

Will Your Information Security Program Score a Compliance Touchdown?

**Paul Reymann
CEO
ReymannGroup, Inc.**

Will Your Information Security Program Score a Compliance Touchdown?

Wow! This year's Superbowl game was one of the best I have seen. I won't say who I was cheering for, but I should have taken those bets.

In many ways, preparing for and playing in the Superbowl has similarities to preparing a winning information security program in time for your next examination. Establishing a winning information security program that scores a touchdown with the regulators, employees, and customers is like preparing for the Superbowl – it requires a good coach or team leader, strategy, testing, training, execution, and adjustments.

Many institutions have a good program and continuously test and adjust it to reflect the changing dynamics of internal and external threats.

A Board approved written information security program may fall short of the final goal line. If every team member (employee) does not understand his or her enhanced roles and responsibilities under the new information security requirements, you will not execute a winning program. Not only does each employee need to know the plan - they must be able to execute it!

Proper training is crucial to your success – and frequently overlooked. As one of the original authors of the GLBA Data Protection Provisions while with the Department of the Treasury and now as President of USA Operations at Compliance Coach, Inc., I see the lack of adequate training emerging as a “sleeper” risk for financial institutions.

The following questions will help you validate the adequacy of your training strategy. If you answer “NO” to any of these questions, you should consider enhancing your training efforts.

1. Have all employees been trained on:
 - The requirements of the new data protection rules?
 - His or her enhanced roles and responsibilities for protecting customer information?
 - Money laundering schemes, enhanced due diligence, and reporting?
 - Pretext phone calling response procedures?
 - Identify theft response procedures?
 - Disaster recovery responsibilities?
 - Internet usage policies & procedures?
 - End user computing policies & procedures?
 - Record storage and retention procedures?
 - Vendor oversight?

2. Is your training:
 - Tailored to your institutions practices?
 - Tracable?
 - Reportable?

A comprehensive training strategy that covers the sensitivity understanding of the regulation and is tailored to your institutions practices will put you inside the compliance 10-yard line everyday! Will your training plan score a compliance touch down?