A.2 Risk assessment process

Introduction

This « [RAP1] say what this is (e.g., document, (web) page) » describes our approach to risk assessment. It explains how we identify, analyse, and evaluate risk; our risk criteria; risk ownership; when we schedule risk assessments; and the validity of our results.

Risk identification

We identify information security risks through a consideration of those issues that are relevant to information security and the scope of our management system. Each risk has two components: an *EVENT* and a *CONSEQUENCE*. The consequences that are relevant to information security are:

Undesirable disclosure of information;

Loss of integrity;

Inability to carry some or all of one's business.

Risk analysis

Risk is then the product:

LIKELIHOOD of the occurrence of the event * severity of the *POTENTIAL CONSEQUENCE*

The dimensions of likelihood are reciprocal time (i.e., $^{1}/_{\text{time}}$ or time^{-1}). We use a logarithmic scale where the number 2 corresponds to once a year. Thus 0 corresponds to once a century, 4, once a week and 7, about every 5 minutes.

Likelihood represents the chance or probability of something happening. However, although some event might be extremely unlikely, once it does occur the *FREQUENCY* of recurrence might be extremely high. As information security controls must contend with the frequency of attack, we often use the terms frequency and likelihood interchangeably and refer to them as *FREQUENCY OR LIKELIHOOD*, or FoL for short.

We measure consequence in terms of money. Again, we use logarithmic scales, with the number 2 representing £1,000. Thus 0 corresponds to £10 and 5 corresponds to £1,000,000. « [RAP2] offset the scale, if necessary, to ensure that the borderline between acceptable and unacceptable risk intersects the top left and bottom right corners of the risk square, i.e., a risk level of 6. With the number 2 representing £1,000, the number 4 represents £100,000. Since the number 2 also represents a year, a risk level of 6 (= 4 + 2) corresponds to an acceptable risk of losing £100,000 per year. If your limit of acceptable risk is, say, £10,000 per year, to retain the number 6 as the limit of acceptable risk, rewrite this sentence to read "…with the

number 2 representing £100. Thus 0 corresponds to £1 and 5 corresponds to £100,000” »

As we use logarithmic scales, the product of likelihood and consequence is determined by summing their logarithmic values. Thus, a risk formed by having a likelihood of 3 and a consequence of 2 corresponds to a risk level of 3 + 2 = 5, i.e., a loss of £10,000 per year. « [RAP3] If you have changed the scale factor you must also change this sentence. Thus, if the number 2 represents £100, rewrite this sentence to read “…, i.e., a loss of £1,000 per year.” »

Risk ownership

A risk owner is a “a person or entity with the accountability and authority to manage the risk”. Their task is to approve the risk treatment plan and residual risk for the risks

that they own. In our organisation « [RAP4] say who or describe the process you use to identify them. »

Risk evaluation

Having identified and analysed our information security risks, we compare them to our risk acceptance criteria (see below).

Risk criteria

The figure shows a graph of severity versus FoL and highlights the regions of acceptable and unacceptable risk. The orange line is the borderline between the regions of acceptable and unacceptable risk.

A risk is deemed acceptable:

if it lies on or below the borderline, i.e., it is in the green, yellow or orange regions; and

risk treatment consists of a mix of:

preventive and detective controls, with a statement declaring the acceptability of any residual risk;

detective and reactive controls, with a statement declaring the acceptability of any residual risk;

preventive, detective, and reactive controls, with a statement declaring the acceptability of any residual risk.

the derivation of residual risk takes proper account of the behaviour of the controls used to treat the risk (see our risk treatment process)

« [RAP5] Create a risk square put it here. »

Scheduling risk assessments

We perform risks assessments periodically according to the schedule presented in our risk assessment results. We also perform risk assessment when we are

considering change or changes are imposed upon us. These are also identified in our risk assessment results.

Validity of results

Repeated risk assessments are:

CONSISTENT, because we apply the same method and criteria each time;

VALID, because the measure of risk is dimensionally correct and, as part of the risk treatment process, it is reviewed and approved by the risk owner;

COMPARABLE, because our method is mathematically sound.