

INTRODUCING CONTROLS

Whenever there is a fair chance that unpleasant things may happen, we try to find means to avoid them. Those means are generally called 'controls'. We find them everywhere. Traffic lights, social codes, table manners etc. etc. By implementing these controls, we hope to avoid mishaps or, at least, we try to limit the damage that may occur.

In the next few modules we will deal with those 'controls'.

Types of controls

We must all agree from the outset that if we use controls we must be able to rely on them. In other words: controls need to do what they are designed for. Controls that are 'occasionally effective' are no controls; they represent an expensive gamble. On the other hand, we may not expect too much of them. Controls never are perfect.

In the PARIS-methodology we distinguish between various types of controls.

Here we will discuss these type briefly. More attention will be paid to them later on in the program.

1. Avoidance

Just don't do it. This seems strange, but you would be surprised to know how many obsolete routines are still in use in companies, just because nobody cared about checking their usefulness.

2 Risk transfer

Here we transfer the risk somewhere else; usually we put it in the hands of a specialised organisation. This is a very common type of control.

2a Outsourcing

This means that parts of the work are done by third parties. Usually this is done because these third parties offer a very specialised service. Think about removing asbestos from derelict buildings.

2b Insurances

This type of risk transfer is frequently used. All types of insurances are available in case any mishap occurs. Ranging from financially covering the costs to legal support etc.

3 Hardware

Put a fence around something, dead man's buttons on trains, the Hadrian Wall etc. This usually works, apart from cases of utmost stupidity or criminal intent.

4 Competence

For any task in your organisation qualifications are required. These qualifications have to be in line with the skills that are expected. The right qualifications for the task offer a certain level of guarantee that risks are minimised.

5 Regulating documents

This really is a tricky one. You can develop procedures and work instructions to your liking, but there is no certainty that people will act accordingly. Therefore regulating documents require a lot of supervision. There also is a fair chance that, once printed, these documents start a life on their own, even after having been revoked officially.

As you will probably have guessed by reading this paragraph, the sequence in which we mentioned these types of controls represent our preference. Controls of type 5 are the least attractive. So when creating controls we first try controls of type 1. If that does not work (sufficiently) we move on further down the line until the risk is sufficiently covered.

Deciding on the preferred type of control

In the previous paragraph we stated that there is a taxonomy in preferences as far as controls are concerned. The most attractive ones were mentioned first and we ended with the ones least attractive. Why is that? The main risk of failing controls lies in the human factor. The lesser their influence on controls, the lesser the risk that they will fail. Machines don't make mistakes. They are just too stupid to do that. When machines fail it is because the human behind its design, maintenance or operation blunders.

The most intensive research on failures is performed when serious disasters occur. And in more than 90% of the cases it comes down to human failures. So when it comes down to select adequate controls, we would prefer controls where the human factor is of the least importance.

From that point of view it is only logical to determine the preferences for the various types of controls likewise.

Therefore the steps we take by selecting/developing controls are:

Firstly: Try Risk avoidance

Secondly: Try Risk transfer

Thirdly: Try Hardware solutions

Fourthly: Try (Increased) competence

Fifthly: Resort to regulating documents.

We prefer to start with the question: can the action that might trigger the risk be avoided? If so, we have found the cheapest solution to our problem.

But often controls do not cover the entire risk, which leaves us with a residual risk.

Now we have to ask: Is this residual risk acceptable?

If the answer is 'Yes' we are done. If the answer is 'No', we need to find a solution for that residual risk.

Next we try to solve that residual risk at the next best level: can it be transferred to a third party?

And so on, and so on.

Combined controls mean additional supervision and maintenance. Thus: additional costs

This is the tricky part when selecting controls. On one hand you are advised to select appropriate controls according to the taxonomy mentioned above. On the other hand we need to warn you that solving the problem of residual risks might force you to apply additional controls.

But controls come at a price. They need to be designed, implemented, maintained and monitored. The more controls you implement, the more additional cost will be the logical consequences.

So there may be a good reason to select a less attractive control (lower in our taxonomy) if those controls deal with the risk in a more effective way.

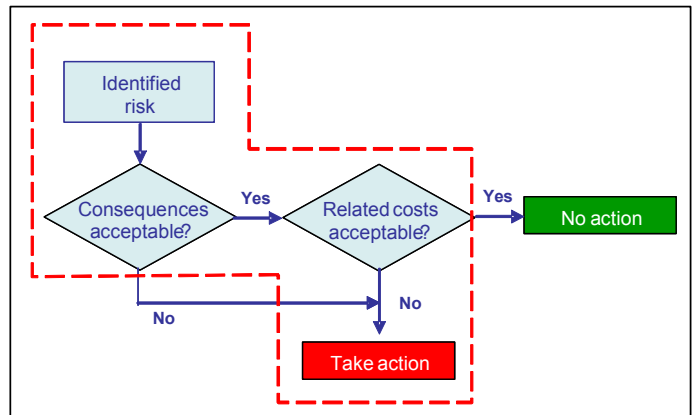
However attractive our taxonomy may be, the more controls you need the more controls have to be managed. Keep that in mind, as managing controls constitutes risks as well.

The costs of controls may be too high

In the module about risk areas, we already stated that there risks have direct consequences and related costs.

If the consequences and the costs were both acceptable, no controls were required. Yet, if any of them was not-acceptable, controls were in order.

But there are exceptions. Sometimes the costs of controls are so high, that we had better take the risk. This decision can only be taken in cases where the direct consequences are acceptable. That is what we will discuss in this paragraph. We have selected this area with a dotted line in this familiar diagram.



So what we need to do, is to make a comparison between the financial consequences per year and the yearly costs that come with the development, implementation and maintenance of controls.

In the Pandora Risk Manager we use a screen to enter the costs, related to each specific control. As controls have to be completely overhauled after a period of three years (at the most), we created three columns: one for the initial year and two for the following years.

	YEAR 1 initial year	YEAR 2	YEAR 3	
Initial costs				
Development costs for this control/these controls:	10,00			
Implementation costs for this control/these controls: <i>(training, newsletters, dissemination of documents etc.)</i>	2,00			
Total initial costs:	12,00			
Yearly costs				
Maintenance costs <i>Yearly review, costs for updates, additional training (for new employees), fresh up activities</i>		4,00	4,00	AVERAGE yearly
TOTALS	12,00	4,00	4,00	6,67

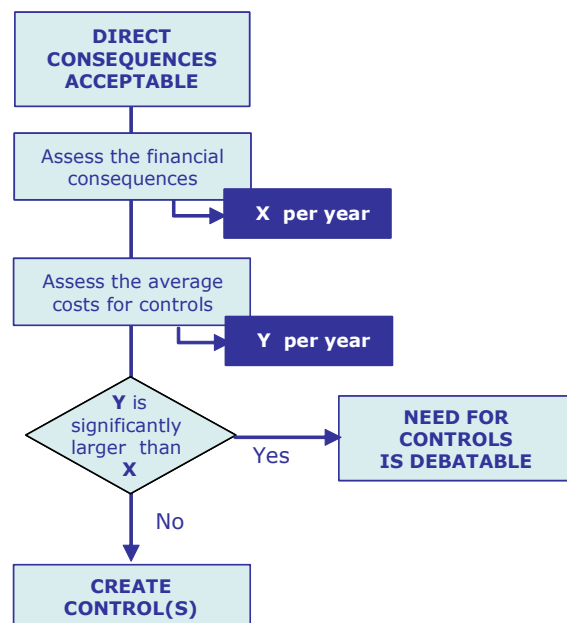
In year 1 we face development and implementation. In the two following years we face maintenance of and additional training. The total costs for those three years provide us with an average costs per year for each control.

Don't worry; the Pandora Risk Manager also provides you with a screen that offers information about the average costs related to the risk.

BUT: although we can be pretty sure about the costs that come with the controls, we can never be sure of the costs that come with a risk. That estimate is much less reliable.

So if we use the algorithm as shown here in order to come to a decision, it is advisable to speak about a 'significant' difference, if we make the comparison.

Just to stay on the safe side.





PANDORA RISK MANAGEMENT
IS A LEONARDO PROJECT
FUNDED BY THE EUROPEAN UNION

THE PANDORA PROJECT TEAM

Business Development Friesland (NL)
Info Transfer Europe (NL)
Funditec (ES)
Innovate (IE)
Fundecyt (ES)
XLAB (SL)
Internet Society Bulgaria (BG)
Instituut Service Management Stenden University (NL)
ICT Center Friesland (NL)
European Business& Innovation Centre Network (BE)

www.pandora-project.eu

These materials can be used free of charge within the Pandora framework. Alteration of these documents in any form or way is not allowed. Commercial use of these materials prior to the written consent of the author is prohibited. The author's e-mail is: hverbeke@home.nl



Are you sure that this is the right control to prevent you from getting lost?

CONTROLS HAVE TO BE STRAIGHT FORWARD

Products you can download freely from our website

An overview of the method

As far as qualitative risk management is concerned, there are various approaches on the market that differ slightly from each other. The method the Pandora project uses is part of the PARIS methodology for process management.

An outline of the training program for managers

Managers play a key-role in risk management in their organisation. Therefore we offer a training program that supports every step in this process. This outline gives you a detailed overview of the training activities.

A training program for managers

This program supports the manager to increase risk awareness in the organisation and to capitalise on the results. It offers a combination of theoretical background information, implementation strategies and practical tips.

A risk assessment card

These cards should be freely distributed in the organisation. They are considered to be an important tool for the identification and assessment of risks. These cards come with an extensive instruction for their use.

The Pandora Risk Manager

This is a simple, stand alone software tool that helps with the assessment of risks, their primary consequences (for people, environment, assets and reputation) and the secondary consequences: money, money and money. It also helps with the comparing the costs related to the incident with the costs related to the development, implementation and maintenance of controls.

This tool comes with a detailed learning manual.

