

Ensuring safe data delivery

NEWS

Unpacking the Compliance Issue

Seizing the initiative in risk management

CNS's Security Chapter Briefing programme recently featured a presentation from the FSA (www.cnsuk.co.uk/resources) addressing the issue of risk management and compliance, with the conclusion that, whether Basel (EU –Capital Requirements Directive) applies or not the management of IT Risk is expected by the FSA.

"The risk of loss resulting from inadequate or failed internal processes, people and systems or from external events."

Basel definition of IT Risk Management

However; having established the significance of IT risk management, it is apparent that compliance is not formally always defined by rules and guidance, even in the case of ARROW and CRD firms. At a granular level, it is the responsibility of each individual company to own its risk management and information security strategies.

Taking Control

Kevin Dowd (Director of Security Assessment at CNS) acknowledged that firms cannot therefore wait for the FSA to stipulate specific controls, but must seize the initiative and examine whether their systems can meet the new requirements. He continued by looking at the industry's reputation for shying away from proper risk assessments and accepting that it is difficult to understand the probability of failure, but that doesn't mean it shouldn't be attempted.

Kevin outlined how companies can address this issue, by considering everything and accepting that sometimes it's not possible to completely quantify risk, but only to measure uncertainty. Some areas which companies could consider are;

Self-assessment: it is common to conduct risk and control self-assessments to measure impact and probability as well as processes.

Forward looking: just because it hasn't happened doesn't mean it won't. Try and consider future scenarios.

Backward looking: internal losses can be used.

Challenges: risk is difficult to measure and can be limited by memory and biases.

Start to Unpack

In looking at these challenges, Kevin Dowd acknowledged that risk and threats are not always straight-forward to measure, but the process of unpacking your systems, to identify these risks and threats, is still extremely important. It's only through better understanding of the whole that risk management can be improved. He suggested the following process to meet some of the challenges and subjects for consideration:

Address the fundamentals

- Make sure you understand what you've got and, as far as possible, measure the risk.

Produce written controls

- Ensure these are at an appropriate level, but can be up scaled as necessary. The government's three tiers of control sets

has taken the emotion out of risk management and made it easier to apply across the institution. Take advantage of established best practice, like ISO27001.

Maintain what you have

- Commit to regular maintenance and reporting.

Good Practice

These ideas correlate with what is generally accepted to be good practice.

- Formal IT risk assessment process
- Link to risk appetite
- Independent challenge
- Regular: Review / update & monitoring
- Reporting to appropriate governance committees
 - Use of internal and external information and data
 - Feeds in to Operational Risk and enterprise-wide risk assessment

Compliance is traditionally seen as an overhead, but it does give us a clear baseline to work to and, in an ideal world, it should just be demonstrating what you already do.

It also doesn't have to be complicated. Often a third party can see more clearly where the risks and threats are during the process of examining the system. Once the system has been unpacked, the controls and maintenance can be relatively straight-forward. Rather than wait for monitoring to become mandatory, isn't it better to know your own, effective risk management strategy is already in place?

Scenario Modelling

CNS is running a scenario modelling day to help organisations identify threats and better understand risk. For more information please contact Shannon Simpson at CNS

shannon.simpson@cnsuk.co.uk

+44 (0) 20 7213 0922

www.cnsuk.co.uk

CNS RISK ASSESSMENT CONSIDERATIONS

IMPACT

- Financial impact can be difficult to quantify
- However, we can look at the elements:
 - Cost to fix
 - Fines
 - Re-work cost
 - Opportunity cost
 - Lost business

BE REALISTIC

- Would the work have been done another day?
- Look for real life incident patterns – can you correlate vs. actual costs or business results in the past?
- With all the above calculations, don't be afraid to quantify your uncertainty. e.g. you might calculate a risk and provide a number, but qualify with the fact that the result is uncertain, and highlight the data required