provided natively by commercial products and services.

Adopting this approach is dependent on having effective and appropriate commercial contracts and agreements in place. It should not be assumed that suppliers’ own standard commercial terms of business will provide an adequate basis for relying on the security provided by any product or service.

Organizations should also note that without risk assessment, the business will have no understanding of the technical and information risks it faces. This could result in a lack of security where it is needed, or the application of security where it is not needed, resulting in security compromise or unnecessary costs.

## Carry Out Risk Assessments to Specify Security Controls

In this approach, the organization chooses an appropriate risk assessment method and makes informed risk management decisions about what security controls it will implement. When making these decisions, the business may choose to:

- manage risks using controls that are independent of any predefined control set,
- use security controls and control sets intended to implement local, national or international policies and standards. These control sets are general in nature and need to be tailored to meet the needs of the organization.

Decisions will be informed by what the organization is, and what it is trying to achieve. Some organizations in certain sectors may need to demonstrate that they have applied security controls to comply with standards or a sector-specific regulatory requirement. For example:

- External factors (e.g. legislation).
- Organizations may need to apply security controls based on the type of information they need to protect (for example those that store and process personal data will need to apply controls to demonstrate compliance with the Data Protection Act (DPA).



Discover the truth at [www.deloitte.ca/careers](http://www.deloitte.ca/careers)

**Deloitte.**

© Deloitte & Touche LLP and affiliated entities.



- Organizations seeking compliance with ISO/IEC 27001 may choose to apply its control set in the context of what it is doing.
- Organizations conducting payment card transactions must apply the security controls and requirements set out in the Payment Card Industry (PCI) Data Security Standard.
- Certain business communities sharing services and infrastructure may choose to develop their own minimum set of security controls against which compliance can be demonstrated to protect the wider community.
- Organizations may choose to implement the advice provided by the control set provided by the Cyber Essentials Scheme.
- Organizations making use of the PSN will need to demonstrate compliance against a prerequisite set of security controls as defined in the conditions for joining the network.

The examples above should not be viewed as an exhaustive list of recommended control sets, as there are many to choose from. Some organizations may need to use a combination of control sets. Irrespective of the method, standard or framework used to make security control choices, decisions must be informed by and traceable to realistic risks affecting something that the organization is actually doing. [1]

### **Choose the Right Risk Assessment Method**

There are many methods for conducting risk assessments, and numerous tools to support them. Most risk assessment methods can be aligned to the approaches described in the ISO 31000 and ISO 27000 series of International Standards which seek to identify, analyze and evaluate risks. The method to be adopted should be appropriate for the organization, so this is ultimately a business decision. It should be scaled to support whatever delivery model is being used and for the target audience.

When choosing a risk assessment method, the organization is likely to need to answer the following questions:

- Will the output allow me to understand and prioritize risks in a meaningful way?
- Can the output be communicated to third parties?
- Is the method of assessment proportionate to what it is I am trying to achieve?
- Will I need to employ specialist resources to use it, or to interpret the output for the organization?
- Are there any costs associated with using the method?

- Can I repeat the method or approach consistently?
- Are there any contractual or commercial restrictions on how I can use the method?
- Will the method support the commercial model operated by my organization?

A discussion of popular methods in use today is provided in the final sections of this guidance, and can be used as a starting point for answering these questions. [1]

#### **4.4 UNDERSTAND THE KEY COMPONENTS OF RISK**

Risk assessments have inputs and outputs. The fundamental inputs to be considered in a risk assessment are threat, vulnerability and impact. Risk is normally realized as a consequence of these inputs, although some risk assessment approaches will include other inputs (such as likelihood and asset value). Regardless of the risk assessment method used, any inputs and outputs should be understandable and meaningful in the context of the business and what it is trying to achieve.

##### **Threat**

Threat describes the source of a risk being realized. Threats to systems and services include people who would seek to do the business harm through technology, and hazards such as environmental disasters and accidents. Some of the threats that an organization may face are beyond the organization's control; they can only use threat-related knowledge to aid risk prioritization.

Where appropriate to their organization's context, the business should apply the threat profile, supplemented if necessary with local or specific threat intelligence where it is available. It is not necessary to consider all threats in all scenarios.

- Where threats are people, organizations should consider the motives that drive individuals to launch an attack, as well as their opportunities and capabilities to do so.
- Modeling threats can be a useful way of helping to understand what threats should be considered and how they may affect individual assets, the organization and what it is doing.
- To achieve consistency between different risk assessments within the same organization, the business should establish an organization-wide or business area specific threat assessment baseline (or baselines), and use them as input to all risk assessments. These baselines will need to be amended if the threat landscape changes, or if something significant changes within the organization.

## Vulnerability

Vulnerability is a weakness which can be exploited by a threat to deliver an impact. A system or service could be compromised through the exploitation of vulnerabilities in people, places, processes or technology.

When assessing their risks, organizations should ensure that they have a clear and realistic understanding of where and how their systems and services are vulnerable. Whilst organizations cannot control the threats they face, they can reduce their vulnerabilities.


## Impact

Impact describes the consequences of a risk being realized. To allow risk evaluation and prioritization, impact should specify the negative effect that a risk's realization would entail.


This should include expected losses (financial and reputation losses) as well as business objectives which would not be achievable as a result of the impact. Organizations can exercise control over the negative impact that realization of a risk would have, and should plan for this to happen.

SIMPLY CLEVER

ŠKODA



**We will turn your CV into an opportunity of a lifetime**



Do you like cars? Would you like to be a part of a successful brand? We will appreciate and reward both your enthusiasm and talent. Send us your CV. You will be surprised where it can take you.

Send us your CV on  
[www.employerforlife.com](http://www.employerforlife.com)



## **Other Inputs**

Some risk assessment methods also consider likelihood and asset values as components of risk and inputs to assessments.

## **Likelihood**

Estimates how likely it is for a threat to occur. It can be captured by examining historical records of compromises to estimate how history will be repeated. Some methods draw on likelihood to help determine vulnerability. Note that metrics of past occurrences are not necessarily a useful indicator of what will happen in the future.

## **Asset Values**

Asset values are used to provide an understanding of what systems, services, information or other assets the organization really cares about. This insight will provide organizations with a view of what it is they really want to protect. Asset valuations are a key consideration when determining the impact input for risk assessment purposes.

## **Risk Assessment Output**

Irrespective of the risk assessment method used, the output should be meaningful, understandable, realistic, and in context so that it informs risk management decisions and cannot be interpreted in different ways by different people.

The level and type of detail provided by the output (i.e. technical or not) will be dependent on who the risk assessment is for and what risk management decision it is meant to inform.

## **Understand What Risks Exist**

To understand what risks exist, the chosen risk assessment method should be applied in the context of what the organization is trying to achieve. To do this, you should know:

- Which risk management decisions the assessment will inform?
- Who is responsible for making them?
- What level of detail is needed?

Before conducting a risk assessment, the organization needs to decide and agree how risk assessment output will be presented. There is little value in a risk analyst producing a large and detailed risk assessment document, when the decision maker will only read the first page. Ensure that the scale and rigor of analysis performed (and the amount of documentation produced) matches the business context and is justified and proportionate.

The output of any risk assessment should be recorded for traceability purposes. Traceability is important so that risk management decisions and investment choices can be traced to an identified risk.

Prioritize the output from a risk assessment to allow the organization to make informed risk management decisions. Any prioritization of risk should be based on a meaningful understanding of what the organization really cares about, not meaningless risk level boundaries. [1]

#### **4.5 COMMUNICATE RISK CONSISTENTLY**

To achieve consistency of assessment, the organization has decided to use the output from the threat, vulnerability and impact assessments as baseline input to all risk assessments carried out for online services. These inputs will be reviewed and updated if necessary every six months as a matter of routine, or when a significant change occurs to the threat or technology landscape (such as a technology vulnerability becoming known, or new attackers targeting the organization).

In terms of communicating with partners, the following information will be provided to organization partners who need confidence that risks have been appropriately managed.

The online service provides customers with the ability to register parking permits over the Internet. The threat posed to the service by serious and organized crime groups has been assessed, and identified risks are being managed through application of appropriate ISO/IEC 27002 security controls.

In the context of the example risk provided here, the controls aimed at keeping applications, operating systems and firmware patched and up to date would be appropriate.

The organization will not accept any risk that results in harm to the finances of customers or employees, breaches in legal or regulatory responsibility, or damage to the finances and reputation of the organization.

The service has been designed and implemented to protect against those threats identified by the threat profile. Security policies and procedures are in place to support the continuous management of technology and information risks relating to the online service, and there is an ongoing regime of independent audit and testing to provide continued confidence in the measures that have been applied.

Though controls have been implemented to manage risks regarding known technology vulnerabilities, there remains a risk that an unknown technology vulnerability maybe exploited to cause harm to the service and its customers.

Irrespective of the approach taken to assessing risks, the outcome should be captured in a way that can be used to inform business decision making. Output from risk assessment and other risk management activities may also need to be communicated to interested third parties.

The results of risk assessments depend largely on the experience and biases of the individual conducting them. As a result, it is difficult to obtain consistent risk assessments from different risk practitioners even when applying the same method. Consistency in risk assessment and risk management is important to enable effective decision making and communication. Consistency does not come from the repeated application of a specific risk assessment method. Consistency is achieved by ensuring that:

- The inputs to and outputs from assessments are meaningful in the context of what the business is trying to achieve.
- Risk professionals do not go about their work in isolation but collaborate with the wider organization to achieve a consistent view of the business context.





- The number 1 MOOC for Primary Education
- Free Digital Learning for Children 5-12
- 15 Million Children Reached

**About e-Learning for Kids** Established in 2004, e-Learning for Kids is a global nonprofit foundation dedicated to fun and free learning on the Internet for children ages 5 - 12 with courses in math, science, language arts, computers, health and environmental skills. Since 2005, more than 15 million children in over 190 countries have benefitted from eLessons provided by EFKI. An all-volunteer staff consists of education and e-learning experts and business professionals from around the world committed to making difference. eLearning for Kids is actively seeking funding, volunteers, sponsors and courseware developers; get involved! For more information, please visit [www.e-learningforkids.org](http://www.e-learningforkids.org).



Different organizations do not have to use the same risk assessment methods in order to communicate risk consistently, provided they use a common language that describes the inputs to and results of their risk assessment and risk management activities. What common language is used is a matter for organizations to agree amongst themselves.

Agreeing how to communicate will create trust amongst a community who need to have confidence in the decisions made by others. Organizations should, as a minimum, be able to communicate:

- The threat context under which risk assessments have been conducted.
- The willingness of their organization to accept risk.
- The status of managed risks, and what any risk valuations actually mean.
- What control measures have been taken and how much rigor has been applied to managing risks within the organization.

You should also:

- Avoid situations where (for example) both organizations articulate risk in terms of levels, but the actual meaning of these levels in each organization differ.
- Communicate risk to third party delivery partners by reflecting real and meaningful risk management requirements in contracts and service level agreements; it is not sufficient to say in a contract or agreement that a system or service must be compliant with the requirements of a particular standard.
- Ensure that security requirements in contracts and agreements are informed by and traceable to real risks or external requirements whilst being communicated in a meaningful and testable way. This will ensure that there is a shared understanding between consumer and provider of what outcome is required. [1]

## **4.6 MAKE INFORMED RISK MANAGEMENT DECISIONS**

Throughout the lifecycle of a system or service, the organization will need to make objective decisions about what needs to be done to manage identified risks. This should be based on a clear and meaningful understanding of risk.

These decisions should be informed and supported by information, subject matter expertise and evidence. It is for the organization to decide how much and what form of information is required, together with the level of expert advice and evidence needed to demonstrate that risks are being managed.



Examples of information and evidence that could be used to support risk management decisions include:

- statements from the organization on what risks it will and will not take to achieve its objectives,
- the output of a risk assessment in the context of what the organization is trying to achieve,
- a description of the security controls that are already in place (or those that are needed to manage the identified risks),
- the cost of controls needed to manage a risk,
- evidence and information on how third parties are managing risk and any contractual considerations that could affect the decision,
- evidence that provides confidence that security controls have been implemented to manage identified risks,
- evidence that provides confidence that security controls will continue to manage risks throughout the whole lifecycle of the system or service,
- a view of the status of risks after they have been managed.

It is important that the organization understands what effect its risk management actions have on the risks it has identified. The organization must be capable of communicating this to partners or authorities as necessary.

### **Residual Risks**

It is not possible to say that a system or service is ‘risk free’, or 100% secure. After risk management action has taken place, some risks will remain. These are often referred to as residual risks.

Some risk management approaches estimate how much a specific risk management action reduces an identified risk from its original state. For example, a risk management action may reduce a risk from high to medium. It is not possible to quantify the level of risk reduction as a result of a single or suite of security controls, and basing risk management decisions on estimates of risk reduction can encourage a false sense of security. [1]

As a minimum, it is better when organizations understand and are able to communicate:

- Which risks are being actively managed?
- How are they being managed?
- Is the organization confident the current measures are effective?
- Any risks that are not being managed at all?

## An Illustration on How to Apply Good Risk Management

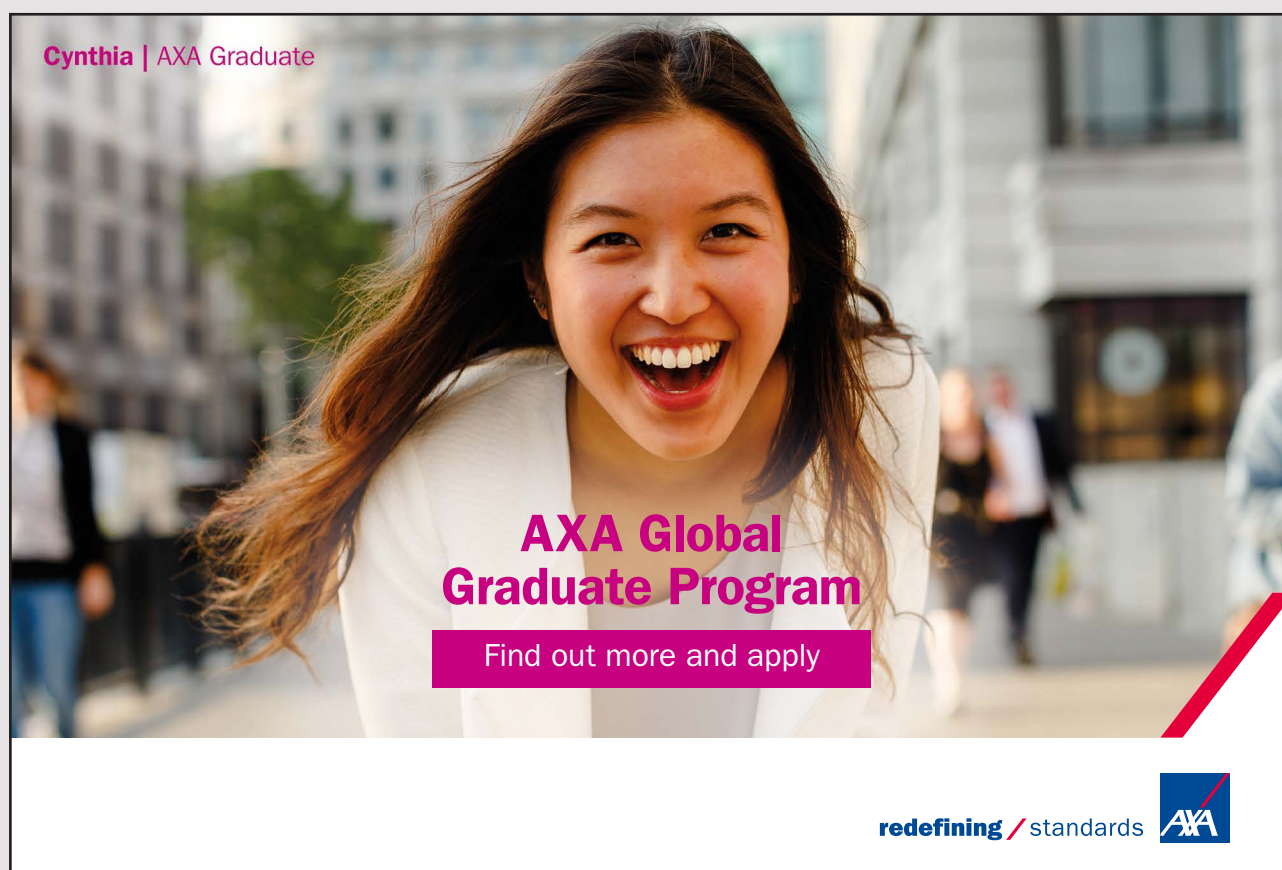
*Start by understanding the business context.*

Business context must be provided by the organization. It is not something that should be left to a risk assessor or analyst to work out for themselves in isolation.

*What is the organization trying to achieve?*

In this case study, a government organization wants to enable its customers to register for residents' parking permits over the Internet. The organization's IT department has been tasked with delivering an online service that will provide customers with the ability to register for parking permits.


The Head of IT is responsible for the successful delivery of the service, and the Head of Public Services has been identified by the organization as being responsible for the security of the service, and for making risk management decisions.



Cynthia | AXA Graduate

**AXA Global Graduate Program**

Find out more and apply

redefining / standards 

*What is important to the organization?*

Customer records have been identified as an important information asset involved in the delivery of the service and the Customer Data Manager is the information asset owner for these assets. The Customer Data Manager has been asked to describe what aspects of them the business cares about, resulting in the following statements.

- An unauthorized release of customer records could result in damage to the privacy and financial well-being of our customers and to the reputation of the organization. This would need to be reported to the Information Commissioners Office (ICO), potentially resulting in financial penalties.
- Any unauthorized change to, or error in customer records could result in damage to the privacy and financial well-being of our customers, to the reputation of the organization, and its compliance with legal and regulatory requirements. This could result in financial penalties and reduced customer confidence in the service and the organization.
- A loss of customer or service access to customer records would cause no physical harm to anyone. A loss of one day could cause minor distress and inconvenience to customers and partners, but could be managed within the customer services department. However, a loss of more than one day would cause inconvenience to customers and reputational damage to the organization that would need to be managed at board level.

*What risks will and won't the organization take?*

The management of the unknown company has agreed the following statement with the organization about what risks it will and will not take with regard to the use of technology to deliver online services to customers.

The organization will make use of technology solutions to realize the benefits of registering parking permits without the need for physical outlets. However, risks that result in the following outcomes will not be accepted:

- harm to the physical well-being of customers and employees,
- harm to the financial well-being of customers and employees,
- breaches of the organization's legal or regulatory responsibilities,
- widespread damage to the reputation of the organization,
- costs or financial damage to the organization.

*Decide on the risk management approach.*

The organization needs to demonstrate that it meets the mandatory security outcomes. It will therefore manage risks to its information, technology and services by developing and communicating a set of security policies and procedures for the service by taking account of the latest sector related advice and guidance on the security of online services.

The organization would like to use common solutions to technology problems where available, but at this time there is no common solution available. The organization therefore needs to conduct its own risk assessment activity to inform risk management decisions.

The organization already has obtained the ISO/IEC 27001 certification for a number of its business areas. Within the scope of those certifications are existing IT systems, and the organization is used to assessing what it does in the context of the controls provided by the standard. A decision has therefore been made that applicable security controls from the standard will be applied to the service.

Confidence that security has been appropriately implemented and maintained and that security policies and procedures are working as expected will be gained by:

- ensuring that the management has been involved in all key security decisions from the outset of the project,
- independent audit and security testing of the service before going live and periodically throughout its operational lifetime.

### **Choose the Right Risk Assessment Method**

At this point in the project, the organization has decided to undertake an initial risk assessment that is consistent with the high-level risk assessment approach described by ISO/IEC 27005. This approach takes threat, vulnerabilities and impact as inputs into a qualitative assessment of risks to the online service.

To achieve this, the organization has employed a technology and information risk subject matter expert to assist in the identification, assessment, documentation and prioritization of risks. A more detailed risk assessment may follow as the project progresses to provide a more thorough understanding of risks and what needs to be done to manage them.

### Understand What Risks Exist

To bring the assessment together, the risk subject matter expert has taken account of and analyzed the threat, impact and vulnerabilities to identify a number of risks that are relevant in the context of the online service. The following extract shows a meaningful risk using the organization’s chosen risk assessment method.

Using the internet, serious and organized crime could exploit known vulnerabilities in the commercial applications used to deliver online services to steal personal information. If realized, this could lead to damage to the privacy and financial well-being of our customers, fraud, a breach of legal or regulatory responsibilities and damage to the reputation of the organization.

### Prioritizing the Resultant Risks

It is now necessary to prioritize identified risks for management purposes. This prioritization should be carried out in the context of the organization and what it cares about.

I joined MITAS because  
I wanted **real responsibility**

The Graduate Programme  
for Engineers and Geoscientists  
[www.discovermitas.com](http://www.discovermitas.com)



**Month 16**  
I was a construction supervisor in the North Sea advising and helping foremen solve problems

Real work  
International opportunities  
Three work placements



**MAERSK**



The example risk that we have identified, if realized, would result in “damage to the privacy and financial well-being of our customers, a breach of legal or regulatory responsibilities and damage to the reputation of the organization.” In the context of what the organization has said it cares about, this risk would clearly be a high priority for the organization to manage.

## 4.7 SUMMARY OF RISK MANAGEMENT

What a risk is, and how it is described, depends entirely on the context of the organization which faces that risk, and on the biases of the individual assessing it.

In the context of wider business risk management, a risk is the potential for either harmful or positive outcomes to impact upon business objectives, including reputation. Organizations cannot develop without taking risks. Technology and information risk is not just about avoidance and mitigation; the pursuit and acceptance of risk creates opportunities and can help deliver business objectives.

Having recognized this wider meaning, this guidance uses the word “risk” to describe the potential for security harm to occur as a result of using technology and information to achieve business objectives.

It is important not to just think about risk in the context of the confidentiality, integrity and availability of technology and information. In addition to these, other things that the organization cares about (e.g. its reputation) may be at risk and should also be taken into account [1].

*Risk is the possibility that reality may be different than we expect.*

For a basic understanding of a risk management system, it is probably necessary to first realize the risks and describe them to further manage and control them in the last stage.

Many people see risks in business and believe that if they are covered, the issue is resolved. Just like driving a car is accompanied by risks that we can and cannot realize, every business field might be also accompanied by risks.

It is therefore necessary to think about risk and realize that even the simplest commercial activity is, in a sense, accompanied by a certain degree of risk. Risk management in the corporate sense is an important part of corporate culture and, more recently, effective management of risks in the form of a compact system that is regularly audited independently provides options for differentiation from the competition. Partly it may be similar as Corporate Social Responsibility and Environmental Policies or the ISO9001 certification.

Risk management at the company level usually begins with an extensive analysis of all major internal processes which provides their technical description or graphic representation. Verbal description and graphic representation (i.e. process map) is used to describe the inputs and outputs within the process described and the main procedural steps that take place within the unit or department.

As an example, imagine that a production company has the following key activities:

- development of new products,
- production,
- service,
- business,
- marketing,
- warehouse management,
- purchasing department,
- consultants,
- finance and reporting,
- human resources.

Within this schematic arrangement, there are specific activities or outputs, where in certain situations appointed bodies exchange or share their information among themselves.

For example, the financial department needs to know the volume of supplied products to be able to invoice customers or it needs to know the volume of ordered supplies and raw materials from the warehouse management department in order to estimate the total payables to their suppliers. Or it can be expected that the department will inform the marketing department of any upcoming products so that they can initiate marketing studies and market research. Another illustrative example is the connection between the consultants and the human resources department, as the HR department will specifically search the job market for candidates with the required profile.



In case that the company has actual process maps of its core processes, the next step is to estimate the time required for the coordination between the departments to decide who has the responsibility to correctly and completely transmit the necessary information.

Companies have process maps which were created to be able to deal with the relevant procedural risks. The risks need to be identified and classified according to their importance and so-called risk catalogue should be created.

In practice, risks are identified using a simple chart where individual risks are plotted according to their *likelihood* and *impact*.

In practice, we focus on about 70% of all identified risks and deliberately eliminate the risks which are highly likely, or with a fatal impact.

**ie** business school

93% OF MIM STUDENTS ARE WORKING IN THEIR SECTOR 3 MONTHS FOLLOWING GRADUATION

**MASTER IN MANAGEMENT**

- STUDY IN THE CENTER OF MADRID AND TAKE ADVANTAGE OF THE UNIQUE OPPORTUNITIES THAT THE CAPITAL OF SPAIN OFFERS
- PROPEL YOUR EDUCATION BY EARNING A DOUBLE DEGREE THAT BEST SUITS YOUR PROFESSIONAL GOALS
- STUDY A SEMESTER ABROAD AND BECOME A GLOBAL CITIZEN WITH THE BEYOND BORDERS EXPERIENCE

Length: 10 MONTHS  
Av. Experience: 1 YEAR  
Language: ENGLISH / SPANISH  
Format: FULL-TIME  
Intakes: SEPT / FEB

**5 SPECIALIZATIONS**  
PERSONALIZE YOUR PROGRAM

**#10 WORLDWIDE**  
MASTER IN MANAGEMENT  
FINANCIAL TIMES

**55 NATIONALITIES**  
IN CLASS

[www.ie.edu/master-management](http://www.ie.edu/master-management) | [mim.admissions@ie.edu](mailto:mim.admissions@ie.edu) | Follow us on IE MIM Experience



Risks can be divided into many categories, groups and subgroups. For the purposes of the basic knowledge of risks, they will usually be divided into external, which may take on the form of market risk, currency risk and political risk, and internal. A common feature of *external* risks is that we do not control these risks. The opposite category is the group of *internal* risks such as operational risk, credit risk, liquidity risk, production risk and process risk. These risks are under our control and can be effectively managed.

Risk management is a long-term process that requires the involvement of all structures of the company and mutual cooperation at all levels of management. The point is that if a company decides that it will manage its risks, it will have a big impact on the internal synergy of the company.

It is necessary to respect the following principles:

- No one may be more important than others.
- The individual units and departments must cooperate.
- Exceptions and privileges exist.

These principles are based on the current practice because each company has its own departments “mentally” hierarchically sorted. For example, the sales department staff are considered to be the “premier league”, and on the other hand, purchasing staff and the finance department are very overlooked and the company management considers it normal.

In such a situation, it would be very inappropriate to change the deadlines for the development of the process maps or make exceptions for a certain “preferred” department that never has to create them. Another aspect of the result is to determine a mandatory format or structure of the data collected. Now, these rules will enable us to work with complex data across the enterprise and get a picture of the situation.

If all departments, sections and units are able to provide documentation in the required scope and quality, it is the first step towards creating a modern risk management system.

Using the example of a schematic workflow for entering invoices received, we can demonstrate where there may be critical points in a commonly used process, which can be reformulated into a verbal description of the specific process risks.

## QUESTIONS

- Does the issued invoice correspond with the order?
- Is there a proper delivery note?
- Have correct data been entered into the information system?
- Are the bank details the same as is the master data file?

## RISKS

- A supplier has not delivered the goods ordered.
- A delivery has not been delivered.
- Data from invoices received were incorrectly recognized.
- Master data are not protected.

The conceptual principle of risk management requires a special set-up of the company which decides to manage its own risks. It is not only the responsibility of the management but every staff member can contribute his or her share towards a common goal.

It is crucial for the successful implementation of a unified and mature risk management environment that the common goal is known and the principle of personal accountability is required.

## 5 WHAT IS QUALITY

- a) Quality is the “status quo” when an expected result has been achieved in the shortest amount of time and with minimum long-term expenses.

Good quality has many different aspects but one of them is keeping a balance between delivery time and associated costs. It is not advisable to plan complicated solutions, which may be technically out of this world, but the customer is not going to be willing to pay for them. Efficiency also means keeping the *Pareto principle* in mind and success in business very much depends on the entrepreneur’s ability to satisfy customers and deliver the best possible product or service with adequate costs, which are acceptable to the customer. The customer is the one, who drives the business, but our own investments have to be in line with the required outputs.



“I studied English for 16 years but...  
...I finally learned to speak it in just six lessons”  
Jane, Chinese architect

ENGLISH OUT THERE

Click to hear me talking before and after my unique course download

- b) Quality also means an ability to eliminate potential errors before they appear. Every production error is very expensive to repair. It is ideal to support and manage activities aimed at eliminating these errors before they appear. Mature companies invest a lot of money into sophisticated detection methods that identify raw materials which are under the acceptance quality limit. According to the old *GIGO (Garbage In Garbage Out)* principle, all parts must be carefully tested before final assembly. If a part does not meet the given quality standards, it is removed from the production process. An analogy might be seen in the car industry. Of what use would a car with a really great engine be if the tires were unable to carry the weight of the car. Complicated mechanical, organizational or administrative units are nothing other than sets of sub-units. Each and every part should meet the given quality standards. These standards must be carefully formulated according to the given industry or best practice standards.
- c) Quality means to get paid after delivering the required services or goods. Every business activity must be economically efficient which also results in a win-win situation. It also means that all investments into raw materials, production and distribution should be covered by the sales price. It is very important for a business to do business where all parties are free of payable obligations; in other words, only where all invoices have been paid. Sometimes, we may see enthusiastic salesmen investing a lot of energy and effort into the acquisition of new clients. They would make an excellent product presentation and arrange the delivery of the goods or services. This is step number one. Step number two must be payments for this from the customer. High-quality companies and quality-oriented companies very often screen their business customers and make a careful selection based on their credit check. To have happy customers means to have customers who pay their invoices on time. And we should not forget that companies do not die because of a lack of ideas but because of a shortage of money.
- d) Quality also requires people with same mental set-up. A high-quality approach requires talented, independent and creative co-workers. It means that your future colleagues must be enthusiastic about quality issues and their implementation into day-to-day practice. The best solution might be to be surrounded by people who share the same vision and quality standards and are interested in working towards quality achievements.

## Basic Quality Work Scheme

Where you stand within the corporate hierarchy is determined by the structures above you and similar structures below you. You are going to receive instructions from your supervisors and you might delegate a lot of tasks to your supporting staff. From the quality perspective, it is a sequential flow of information which must be defined in three basic steps:

- Task definition
- Optimal solution
- Handover and acceptance

### *Task Definition*

A well-defined task definition should contain at least three basic parameters – what is wanted, what the solution should look like and when we need the full delivery. Based on the best practices, a well-defined task definition leaves very small room for guessing. Another well desired outcome of proper task definition is the elimination of future disputes.

### *Optimal Solution*

The preparation of the optimal solution requires a number of various steps, including searching for available information, several options, and offering to discuss with the person assigning the task and coordinating with other parties involved. To deliver an optimal solution should be a natural ambition of every professional team. Delegation of tasks and personal responsibility are key to professional growth.

### *Handover and Acceptance*

This is more of a formal action, but a very important one. Proper and straight acceptance of a delivered task solution is key to the success and formal closure of an activity loop. The existence of a formal handover protocol is clear evidence proving that the customer received the completed work. Another assigned activity is feedback from the customer. Such feedback might be informal or formal and it is always the “bridging factor” of mutual cooperation between the customer and the cooperating teams.

Even the relatively common administration practices described above might help eliminate the issues and unproductive discussions about who was supposed to deliver what. Most problematic is the situation when a project team thought the results have been delivered but have no formal proof because the handover protocol is missing.

## 5.1 BRIEF LOOK AT QUALITY SYSTEMS

All current quality systems were based on the general idea of ensuring the delivery of high-quality results. Professor Deming defined the four-phase cycle which is still valid and in use. The so-called Deming Cycle contains the following phases:

- Plan (What to do, How to do)
- Do (Do what is planned)
- Check (Was everything done according to the planned measures)
- Act (How to correct deviations, How to improve next time)

The basic concept of quality management is the elimination of all the conditions which may negatively affect the quality of the final product. The aim of quality management is to ensure production of goods or services with no delay or need for re-assembly.



In the past 5 years we have drilled around

# 95,000 km

—that's more than **twice** around the world.

**Who are we?**  
We are the world's leading provider of reservoir characterization, drilling, production, and processing technologies to the oil and gas industry.

**Who are we looking for?**  
We offer countless opportunities in the following domains:

- Operations
- Research, Engineering, and Manufacturing
- Geoscience and Petrotechnical
- Commercial and Business

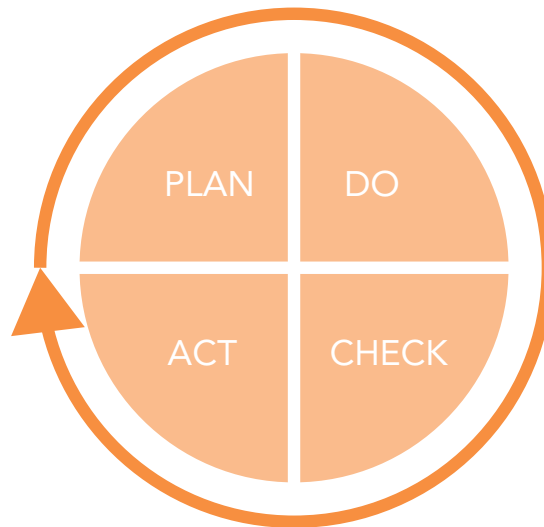
We're looking for high-energy, self-motivated graduates with vision and integrity to join our team.

[careers.slb.com](https://careers.slb.com)

**What will you be?**

**Schlumberger**





**Fig. 1** Deming Cycle source: [www.expertprogrammanagement.com](http://www.expertprogrammanagement.com)

## 5.2 ISO

The International Standard Organization (ISO) is an organization bridging the gap between the public and private sectors using various quality standards. ISO is trying to unify technical standards and contribute an increase in quality.

ISO9000 is focused on the basics of quality management, defines important terms and the scope of the necessary documents and publications required by this standard within an organization.

ISO9001 sets out quality management requirements used to prove the ability of an organization to fulfill quality requirements defined by customers and quality-related legislation without verification.

ISO9004 is a brief manual for the implementation of a quality management system, expanding the framework of ISO9001. This standard allows an organization to effectively meet the demanding expectations of its customers.

Unfortunately, the ISO concept is not widely used. Due to its vague position among other legal requirements, ISO has become a synonym for sunk certification costs with no visible improvement of the administrative or production processes.

ISO is, by definition, only a bundle of recommendations, which are very well constructed, but their limited legal applicability is going to be a problem for better use of ISO standards. Compared with other quality management tools, ISO has the widest definitions and can impact a lot of areas within the corporate administration, IT processes and risk management. [2]

### 5.3 KAIZEN

Kaizen is the practice of continuous improvement. Kaizen was originally introduced to the West by Masaaki Imai in his book *Kaizen: The Key to Japan's Competitive Success* in 1986. Today, Kaizen is recognized worldwide as an important pillar of an organization's long-term competitive strategy. Kaizen is continuous improvement that is based on certain guiding principles:

- Good processes bring good results.
- Go see for yourself to grasp the current situation.
- Speak with data, manage by facts.
- Take action to contain and correct root causes of problems.
- Work as a team.
- Kaizen is everybody's business.

One of the most notable features of kaizen is that big results come from many small changes accumulated over time. However, this has been misunderstood to mean that kaizen equals small changes. In fact, kaizen means everyone is involved in making improvements. While the majority of changes may be small, the greatest impact may be Kaizens that are led by senior management as transformational projects, or by cross-functional teams as Kaizen events.

Kaizen is a practice based on continuous improvement made by everybody, every day and everywhere.

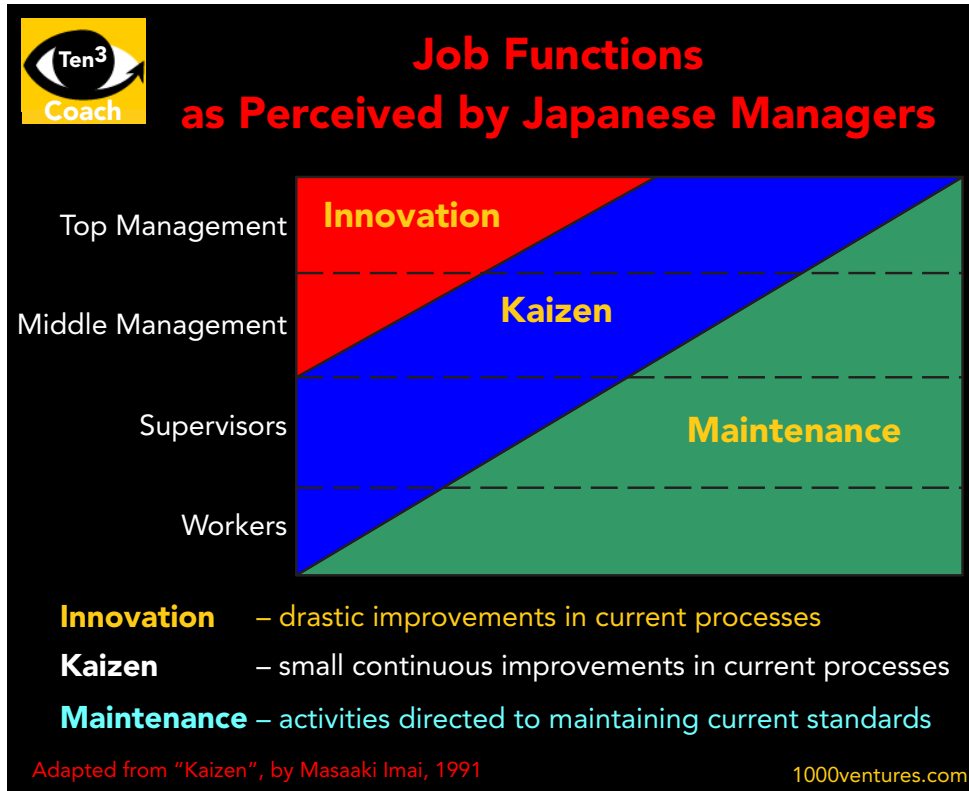


Fig. 2 Japanese quality systems source: [1000ventures.com](http://1000ventures.com)

Excellent Economics and Business programmes at:



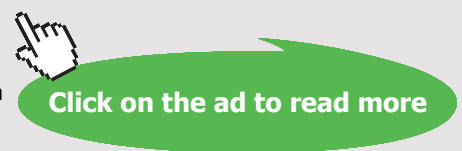
university of groningen



**“The perfect start of a successful, international career.”**

**CLICK HERE**  
to discover why both socially and academically the University of Groningen is one of the best places for a student to be

[www.rug.nl/feb/education](http://www.rug.nl/feb/education)



## 5.4 LEAN

The core idea is to maximize customer value while minimizing waste. Simply, lean means creating more value for customers with fewer resources.

A lean organization understands customer value and focuses its key processes to continuously increase it. The ultimate goal is to provide perfect value to the customer through a perfect value creation process that has zero waste.

To accomplish this, lean thinking changes the focus of management from optimizing separate technologies, assets, and vertical departments to optimizing the flow of products and services through entire value streams that flow horizontally across technologies, assets, and departments to customers.

Eliminating waste along entire value streams, instead of at isolated points creates processes less human effort and less time to make products compared with traditional business systems. Companies are able to respond to changing customer desires with high variety, higher quality, lower costs and faster production times. A lion's share for these achievements belongs to the increase of IT services. Technological changes are drivers to the more efficient and effective production environment.

### **Lean for Production and Services**

A popular misconception is that lean is suited for manufacturing only. Lean could be applied in every business and every process. It is not a cost reduction program but a way of thinking and acting for an entire organization.

Businesses in all industries and services, including healthcare and governments, are using lean principles as the way they think and do. Many organizations choose not to use the word lean, but to label what they do as their own system, such as the Toyota Production System or the Danaher Business System. Why? To drive home the point that lean is not a program or short-term cost reduction program, but the way the company operates. The word transformation or lean transformation is often used to characterize a company moving from an old way of thinking to lean thinking. It requires a complete transformation on how a company conducts business. This takes a long-term perspective and perseverance.

### **Purpose, Process, People**

Managers and executives embarked on lean transformations think about three fundamental business issues that should guide the transformation of the entire organization:

*Purpose:* What customer problems will the enterprise solve to achieve its own purpose of prospering?

*Process:* How will the organization assess each major value stream to make sure each step is valuable, capable, available, adequate, flexible, and that all the steps are linked by flow, pull, and leveling?

*People:* How can the organization ensure that every important process has someone responsible for continually evaluating that value stream in terms of business purpose and lean process? How can everyone touching the value stream be actively engaged in operating it correctly and continually improving it?

## 5.5 SIX SIGMA

Six Sigma at many organizations simply means a measure of quality that strives for near perfection. Six Sigma is a disciplined, data-driven approach and methodology for eliminating defects (driving toward six standard deviations between the mean and the nearest specification limit) in any process – from manufacturing to transactional and from product to service.

The statistical representation of Six Sigma describes quantitatively how a process is performing. To achieve Six Sigma, a process must not produce more than 3.4 defects per million opportunities. A Six Sigma defect is defined as anything outside of customer specifications. A Six Sigma opportunity is then the total quantity of chances for a defect.

The fundamental objective of the Six Sigma methodology is the implementation of a measurement-based strategy that focuses on process improvement and variation reduction through the application of Six Sigma improvement projects. This is accomplished through the use of two Six Sigma sub-methodologies: DMAIC and DMADV.

The Six Sigma DMAIC process (define, measure, analyze, improve, control) is an improvement system for existing processes falling below specification and looking for incremental improvement.

The Six Sigma DMADV process (define, measure, analyze, design, verify) is an improvement system used to develop new processes or products at Six Sigma quality levels. It can also be employed if a current process requires more than just incremental improvement. Both Six Sigma processes are executed by Six Sigma Green Belts and Six Sigma Black Belts, and are overseen by Six Sigma Master Black Belts.

Many frameworks exist for implementing the Six Sigma methodology. Six Sigma Consultants all over the world have developed proprietary methodologies for implementing Six Sigma quality, based on the similar change management philosophies and applications of tools.



Fig. 3 Six Sigma, Kaizen and Lean concepts source: [iSix Sigma.com](http://iSixSigma.com)

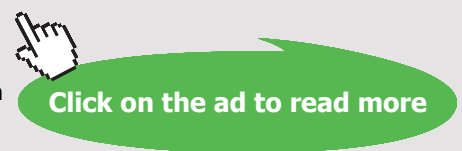
## American online

# LIGS University

is currently enrolling in the  
Interactive Online **BBA, MBA, MSc,**  
**DBA and PhD** programs:

- ▶ enroll **by September 30th, 2014** and
- ▶ **save up to 16%** on the tuition!
- ▶ pay in 10 installments / 2 years
- ▶ Interactive **Online education**
- ▶ visit [www.ligsuniversity.com](http://www.ligsuniversity.com) to find out more!

**Note:** LIGS University is not accredited by any nationally recognized accrediting agency listed by the US Secretary of Education. [More info here.](#)





## 5.6 HAMBURGER UNIVERSITY

Based on the idea of McDonald's top management, a special educational facility was created in 1961 to ensure continuous development and education. The college received credit recommendations from the American Council on Education (ACE), the United States' oldest and most recognized unifying body for higher education. The Hamburger University focuses on teaching management capabilities for the best employees with full respect for the McDonald's global values i.e. products, customers and money. [5]



**Fig. 4** Illustration of McDonald's values source: own pictures

Ray Kroc once said: "If we are going to go anywhere, we've got to have talent. And, I'm going to put my money in talent." Hamburger University continues to promote that philosophy every day. [5]



**Fig. 5** Hamburger University in Illinois, USA source: McDonald's



## 5.7 HOW DO WE DIFFERENTIATE BETWEEN PROFESSIONAL AND AMATEUR?

Wherever you work, you will be surrounded by your colleagues and peers. Never forget that effective cooperation starts and ends with people with predictable and professional manners.

Amateur may be characterized by the following:

- Always looks for a solution.
- Overestimates own skills.
- Requires constant supervision.
- Continual checking needed.
- Does not cooperate with the others.
- Works inefficiently.
- Bad time management.
- Has no slack.

I would say no one wants to cooperate with someone who is the “brake on the wheel” within the current team spirit business environment. Professionals should be characterized by the following:

- Uses standard solutions in standard situations.
- Knows his/her limits.
- Does not require constant supervision.
- Consults the results of the work.
- Works effectively.
- Is organized.
- Does have a slack.

In the real business day-to-day work, it is important to respect the principle of 3A's, i.e. always deliver the best possible results, always adopt the “can-do” approach and always stand on the basic ground.

The management supports quality in many possible ways. The most important question might be whether the management focuses on what the customer wants. This is an essential and logical requirement. If the supporting departments focus on defining how to achieve what the customer wants in terms of production guidelines and working instructions, the result could not be wrong. To make the circle complete, the supply departments should concentrate on getting everything that is needed in the set time, quality and quantity.

If all these three segments click together, quality will be satisfactory for all stakeholders. To support this way of thinking, the concept of best practice should not be forgotten. Key decision makers should ask the following:

- Do we have any similar business experience?
- Was the previous solution acceptable for the customer?
- Was it profitable for us?
- Was it manageable for us?

In the current world, many “old fashioned” structures are going to be suppressed by the brand new world of clever application, newly developed software and magic technology which supports the business every day. But we should keep the idea how communicate to our audiences which may differ. Whether the issue of quality is presented to the CEO, team of software developers or workshop staff, we should speak straight, we should not hide any facts, we should avoid misunderstanding of an idea and respect the overall quality principles.



**DON'T EAT YELLOW SNOW**

What will your advice be?

Some advice just states the obvious. But to give the kind of advice that's going to make a real difference to your clients you've got to listen critically, dig beneath the surface, challenge assumptions and be credible and confident enough to make suggestions right from day one. At Grant Thornton you've got to be ready to kick start a career right at the heart of business.

Sound like you? Here's our advice: visit [GrantThornton.ca/careers/students](http://GrantThornton.ca/careers/students)

Scan here to learn more about a career with Grant Thornton.



 **Grant Thornton**  
An instinct for growth™

© Grant Thornton LLP. A Canadian Member of Grant Thornton International Ltd

## 6 SARBANES-OXLEY ACT AND ITS IMPLICATIONS

The Sarbanes-Oxley Act of 2002, sponsored by Paul Sarbanes and Michael Oxley, represents a huge change to federal securities law. It came as a result of the corporate financial scandals involving Enron, WorldCom and Global Crossing. Effective in 2006, all publicly-traded companies are required to implement and report internal accounting controls to the SEC for compliance. [6]

### 6.1 PREFACE

Every company, as has been established, is basically a unique combination of three basic factors – human resources, planned activities and outputs. The world of business is very wide and every company might be different in terms of the capital employed, size, number of employees and variety of production.

Every company has some owners who may be individuals or institutional investors. The reason, why owners are interested in a company, is the expectation of profit. Pure profit is the key motivation for entrepreneurs, institutional investors and owners.

Every company should be growing. The expansion of business is a visible mark of success. In the life of a well-managed and profitable company should come the moment when it is willing to sign up for IPO; in other words, to issue their own stocks and get money from investors. When preparing for a successful IPO, the company has a very long road ahead and it is required to meet dozens of specific conditions.

### 6.2 U.S. CAPITAL MARKET

In the United States, these conditions are specified by the SEC (Security Exchange Commission) and NYSE (New York Stock Exchange) or NASDAQ (National Association of Securities Dealers Automated Quotations). For a long time, NYSE and NASDAQ have represented the most reputable places where companies are selling their stocks. NYSE was established as a place for exchanging stocks in 1817 and NASDAQ was opened in 1972 as a place primarily reserved for technology company stock.

The whole system of the closed circle that includes companies, their IPOs and financial resources is based on mutual trust. Stock buyers trust that the companies are not cheating with the presented financial results. For a very long time, this system worked very well. Business activities on the NYSE are monitored by the special Dow Jones Index (DJI) which reflects the volume of money flow on a daily basis.

If investors are interested in the stock market, the DJI is going up and when they leaving the stock market, the DJI is going down. The daily position of the DJI indicates the “investors’ appetite” for putting their money into the stocks.

The picture below shows the symptomatic decrease of the DJI within very few days.

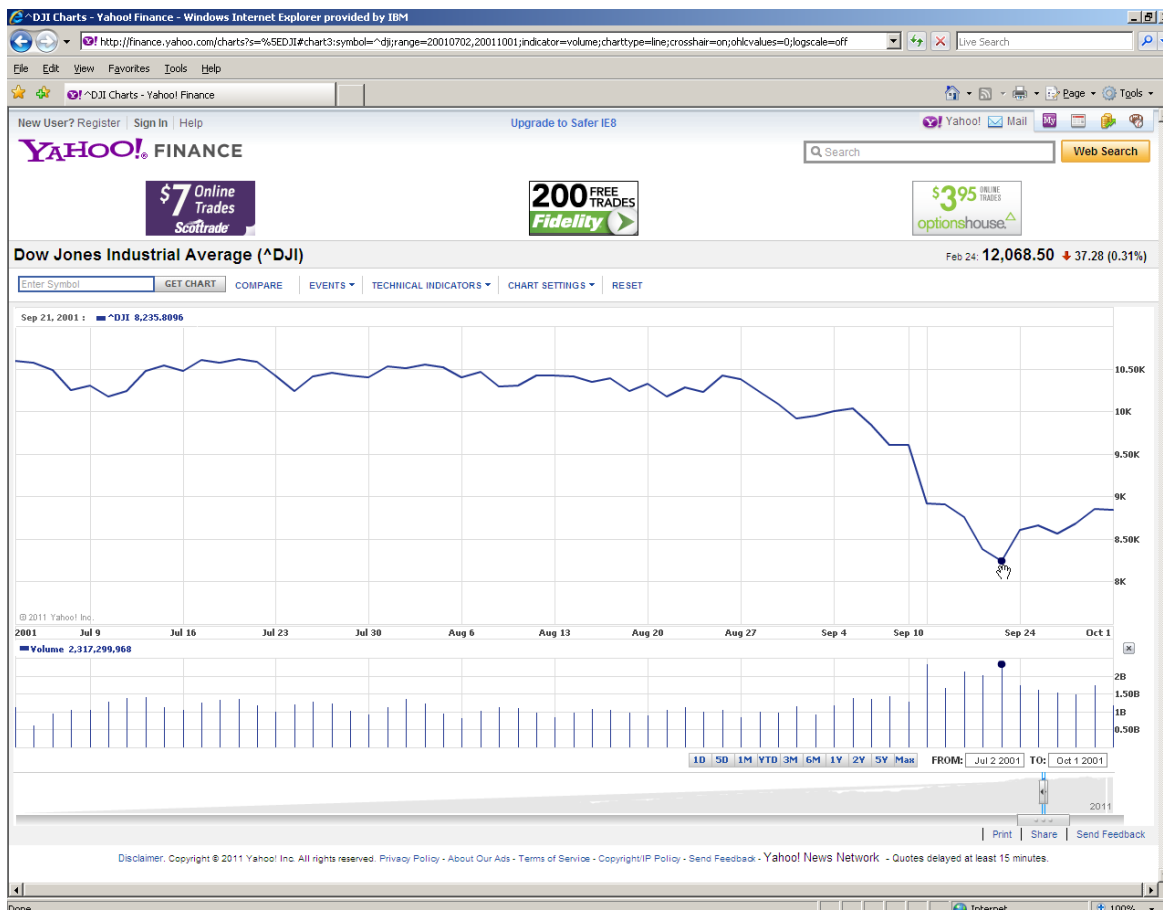


Fig. 6 Dow Jones Index

This was a significant moment for the U.S. capital market. Based on the news presented by the media, investors started to close their investment positions and leave the stock market. There were two main reasons for this: ENRON and MCI WorldCom.

### 6.3 THE ENRON STORY

The ENRON story is considered to be one of the most notorious in American history and is considered by many historians and economists alike to have been an unofficial blueprint for a case study on White Collar Crime in the United States.



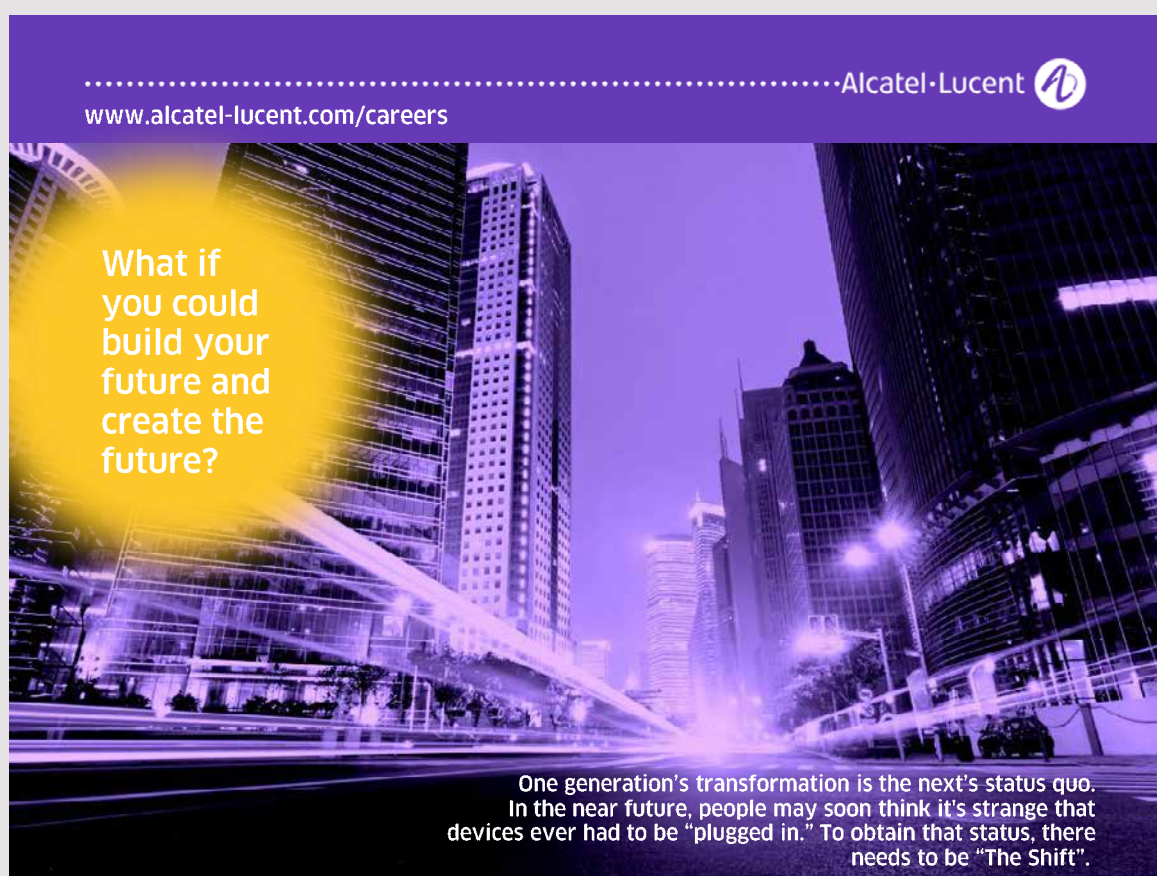
### *The Deregulation*


While the term regulation within a commercial and corporate setting typically applies to the government's ability to regulate and authorize commercial activity and behavior with regard to individual businesses, the ENRON executives applied for – and were subsequently granted – government deregulation. As a result of this declaration of deregulation, ENRON executives were permitted to maintain agency over the earnings reports that were released to investors and employees alike.

This agency allowed for ENRON's earning reports to be extremely skewed in nature – losses were not illustrated in their entirety, prompting more and more investments on the part of investors wishing to partake in what seemed like a profitable company.

### *Misrepresentation*

By misrepresenting earnings reports while continuing to enjoy the revenue provided by the investors not privy to the true financial condition of ENRON, the executives of ENRON embezzled funds funneling in from investments while reporting fraudulent earnings to those investors; this not only proliferated more investments from current stockholders, but also attracted new investors desiring to enjoy the apparent financial gains enjoyed by the ENRON corporation.



.....Alcatel-Lucent 

[www.alcatel-lucent.com/careers](http://www.alcatel-lucent.com/careers)

What if you could build your future and create the future?

One generation's transformation is the next's status quo. In the near future, people may soon think it's strange that devices ever had to be "plugged in." To obtain that status, there needs to be "The Shift".

*Fraudulent Energy Crisis*

In the year 2000, subsequent to the discovery of the crimes listed in the above ENRON Scandal Summary, ENRON had announced that there was a critical circumstance within California with regard to the supply of Natural Gas. Due to the fact that ENRON was a then-widely respected corporation, the general population was not wary about the validity of these statements.

However, upon retroactive review, many historians and economists suspect that the ENRON executives manufactured this crisis in preparation of the discovery of the fraud they had committed – although the executives of ENRON were enjoying the funds rendered from investments, the corporation itself was approaching bankruptcy.

*Embezzlement*

The acts of embezzlement undertaken by ENRON executives may be defined as a criminal activity involving the unlawful and unethical attainment of monies and funding by employees; typically, funds that are embezzled are intended for company use in lieu of personal use. While the ENRON executives were pocketing the investment funds from unsuspecting investors, those funds were being stolen from the company, which resulted in the bankruptcy of the company.

*Losses and Consequences*

Due to the actions of the ENRON executives, the ENRON Company went bankrupt. The loss sustained by investors exceeded \$70 billion. Furthermore, these actions cost both trustees and employees upwards of \$2 billion; this total is considered to be a result of misappropriated investments, pension funds, stock options, and savings plans – as a result of the government regulation and the limited liability status of the ENRON Corporation, only a small amount of the money lost was ever returned.

**6.4 THE MCI WORLDCOM STORY**

WorldCom was a telecommunications company that underwent a merger with fellow telecommunications company MCI in 1997; subsequent to the merger of these 2 giants within the telecommunications industry, the conglomerate company was renamed “MCI WorldCom”.

In 1999, the Sprint Telecommunications Company had planned to merge with the MCI WorldCom Company, yet a government regulation prohibited this merger from taking place due to presumable violations of anti-trust statutes. However, upon mention of WorldCom, historians and economists alike agree that public focus is seldom drawn to the commercial development of this conglomerate in lieu of the accounting scandal in which it was involved in 2002; the WorldCom Company name may tend to draw more focus to the massive financial loss resulting from the presumed unraveling of the company due to the fraudulent operation of the company itself.

### *Accounting Scandal*

The WorldCom accounting scandal was a financial scandal that involved the MCI WorldCom telecommunications company. Although the investigative reports provided by the Securities and Exchange Commission – as well as those belonging to private auditors who undertook additional investigation – state that the WorldCom scandal began in 2000, no specific date currently exists. However, these investigative reports successfully named and classified the nature of the accounting scandal, as well as succeeded with regard to its respective criminal indictments.

### *Finances and Investments*

Bernard Ebbers was a Canadian Entrepreneur who not only gained notoriety for the founding of the WorldCom Company, but also acted as the company's Chief Operations Officer (CEO) both prior to – and following – its merger with MCI, and subsequently Sprint. Following the merger, Ebbers earned a large amount of capital in addition to a vast amount of company stock; the merger resulted in the disbursement of stocks and assets resulting in Bernard Ebbers remaining the primary shareholder and CEO.

### *Insider Loans and Lending*

Subsequent to the decline of the MCI WorldCom stock with regard to the commercial market, Bernard Ebbers had begun to lose a vast amount of capital; as a result, he found himself to be unable to provide sufficient maintenance to other investments that he had undertaken. Ebbers approached the board of MCI WorldCom and requested a loan of \$400 million in order to provide him with the financial relief necessary to upkeep his peripheral expenses and investments; the executive board agreed to provide Ebbers with a loan in order to sway him from selling the entirety of his shares – the board feared that the selling of Ebbers' shares would not only promote a sense of panic with regard to other investors in MCI WorldCom, but would also present an opportunity for a hostile takeover.



Subsequent to the release of the loan to Bernard Ebbers, the executive board witnessed the gradual insolvency of the company; both the \$400 million given to Ebbers existing in tandem with the declining profits sustained by MCI WorldCom placed the company on the brink of bankruptcy. In lieu of informing MCI WorldCom investors of the true state of the company, a number of executives purposefully misrepresented the company's earnings and spending; this accounting fraud purportedly resulted in the fraudulent reporting of upwards of \$11 billion that the company did not have.

### *Conclusion*

MCI WorldCom filed for Chapter 11 bankruptcy in 2004 and was acquired by the Verizon telecommunications company; Bernard Ebbers was both indicted – and subsequently sentenced to a 25-year prison sentence.



**Maastricht University**

*Leading in Learning!*

**Join the best at  
the Maastricht University  
School of Business and  
Economics!**

#### Top master's programmes

- 33<sup>rd</sup> place Financial Times worldwide ranking: MSc International Business
- 1<sup>st</sup> place: MSc International Business
- 1<sup>st</sup> place: MSc Financial Economics
- 2<sup>nd</sup> place: MSc Management of Learning
- 2<sup>nd</sup> place: MSc Economics
- 2<sup>nd</sup> place: MSc Econometrics and Operations Research
- 2<sup>nd</sup> place: MSc Global Supply Chain Management and Change

Sources: Keuzegids Master ranking 2013; Elsevier 'Beste Studies' ranking 2012; Financial Times Global Masters in Management ranking 2012

**Maastricht University is the best specialist university in the Netherlands (Elsevier)**

**Visit us and find out why we are the best!  
Master's Open Day: 22 February 2014**

[www.mastersopenday.nl](http://www.mastersopenday.nl)

## 6.5 LESSONS LEARNT

An audit and the investigation of the top management of ENRON and WorldCom provide a great historical experience. To summarize the lessons learnt, the following could be said:

- Both companies violated the principles of fair and true reporting of financial results.
- Both companies handled the company financial resources for the benefit of top and middle management.
- Both companies violated the GAAP principles.

These scandals reignited the debate over the relative merits of US GAAP, which takes a “rules-based” approach to accounting, versus the International Accounting Standards and UK GAAP, which takes a “principles-based” approach. The Financial Accounting Standards Board announced that it intends to introduce more principles-based standards. More radical means of accounting reform have been proposed, but so far have very little support. The debate itself, however, overlooks the difficulties of classifying any system of knowledge, including accounting, as rules-based or principles-based. This also led to the establishment of Sarbanes-Oxley.

## 6.6 SARBANES-OXLEY ACT

U.S. lawmakers used this as an opportunity to increase regulation. The Congress initiative led by Senator Mr. Sarbanes and Representative Mr. Oxley prepared a special law which reduced the possibilities of manipulated reporting of financial results. The Sarbanes-Oxley Act was named after its sponsors U.S. Senator Paul Sarbanes (D-MD) and U.S. Representative Michael G. Oxley (R-OH). As a result of SOX, top management must individually certify the accuracy of financial information. In addition, penalties for fraudulent financial activity are much more severe. Also, SOX increased the oversight role of boards of directors and the independence of the outside auditors who review the accuracy of corporate financial statements.

### *Direct Implications:*

#### 1. Public Company Accounting Oversight Board (PCAOB)

Title I consists of nine sections and establishes the Public Company Accounting Oversight Board, to provide independent oversight of public accounting firms providing audit services (“auditors”). It also creates a central oversight board tasked with registering auditors, defining the specific processes and procedures for compliance audits, inspecting and policing conduct and quality control, and enforcing compliance with the specific mandates of SOX.

## 2. Auditor Independence

Title II consists of nine sections and establishes standards for external auditor independence, to limit conflicts of interest. It also addresses new auditor approval requirements, audit partner rotation, and auditor reporting requirements. It restricts auditing companies from providing non-audit services (e.g., consulting) for the same clients.

## 3. Corporate Responsibility

Title III consists of eight sections and mandates that senior executives take individual responsibility for the accuracy and completeness of corporate financial reports. It defines the interaction of external auditors and corporate audit committees, and specifies the responsibility of corporate officers for the accuracy and validity of corporate financial reports. It enumerates specific limits on the behaviors of corporate officers and describes specific forfeitures of benefits and civil penalties for non-compliance. For example, Section 302 requires that the company's "principal officers" (typically the Chief Executive Officer and Chief Financial Officer) certify and approve the integrity of their company financial reports quarterly.

## 4. Enhanced Financial Disclosures

Title IV consists of nine sections. It describes enhanced reporting requirements for financial transactions, including off-balance-sheet transactions, pro-forma figures and stock transactions of corporate officers. It requires internal controls for assuring the accuracy of financial reports and disclosures, and mandates both audits and reports on those controls. It also requires timely reporting of material changes in financial condition and specific enhanced reviews by the SEC or its agents of corporate reports.

## 5. Analyst Conflicts of Interest

Title V consists of only one section, which includes measures designed to help restore investor confidence in the reporting of securities analysts. It defines the codes of conduct for securities analysts and requires disclosure of knowable conflicts of interest.

## 6. Commission Resources and Authority

Title VI consists of four sections and defines practices to restore investor confidence in securities analysts. It also defines the SEC's authority to censure or bar securities professionals from practice and defines conditions under which a person can be barred from practicing as a broker, advisor, or dealer.

## 7. Studies and Reports

Title VII consists of five sections and requires the Comptroller General and the SEC to perform various studies and report their findings. Studies and reports include the effects of consolidation of public accounting firms, the role of credit rating agencies in the operation of securities markets, securities violations, and enforcement actions, and whether investment banks assisted Enron and others to manipulate earnings and obfuscate true financial conditions.

## 8. Corporate and Criminal Fraud Accountability

Title VIII consists of seven sections and is also referred to as the “Corporate and Criminal Fraud Accountability Act of 2002”. It describes specific criminal penalties for manipulation, destruction or alteration of financial records or other interference with investigations, while providing certain protections for whistle-blowers.

## 9. White Collar Crime Penalty Enhancement

Title IX consists of six sections. This section is also called the “White Collar Crime Penalty Enhancement Act of 2002.” This section increases the criminal penalties associated with white-collar crimes and conspiracies. It recommends stronger sentencing guidelines and specifically adds failure to certify corporate financial reports as a criminal offense.



**Empowering People.  
Improving Business.**

BI Norwegian Business School is one of Europe's largest business schools welcoming more than 20,000 students. Our programmes provide a stimulating and multi-cultural learning environment with an international outlook ultimately providing students with professional skills to meet the increasing needs of businesses.

BI offers four different two-year, full-time Master of Science (MSc) programmes that are taught entirely in English and have been designed to provide professional skills to meet the increasing need of businesses. The MSc programmes provide a stimulating and multi-cultural learning environment to give you the best platform to launch into your career.

- MSc in Business
- MSc in Financial Economics
- MSc in Strategic Marketing Management
- MSc in Leadership and Organisational Psychology

**BI NORWEGIAN BUSINESS SCHOOL**

EFMD  
**EQUIS**  
ACCREDITED

[www.bi.edu/master](http://www.bi.edu/master)

## 10. Corporate Tax Returns

Title X consists of one section. Section 1001 states that the Chief Executive Officer should sign the company tax return.

## 11. Corporate Fraud Accountability

Title XI consists of seven sections. Section 1101 recommends a name for this title as “Corporate Fraud Accountability Act of 2002”. It identifies corporate fraud and records tampering as criminal offenses and joins those offenses to specific penalties. It also revises sentencing guidelines and strengthens their penalties. This enables the SEC to resort to temporarily freezing transactions or payments that have been deemed “large” or “unusual”.

Non-compliance with SOX law would mean the penalty of 5,000,000 USD or 20 years in prison or both. The SOX law changed the way how the companies understood their risks assigned to financial reporting operations. To meet all these newly imposed rough conditions, all eligible companies were required to comply with five key principles:

- Brighter financial reporting risk management.
- Careful mapping of the financial processes.
- Creation of internal controls.
- Definition of Process Owner within the company.
- Definition of Control Owner within the company.

## 6.7 EVOLUTION OF SOX

As each human invention may grow over time, the SOX completed its own development within a few years. These are the key development stages:

### SOX302

The essence of Section 302 of the Sarbanes-Oxley Act states that the CEO and CFO are directly responsible for the accuracy, documentation and submission of all financial reports as well as the internal control structure to the SEC. Periodic statutory financial reports are to include certifications that the signing officers are responsible for internal controls and have evaluated these internal controls within the previous ninety days and have reported on their findings; a list of all deficiencies in the internal controls and information on any fraud that involves employees who are involved with internal activities; and any significant changes in internal controls or related factors that could have a negative impact on the internal controls.

## **SOX404**

Section 404 is the most complicated, most contested, and most expensive to implement of all the Sarbanes-Oxley Act sections for compliance. All annual financial reports must include an Internal Control Report stating that management is responsible for an “adequate” internal control structure, and an assessment by management of the effectiveness of the control structure. Any shortcomings in these controls must also be reported. In addition, registered external auditors must attest to the accuracy of the company management assertion that internal accounting controls are in place, operational and effective. Issuers are required to publish information in their annual reports concerning the scope and adequacy of the internal control structure and procedures for financial reporting. This statement shall also assess the effectiveness of such internal controls and procedures. The registered accounting firm shall, in the same report, attest to and report on the assessment on the effectiveness of the internal control structure and procedures for financial reporting.

## **SOX906**

Section 906 addresses criminal penalties for certifying a misleading or fraudulent financial report. Under SOX 906, penalties can be upwards of \$5 million in fines and 20 years in prison or both. Section 906 certifications must accompany a company’s periodic report. It is unclear whether Congress intended the certifications to be “filed” as part of a periodic report or submitted along with a periodic report as supplemental materials.

## **6.8 COSO**

The introduction of such a massive regulation tool required the implementation of a special coordination legal body. The purpose of this newly established organization was to educate and manage the coordination of implementation of SOX principles.

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) is a joint initiative of five private sector organizations and is dedicated to providing thought leadership through the development of frameworks and guidance on enterprise risk management, internal control and fraud deterrence. [3]



Fig. 7 COSO cube source: [COSO.com](http://COSO.com)

The COSO framework still provides for three categories of objectives – operations, reporting, and compliance – and still consists of five integrated components of internal control – control environment, risk assessment, control activities, information and communication, and monitoring activities.

## Need help with your dissertation?

Get in-depth feedback & advice from experts in your topic area. Find out what you can do to improve the quality of your dissertation!

[Get Help Now](#)



Go to [www.helpmyassignment.co.uk](http://www.helpmyassignment.co.uk) for more info





The COSO framework continues to be adaptable to a given organization's structure, allowing you to consider internal controls from an entity, divisional, operating unit, and/or functional level, such as for a shared services center. Finally, the important role of management judgment in designing, implementing, and maintaining internal control, as well as assessing its effectiveness, is retained.

### **Control Environment**

1. Demonstrates commitment to integrity and ethical values.
2. Exercises oversight responsibility.
3. Establishes structure, authority, and responsibility.
4. Demonstrates commitment to competence.
5. Enforces accountability.

### **Risk Assessment**

6. Specifies suitable objectives.
7. Identifies and analyzes risk.
8. Assesses fraud risk.
9. Identifies and analyzes significant change.

### **Control Activities**

10. Selects and develops control activities.
11. Selects and develops general controls over technology.
12. Deploys through policies and procedures.

### **Information and Communication**

13. Uses relevant information.
14. Communicates internally.
15. Communicates externally.

### **Monitoring**

16. Conducts ongoing and/or separate evaluations.
17. Evaluates and communicates deficiencies. [4]

The Sarbanes-Oxley Act (SOX) and all its consequences represent a major change for the world's top corporations. More than a decade after its implementation, some American economists are raising critical voice against SOX. According to them, there is no direct evidence the full implementation of all necessary changes might prevent a company from committing fraud or financial reporting failure.

The implementation of the Sarbanes-Oxley Act into every existing company is a huge and long term investment that draws a lot of financial resources from the cash flow. The implementation and maintenance of a fully functional environment also requires high human resources investments and special fees for external consultants.

To avoid this, many companies have decided to de-list their stocks from the NYSE or prepare their IPOs in cooperation with non-U.S. stock exchanges.

The message is clear. Such companies are trying to avoid huge financial investments and they are likely listed in Frankfurt, London or any major Asian stock exchange. The future of the formal applicability very much depends on the future political and economic situation in the USA. If the future President of the United States initiates such a change, companies with implemented and assessed internal controls would use the COSO principles. However, all newly established companies might create some form of a controlled environment partly based on the previous formal principles because every stakeholder might appreciate some kind of relative assurance that things are as they should be. But the face of business will change one day.

## 7 COMPLIANCE

Compliance or acting according to a set of rules is a fact of doing business whether you are a business owner, executive, HR manager or sales representative. Navigating the path to compliance requires proactive planning and organization but does not have to be overwhelming. Compliance is a multifaceted and complex matter. It requires a well-thought-out plan with the right policies and procedures in place to ensure requirements are met in a timely manner and a pristine record-keeping system to document those procedures. Depending upon the size and focus of your business, you may opt to have an in-house compliance professional or entire department working to identify, prevent, monitor, resolve and advice with regard to compliance risks.

### 7.1 DEFINITION OF COMPLIANCE

The concept of legal compliance is not only a legal but also a corporate category that generally means the definition and adherence to ethical and legal rules of conduct by a business or business group (corporation) and its employees not only in the sphere of purely commercial relations, but also in other areas of its activity and existence.



Brain power

By 2020, wind could provide one-tenth of our planet's electricity needs. Already today, SKF's innovative know-how is crucial to running a large proportion of the world's wind turbines.

Up to 25 % of the generating costs relate to maintenance. These can be reduced dramatically thanks to our systems for on-line condition monitoring and automatic lubrication. We help make it more economical to create cleaner, cheaper energy out of thin air.

By sharing our experience, expertise, and creativity, industries can boost performance beyond expectations. Therefore we need the best employees who can meet this challenge!

The Power of Knowledge Engineering

Plug into The Power of Knowledge Engineering.  
Visit us at [www.skf.com/knowledge](http://www.skf.com/knowledge)

**SKF**

The purpose of defining these standardized rules of corporate behavior accepted voluntarily in the form of binding internal regulations of the company, generally referred to as corporate compliance, is in fact a particularly clear and explicit declaration of “corporate liability” both externally and internally.

The conduct of business and other related relations are in full compliance with all ethical and legal rules on competition, financial and fiscal integrity, environmental protection and employee relations, including ensuring equal opportunities.

## **7.2 DEFINITION OF RISK COMPLIANCE**

Risk compliance is compliance with the requirements defined by law, regulation authorities and best practices in the field. Risk compliance means that a company has its risks under control and has a system that prevents the risk from growing.

Compliance risk is defined as the risk of legal sanctions, material financial loss, or loss to reputation a company may suffer as a result of its failure to comply with laws, its own regulations, code of conduct, and standards of best/good practice.

## **7.3 DEFINITION OF CORPORATE COMPLIANCE**

In a broader context, corporate compliance can be perceived as an integral part of a broader category called “Corporate Social Responsibility” (CSR) which is gradually starting to be considered one of the decisive factors that strongly influences a company’s economic success.

From the perspective of the company (group) as a competitor, illegal or even unethical behavior can bring, for example, immediate negative legal and business consequences (legal penalties, criminal prosecution, immediate termination of business relationships).

Any failure on the part of the management and control system of the company may ultimately result in a fundamental threat to its social credibility with a possibly fatal impact on the further development of its business and existence itself.

## **7.4 WHAT IS COMPLIANCE**

- The company assets meet the legal requirements.
- The company has developed the required mechanisms.
- Employees of the company perform their activities in compliance with applicable laws.
- The company honors its commitments to the state or location.

Compliance is either a state of being in accordance with established guidelines or specifications, or the process of becoming so. The definition of compliance can also encompass efforts to ensure that organizations are abiding by both industry regulations and government legislation [7].

In real life, the term compliance would mean the organization is willing to invest financial and human resources in a process that guarantees legal business operations.

The purpose of a compliance program is to encourage cultural and ethical conduct towards compliance with the law. Every corporate compliance program should be focused on risk identification, standards, procedures and controls. This might be supported by various training in communication with focus on aspects such as discipline and proper reporting.

Compliance set-up has an implementation phase and a maintenance phase. What are the major common mistakes which may arise during implementation of a corporate compliance program? There could be failures in identifying and quantifying material risks, failures while delivering on multi-level management commitments, failure based on the wrong integration of any of the corporate functions and, last but not least, also failure in providing fair remuneration to employees.

Similarly, there are critical mistakes which may arise in the maintenance phase. What might such mistakes be? There could be mistakes such as a failure to monitor the effectiveness of the compliance program, failure to keep senior management informed, failure to properly train employees, and failure to report violation of compliance rules.

## 7.5 WHAT IS NON-COMPLIANCE

- The company is involved in corruption.
- The company infringes competition rules.
- The company concluded a market sharing agreement.
- The company violates the prudent fiduciary principle.
- The company falsely informs about the properties of the product.

All compliance activities are generally supported by auditors who play a role in the audit. The key purpose and meaning of the audit is to express an independent opinion in line with international audit standards. This independent opinion is delivered by a qualified and independent auditor based on the reliability of the financial reports.

Due to the issues of non-compliance with valid regulations, a company may face legal consequences, penalties and other road-blockers. CFOs and CEOs are adequately informed about the costs of non-compliance. The outcomes of non-compliance might be in the form financial penalties, brand or reputation damage, loss of shareholder confidence, business disruptions or forced change in the strategic direction of the core business. The costs of non-compliance are not just financial. There are many more reasons to make sure the company complies with all the valid regulations because there is a lot at stake.

## 7.6 WHO IS AN AUDITOR

An auditor is a person who is authorized to perform audit activities, which includes carrying out statutory audits, management review, verification of accounting records and other economic information. This requires great theoretical and practical knowledge in the field of accounting and reporting in their current form and related legislation. Moreover, an auditor must be independent and abide by professional ethics.

Adherence to these principles is controlled by the Chamber of Auditors of the Czech Republic, a membership in which is mandatory for every auditor.

# TURN TO THE EXPERTS FOR SUBSCRIPTION CONSULTANCY

Subscribe is one of the leading companies in Europe when it comes to innovation and business development within subscription businesses.

We innovate new subscription business models or improve existing ones. We do business reviews of existing subscription businesses and we develop acquisition and retention strategies.

Learn more at [linkedin.com/company/subscribe](https://www.linkedin.com/company/subscribe) or contact Managing Director Morten Suhr Hansen at [mha@subscribe.dk](mailto:mha@subscribe.dk)

**SUBSCRIBE** - to the future

The auditor verifies that the information in the financial statements present fairly the assets and liabilities, financial position and results of the company in accordance with the rules described by any accounting regulations.

## 7.7 AUDIT RUN

The basis for the auditor's work is permanent and close contact with the client in order to obtain the maximum amount of information possible in order to assess the current situation, identify deficiencies and inaccuracies, and propose methods for their removal in order to give a positive audit opinion.

This objective is achieved by conducting an audit of financial statements in the form of intermediate and internal audits, which focus on the gaps in accounting procedures, document circulation, internal control, financial liquidity, which ensures that any identified deficiencies and inaccuracies are continually repaired and the level of accounting is constantly increasing throughout the year.

The main outcome of an audit run is an audit report. An audit report summarizes all findings of the audit team from the audit. The audit report also contains proposed corrective actions which are normally pre-discussed with the management of the audited company.

The audit report should be signed by the lead auditor and the CEO of the audited company as well. All audit findings and corrective actions must be formally accepted by the time of the sign-off. The management of the audited company has 12 months to improve the internal processes and on-site practices to address the finding in the audit report.

Each and every audit has five phases:

1. Initial meeting

During the initial meeting, the lead auditor introduces the members of the audit team and explains the planned scope and purpose of the audit. The audit team informs the management of the audited company about the duration of the audit and the level of the required support and assistance.

2. Audit activities

Individual audit specialists carry out their individual audit search activities. They are mainly "shadowing" the key audited process functions and re-performance of the key activities. The purpose is to complete their own independent check regarding the validity of the audited systems and procedures.



### 3. Monitoring the findings

Every day, the audit team members save and consult their findings from their individual audit trials. The lead auditor manages the interpretation of the findings and makes sure they are correctly assessed.

### 4. Completion of audit activities

When all on-site audit activities are completed, the audit team no longer requires assistance and support from the staff of the audited company. In other words, the auditors are not searching for more evidence anymore and they are concentrating on the preparation of the audit report. The management of the audited company is formally informed about all major findings.

### 5. Closing meeting

During this meeting, the lead auditor summarizes the overall opinion of the audited processes and informs the management about the audit statement which will be in the audit report. The management of the audited company formally accepts the audit report and becomes familiar with it. At the end of the meeting, the date of the remediation audit might be discussed.

## 7.8 AUDIT STATEMENTS

The most important part of the audit report is the overall statement issued by the auditor at the end of the audit activities. The statement itself shows the level of satisfaction of the auditor with the compliance principles, internal process descriptions, internal operation manuals and instructions and the real life practice. There are four types of opinions which the auditor may issue:

### *Qualified Opinion*

The auditor shall express a qualified opinion when having obtained sufficient appropriate audit evidence, concludes that misstatements, individually or in the aggregate, are material, but not pervasive, to the financial statements; or the auditor is unable to obtain sufficient appropriate audit evidence on which to base the opinion, but the auditor concludes that the possible effects on the financial statements of undetected misstatements, if any, could be material but not pervasive.

### *Adverse Opinion*

The auditor shall express an adverse opinion when the auditor, having obtained sufficient appropriate audit evidence, concludes that misstatements, individually or in the aggregate, are both material and pervasive to the financial statements.

*Disclaimer of Opinion*

The auditor shall disclaim an opinion when the auditor is unable to obtain sufficient appropriate audit evidence on which to base the opinion, and the auditor concludes that the possible effects on the financial statements of undetected misstatements, if any, could be both material and pervasive.

The auditor shall disclaim an opinion when, in extremely rare circumstances involving multiple uncertainties, the auditor concludes that, notwithstanding having obtained sufficient appropriate audit evidence regarding each of the individual uncertainties, it is not possible to form an opinion on the financial statements due to the potential interaction of the uncertainties and their possible cumulative effect on the financial statements.

*Consequence of an Inability to Obtain Sufficient Appropriate Audit Evidence Due to Management-Imposed Limitation after the Auditor Has Accepted the Engagement*

If, after accepting the engagement, the auditor becomes aware that management has imposed a limitation on the scope of the audit that the auditor considers likely to result in the need to express a qualified opinion or to disclaim an opinion on the financial statements, the auditor shall request that management remove the limitation.



What do you want to do?

No matter what you want out of your future career, an employer with a broad range of operations in a load of countries will always be the ticket. Working within the Volvo Group means more than 100,000 friends and colleagues in more than 185 countries all over the world. We offer graduates great career opportunities – check out the Career section at our web site [www.volvogroup.com](http://www.volvogroup.com). We look forward to getting to know you!

**VOLVO**  
AB Volvo (publ)  
[www.volvogroup.com](http://www.volvogroup.com)

VOLVO TRUCKS | RENAULT TRUCKS | MACK TRUCKS | VOLVO BUSES | VOLVO CONSTRUCTION EQUIPMENT | VOLVO PENTA | VOLVO AERO | VOLVO IT  
VOLVO FINANCIAL SERVICES | VOLVO 3P | VOLVO POWERTRAIN | VOLVO PARTS | VOLVO TECHNOLOGY | VOLVO LOGISTICS | BUSINESS AREA ASIA

If management refuses to remove the limitation, the auditor shall communicate the matter to those charged with governance, unless all of those charged with governance are involved in managing the entity and determine whether it is possible to perform alternative procedures to obtain sufficient appropriate audit evidence.

If the auditor is unable to obtain sufficient appropriate audit evidence, the auditor shall determine the implications as follows: If the auditor concludes that the possible effects on the financial statements of undetected misstatements, if any, could be material but not pervasive, the auditor shall qualify the opinion.

If the auditor concludes that the possible effects on the financial statements of undetected misstatements, if any, could be both material and pervasive so that a qualification of the opinion would be inadequate to communicate the gravity of the situation, the auditor shall withdraw from the audit, where practicable and possible under the applicable law or regulation. If withdrawal from the audit before issuing the auditor's report is not practicable or possible, disclaim an opinion on the financial statements.

## **7.9 HOW TO DEAL WITH AUDITORS**

A fair approach and open communication are crucial for an effective audit run. Nowadays, auditors require a lot of various financial documentation before the audit starts to create a global picture of the key financial position of the audited company, its liabilities and receivables, and its key customers and projects. It is important to deliver all types of the required information because it supports specialized audit software which automatically detects any possible pitfalls.

Auditors should be treated by the management and staff of the audited company as a special kind of internal advisors and their smooth work heavily depends on the flow of the required information. In case the auditors ask direct or open questions, please do not be shy to answer them. The audited staff should explain work processes, deliver the required evidence supporting the current workflow and make sure that evidence is in line with manuals and valid work instructions.

## 8 PROCESS DRIVEN ORGANIZATIONS AND OPERATION EXCELLENCE PRINCIPLES

This section focuses on the overall principles of key processes within an organization and the idea of Operation Excellence which is a major driver on the path to the success for many companies.

Process driven organizations are the exact opposite of people driven organization. This relies on the principles of corporate law which states that any organization is a separate entity which has come into existence. Its existence is different from and not dependent on the existence of its promoters. It is an artificial person created by law.

The very idea of thinking about organizations as an abstract creature brings to mind exciting ideas. It is about creating an organization which has perpetual succession (never-ending life) and is not bound by constraints of time, skill and morality of its members.

Any multinational corporation that you see is the embodiment of this process approach. It is because they are not bound by human limitations that they can operate in many continents across the globe simultaneously. These organizations grow in terms of knowledge, scale of operations and efficiency irrespective of the contribution of their members.

It must be understood that an organization is not completely independent of people. Otherwise Unilever would be a mega robot, not a mega corporation! These organizations require contribution from laborers in the form of energy to get work done as well as the basic mental acumen to follow the series of instructions tabled as the “best practice”. This can be done by every other person therefore the reduction in dependency on specific people.

Here are some of the principles of process driven organizations:

*Institutionalized Knowledge:* The knowledge of a process driven organization lies not in its people but in the system. The organization scans the environment to update its best practices with regards to every activity that needs to be performed. This procedure is then explicitly documented. Any literate person with basic domain knowledge can read and follow a series of steps. In recent years, even computers have been programmed to do so and automation of tasks has become possible.

*No Limits on Time:* A process driven organization has virtually unlimited time. Since there is a mechanism created to transfer the skill from the system to any person as and when required, the system can expand almost endlessly. This means that if a process driven organization finds constraints on its labor hours, it can simply hire new people and train them as opposed to people driven organizations which would have to forego the opportunity.

*Self-Governing Mechanism:* A process driven organization exercises control through various actors and systems in the organization. Data regarding various activities is compiled and measured on a regular basis to prevent any immoral acts. Behavior of the system is governed by a set of pre-determined rules and policies.

**gaiteye**<sup>®</sup>  
Challenge the way we run

**EXPERIENCE THE POWER OF FULL ENGAGEMENT...**

**RUN FASTER.  
RUN LONGER..  
RUN EASIER...**

**READ MORE & PRE-ORDER TODAY  
WWW.GAITEYE.COM**

*Easy Replication:* The best feature of a process driven organization is that it can be easily replicated. Hence if an organization wanted to replicate its operations in another continent, it could take the same system and implement it with minor modifications. This gives the organizations an edge. Scalability is an important characteristic for the organization to grow and function in the long run.

## 8.1 PROCESS DEFINITION

The process is a generic term for progressive step-by-step encapsulated activities which have defined beginning and the end. Transformation of material, financial and informational resources into a brand new product is made through processes. Each and every process requires defined inputs which may come from the previous processes and exact outputs needed by another processes.

Complicated processes could be split into several sub-processes. Every process has to be described in the form of a standardized style (workflow charts or text description) and authorized by the process owner.

## 8.2 ORGANIZATION AND PROCESSES

There are several options how an organization could define its processes within the correct organization framework. Here are the common phases:

- a) Processes are defined by the needs of the organization.

Every organization focused on its efficient productivity has to organize its resources according to the business needs which means delivering what the customer needs. To fulfill this primary target, the organization should have evidence about its own work flows and potential cooperation channels. Processes may differ in terms of complexity, length and internal cooperation. The most important aspect is that proper process mapping might help the organization define core business and side business.

- b) Processes are results of the evolution of administration of the organization.

When organization is small, the need for proper process definition and evidence is not so hot. As the organization grows, the need for clearly defined internal or external suppliers will arise. After some time, there is a need to have defined processes and relevant documentation. Good, adequate or plain process description is a sign of the maturity of the organization.



c) Processes have its own history.

Version identification should be used for every process description. In combination with the validity date, it makes life easier for newcomers, auditors or newly appointed management. When reviewing the process using the history of changes, improvement might be visible.

d) Processes are changeable.

Each and every process may be changed if such a need exists. New software, new technologies, new production technology might trigger the process change. Keeping one process map for a long time shows a low interest in process administration and addressing adopted changes.

### **8.3 EXECUTIVE PROCESSES**

Executive processes are focused purely on the overall delivery of the expected results. Executive processes are driven and controlled by the appointed managers who are responsible for their execution. Executive processes are associated with quality issues and their role is to transform the resources into the final product.

Example: steel production, software project delivery, car assembly line.

### **8.4 MANAGERIAL PROCESSES**

These processes are focused purely on planning, control and management. Appointed managers are controlling the progress according to their reporting lines (development of a new products, production volume and profitability of production).

Example: development of a new product, production volume, profitability of production.

### **8.5 SUPPORTIVE PROCESSES**

These processes are focused purely on the full support for all internal customers. It means the key function is to deliver all the necessary goods or services required for the completion of the final product or service. Supportive processes can be outsourced.

Example: procurement, stock management, logistic services.



## 8.6 OPERATIONAL EXCELLENCE

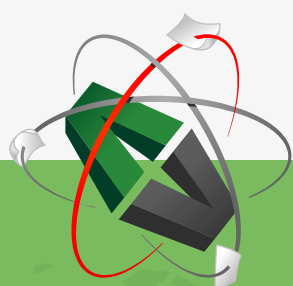
The Operational Excellence (OpEx) is a managerial approach based on the process-oriented organizational culture. The key enabler for the OpEx is the departmental and divisional structure based on their inter-connections and information workflow. In the event that the organization has a rock solid purely administrative culture, the principles of Operation Excellence would not be easy to implement. It means that management structures should ignore the traditional hierarchical organizational structures and give responsibilities to individual employees.

An organization heading to the Operation Excellence (OpEx) will use the business processes as the basic ground of the management. Business processes are the natural sequences of activities of information flows across the organization.

The Operation Excellence is based on three basic conditions:

1. Repeatability
2. Predictability
3. Measurability

This e-book  
*is made with*  
**SetaPDF**



PDF components for PHP developers

[www.setasign.com](http://www.setasign.com)

World class companies are able to measure themselves and be informed about their actual capacity to perform their tasks. The fact that their business processes are organized and documented gives them a high potential to have efficient management.

The Operational Excellence (OpEx) is a risk mitigation tool because it eliminates failure or improvisation within the standard operations.

Operational Excellence (OpEx) is a critical driver for business success and a key part of an enterprise execution strategy. Operational Excellence is defined as the systematic management of process safety, personal safety and health, environment, reliability and efficiency to achieve world-class performance.

Operational Excellence is the pursuit of conducting business in a manner that continuously improves the quality of goods and services. It is reduced to achieve competitive superiority. From a core manufacturing point of view, there are three pillars of operational excellence; they are production planning and control, manufacturing execution and operational effectiveness of people, processes and assets. Tight coordination among these three pillars is required in order to achieve overall operational excellence.

Operational excellence is a systematic approach to attaining world-class performance in productivity, quality and delivery of services and/or goods. It is the goal of achieving superior yields, lead time and through-put while eliminating waste.

Operational Excellence is normally centered across the following three main pillars:

### **Production Planning and Control**

In the production planning phase, production plans and schedules are driven by accurate demand capture/forecasting capabilities. The production planning takes into account business objectives and manufacturing and supply constraints in order to maintain required inventory levels and certain pre-defined service levels. The production schedule executed at the plant level needs to keep the plan in sync with the entire supply chain plan, ensuring optimal asset utilization. In this phase, one often needs to manage supplier quality and deviations between forecasts and planned deliveries. Additionally, one needs to know what got executed so that changes can be made to the production plans in the planning stage. This would necessitate real-time visibility into operations, resources and assets.

### **Manufacturing Execution**

The business capability required in this phase would be the ability to generate feasible and executable production schedules that take into account bottleneck information from the shop floor in real time. It should have adequate quality controls embedded for in-process and finished goods inspection. It should have the ability to adapt to scheduled changes and to react to unplanned downtimes. Additionally, it requires a mechanism to minimize deviations in quality, performance and occurrence of downtimes along with means to analyze root causes so as to avoid recurrences. Apart from production execution capabilities the ability to comply with the regulatory and corporate requirements need to be put in place. A complete traceability and genealogy functionality needs to be enabled as the products move through the manufacturing value chain. Finally, execution details such as consumption, yield, deviation, etc. need to be communicated with the enterprise systems in order to close the loop for the production plans.

### **Operational Effectiveness of People, Processes and Assets**

In addition to planning and execution, the effectiveness of people, processes and assets plays an important role in overall operational excellence. The overall equipment effectiveness (OEE) of assets needs to be monitored at the plant level. OEE consists of availability, performance and quality. Availability reflects equipment and process uptime; performance reports the speed of production as compared with design standards; quality indicates process yield through that equipment. These elements constitute a benchmark for the manufacturing asset's effectiveness. Similarly, processes need to be leaner, agile and adaptable to change with no waste or non-value added activities. Finally, people need to be empowered, trained and provided with the right amount of data so as to successfully perform their job functions within the organization.

More often than not, we find that these three pillars operate in functional silos with little or no coordination. Different systems and software are used to enable these processes. These systems include various Enterprise systems (ERP, SCM), plant floor IT systems (MES, LIMS, QMS) and process control and automation systems (SCADA, PLC, DCS). While disparate point solutions are required to address critical functionalities associated with planning, asset management, quality and execution, without interoperability and integration it is extremely difficult, if not impossible, to drive operational excellence in an on-going manner. A holistic approach that takes unified systems view, is critical in the drive towards an overall continuous performance improvement.

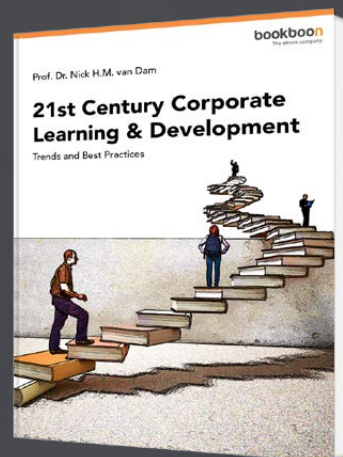


Fig. 8 Operation Excellence principles source: [www.faberinfinite.com](http://www.faberinfinite.com)

# Free eBook on Learning & Development

By the Chief Learning Officer of McKinsey

**Download Now**



Download free eBooks at [bookboon.com](http://bookboon.com)

**Click on the ad to read more**

Some key benefits achieved by the process industry in the course of its journey toward of operational excellence are:

*End-to-Visibility into Operations:*

1. complete transparency across the value chain,
2. reduced costs by cost-effectively and efficiently managing the end-to-end operational processes,
3. accelerated decision making with complete visibility into operations performance,
4. actionable data for the right person at the right time

*Highly Efficient Operations:*

1. integrated and standardized operations,
2. automated tasks, alerts, notifications for proactive resolution,
3. fast access to relevant data from multiple sources

*Compliant Operations:*

1. Reduced cost of quality (rejects, reworks, etc.).
2. Reduced cost of compliance.
3. Delivering high-quality products and services with integrated quality standards.
4. Integrated quality management with operations, ensuring regulatory, legal and environmental standards.

*Industry Leadership:*

1. improved customer service by delivering on promises,
2. sustained superior performance by ensuring continuous improvement of processes,
3. easy adoption of initiatives such as Lean, Six Sigma, etc.
4. ability to innovate industry best practices

## **8.7 KEY PERFORMANCE INDICATORS (KPIs)**

A key performance indicator (KPI) is a business metric used to evaluate factors that are crucial to the success of an organization. KPIs differ per organization; business KPIs may be net revenue or a customer loyalty metric, while government might consider unemployment rates.

KPIs are applied in business intelligence (BI) to gauge business trends and advise tactical courses of action. Before KPIs can be identified, the following requirements must be met:

- a predefined organizational process,
- clear business objectives for the process,
- quantitative and qualitative measurements,
- an active approach to finding and remedying enterprise variances.

KPIs are above all else, a set of indicators to measure data against, a sort-of enterprise success gauge. Ultimately, they help an organization assess progress toward declared goals.

### **Customer Metrics**

**Customer Lifetime Value (CLV):** Minimizing cost is not the only (or the best) way to optimize your customer acquisition. CLV helps you look at the value your organization is getting from a long-term customer relationship. Use this performance indicator to narrow down which channel helps you gain the best customers for the best price.

**Customer Acquisition Cost (CAC):** Divide your total acquisition costs by the number of new customers in the time frame you are examining. Voila! You have found your CAC. This is considered one of the most important metrics in e-commerce because it can help you evaluate how cost effective your marketing campaigns have been.

**Customer Satisfaction & Retention:** On the surface, this is simple: make the customer happy and they will continue to be your customer. Many firms argue, however, that this is more for shareholder value than it is for the customers themselves. You can use multiple performance indicators to measure CSR, including customer satisfaction scores and percentage of customers repeating a purchase.

**Net Promoter Score (NPS):** Finding out your NPS is one of the best ways to indicate long-term company growth. To determine your NPS score, send out quarterly surveys to your customers to see how likely it is that they will recommend your organization to someone they know. Establish a baseline with your first survey and put measures in place that will help those numbers grow quarter to quarter.

**Number of Customers:** Similar to profit, this performance indicator is fairly straightforward. By determining the number of customers you have gained and lost, you can further understand whether or not you are meeting your customers' needs.

## Process Metrics

**Customer Support Tickets:** Analysis of the number of new tickets, the number of resolved tickets, and resolution time will become the best customer service department in your industry.

**Percentage of Product Defects:** Take the number of defective units and divide it by the total number of units produced in the time frame you are examining. This will give you the percentage of defective products. Clearly, the lower you can get this number, the better.

**OB Efficiency Measure:** Efficiency can be measured differently in every industry. Let's use the manufacturing industry as an example. You can measure your organization's efficiency by analyzing how many units you have produced every hour, and what percentage of time your plant was up and running.

## People Metrics

**Employee Turnover Rate (ETR):** To arrive upon your ETR, take the number of employees who have departed the company and divide it by the average number of employees. If you have a high ETR in your department, spend some time examining your workplace culture, employment packages, and work environment.



www.sylvania.com

We do not reinvent  
the wheel we reinvent  
light.

Fascinating lighting offers an infinite spectrum of possibilities: Innovative technologies and new markets provide both opportunities and challenges. An environment in which your expertise is in high demand. Enjoy the supportive working atmosphere within our global group and benefit from international career paths. Implement sustainable ideas in close cooperation with other specialists and contribute to influencing our future. Come and join us in reinventing light every day.

Light is OSRAM

OSRAM  
SYLVANIA



**Percentage of Response to Open Positions:** When you have a high percentage of qualified applicants apply for your open job positions, you know you are doing a good job maximizing exposure to the right job seekers. This will lead to an increase in interviewees, as well.

**Employee Satisfaction:** Happy employees are going to work harder – it is as simple as that. Measuring your employee satisfaction through surveys and other metrics is vital to your departmental and organizational health.

The right KPIs for you might not be the right KPIs for another organization. Make sure you have researched as many key performance indicator examples as you can to determine which ones are appropriate for your industry. From there, determine which KPIs will help you further understand and meet your goals, and then integrate them throughout your department. KPIs should match your strategy, not just your industry.

## 8.8 KEY RISK INDICATORS (KRI)

The Key Risk Indicators (KRI) metrics can be considered, which help to determine the direction from where the risks are coming, so they are extremely useful in any enterprise. A key risk indicator is a measure which indicates the level or trend of risk.

The metric can identify the deviation or likely deviation from the target for a strategic objective of the enterprise. By measuring the value of metrics, risk metrics are used to warn in advance that the next strategic objective metric is unfavorable.

It is very important to choose the right number of metrics. If an enterprise implements too many metrics, managing these will steal from the time allocated for other tasks and will provide too much information to shareholders. They will end up not to distinguish critical information and the system will provide information of limited value. On the other hand, if too few metrics are implemented, the decision making process will be difficult, since there is no critical information. KRI metrics cannot provide value unless measured, because you cannot control what you cannot measure.

## 9 INTERNAL CONTROLS AND RISK MITIGATION

Risk is the probability that an event or action will adversely affect the organization. The primary categories of risk are errors, omissions, delay and fraud. In order to achieve goals and objectives, management needs to effectively balance risks and controls. Therefore, control procedures need to be developed so that they decrease risk to a level where management can accept the exposure to that risk. By performing this balancing act, “reasonable assurance” can be attained.

In order to achieve a balance between risk and controls, internal controls should be proactive, value-added, and cost-effective and address exposure to risk.

There are generally three requirements for fraud to occur – motivation, opportunity and personal characteristics. Motivation is usually situational pressure in the form of a need for money, personal satisfaction, or to alleviate a fear of failure. Opportunity is access to a situation where fraud can be perpetrated, such as weaknesses in internal controls, necessities of an operating environment, management styles and corporate culture. Personal characteristics include a willingness to commit fraud. Personal integrity and moral standards need to be “flexible” enough to justify the fraud, perhaps out of a need to feed their children or pay for a family illness.

It is difficult to have an effect on an individual’s motivation for fraud. Personal characteristics can sometimes be changed through training and awareness programs. Opportunity is the easiest and most effective requirement to address to reduce the probability of fraud. By developing effective systems of internal control, you can remove opportunities to commit fraud.

### **People at every level of an organization affect internal control**

Internal control is, to some degree, everyone’s responsibility. Generally, administrative employees at the department-level are primarily responsible for internal control in their departments. Consequently, the responsibility for controls over accurate financial and reporting primarily falls under the oversight of the institution’s business officers.

### **Effective internal control helps an organization achieve its operations, financial reporting, and compliance objectives**

Effective internal control is a built-in part of the management process (i.e., plan, organize, direct, and control). Internal control keeps an organization on course toward its objectives and the achievement of its mission, and minimizes surprises along the way. Internal control promotes effectiveness and efficiency of operations, reduces the risk of asset loss, and helps to ensure compliance with laws and regulations. Internal control also ensures the reliability of financial reporting (i.e. all transactions are recorded and all recorded transactions are real, properly valued, recorded on a timely basis, properly classified, and correctly summarized and posted).

### **Internal control can provide only reasonable assurance**

It means not absolute assurance regarding the achievement of an organization's objectives. Effective internal control helps an organization achieve its objectives; it does not ensure success. There are several reasons why internal control cannot provide absolute assurance that objectives will be achieved: cost/benefit realities, collusion among employees, and external events beyond an organization's control.



Discover the truth at [www.deloitte.ca/careers](http://www.deloitte.ca/careers)

**Deloitte.**

© Deloitte & Touche LLP and affiliated entities.

Internal controls mitigate risks, decrease fraud, establish standard operating procedures, and organize information. You would probably agree that your business needs to operate seamlessly internally to continuously offer the highest quality of service to your clients. So it is important to have at least a basic understanding of controls.

Many models have been established to help your clients identify and offset control risk. The Sarbanes-Oxley Act of 2002 recommends the Committee of Sponsoring Organizations (COSO) model as a means for companies to identify and mitigate risk that can lead to financial misstatement. The COSO model is just one representation that can be used, and at its heart it guides management through the implementation of a control framework that is measurable and targeted at reducing risk.

## 9.1 DEFINITION

Internal controls are defined by five components of internal controls. These components may answer five key questions – who provides the internal control, what is the key activity of the internal control, why the internal control has been implemented, when the internal control should be made and what is the evidence the internal control has been actioned.

**Control environment:** This term refers to the attitude of the company, management, and staff regarding internal controls. Do they take internal controls seriously, or do they ignore them? Your client's environment is not very good if, during your interviews with management and staff, you see a lack of effective controls or notice that previous audits show many errors.

The control environment sets the tone for the organization and influences how employees conduct their activities and carry out their control responsibilities. The control environment is the foundation for all other components of internal control and provides structure and discipline. Developing a strong culture of control consciousness within the institution is one of the most cost-effective and efficient ways that internal control over financial reporting can be implemented. Its effect can permeate throughout the institution, directly impacting each of the other components of internal control. Among the important factors are the attitude, awareness, and actions of management and directors concerning internal control. The personal characteristics, philosophy, and operating style of members of management can have a significant influence on the organization's commitment to reliable financial reporting.

The following table will provide some guidance on control environment principles (controls) and related control objectives (purpose of controls) as well as possible ways to document that those objectives are being met:


- a) For integrity and ethical values, the control objectives are management, who, through its attitudes and actions, demonstrates character, integrity, and ethical values; sound integrity and ethical values, particularly of top management, are developed and set the standard of conduct for the organization and financial reporting. The relevant documentation could include an employee code of conduct. It also provides a method for reporting violations through whistleblower provisions.
- b) For commitment to completeness, the control objective is the entity's commitment to competence in the requirements of particular jobs and in translating those requirements into knowledge and skills. The relevant documentation could include employee training and evaluation records.
- c) For attention and oversight provided by a board of directors or audit committee, the control objective is to ensure that the board of directors and/or audit committee is actively involved and has significant influence over the entity's internal control environment and its financial reporting. The relevant documentation could include corporate bylaws and formal policies for financial reporting, audit committee reports or whistleblower program and rules.
- d) For management's philosophy and operating style, the control objective is to ensure that the philosophy and operating style are consistent with a sound control environment and have a pervasive effect on the entity, the management analyzes the risks and benefits of new ventures, assesses turnover among employees, investigates and resolves improper business practices, views accounting as a means to monitor and control the various activities of the organization, and adopts accounting policies that reflect the economic realities of the business. The relevant documentation could include the degree of care taken in developing policies and procedures related to financial reporting.
- e) For organizational structure, the control objective is to ensure that the principles of the organizational structure are appropriately designed to promote a sound control environment; and that authority and responsibility, appropriate reporting lines, and free flow of information across the organization provide unfettered influence to effectively run the entity and support effective financial reporting. The relevant documentation could include organizational charts reflecting the roles and responsibilities or defined job duties of key employees.

- f) For the manner of assigning authority and responsibility, the control objective is to ensure that the entity assigns authority and responsibility to provide a basis for accountability and control. The relevant documentation could include clearly defined responsibilities and authority limits (segregation of duties).
- g) For human resources policies and procedures, the control objective is to ensure that human resource policies and procedures send messages to employees regarding expected levels of integrity, ethical behavior, and competence. The relevant documentation could include human resources policy manual, ethics training, formal job descriptions or emphasis on accountability.


An effective control environment is an environment where competent people understand their responsibilities, the limits to their authority, and are knowledgeable, mindful, and committed to doing what is right and doing it the right way. They are committed to following an organization's policies and procedures and its ethical and behavioral standards. The control environment encompasses technical competence and ethical commitment; it is an intangible factor that is essential to effective internal control.

SIMPLY CLEVER

ŠKODA



**We will turn your CV into an opportunity of a lifetime**



Do you like cars? Would you like to be a part of a successful brand? We will appreciate and reward both your enthusiasm and talent. Send us your CV. You will be surprised where it can take you.

Send us your CV on  
[www.employerforlife.com](http://www.employerforlife.com)



## 9.2 SUGGESTIONS FOR EFFECTIVE CONTROL ENVIRONMENT

Listed below are some suggestions to enhance a department/business unit's control environment. This list is not intended to be all-inclusive, or applicable for all departments, however, it should be helpful in promoting an effective control environment.

Make sure that the following policies and procedures are available in your department (hard copy or Internet access): business procedures, employees purchasing manuals, policies and procedures manuals.

Make sure that departments have well-written departmental policies and procedures which address their significant activities and unique issues: employee responsibilities, limits to authority, performance standards, control procedures, and reporting relationships should be clear.

- Make sure that employees are well acquainted with the Institution's policies and procedures that pertain to their job responsibilities.
- Discuss ethical issues with employees. If any employees need additional guidance, make sure that it is provided.
- Make sure that employees comply with the conflict of interest policy and disclose potential conflicts of interest (e.g., ownership interest in companies doing business or proposing to do business with a new customer).
- Make sure that job descriptions exist, clearly state responsibility for internal control, and correctly translate desired competence levels into requisite knowledge, skills, and experience; make sure that hiring practices result in hiring qualified individuals.
- Make sure that the department has an adequate training program for employees.
- Make sure that employee performance evaluations are conducted periodically. Good performance should be valued highly and recognized in a positive manner.
- Make sure that appropriate disciplinary action is taken when an employee does not comply with policies and procedures or behavioral standards.

**Risk assessment:** In a nutshell, you should evaluate whether management has identified its riskiest areas and implemented controls to prevent or detect errors or fraud that could result in material misstatements. For example, has management considered the risk of unrecorded revenue or expense transactions?



The central theme of internal control is to identify risks to the achievement of an organization's objectives and to do what is necessary to manage those risks. Another way of saying this is that risk assessment is the process of setting objectives; prioritizing and linking those objectives; and identifying, analyzing, and managing risks relevant to achieving those objectives.

Risk assessment is the identification and analysis of risks associated with the achievement of operations, financial reporting, and compliance goals and objectives. This, in turn, forms a basis for determining how those risks should be managed.

To properly manage their operations, managers need to determine the level of operational, financial and compliance risk they are willing to assume. Risk assessment is one of management's responsibilities and enables management to act proactively in reducing unwanted surprises. Failure to consciously manage these risks can result in a lack of confidence that operational, financial and compliance goals will be achieved.

A risk is anything that could jeopardize the achievement of an objective. The following are common questions that management should ask themselves to help identify risks:

1. What could go wrong?
2. What assets should we be protecting?
3. How do we protect our assets?
4. What do we do to prevent theft/fraud?
5. What activities are regulated by outside authority (federal or state)?
6. What external exposures do we have?
7. How could someone disrupt operations?
8. How do we know we are achieving our objectives?
9. How would this look to an outsider?

There are several steps in the risk assessment process. First, objectives need to be set before risk assessment begins. Second, management must identify the risks associated with achieving objectives, next management must perform a risk analysis to determine the extent of the risk and how it should be managed, and finally control activities should be implemented to manage risks. As a follow-up step, institutions should have effective monitoring in place to ensure controls are being consistently performed.

For financial reporting, appropriate control objectives would be:

- Entity and financial reporting objectives are established, documented, and communicated.
- Accounting principles are properly applied in the preparation of the financial statements.

For management of financial reporting risks, appropriate control objectives would be:

- Management has established practices for the identification of risks affecting the entity.
- Management considers the entire organization as well as its extended relationships in its risk assessment process.
- Management has implemented mechanisms to anticipate, identify, and react to changes.
- Management evaluates and mitigates risk appropriately.

For consideration of fraud risks, an appropriate control objective would be:

- Management has developed an appropriate fraud risk assessment and monitoring process.

After control objectives are established, management should identify risks that would prevent these objectives from being met. Both external and internal factors affect risk. When an organization identifies and assesses various risks, it is important that the process be comprehensive. In this risk assessment process, the many interrelationships of factors should be considered including relationships between the organization and relevant third parties such as customers, suppliers, regulatory entities, etc.



- The number 1 MOOC for Primary Education
- Free Digital Learning for Children 5-12
- 15 Million Children Reached

**About e-Learning for Kids** Established in 2004, e-Learning for Kids is a global nonprofit foundation dedicated to fun and free learning on the Internet for children ages 5 - 12 with courses in math, science, language arts, computers, health and environmental skills. Since 2005, more than 15 million children in over 190 countries have benefitted from eLessons provided by EFKI. An all-volunteer staff consists of education and e-learning experts and business professionals from around the world committed to making difference. eLearning for Kids is actively seeking funding, volunteers, sponsors and courseware developers; get involved! For more information, please visit [www.e-learningforkids.org](http://www.e-learningforkids.org).

Risks should also be identified at the activity level. Besides contributing to the risk identification process at the organization level, activity level risks also take into account those risks associated with business operations and activities. Listed below are accounts and other disclosure items that are normally significant at the Financial Statement level:

**Balance sheet items:** cash, petty cash, capital assets, payables, capital leases

**Profit and loss statement:** sales and services, operating expenses, cash disbursement, salaries and benefits, credit card expenses

**Other items:** journal entries, accruals, special items

After risks have been identified, management should conduct a risk analysis to determine likelihood of risk occurring, potential impact if risk were to occur (quantitative and qualitative factors should be considered), how the risk will be managed (what actions will be taken). Prioritizing risks in this manner helps to direct resources in a manner to properly manage the most significant risks.

The final step in the risk assessment process will be to establish control activities in response to perceived risks. For the purposes of financial reporting, those “risks” relate to the following assertions inherent in financial statements:

*Existence or occurrence* – states that assets, liabilities and ownership interests exist at a particular date (balance sheet date) and that recorded transactions are those that have actually occurred during a given period.

*Completeness* – indicates that all transactions and events that have occurred during the period have been recorded in the financial statements.

*Rights and obligations* – states that as of a given date, assets are the rights of the organization and the liabilities are the obligations of the organization.

*Valuation or allocation* – indicates that assets, liabilities, revenues and expenses are recorded in the financial statements at the appropriate amounts in accordance with accounting principles and that they are mathematically correct and summarized properly.

*Presentation and disclosure* – addresses that items appearing in the financial statements are properly described, sorted and classified.

## External Auditor's Consideration of Risk

Auditing standards require the external auditor to obtain a sufficient knowledge of management's risk assessment process to evaluate how management considers risks relevant to financial reporting objectives. Auditors normally focus on the following issues:

- How does management identify risks relevant to financial reporting?
- How does management estimate the significance of the risks?
- How does management assess the likelihood of their occurrence?
- How does management decide on actions to manage those risks?

Since auditors take this approach, it is imperative that management conduct a risk analysis to prioritize risks and make sure that organizational resources are properly utilized to manage significant risks to reduce the likelihood of occurrence.

The auditor is also required to evaluate whether the entity's controls sufficiently address the identified risks of material misstatement due to fraud and the risks of management override of other controls. Such controls might include those relating to:

- significant or unusual transactions,
- journal entries and adjustments made in the period-end financial reporting process,
- related party transactions,
- significant management estimates.

Incentives for and pressures on management to falsify or inappropriately manage financial results.

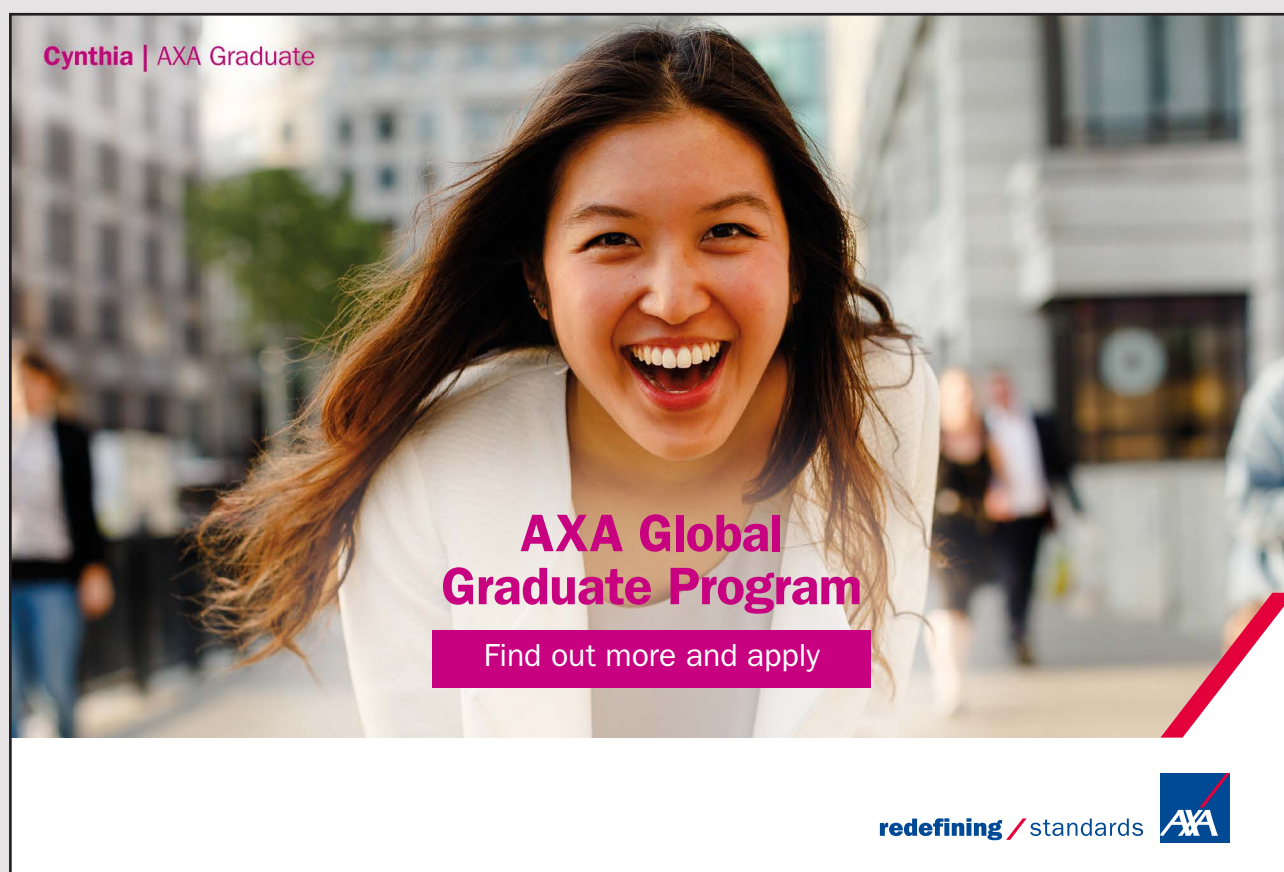
**Control activities:** These are the policies and procedures that help ensure that management's directives are carried out. One example is a policy that all company payments of more than EUR 500 would require two signatures.

**Information and communication:** You have to understand management's information technology, accounting, and communication systems and processes. This includes internal controls to safeguard assets, maintain accounting records, and back up data.

**Monitoring** involves understanding how management monitors its controls – and how effective the monitoring is. The best internal controls are worthless if the company does not monitor them and make changes when they are not working. For example, if management discovers that tagged computers are missing, it has to set better controls in place. The client may need to establish a policy that no computer gear leaves the facility without managerial approval.

Since institutions and their personnel continuously change, it is essential that controls be monitored over time to determine whether they continue to be relevant and are able to address new risks to the institution. Monitoring is a process that assesses the quality of an organization's internal control over time and involves assessing the design and operation of controls on a timely basis and taking actions as necessary. Monitoring activities can also reveal evidence or symptoms of fraud.


There are a number of reasons that an internal control system may change over time. The manner in which controls are placed in operation may change. This may be because controls are applied differently as control processes continue to evolve, or controls that were previously effective may no longer be performed, or just may not be effective. Among the reasons that control procedures may no longer be effective are changes in personnel, less effective training or supervision, limitations on time or resources, or other pressures. In addition, the risks and conditions that control procedures were designed to address may change, which would impact control effectiveness.



**Cynthia | AXA Graduate**

**AXA Global Graduate Program**

Find out more and apply

redefining / standards 



A good monitoring process helps ensure that control activities and other planned actions to affect internal controls are carried out properly and in a timely manner sufficient to ensure that the end result is effective internal controls. Ongoing monitoring activities should include various management and supervisory activities which evaluate and improve the design, execution, and effectiveness of internal controls. Periodic monitoring activities, such as self-assessments by various departments and internal audit appraisals, also provide helpful information.

Managers, like auditors, do not need to look at every piece of information to determine if controls are functioning properly. Managers should focus their efforts on high risk areas. They can use spot checks of transactions or basic sampling techniques to gain a reasonable level of confidence that the controls are functioning as intended.

### **9.3 INTERNAL CONTROLS PRINCIPLES**

Every internal control is assigned to the specialized role called Control Owner. This is the person responsible for completing the assigned internal control according to the internal control description.

All internal controls should respect the following five principles:

- **Organizational**  
The organizational principle means the internal controls are linked with the current organizational structure, competencies and responsibilities.
- **Integration**  
This principle means all operations are provided in line with business law in combination with business ethics and they are investigated. All possible errors are remediated.
- **Universal**  
All internal controls are centered on the critical parts or activities of the organization. This principle is focused on risk management.
- **Consistency**  
The organizational structure is relatively stable and not changed very often. All internal controls have to operate in the consistent organizational framework for a long period of time.
- **Information**  
Financial, managerial or accounting information should be accessible, verified, sorted and archived for all classified users.

## 9.4 IMPLEMENTATION OF INTERNAL CONTROLS

The importance of having implemented the internal controls increased over last years. Within the SME segment, the implementation of the internal controls is very popular.

Each and every implementation starts with completed process maps and clear evidence of all assigned relevant risks.

After consultation among the Process Owner, Internal Control Specialist and Control Owner, the description is going to be drafted, tested and finally agreed.

Each and every internal control should be commonly understood and its description should be written in a style that leaves no room for questions. In the other words, everybody who reads and operates within internal control should be fully informed about what exactly are the output, evidence and key activities.

The implementation of internal controls is not a short journey. It may take several months to create the proper system which enables the organization to mitigate risks through internal controls.

## 9.5 EXAMPLES OF INTERNAL CONTROL WORDING

Here are several examples of interaction between risks and solutions as applied by an organization applied in its day-to-day business practice.

*Risk:* General ledger accounts are not classified accurately in the financial statement structure (assets/liabilities/income statement, etc.).

*Solution:* In the month of January, the full set of the Chart of Accounts is verified for alignment with the Group Chart of Accounts and Accounting & Reporting Guidelines, dated and signed by the SAS General Accounting Manager. Exceptions detected during the review of the full set of the Chart of Accounts are escalated, resolved and documented in the same way as exceptions detected during monthly verification of changes.

*Risk:* Journal entries are not posted in the correct accounting period.

*Solution:* SAP configuration allows only one period to be open at a given time, and transactions can only be posted to that open period.



*Risk:* Exchange rates for consolidating the results of foreign reporting units or for translating foreign currency account balances are not accurate.

*Solution:* Cash Manager daily verifies that the latest exchange rates were correctly recorded in SAP (either by automated interface or manual entry). The daily printed list of exchange rates in SAP is dated and signed by the Cash Manager and retained at the accounting center.

## 9.6 RECOMMENDATIONS

When creating an internal control system, which should mitigate risks, we should keep in mind that this is a long-term and quite sophisticated process. It starts with the definition of company risks within the most critical processes. After that, new roles of Process Owners and Control Owners should be established and properly communicated.

I joined MITAS because  
I wanted **real responsibility**

The Graduate Programme  
for Engineers and Geoscientists  
[www.discovermitas.com](http://www.discovermitas.com)



**Month 16**  
I was a construction supervisor in the North Sea advising and helping foremen solve problems

Real work  
International opportunities  
Three work placements



**MAERSK**

The whole journey continues across the design of each and every internal control which might be assigned to the each and every risk. All internal controls should respect the unified design and used wording which must be easy to understand for Control Owners. Please do not forget to also incorporate a test plan into the description of every internal control. A test plan formulates the best way to achieve unambiguous assurance that the necessary evidence about internal control use could be obtained. In other words, a test plan is a guide on where to find proof that the Control Owner does his/her job.

The implementation of a whole set of internal controls should be properly planned and managed. All persons involved must act so as to avoid any potential delay because it is very important to roll out the full structure of the process driven organization including the internal controls system. At the end of the implementation phase, each and every Process Owner and Control Owner should officially confirm an official entry of the implemented internal controls into effect. Starting the following day, the officially accepted internal controls have to be respected and relevant evidence has to be created and stored.

It is recommended to require the Control Owners to submit an official confirmation that the internal control within their ownership works correctly and does not require any updates at the end of every quarter. If a need for change arises due to a change in the process itself due to the implementation of new technology within the current process, the implemented internal controls must be changed. It is very important that these changes are made in a proper and timely manner. There will be no disputes in the future starting from the date of the new control description.

The administration of the internal controls should be centralized. In the ideal case, all valid and implemented internal controls are stored in some database. The content of such a database should contain the internal control descriptions, names of all Process Owners and Control Owners, change register, testing results and remediation plans. Access to this centralized database should be restricted and carefully managed.

Please note that the internal control environment is part of the high value of the company's know-how and it may be used for the continual improvement and during the time of various internal or external audits. Auditors generally like to see some kind of a solid risk mitigation framework.

## Information Systems

Information systems are used to generate information necessary to carry out many control activities. An information system may be computerized, manual, or a combination of the two, depending on the size and complexity of the organization. The information system relevant to financial reporting (the “financial reporting system”) consists of automated and manual procedures and records established to initiate, record, process, and report organization transactions (as well as events and conditions) and to maintain accountability for the related assets, liabilities, and equity.

An effective financial reporting system includes methods and records for:

- identifying and recording all valid transactions, describing the transactions on a timely basis and in enough detail to permit proper classification in the financial statements,
- valuing transactions in a way that allows them to be reported at their proper amounts in the financial statements,
- providing sufficient information to permit recording of transactions in the proper accounting period,
- properly presenting the transactions and related disclosures in the financial statements.

The quality of information generated by an institution’s information systems is critical to the institution’s operations and success. Whether the information stems from automated or manual systems, the quality of the information affects whether management will be able to make appropriate decisions relating to managing and controlling the organization’s activities. The important factors to consider in determining the quality of an information system are:

- whether the needed information is provided,
- whether the needed information is provided on a timely basis,
- whether the information is current,
- whether the information is accurate, and
- whether the information is easily accessible by the appropriate persons.

While the focus here is on information systems at the functional level because of the significance information systems have on the flow of information for significant transaction classes and processes that relate to key financial reporting areas, information systems have implications at the organizational level as well. The consideration of the information process at the organization level focuses on making an overall evaluation of whether the institution has established an overall process or structure to ensure that financial reporting objectives as a whole have been achieved.

When evaluating the effectiveness of information systems the following factors should be considered:

- Does external and internal information obtained from the information systems provide management with necessary reports on the organization's performance relative to ensuring reliable financial reporting and safeguarding of assets?
- Do the information systems provide the right information on time to the right people, so that they may fulfill their responsibilities effectively and efficiently?
- Are information systems developed and revised under a strategic plan that is linked to the organization's overall objectives and strategies?
- Does management show their commitment to developing appropriate information systems by assigning appropriate resources?

The evaluation for controls of information systems is largely based on the flow of information for significant transaction classes and processes that relate to key financial reporting areas which take place at the control activities level.

**ie** business school

**93%**  
OF MIM STUDENTS ARE  
WORKING IN THEIR SECTOR 3 MONTHS  
FOLLOWING GRADUATION

**MASTER IN MANAGEMENT**

- STUDY IN THE CENTER OF MADRID AND TAKE ADVANTAGE OF THE UNIQUE OPPORTUNITIES THAT THE CAPITAL OF SPAIN OFFERS
- PROPEL YOUR EDUCATION BY EARNING A DOUBLE DEGREE THAT BEST SUITS YOUR PROFESSIONAL GOALS
- STUDY A SEMESTER ABROAD AND BECOME A GLOBAL CITIZEN WITH THE BEYOND BORDERS EXPERIENCE

Length: 10 MONTHS  
Av. Experience: 1 YEAR  
Language: ENGLISH / SPANISH  
Format: FULL-TIME  
Intakes: SEPT / FEB

**5 SPECIALIZATIONS**  
PERSONALIZE YOUR PROGRAM

**#10 WORLDWIDE**  
MASTER IN MANAGEMENT  
FINANCIAL TIMES

**55 NATIONALITIES**  
IN CLASS

[www.ie.edu/master-management](http://www.ie.edu/master-management) | [mim.admissions@ie.edu](mailto:mim.admissions@ie.edu) | [f](#) [t](#) [i](#) Follow us on IE MIM Experience

Since the effectiveness of information systems is inherently connected to how control activities are designed and implemented, specific applications will be discussed in the following section on control activities.

### **Control Activities**

Control activities are those actions that are taken to address risks that threaten the entity's ability to achieve its objectives, one of which is reliable financial reporting. Control activities are usually supported by a policy that establishes what should be done, and the procedure that implements the policy.

### **Nature of Controls**

Controls can generally be broken down into two broad categories: manual controls, and automated controls. Those two categories can be broken down further as follows:

*Manual controls* are controls that are manually performed by individuals. They may be solely manual where no IT generated reports are used or they may be IT-dependent whereby an employee is using a system-generated report to test the validity of a particular control.

*Application controls* are performed entirely by the computer system.

*Preventive controls* attempt to deter or prevent undesirable events from occurring. They are proactive controls that help to prevent a loss. Examples of preventive controls are separation of duties, proper authorization, adequate documentation, and physical control over assets.

*Detective controls*, on the other hand, attempt to detect undesirable acts. They provide evidence that a loss has occurred but do not prevent a loss from occurring. Examples of detective controls are reviews, analyses, variance analyses, reconciliations, physical inventories, and audits.

Both types of controls are essential to an effective internal control system. From a quality standpoint, preventive controls are essential because they are proactive and emphasize quality. However, detective controls play a critical role providing evidence that the preventive controls are functioning and preventing losses.

## Types of Control Activities

Control activities occur throughout the organization, at all levels and in all functions. They include a range of detective and preventive control activities as described below:

### **Approvals, Authorizations, and Verifications** (Manual and/or IT-Dependent, Preventive):

Management authorizes employees to perform certain activities and to execute certain transactions within limited parameters. In addition, management specifies those activities or transactions that need supervisory approval before they are performed or executed by employees. A supervisor's approval (manual or electronic) implies that he or she has verified and validated that the activity or transaction conforms to established policies and procedures.

Authorization and approval are the most important elements of this control activity. Some specific control aspects should be observed. For example, appropriate limits should be established for approval authority, blank approval forms should never be signed, passwords for electronic approval authority should never be shared, person initiating transaction should not also approve transaction, and written policies and procedures should be available with documents approval levels and limits.

### **Reconciliations** (Manual and/or IT Dependent, Detective):

An employee relates different sets of data to one another, identifies and investigates differences, and takes corrective action, when necessary.

This control activity helps ensure accuracy and completeness of transactions. Examples would be monthly bank reconciliations, monthly financial report reconciliations, etc. A critical element to remember is that a reconciliation is no good unless the variances identified are researched, explained and resolved.

### **Reviews of Performance** (Manual and/or IT Dependent, Detective):

Management compares information about current performance to budgets, forecasts, prior periods, or other benchmarks to measure the extent to which goals and objectives are being achieved and to identify unexpected results or unusual conditions that require follow-up.

This control activity also includes management's review of reconciliations, reports and other information generated from item [2] above which substantiates the accuracy of the reconciliations performed.



**Security of Assets** (Manual and IT-Dependent Manual, Preventive and Detective):

Access to equipment, inventories, securities, cash and other assets should be restricted. Also, assets should be periodically counted and compared to amounts shown on control records. This control activity is critical because liquid assets, vital documents, critical systems and confidential information must be safeguarded against unauthorized acquisition, use or disposition. Generally limiting access to these assets is the best way to protect them whether by physical controls such as locked doors or alarm systems or by IT controls such as passwords, data encryption, etc. Periodic inventory counts should be made and perpetual inventory records should be maintained.

**Segregation of Duties** (Predominately Manual, Preventive):

Duties are segregated among different people to reduce the risk of error or inappropriate action. Normally, responsibilities for authorizing transactions, recording transactions (accounting), and handling the related asset (custody) are divided.



"I studied English for 16 years but...  
...I finally learned to speak it in just six lessons"  
Jane, Chinese architect

ENGLISH OUT THERE

Click to hear me talking before and after my unique course download



Typically no one person should initiate a transaction, approve the transaction, record the transaction, reconcile balances, handle assets, and review reports. Segregation of duties is one of the best fraud deterrents and if the size of the staff prevents adequate segregation of duties, then a compensating control activity such as supervisory reviews must be implemented. Completion of the segregation of duties matrix will help identify areas where compensating controls are needed.

**Controls over Information Systems** (IT-Dependent Manual and Automated, Preventive and Detective):

Generally speaking there are four types of IT controls: general controls, IT-dependent manual controls, application controls, and end-user computing controls.

**General controls** – set the tone within the IT control environment by supporting the functioning of application controls and IT-dependent manual controls. These commonly include controls over data center operations, system software acquisition and maintenance, access security, and application system development and maintenance.

**IT-dependent manual controls** – These are processes that are manually performed by individuals, but rely on computer-generated information. To ensure the effectiveness of IT-dependent manual controls, one must validate the accuracy and completeness of the system-generated report and the effectiveness of the manual portion of the control.

**IT application controls** – These are “computer controls” based on the institution’s business rules (system settings). These controls determine how transactions will be input, processed and output by the computer system. Input controls ensure the complete and accurate recording of authorized transactions by only authorized users; identify rejected, suspended, and duplicate items; and ensure resubmission of rejected and suspended items. Examples of input controls are error listings, field checks, limit checks, self-checking digits, sequence checks, validity checks, key verification, matching, and completeness checks.

Processing controls ensure the complete and accurate processing of authorized transactions. Examples of processing controls are run-to-run control totals, posting checks, end-of-file procedures, concurrency controls, control files, and audit trails.

Output controls ensure that a complete and accurate audit trail of the results of processing is reported to appropriate individuals for review. Examples of output controls are listings of master file changes, error listings, distribution registers, and reviews of output.

**End-user computing controls** – This type of IT control comes into play when using departmentally developed spreadsheets or data bases as tools for performing work which extends to the information reported in the financial statements. Important control elements would be employee access, accuracy and process integrity, backup and review. An example would be Navision reports that are used in financial reporting.

Control activities must be implemented thoughtfully, conscientiously, and consistently. A procedure will not be useful if performed mechanically without a sharp continuing focus on conditions to which the policy is directed. Further, it is essential that unusual conditions identified as a result of performing control activities be investigated and appropriate corrective action be taken.

In the past 5 years we have drilled around

# 95,000 km

—that’s more than **twice** around the world.

**Who are we?**  
We are the world’s leading provider of reservoir characterization, drilling, production, and processing technologies to the oil and gas industry.

**Who are we looking for?**  
We offer countless opportunities in the following domains:

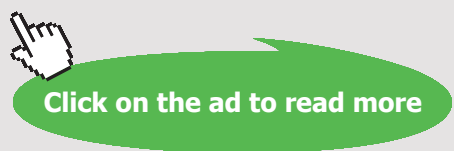
- Operations
- Research, Engineering, and Manufacturing
- Geoscience and Petrotechnical
- Commercial and Business

We’re looking for high-energy, self-motivated graduates with vision and integrity to join our team.

[careers.slb.com](http://careers.slb.com)

**What will you be?**

## Schlumberger



# 10 PROCESS MAPS

A flowchart is a picture of the separate steps of a process in sequential order. Elements that may be included are: sequence of actions, materials or services entering or leaving the process (inputs and outputs), decisions that must be made, people who become involved, time involved at each step and/or process measurements. The process described can be anything: a manufacturing process, an administrative or service process, a project plan. This is a generic tool that can be adapted for a wide variety of purposes.

## 10.1 DEFINITION

A process map is a set of activities and operations of the company employees related to the company activities in order to fulfill the business objective.

An essential element of process maps is a process that reflects the degree to which the information needs of businesses for the use of information technology are met – information system.

Process maps can be defined as a schematic representation of the process as a sequence of actions. This is a summary of the activities and operations of the company employees related to the company activities in order to fulfill the business objective.

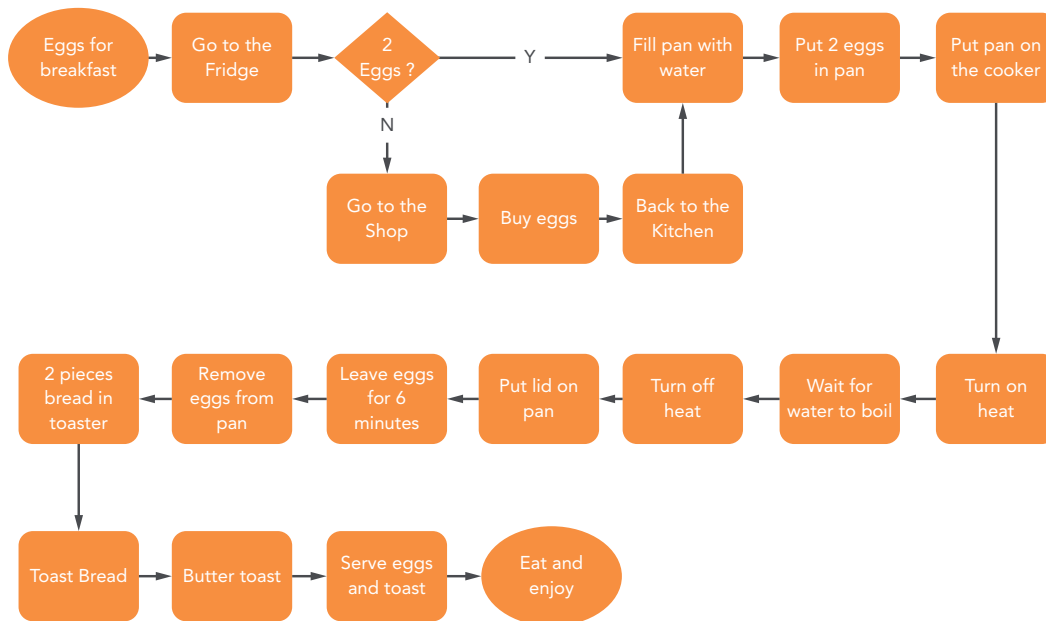


Fig. 9 Eggs preparation process source: own workflow

Creation of process maps requires agreement on the model convention. It means using internationally accepted symbols for each and every documented step or activity (document, data storage, step, verification or pre-defined procedure).

Danger can lurk in incorrectly executed analysis, poorly chosen approach and process analysis tools. The analysis itself may sometimes entail disproportionately large amounts of work in comparison with its real benefits. For this reason, organizations often hire specialized professionals.

The term business process management (BPM) covers how we study, identify, change, and monitor business processes to ensure they run smoothly and can be improved over time. Often framed in terms of the daily flow of work – and yes, “workflow” generally does fit under the process improvement umbrella – it is an important piece of the access and use puzzle since no or poor process really degrades your ability to get at and leverage information. BPM is best thought of as a business practice, encompassing techniques and structured methods. It is not a technology, though there are technologies on the market that carry the descriptor because of what they enable: namely, identifying and modifying existing processes so they align with a desired, presumably improved, future state of affairs. It is about formalizing and institutionalizing better ways for work to get done.

Successfully employing BPM usually involves the organizing around outcomes, not tasks to ensure the proper focus is maintained; correcting and improving processes before (potentially) automating them; otherwise all you’ve done is make the mess run faster; establishing processes and assigning ownership lets the work and improvements simply drift away – and they will, as human nature takes over and the momentum dies out; standardizing processes across the enterprise so they can be more readily understood and managed, errors reduced, and risks mitigated; enabling continuous change so the improvements can be extended and propagated over time; improving existing processes, rather than building radically new or “perfect” ones, because that can take so long as to erode or negate any gains achieved. BPM should not be a one-time exercise. It should involve a continuous evaluation of the processes and include taking actions to improve the total flow of processes. This all leads to a continuous cycle of evaluating and improving the organization.

The steps that can be recognized in BPM are:

1. Analyze
2. Re-design and model
3. Implement
4. Monitor
5. Manage
6. Automate

Getting information to where it needs to go, when it needs to go there, is only part of the solution – much of the rest involves first requesting the insights you need, and then having those insights communicated to you in an immediately usable format. This is what reporting and querying software is all about.

Success depends in large measure on how well you label the data in your repositories so it can be identified and included when an appropriate query comes along. A major boost toward accomplishing this goal exists in the form of the common warehouse model (CWM), a complete specification of syntax and semantics that data warehousing and business intelligence tools can leverage to successfully interchange shared metadata.

Released and owned by the Object Management Group (OMG), the CWM specifies interfaces that can be used to enable the interchange of warehouse and business intelligence metadata between warehouse tools, warehouse platforms, and warehouse metadata repositories in distributed heterogeneous environments. It is based on three standards:

- UML – Unified Modeling Language, an Object Management Group (OMG) modeling standard,
- MOF – Meta Object Facility, an OMG metamodeling and metadata repository standard,
- XMI – XML Metadata Interchange, an OMG metadata interchange standard.

Excellent Economics and Business programmes at:



university of  
 groningen



“The perfect start  
 of a successful,  
 international career.”

**CLICK HERE**  
 to discover why both socially  
 and academically the University  
 of Groningen is one of the best  
 places for a student to be

[www.rug.nl/feb/education](http://www.rug.nl/feb/education)

CWM models further enable users to trace the lineage of data by providing objects that describe where the data came from and when and how it was created. Instances of the models are exchanged via XML Metadata Interchange (XMI) documents.

The simplest of these is cleverly known as routing or simple workflow. It moves content – very often in the form of conventional documents. From one place or person to another, and when task A is complete, it allows for task B to begin. Routing tends to be ad-hoc, without any automated rules processing, and with little or no integration between the process management and the affected applications. Instead, it is pretty much person-to-person.

Workflow is more than just simply moving things from A to B to C to D because it allows tasks to be carried out in parallel, saving time and increasing productivity. Able to manage multiple processes taking place at the same time, it accommodates exceptions and conditions by applying user-defined rules.

BPM itself is perhaps the “ultra” process improvement technique because it explicitly addresses the complexity of inter-application and cross-repository processes, and incorporates data-driven, as well as, content-driven processes – all on an ongoing basis.

Usually driven by business rules, it involves a lot of operational analysis and flow charting, and the more sophisticated offerings in the space include not only process designers, but also simulation tools so processes can be run virtually to identify bottlenecks or other issues related to either people or underlying infrastructure.

We must bear in mind that business processes should include the mobile workforce and how mobile device factor into the accomplishment of the overall organizational goals.

## 10.2 PROCESS MANAGEMENT

Process management is based on the professionally recognized methodology and includes the following phases:

- Initialization  
Initialization of the project is also among the initial processes. Planning includes output quality (targets), project planning, risk analysis and strategic planning, setting controls and standard documents.

- **Planning**  
Planning is always characteristic for the beginning of a new stage. It includes the creation of a skeletal plan, defining and subsequent analysis of the product, identifying activities and assigning resources, planning to create a calendar plan of utilization of human resources, risk analysis and finally building the plan itself.
- **Management**  
This is one of the main management processes. It interacts with most other processes and manages the life cycle of the project (i.e. from its initialization until its completion). This process follows initialization and approval of the project itself, approval phase of the plan and project closure.
- **Control**  
Control manages the execution of project activities. It includes approval during the stage, writing and problem analysis, status and stage of its report, corrective actions, escalating issues and taking over the finished work.
- **Realization**  
These are activities and threads fulfilling their own purpose and the objective of the process management project.
- **Limitation**  
This process follows the inspection process. These activities include changes in the project plan to change targets or project benefits, modifying the list of risks, reporting the late stage and creating a crisis scenario.
- **Closure**  
This process includes activities that relate to activities undertaken after the completion. In particular, this entails the decomposition of the project, identifying activities and their connections, and feedback from the evaluation project.

### 10.3 PROCESS RISKS

A process risk is a risk related to the chance that the (execution of the) process (the test process in this case) does not live up to the expectations. As such, process risks are related to process control. Success is threatened by two risk types: risks related to the execution of the internal process and risks related to external threats.



### Internal Process Risks

A project or test plan is used to tackle a number of known process risk areas in advance. The quality of the plan and plan execution control have a direct bearing on the internal process risks.

### External Process Risks

Process risks also have a relationship with possible disruptions from outside. The external risks for these environmental factors are generally impossible to control. However, a project can try to anticipate these events to minimize the resulting damage as much as possible.

The damage associated with a process risk can generally be expressed in terms of the extra time and money required for the process to achieve the desired results.

Throughout the test process, the test manager must implement measures to manage the process risks that threaten the success of his results. As such, it is important for a test manager to specify the risks to the test process explicitly. The client and other stakeholders will have a better understanding of the risks to the test process and keep them in mind when managing the total execution process.



**American online**  
**LIGS University**  
is currently enrolling in the  
**Interactive Online BBA, MBA, MSc,**  
**DBA and PhD programs:**

- ▶ enroll **by September 30th, 2014** and
- ▶ **save up to 16%** on the tuition!
- ▶ pay in 10 installments / 2 years
- ▶ Interactive **Online education**
- ▶ visit [www.ligsuniversity.com](http://www.ligsuniversity.com) to find out more!

**Note: LIGS University is not accredited by any nationally recognized accrediting agency listed by the US Secretary of Education. More info [here](#).**

We should note that confusion may result if the chance of failure of a process risk is also part of the chance of failure of a product risk.

### **Example**

In the product risk analysis, the deployment of inexperienced developers is specified as one cause of the higher chance of failure for a certain object part. A vital customer process will be shut down if the object part fails, resulting in loss of hours and revenue for the customer organization. The chance that inexperienced developers will be deployed cannot yet be determined because the development team has not yet been established. If inexperienced developers are deployed, the chance of failure will increase. A mitigating measure in this situation is to classify the object part in a higher risk class. As a result, the object part must be tested more thoroughly.

In this process risk analysis, the test manager identifies the deployment of inexperienced developers as a threat to the progress of the test process. Inexperienced developers may deliver lower software quality, which would result in more retesting than was planned originally. This would endanger the deadline. The test manager discusses the process risk with the project manager. It becomes clear that inexperienced developers will indeed be deployed. The test manager proposes to schedule more time for retesting this object part. The project manager does not agree and therefore decides to accept the risk and the damage that may result. He could also take compensatory measures beyond testing, e.g. coaching the inexperienced developers.

# 11 FINAL RECOMMENDATIONS AND REMARKS

Here are some of the more common mistakes that I have come across regularly, with some steps to take to avoid them.

## **Mistake 1: Done only for legal reasons**

Of course, for all but the smallest of operations, there is a legal requirement. But the prime reason for carrying out risk assessments is that they are a key tool in how you manage safety; without assessments, you cannot adequately manage the risks.

## **Mistake 2: Done from the desktop**

I have seen advertisements for software that say risk assessments can be done from the desktop. No, you have to view the operations and discuss what actually happens (not just what should happen) with the people involved. Be warned: some things that turn up will alarm you.

## **Mistake 3: Covering only control measures in place**

Of course, you need to know these, but far more important is what controls should be in place, but are not. What you should get out of your risk assessments should include: What actions do we need to take to get in control and what actions do we need to take to stay in control?

The first one is obvious, but people often miss the second. For example, if a hazard is avoided by having guards interlocked to the control system so that the equipment is prevented for running when a guard is open, then you need to periodically check that these interlocks still work. This is even more important when you have trips or alarms which only come into effect when a fault occurs, for example when there is excessive temperature or an item (like a finger) is drawn into an in-running nip.

**Mistake 4: No management plan**

What tends to happen is that you just have individual risk assessments, with no view of the big picture. What you really need as an output of your risk assessments is a list of actions, in descending order of risk so that you can tackle the big issues first. The software I use has this as an integral output, but you can always cut and paste actions manually. So, your management plan should be to address the highest scores first and work on moving the risks towards the green and white end of the spectrum shown below.

**Mistake 5: No ranking**

Because you need an overview of all your risks, you need to rank them so that the serious risks are at the top of your list. I use a non-linear scoring system because it emphasizes the more serious outcomes and I am also a fan of color-coding.

The whole area of modern risk management is relatively modern fresh air in the new business conceptual out-of-box thinking. Traditionally managed companies spent a lot of financial, human and other resources to keep the process of transformation in the most efficient way. For many decades companies carefully tuned up their processes to be highly efficient and economically profitable.

The production of various goods, services and other requests to fulfill the customer demands and expectations always has been a race among the need, resources and completion. The time, energies and other various resources were organized with the one aim to be achieved.

Risks and adequate risk management is a must. The essential substance of risk management is to avoid complications and losses assigned to the risk activities. Risks costs money and require a lot of energy which needs to be invested in correcting the risk-affected areas. Management of risk is closely related to quality management.

My plan was to present the full picture of all aspects related to risk management. Within the text above, I tried to familiarize all readers with the concept of quality management systems, the Sarbanes-Oxley Act, compliance, process driven organizations, internal controls, and I briefly touched on the fundamentals of process maps.

## 12 CLOSING NOTE

The aim of this book was to deliver a very concentrated study material for students and all others who are interested in modern risk management. Risk management as a whole has a much wider scope than is presented in this document. The world of the modern business definitely requires capable risk managers and devoted specialists. Such risk management staff have a great impact on the life of their organizations because in the world of heavy regulation in many other areas risk management itself might be the one truly “free” area.

Risk management requires all tools and methods that would help risk managers start their independent exploration and creation of their further special applications and new tailor-made tools. My book delivered some basic fundamental ground which I marked as “must-know”. Just like all kids have to learn mathematic or grammar, similarly, every risk manager needs to know the basic terminology of risk management, tools like COSO and at least what the purpose and role of internal control is.



**DON'T EAT YELLOW SNOW**

What will your advice be?

Some advice just states the obvious. But to give the kind of advice that's going to make a real difference to your clients you've got to listen critically, dig beneath the surface, challenge assumptions and be credible and confident enough to make suggestions right from day one. At Grant Thornton you've got to be ready to kick start a career right at the heart of business.

Sound like you? Here's our advice: visit [GrantThornton.ca/careers/students](https://www.grantthornton.ca/careers/students)

Scan here to learn more about a career with Grant Thornton.



 **Grant Thornton**  
An instinct for growth™

© Grant Thornton LLP. A Canadian Member of Grant Thornton International Ltd

The tools of risk management might change but the key principles will remain. In a couple of years, the Sarbanes-Oxley Act (SOX) will be probably replaced or fully eliminated from the U.S. legislation. But the SOX internal principles of risk management for financial and risk operations will always require some kind of an artificial risk mitigation framework. The basic idea will stay and should be a source of inspiration for all future “law designers” who will be dealing with risk mitigation.

The worldwide impact of risk management activities will not change the world of business but the approach of the financial and supervisory authorities. Even today, if a company were able to present its own risk maps, risk mitigation plans or show an internal control environment according to the COSO principles, such a company would gain credit for sure.

I would like to thank all the people on the management team of the Faculty of Informatics and Statistics of the University of Economics, Prague for enormous support and help and my thanks also go to the Bookboon printing house for their flexibility.

Last but not least, I would like to thank my family for their endless patience.

# REFERENCES

1. Managing information risk <https://www.gov.uk/government/collections/risk-managementguidance#case-studies>
2. ISO <http://www.iso.org/iso/home.html>
3. COSO: Guidance on Internal Controls <http://www.coso.org/ic.htm>
4. COSO [https://en.wikipedia.org/wiki/Committee\\_of\\_Sponsoring\\_Organizations\\_of\\_the\\_Treadway\\_Commission](https://en.wikipedia.org/wiki/Committee_of_Sponsoring_Organizations_of_the_Treadway_Commission)
5. Hamburger University [http://www.aboutmcdonalds.com/mcd/corporate\\_careers/training\\_and\\_development/hamburger\\_university.html](http://www.aboutmcdonalds.com/mcd/corporate_careers/training_and_development/hamburger_university.html)
6. Sarbanes – Oxley 302/404/906 <http://www.sarbanes-oxley-101.com/>
7. Compliance <http://searchdatamanagement.techtarget.com/definition/compliance>



# LIST OF FIGURES

Fig. 1 Deming Cycle source: <a href="http://www.expertprogrammanagement.com">www.expertprogrammanagement.com</a>	37
Fig. 2 Japanese quality systems source: <a href="http://1000ventiures.com">1000ventiures.com</a>	39
Fig. 3 Six Sigma, Kaizen and Lean concepts source: <a href="http://iSix Sigma.com">iSix Sigma.com</a>	42
Fig. 4 Illustration of McDonald’s values source: own pictures	43
Fig. 5 Hamburger University in Illinois, USA source: McDonalds’s	43
Fig. 6 Dow Jones Index	47
Fig. 7 COSO cube source: <a href="http://COSO.com">COSO.com</a>	57
Fig. 8 Operation Excellence principles source: <a href="http://www.faberinfinite.com">www.faberinfinite.com</a>	75
Fig. 9 Eggs preparation process source: own workflow	102

.....Alcatel-Lucent 

[www.alcatel-lucent.com/careers](http://www.alcatel-lucent.com/careers)

What if you could build your future and create the future?

One generation's transformation is the next's status quo. In the near future, people may soon think it's strange that devices ever had to be "plugged in." To obtain that status, there needs to be "The Shift".

