April 13, 2009

The eLearning Guild's
LEARNING SOLUTIONS SM
Practical Applications of Technology for Learning
e-Magazine

THIS WEEK: Management Strategies

What's Your E-Learning Strategy for Compliance Training?

By David Becker

Support of socio-political agendas, or simple fear of censure, leads to much of today's compliance training. However, designing a compliance training strategy based on a risk assessment model and treatment hierarchy can reduce these influences. It can drive a more rational, measurable, and aligned approach to compliance training. This can result in better compliance at reduced cost, but even more, it can also contribute to brand value and increased revenue.

The global financial crisis (or GFC) is pushing organizations to review and consolidate their spending and business activities. The legislative environment is ripe for significant change in response to the GFC and to climate change. Now is a good time to rationalize your compliance training strategy.

Knee-jerk reactions: FAIL

Here are three examples of poorly thought-out compliance training.

A financial services company recently spent a large sum of money developing a very media-rich e-Learning module focused on unacceptable sexual harassment behaviors, the consequences for the people involved, and the impacts on the organization. The module ended with a mandatory summative assessment generating scores and completion records.

Company managers gave a range of reasons for this approach, including, "It's important that staff understand their obligations under the law," and, "The

Compliance training is a huge application area for e-Learning. Yet much of this training has its basis in reaction rather than a strategy based on risk assessment. This week's article presents a rational, measureable, and aligned approach to compliance training. Use it and reap benefits in better compliance, reduced costs, greater brand value, and increased revenue!

A publication of
THE ELEARNING GUILD

company has an obligation to provide a safe workplace for its staff." When asked how many serious sexual harassment incidents they had dealt with in the last year, the answer was, "No serious incidents, and just a couple of minor ones."

Eventually someone admitted that a generalized fear of legal action had led to the development of the module. So the question must be asked, was this expensive e-Learning module the appropriate response to the assessed risk?

In contrast, a sports and entertainment venue put together a large safety curriculum. It consisted of contractor induction modules based on a "tick and flick" approach. That is, it exposed learners to basic text and graphic screens of regulations, asked them to confirm their understanding, and recorded their responses. This venue spends massive amounts of money on insurance, they experience many small accidents, and from time-to-time a major one. All of these significantly impact their bottom line.

In this case the risk is manifest. So why is the response so cursory? Was the cost of lowering the rate of accidents through training higher than the cost of insuring against them and compensating those who had suffered? Had anyone actually run the numbers? No.

Finally, a large Government department undertook an enterprise-wide privacy training program. This program was a reaction to direction from a senior official who was embarrassed by several high-profile breaches of privacy laws that had made national headlines. These breaches cost the Department damage to their reputation, and many thousands of dollars in investigating and fixing them. Other minor breaches were also a regular occurrence.

The Department carefully put together the training response to fit within their privacy training framework. It specifically targeted the most commonly occurring and serious breaches, and it also fit within a modest budget.

These real-life examples illustrate a very common weakness: the tendency to select and fund compliance-based training targets in reaction to perceived threats, and to internal or external socio-political pressures. But is there a more rational approach?

Rational approach

Compliance management, as a subset of risk management, usually employs two rational tools. The first is risk assessment, and the second is the hierarchy of controls.

Risk can be assessed in three ways: the likelihood

[D]esigning a … strategy based on a risk assessment model and treatment hierarchy … can drive a more rational, measurable, and aligned approach to compliance training. This can result in better compliance at reduced cost, but even more, it can also contribute to brand value and increased revenue.

The eLearning Guild's
LEARNING SOLUTIONS℠
Practical Applications of Technology for Learning e-Magazine

Publisher David Holcombe

Editorial Director Heidi Fisk
Editor Bill Brandon
Copy Editor Charles Holcombe

Design Director Nancy Marland Wolinski

The eLearning Guild™ Advisory Board
Ruth Clark, Lance Dublin, Conrad Gottfredson, Bill Horton, Bob Mosher,Marc Rosenberg, Allison Rossett

Copyright 2002 to 2009.
Learning Solutions e-Magazine™ (formerly **The eLearning Developers' Journal™**). Compilation copyright by The eLearning Guild. All rights reserved. Please contact ***The eLearning Guild*** for reprint permission.

Learning Solutions e-Magazine™ is published weekly for members of ***The eLearning Guild***, 375 E Street, Suite 200, Santa Rosa, CA 95404. Phone: +1.707.566.8990. www.eLearningGuild.com

Learning Solutions e-Magazine™ is designed to serve as a catalyst for innovation and as a vehicle for the dissemination of new and practical strategies, techniques, and best practices for e-Learning design, development and management professionals. It is not intended to be THE definitive authority … rather, it is intended to be a medium through which e-Learning professionals can share their knowledge, expertise, and experience. As in any profession, there are many different ways to accomplish a specific objective. **Learning Solutions** will share many different perspectives and does not position any one as "the right way," but rather we position each article as "one of the right ways" for accomplishing an objective. We assume that readers will evaluate the merits of each article and use the ideas they contain in a manner appropriate for their specific situation.

The articles in **Learning Solutions** are all written by people who are actively engaged in this profession – not by journalists or freelance writers. Submissions are always welcome, as are suggestions for future topics. To learn more about how to submit articles and/or ideas, please visit our Web site at www.eLearningGuild.com.

that a given risk will become a reality, how often this risk will occur, and the impacts on the organization should it do so.

These risks are subject to a hierarchy of controls, with the higher controls being better than the lower ones at managing the risk. These controls are to:

- *avoid* or eliminate the risk,
- *reduce* the likelihood of it occurring, and minimize its impacts should it occur,
- *transfer* the risk by outsourcing the activity or insuring against it, and
- *retain* the risk, in which case you budget for the risk being realized.

Let's apply this rational framework to the earlier case studies. In the financial services company, sexual harassment was fairly unlikely, fairly infrequent, and had only minor impacts on the organization. The training strategy tried to avoid and reduce this risk, and perhaps to transfer it, by recording each staff member's score. This would allow the company to potentially transfer the liability to the individual, should an incident occur.

Generally speaking, the higher levels of control are more expensive and harder to apply successfully, so in this instance, for a pretty low-end risk, the company applied the most expensive and difficult controls. Why?

It is likely that fear of future legal costs, brand damage, and Government intervention and regulation probably played a role. Call me cynical, but it is unlikely that creating a safe workplace for their staff was much of a factor. So the driver is actually proactive, which is great, but not rational or data-driven, because little evidence existed to suggest that their fears would be realized.

In the second case, the risk of a health and safety incident at the sports venue was highly likely, it happened often, and the impacts ranged from moderate to severe. Yet their primary control strategies were transfer and retain.

It is possible, given the high turnover of contract staff, that the cost of using training to avoid or reduce this risk was higher than the cost of insurance. However, given that premiums only ever go up, and generally include penalties for claims, this strategy would eventually cease to be viable.

In this case, the underpinning beliefs were multiple: learners were highly resistant to training, it would take too long, and they need to be on site quickly. And, of course, that old chestnut, "by recording their results, we transfer the liability to the contractor anyway" (a commonly held assumption, that delivers mixed results in reality). So are these reasons valid? Maybe, or maybe not, but they are certainly not founded on evidence.

Lastly, the Government department was faced with a risk of privacy breaches that was moderately likely, quite frequent, and the impacts of which ranged from minor to severe. Their response was carefully budgeted and focused on avoidance, which, as a top level of control, was appropriate to the risk. The strategy may also have employed a bit of transfer by recording the assessment results. So in this example, the department did take an evidence-based approach.

How might your organization apply this framework to create a rational compliance training strategy?

The first step in creating such a strategy is to set its scope and broad intentions. To do this, you must first understand the organization's compliance system, operating environment, and standards for compliance.

Set scope and intentions

An organization's compliance system comprises the regulations with which it must comply and the policies to which it has committed. The organization's processes and procedures implement the regulations and policies. Or put more simply, the regulations and policies establish the "why and what," and the processes and procedures describe the "who, how, and when."

While a lot of compliance training attends to the regulatory and policy level, and therefore employs knowledge and awareness training, an effective training framework must actually target both levels.

Consider the earlier case of the Government department implementing privacy training. Typically, this kind of training focuses on building staff understanding of the principles governing privacy, with the expectation that this constructivist approach will enable staff to apply the policy in any situation.

Privacy breaches usually result from procedural non-compliance, for example, taking sensitive information home to work on at night. To be effective, the training must target both the policy and its associated procedures.

Understanding compliance through a systems approach offers a great advantage. It makes it possible to identify and target systemic failures and disconnects between policy and its operationalization, not only for training, but also for process improvement.

It is also necessary to understand an organization's compliance environment. Often referred to as an ecosystem, the compliance environment encompasses the organization, its regulatory authorities, its suppliers, its sales channels, its partners, its customers, and so on.

An effective training strategy must consider all these stakeholders, and how their interdependence produces compliance. It must also consider how much compliance training responsibility it will hold, and how much it will push outward to its ecosystem.

Consider the cell-phone carrier that receives many customer complaints about misunderstandings over its fair use policy. Under this policy, the carrier caps charges only until the customer reaches certain call and data volumes. After that point, additional charges apply.

The company responds with a product training program across its entire direct and partner sales network. It does this at considerable cost to itself in "time away from selling." But, upon more careful analysis, the company discovers that complaints were primarily arising from the customers of only one of its channel partners. Could this training have been more targeted? Yes, and perhaps the company could have shifted responsibility for the training to the channel partner.

Having considered the organization's systems, the ecosystem within which it operates, and the interplay between its components, some standards for the level of compliance must be set.

Typically, the definition of compliance training involves its ability to help staff avoid non-compliance. But the benefits of exceeding minimum compliance standards are both tangible, through reduced waste, rework, and increased revenue, and they are intangible, through improved brand perception, greater attractiveness to new recruits, and so on.

Exceeding compliance standards can also save money by anticipating tightening regulatory constraints and acting to meet tomorrow's standards within today's cost structures. Indeed, this achievement can actually

Compliance management, as a subset of risk management, usually employs two rational tools. The first is risk assessment, and the second is the hierarchy of controls.

Table 1 *Compliance training strategy: scope and intentions*

Compliance area	Standard	Audiences affected	Strategies
Emission standards	EURO 2012 targets for energy efficiency	Head office staff Warehouse staff Facilities management contractors Distribution contractors Channel partner staff Customers	Set facilities management and distributed standards and monitor compliance Train staff on energy efficiency measures Train channel partners on promoting green credentials to customers Offer fee-for-service training to partners on how to implement in their own business
Anti-discrimination Act	Anti-discrimination Act	Head office staff Warehouse staff	Basic training and assessment plus annual refresher
Federal Privacy Act	Minimum required	Head office staff Warehouse staff Channel partner staff	Basic training and assessment plus annual refresher for staff Specialist training programs to target areas of non-compliance Free training to channel partner staff on privacy and CRM system

deliver a new revenue stream through selling compliance training to ecosystem members, such as product certification training to resellers, and even to the broader market.

Numerous examples of this kind of compliance training exist. These include affirmative action programs that take staff training beyond the minimum gender discrimination requirements. They include carbon reduction training programs that focus on switching off lights and appliances, reducing paper use, and so on, once again exceeding minimum environmental regulations.

Setting standards for each compliance requirement to determine if they will be met or exceeded, and to what level, helps inform your decisions on targeting and funding of compliance training.

Bringing together this analysis about the organization's compliance system, its environment, and its standards, sets the scope and broad intentions of your compliance training strategy as exemplified in Table 1 on page 4.

Armed with an understanding of the organizations' compliance training scope and intentions, we can now apply a rational framework.

Identify risks

This framework is applied at three levels. At the highest level, it can underpin the identification of risks to be controlled through training. At the curriculum level, it can help select the training objectives to be addressed. Finally, at the learning design level, it can help determine suitable learning theories and activities. Let's begin with risk identification.

To do this, let us combine all three earlier case studies into one fictional company and examine the risks it faces. (See Table 2.) At this stage, a general analysis of all the non-compliance risks facing an organization should be conducted, and they should be as precisely defined as possible.

Already it is clear, from the table, that the sexual harassment risk, being small, might be controlled though other low cost controls such as contract clauses and performance management metrics. This leaves us with the health and safety and the privacy breach risks, both of which might be candidates for training.

Select training objectives

As an example let's focus on just the privacy breach risk, examining it at a more detailed level, and with consideration for the audience numbers to be trained. (See Table 3 on page 6.)

In this analysis, just a few examples were provided and the risk was considered from multiple perspectives, including the type, mechanism, and source. This multidimensional analysis helps in understanding the nature of the risk and how best to address it. From this table our training focus and budget can be further narrowed.

For example, you might consider a training intervention for staff with access to sensitive financial information, because, while the likelihood and frequency are low, the impact is so great that it may be worthwhile.

However, this is where the analysis becomes valuable in making training decisions. One can easily imagine the finance executives being sent on intensive and expensive training courses after the previous leak in a knee-jerk response to the serious financial impacts, but it is probable that training did absolutely nothing to reduce a risk that was already vanishingly small.

On the other hand, training thousands of staff on how to prevent privacy breaches while information is in transit, offers excellent potential to reduce the likelihood and frequency of information being leaked through that mechanism. A similar, if less powerful (because the impacts are lower) business case can also be made for training to reduce internal leaks through misfiling.

Having selected some training objectives to be funded, it is critical at this point to assign some metrics. Contrary to many LMS vendors' claims that a dashboard showing the percentage of staff

Risk can be assessed in three ways: the likelihood that a given risk will become a reality, how often this risk will occur, and the impacts on the organization should it do so.

Table 2 *General analysis of non-compliance risks for a fictional company*

Risk	Likelihood	Frequency	Impact
Sexual harrassment	About 2% chance per year	Averaging less than 2 reports per year	Genarally resolved with brief counseling and performance management interventions
Health and safety incidents	About 10% chance per year	Averaging about 2 minor incidents per month, and 1 major per year	Minor incidents require < 3 hours on average to investigate and no medical costs Major incidents take, on average, 70 hours to investigate, and cost $90K, on average, for medical expenses, insurance premium increases, and fines. On one occasion, has resulted in union action and a site shutdown, estimated to have cost in excess of $250K.
Privacy breaches	About 5% chance per year	Averaging about 7 minor incidents per month, and 2 major incidents per year	Minor incidents take < 12 hours, on average, to investigate and fix Major incidents take, on average, 110 hours and $1,200K to investicate, and also involve intangible costs as embarrassment to public officials is considered to be very serious.

that have passed a sexual harassment course is a measure of risk control, compliance training can only be measured through its actual effects on compliance, or, as previously discussed, the degree to which compliance levels are exceeded.

Training analytics is a large subject in its own right. Suffice to say that compliance training must be measured on its impact, and work must be done to isolate the metrics from other effects, so the true value of the training in moving the metric can be determined. Finally, compliance training metrics should be measurable at a sufficiently granular level to allow for highly-targeted remedial training of individuals, targeted improvements in compliance process sub-components, and targeted improvements in the training programs themselves.

Develop learning design

Having identified the training objectives, let's work out the kinds of learning theories and activities that might be commensurate with their risk profile.

In Table 4 on page 7, each control level is assigned suitable training approaches, but some cells are blank, indicating that, for example, no training is planned for avoiding low frequency/high impact risks.

However, this is an example only. Each organization's table would vary depending on the kinds of risks they face and the resources available to manage them. It would also vary according to other factors, such as the organization's commitment to good corporate citizenship, its environmental policies, its branding as an employer of choice, and so on.

Whilst these factors may not be considered risks underpinned by data, they do have specific and measurable purposes, and can therefore form part of a rational compliance management strategy.

The key consideration is the level of training and assessment intensity needed to achieve the level of control desired. For example, laboratory workers required to frequently apply a new diagnostic, testing for a life threatening disease, would be good targets for a comprehensive certification program (avoid), while electrical contractors being inducted into a new building site might only need confirm their understanding of the company's sexual harassment policy (transfer).

In this way, the costs of compliance training can be effectively controlled by assigning more funds to those risks that are both more likely to become a reality, and more likely to have serious impacts should they do so.

Costs can be further managed through the assignment of delivery channels and approaches to this same matrix. This is based on the assumption that more expensive training delivery channels and approaches are more effective, which, of course, is not necessarily true. But from a budgeting perspective, this approach allows you to control where your budget is spent, with funds being allocated based on risk and reward.

At this point it is worth mentioning the e-doc scenario. In an earlier case study the "tick and flick" approach was identified as inadequate as a risk management control. However, it has its place in our toolkit as a very low-cost response to minor risks. It can play a role in partially transferring risk to the learner, by making them aware of their responsibilities.

In wrapping up this proposed approach to compliance training strategy, it must be noted that, like any strategy, it should be regularly reviewed and reset, to adapt to changing organizational objectives, and to move training resources away from risks in decline and towards emerging risks.

Closing remarks

For small to medium enterprises, this framework, with its reliance on an evidence-based approach, may be beyond their capacity to resource. However, even a subjective analysis of the risks, using anecdotal evidence, will yield excellent recommendations for targeting compliance training for the maximum return on investment.

Larger organizations, with their dedicated compliance management departments, will already collect

[R]isks are subject to a hierarchy of controls, with the higher controls being better than the lower ones at managing the risk. These controls are to:* avoid *or eliminate the risk,* reduce *the likelihood of it occurring, and minimize its impacts should it occur,* transfer *the risk by outsourcing the activity or insuring against it, and* retain *the risk, in which case you budget for the risk being realized.

Table 3 *Analysis of privacy breach risk*

	Risk Dimensions			
Risk source	**Likelihood**	**Frequency**	**Impact**	**Comments**
Type: Leak of sensitive financial data to media	So low that it's hard to measure	< 1 in past 5 years	Resulted in major Government inquiry costing in excess of $3.2M	Very few people have access to this type of information
Mechanism: Leaks occurring when information is in transit	Around 25% of staff take sensitive information out of the office, or send it electronically or via post	Dozens of times daily	Massive variation, from documents going missing and never resurfacing, to laptops being stolen and whole filing cabinets disappearing, ranging in cost from a few dollars to many hundreds of thousands of dollars	More than 3,000 staff have access to sensitive information
Cause: Accidental leaks arising from poor filing practices	Estimated that around 40% of leaks result from accidental misfiling	Dozens of times daily	Generally small impacts as the files remain inside the premises and leaks are to other staff or departments	More than 8,000 staff file documents as part of their duties

much of the data upon which this framework relies. For these organizations, the learning and compliance functions, while separate, most likely already collaborate in determining the risks most suitable for training interventions.

However, as the examples given show, regardless of the organizations' size, these selections are sometimes poorly made, and based on fear of censure, or in response to socio-political agendas at work within the organization.

In part this is due to a risk management paradigm that, to some degree, is still ruled by fear. But new thinking is emerging, in which compliance is not just a mechanism to manage risk and control costs, but also contributes to brand value and revenue.

Training departments also need to recognize their proclivity towards socio-political influences when setting training agendas. With the advent of technology-enabled learning, the training department's capacity to influence the organization's performance, and its accountability to do so, has dramatically increased.

This is leading to a more widespread adoption of evidence-based learning and development strategy that gives consideration, but not undue power, to socio-politically driven training agendas.

Author Contact

For over fifteen years, David Becker has been helping clients around the world create learning and development strategies to increase revenue, manage risk, improve performance, and reduce costs. He can be contacted at david@eLearningconsultant.com.au.

Discuss these articles in the "Talk Back to the Authors" Forum of Community Connections (http: // www.elearning-guild. com/community_connections/forum/categories. cfm? catid= 17&entercat =y). You can address your comments to the author(s) of each week's article, or you can make a general comment to other readers.

Additional information on the topics covered in these articles is also listed in the Guild Resource Directory.

An organization's compliance system comprises the regulations with which it must comply and the policies to which it has committed. The organization's processes and procedures implement the regulations and policies.

Table 4 *Instructional activities organized by risk profile and control level*

	Control Level			
Risk profile	**Avoid**	**Reduce**	**Transfer**	**Retain**
High frequency/ High impact	Certification using a blend of classroom, virtual learning environment, and workplace observation	Ongoing professional development and assessment, using a Web 2.0 portal, monthly mentoring sessions, and an annual conference		
High frequency/ Low impact	Significant online and classroom induction training and assessment	Bi-annual online refresher training and a quiz		
Low frequency/ High impact			Minor, regular online awareness-raising presentations, and a quiz	
Low frequency/ Low impact			Annual confirmation of understanding, using an e-doc with completion tracking	

Do you have an interesting strategy or technique to share?

Get It Published in...

The eLearning Guild's LEARNING SOLUTIONS e-Magazine
Practical Applications of Technology for Learning

This publication is by the people, for the people. That means it's written by YOU the readers and members of ***The eLearning Guild***! We encourage you to submit articles for publication in **Learning Solutions e-Magazine**. **Refer to www.eLearningGuild.com for Author Guidelines.**

The eLearning Guild is a global membership organization like no other...

A singular focus on the art, science, technology, and business of e-Learning — and the collective knowledge of more than 33,750 members worldwide — are what sets The eLearning Guild apart...

Discover

How YOU Can Make a Difference...

The eLearning Guild is dedicated to meeting the needs of anyone involved in the management, design, and development of e-Learning. It's a member-driven Community of Practice and online information center that will equip you with everything you need to ensure that your organization's e-Learning efforts are successful.

The Guild offers four levels of individual and group membership. Starting at the FREE Associate level, the benefits you can gain from membership will enhance your professional experience. At the higher levels, you'll discover the Guild can be the core of your entire professional development program.

Join Today!

"Attending The eLearning Guild's Annual Gathering helped me realize the Guild's honesty and commitment to what e-Learning is all about — improving performance. Great conference, but even more — great Community of Practice!"

DAVID BRAUN, TRAINING & PERFORMANCE SUPPORT SUPERVISOR, SASKPOWER

Associate

- Every Issue of Learning Solutions e-Magazine
- Annual Salary & Compensation Report
- Social Networking Services
- The Guild Job Board
- Resource Directory
- Discount Programs
- Online Buyers Guide, e-Books, and Case Studies

Member

Everything Associates receive, and...

- Guild Research Reports
- 20% Event Discounts
- Enhanced Job Board Access
- Enhanced Discount Programs

Member Plus

Everything Members receive, and...

- Online Forum Participation (more than 120 live sessions in 2009)
- Online Events Archive (more than 480 session recordings in all)

Premium Member

Everything Members Plus receive, and...

- One Full Conference Registration (The eLearning Guild Annual Gathering or DevLearn Conference & Expo)
- One Pre-conference Workshop

Check it Out! *Visit* **www.eLearningGuild.com** *or call* **707.566.8990**