

Evaluating the effectiveness of regulatory training and awareness solutions

This article first appeared in The Compliance Institute Gazette, Issue 171, November 2009

Introduction

To what extent does training in your organisation reduce regulatory risk? Is the design and delivery of regulatory training in your organisation informed by a robust evaluation of existing provision? Are you able to calculate the return on your training investment?

If you are unable to answer these questions, you are certainly not alone! A quick glance at a random sample of UK plc annual reports reveals that many of our best known corporates report their training in terms of training spend per annum with little attention paid to the value that training delivers, or the extent to which it minimises risk and reinforces compliance.

The paucity of models available to organisations is perhaps a key reason why so few organisations evaluate their training. Half a century ago, Donald Kirkpatrick¹ wrote about four levels of evaluation which he called reaction, learning, behaviour and results. He said that an evaluation of the effectiveness of training required organisations to measure what learners thought of their training, how much they had learned, what behaviours had changed, and how training had impacted on results.

Since 1959 there have been various attempts at developing alternative models, but Kirkpatrick's remains the most widely recognised. In spite of this, its use is sporadic. But Kirkpatrick's model should not be easily dismissed, since it has real relevance for those of us operating in regulated environments, engaged in changing employee attitudes and behaviours so that risk is minimised and compliance is enforced.

Knowing the value that is derived from training is just as important as knowing how effective it is so that we can pinpoint how to meet employee and organisational needs, plan, design, develop, refine and deploy future training. Kirkpatrick's four level model has much to tell us so that we can achieve all these things; each level is therefore explored in turn.

Level 1 – reaction level evaluation

This level is perhaps the most widely used. Most commonly referred to as 'the happy sheet', it is typically conducted in the form of a questionnaire which learners complete at the conclusion of their training. Sadly, its emphasis is frequently restricted to the suitability of the training venue, the perceived quality of the learning materials provided and the

effectiveness of the trainer. Whilst these are legitimate, they fail to capture the extent to which learners perceived the training itself to be effective.

High quality reaction level evaluation asks questions about the extent to which training has met its intended objectives. For information security, for example, this might mean asking learners to provide ratings against a number of questions as shown in Figure 1 below.

As a result of the training provided I:	Low		High		
now know the steps I must take to securely transfer information between my organisation and third parties	1	2	3	4	5
Know under what circumstances I may disclose personal information to callers	1	2	3	4	5

Figure 1: Examples of reaction level questions

Other approaches provide learners with statements representing two opposite extremes and invite them to indicate, which, following training most closely resembles their perception. An example is illustrated in Figure 2 below.

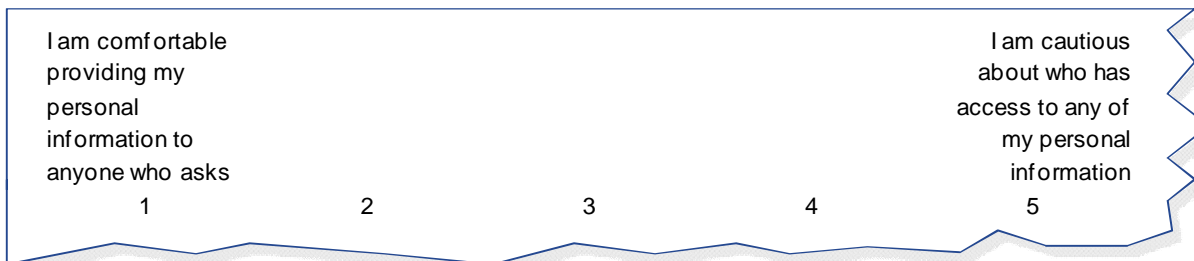


Figure 2: Alternative example of a reaction level question

Critics cite that Level 1 approaches provide a picture only of learner perception; they do not assess the extent to which new learning has been applied in the workplace. True enough, yet it can nevertheless be useful for two reasons. For those developing and deploying regulatory training it provides a temperature check of the extent to which training has changed learner attitudes. Second, as organisations turn increasingly to computer-based training, (CBT), asking questions of learners immediately after they complete their training about, for example, ease of navigation are crucial to ensuring its effectiveness.

However, to really gauge the extent to which training has been transferred into the workplace and to determine an organisation's return on investment, evaluation needs to go further.

Level 2 evaluation – learning

Level 2 evaluation is used more frequently than maybe is realised, especially by organisations delivering training through CBT. It involves testing learners' knowledge pre and post training, so providing statistical evidence of completion of training and, some would say, the acquisition of knowledge.

Yet there are three pitfalls to watch out for when evaluating at this level. First, because it lends itself to statistical analysis, over-reliance is often placed on this method of evaluation. Questions asked through CBT platforms are generally multiple-choice in nature, which raises the spectre of the test governing the nature of the learning content itself. To illustrate the point, suppose, for example, at the end of anti-money laundering (AML) training for front line employees (rather than specialists), learners are asked which two Acts of Parliament give rise to a criminal offence if there is a failure to make a Suspicious Activity Report, or what, from four different options, is the maximum prison sentence for any person 'tipping off' a suspected money launderer who may be under investigation by the authorities. The focus of training quickly shifts to emphasising legislation and regulation, since it is easy to test these areas, rather than on helping learners to become familiar with identifying suspicious transactions as they arise, and knowing how to escalate and report their suspicions.

Second, tests such as these frequently test short term memory rather than real learning. Third, people do not always do what they know they should.

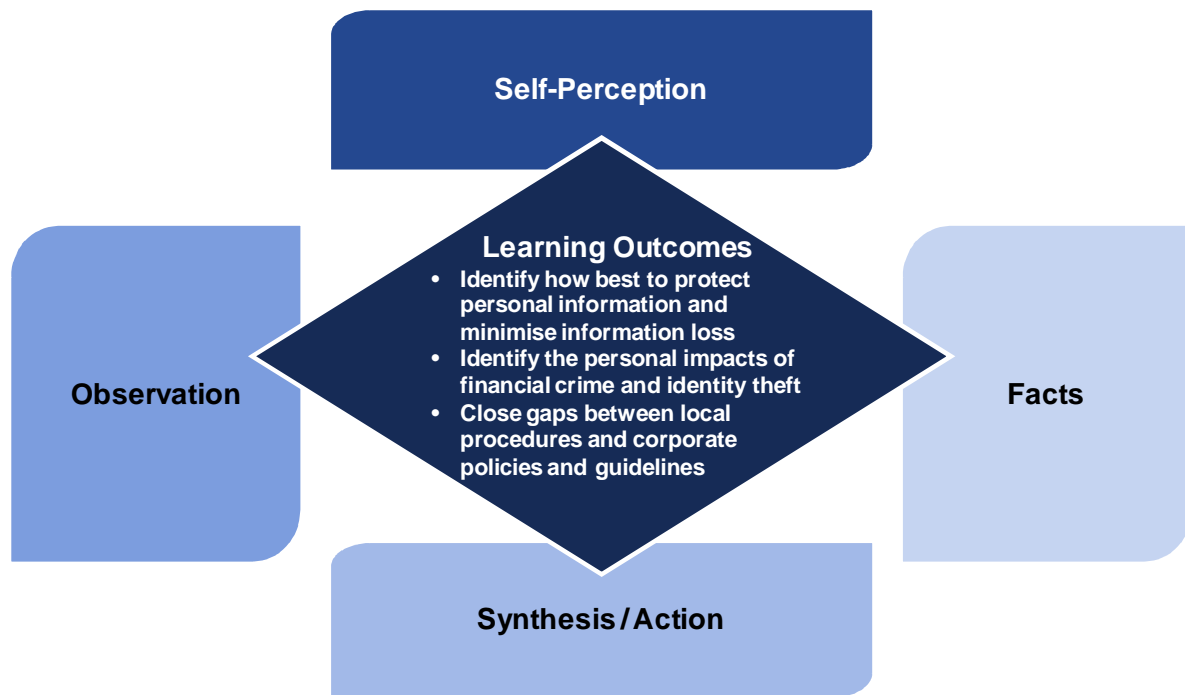
Third, statistical analysis of test results rarely provide hard evidence that real behaviour has changed or that regulatory risk has been reduced. A further layer of evaluation that helps us to assess the extent to which behaviour has changed is needed.

Level 3 evaluation – behaviour

Behaviour is perceived to be the hardest level to conduct for three reasons. First, to be truly useful, it needs to be conducted some time after training has been completed, typically, between three and six months post-training. It is not difficult to see why this level of evaluation so often slips from busy agendas! Second, there is a perception that the evaluation of behavioural change is shrouded in mystique and requires extraordinary skills that ordinary people do not possess! Nothing could be further from the truth! Whilst our attitudes and beliefs are generally hidden from others unless we wish to reveal them, our behaviours are visible to and observable by others. This means we can create a framework for evaluating the extent to which desired behaviours are being demonstrated.

Third, as soon as we begin to think about how to evaluate behavioural change, we realise we must give consideration to what are the desirable behaviours we wish to promote through training in addition to what knowledge people will need in order to carry out their work. For information security, for example, we may wish to see changes in the behaviours of our employees at their workstations; locking their computer screens; preserving and maintaining password security; preventing 'tailgating'; removing sensitive documents from printers; or conducting rigorous and intelligent identification and verification procedures when taking calls. This leads to the perhaps obvious conclusion that the evaluation of training needs to be planned and considered before the training itself is even designed and delivered!

How behavioural change is evaluated following training will vary from one organisation to another, but a generic framework is illustrated in Figure 3 below.



(c) The Fifth Business Experience Ltd

Figure 3: a framework for conducting level 3 evaluation

Self perception: Self-perception plays a part in this level of evaluation just as it does in Level 1. Conducting ‘pulse’ checks that garner quantitative and qualitative data from employees indicating the extent to which they perceive their behaviour has changed is part of the legitimate and valid mix of data that helps us understand what has changed.

Observation: collecting feedback from managers, (who after all, have additional responsibility for ensuring compliance, minimising risk, and protecting personal information) can reveal valuable insights. For example:

- whose and how many Blackberries are left unlocked and unattended on workstations?
- whose and how many desks are littered with sensitive documents for anyone to see in an open plan environment?
- where data (even encrypted) is held on removable media, after training, is it being locked away securely?

Other novel approaches to capturing observations can also be deployed. Recruiting actors to pose as customers or visitors is one innovative approach. The actors are briefed to ask questions of employees around the organisation and then provide debriefs of their experiences. The degree of ease or difficulty with which they have garnered sensitive

information provides organisations with rich material that exposes areas of continuing weakness and pinpoints areas for further remedial action.

Facts: collecting outputs from risk / audit teams, gap analyses and change plans, and monitoring the extent to which previously agreed actions have been taken against agreed timescales provides a further dimension of the effectiveness of training and awareness programmes.

Synthesis / action: From behavioural evaluation, risk, compliance, information security, data protection, fraud and other relevant teams can synthesise findings, identify trends and patterns, and therefore pinpoint short / medium / long-term actions (remedial and developmental) to reinforce messages and promote the required behaviours.

Level 4 evaluation – results

Organisations rarely evaluate training at level 4 and therefore have little notion as to what is their return on their investment in training.

But capturing results for regulatory training is not difficult. Organisations evaluating the effectiveness of information security training, might, for example, capture over time:

- numbers of breaches of the Data Protection Act occurring and near misses;
- costs of internal detection, investigation; and notification;
- costs of informing customers of any steps taken following a breach.

There will, of course, be many other statistics from which organisations can draw to support meaningful Level 4 evaluations.

What is clear is that particularly during turbulent economic conditions such as those we are currently experiencing, organisations need to make their training investments work harder and more effectively for them. Spending money on training does not in itself guarantee risk is being reduced or compliance is being maintained. Evaluating the effectiveness of training is consequently becoming increasingly important so that organisations can assure themselves that their training investment is being spent wisely and that they are getting real value from their efforts.

(Ken Cohen is Director of The Fifth Business Experience Limited, which specialises in the design and delivery of innovative training and development solutions and in bringing regulatory training to life. He can be contacted at ken.cohen@fifth-business.co.uk)

¹ 'Evaluating Training Programmes', Donald Kirkpatrick and James Kirkpatrick, Berrett-Koehler, 3rd edition, 2006