In this summary, risk is categorized into five focus areas, regulatory, legal, etc. Each of these categories is assigned an overall risk rating, based on the summation of threats that comprise that risk category. A description then summarizes the risk. Notice, the description does not have all the answers, this would be best left for an Action Plan. However, it also does not only focus on problems. It points out areas where there are good controls.

This type of summary is a good way to open a conversation about risk with executive leadership. It is accessible, written in business language, and definitive.

Conclusion

The key to making risk communication work is simplification. Risk is a very complex concept. It is difficult for anybody to understand, let alone executives. The emotional nature of risk can also cloud judgment, which can lead to bad decisions.

Simplicity and brevity cut right to the issue. The shorter and more succinct risk intelligence is, the more likely executives will not only understand it, but accept it and do something about it.

BIBLIOGRAPHY

Schneier, B. (2008, January 18). *The Psychology of Security*. Retrieved February 12, 2014, from Schneier on Security: https://www.schneier.com/essay-155.html

Stennion, R. (2012, October 16). *Why Risk Management Fails in IT*. Retrieved February 10, 2014, from NetworkWorld: http://www.networkworld.com/news/tech/2012/101512-risk-management-263379.html