A.3 Risk treatment process

Introduction

This « [RTP1] say what this is (e.g., document, (web) page) » describes our approach to risk treatment. It explains how we treat risk and formulate a risk treatment plan; how we ensure we have not omitted any necessary controls, formulate a Statement of Applicability and gain approval for the risk treatment plan and residual risks.

There is a risk treatment plan (RTP) for each event. However, in the real world, controls do not know which RTP they belong to and they will come into operation as soon as their preconditions for operation are satisfied. Thus, in effect, RTPs operate in parallel.

Treating risk

Risk treatment options

We treat risk by applying controls that modify the risk in such a way that it meets our risk acceptance criteria. As risk is the product of likelihood and consequence, the only two parameters that a control can modify are FoL and severity. Controls can:

a) ACT IN ATTEMPT TO PREVENT THE OCCURRENCE OF THE EVENT OR DETECT IT IN SUFFICIENT TIME FOR OUR ORGANISATION TO DEAL WITH IT. IF SUCCESSFUL, THESE CONTROLS REDUCE FOL;
b) REACT TO THE CONSEQUENCE AND IF SUCCESSFUL REDUCE ITS SEVERITY.

Moreover, controls may act to reduce the FoL or severity to zero (minus ∞ on a log scale) or some very small value; or reduce it by some factor (e.g., the treated risk is $^{1}/_{N^{th}}$ of the untreated risk. We may perform the control ourselves, or outsource it « [RTP2] Note that if your organisation is part of a legal entity, you might add: and in some cases it is already performed by another organisation, although we could augment it. ». We are also aware that in reducing risk for one variety of consequence (e.g., the undesirable disclosure of information) we might be forced to increase it for another (e.g., the inability to carry some or all of one's business). Thus, there are a wide range of risk treatment options that we can use.

Determination of controls

We take each event in turn and proceed in a story board fashion. We first look towards preventing the event and then to detecting it. We then consider how to react to each of the associated consequences. We finish when we are satisfied that the residual risk is acceptable, and check that by verifying that the modification of FoL

and severity necessary to render the risk acceptable is consistent with the control behaviour.

We either design the controls or make use of existing commercially available technology to meet our need to modify risk at the point where we invoke the control in the story.

Comparison with Annex A

We recognise that it is possible, through error or oversight, to omit necessary controls from our risk treatment plans. We therefore compare our controls with those in Annex A. We do this by taking each Annex A control in turn (see our Statement of Applicability page) and:

For each Annex A control in turn we:

1. DECIDE WHETHER IT APPLIES TO US OR NOT. IF NOT, WE EXCLUDE IT ON GROUNDS OF NOT APPLICABLE AND RECORD WHY.
2. IF IT IS OBVIATED BY A CUSTOM CONTROL (E.G., BECAUSE THE CUSTOM CONTROL AVOIDS THE RISK THAT THE ANNEX A CONTROL IS INTENDED TO MITIGATE), WE EXCLUDE IT ON GROUNDS OF BEING OBVIATED AND RECORD WHY.
3. IF IT DOES THE SAME JOB AS A CUSTOM CONTROL, WE DECLARE IT AS A VARIANT. THIS EXCLUDES THE ANNEX A CONTROL AND REPLACES IT WITH OUR CUSTOM

CONTROL. WE EXPLAIN THE REASON FOR DOING SOMETHING DIFFERENT AND WHAT WE DO INSTEAD.

4. OTHERWISE, WE DECLARE THE ANNEX A CONTROL AS A NECESSARY CONTROL.
5. For *ALL* necessary controls, we:

    a) cross-reference the control back to the risk treatment plans in which the control is used.
    b) record the implementation status of the control:

        i. Implemented
        ii. In progress
        iii. Not yet implemented.

If we determine that an Annex A control applies but does not feature in our risk treatment plans, we determine where it should go and rework the plan (or plans) accordingly.

Formulating risk treatment plans

We create one risk treatment plan per event. The layout of each plan is:

1. A description of the event;
2. The risks before treatment (presented in a table of likelihoods and consequences, and a corresponding graph);
3. The risk treatment plan story:

    a) Preventing the event;
    b) Detecting the event;
    c) Reacting to the consequence(s);

4. The risks after treatment (presented in a table of likelihoods and consequences, and a corresponding graph) together with:

    a) Our rationale for why the risk acceptance criteria are met;
    b) Evidence that the risk owner has approved the plan and has accepted the residual risk.

5. An index to earlier versions of the plan, should they exist.

The residual risk calculations are performed by IMS-Smart software which allows us to ensure that, having decided upon the control behaviour, the calculations are consistent with that behaviour.

Risk owner approval

The risk owners meet to review and approve the risk treatment plans and the results are recorded in the minutes of those meetings.