Risk Mitigation.

For my company security is everything, because we do not want to lose profits or valuable information and have it sold on the dark web and such. Every company is required to have the minimum amount of security by FIPS, but we will go above and beyond on it. SOA is a proper way to keep everything organized and know what all is going on in your network. One thing to help set up a SOA is to identify and analyze risk that are happening. This gives a good idea on what kind of security is needed. Secondly you need to choose some controls to treat the risk you see. You either want to retain or tolerate the risks, avoid terminating risks, share or transfer risks, or modify or treat the risk. All these things are some ways you can deal with the risks that you have analyzed and identified. The next step in this is developing a Risk Treatment Plan or RTP. An RTP provides a summary of each of the identified risks, the responses that have been determined for each risk, the risk owners, and the target date for applying the risk treatment. Once this has been in place, you then can set a date and time on when you want to deplete the risk brought at hand. Providing a list of implemented controls also helps quite a bit. This list contains information if a control has been applied or not and what to try next in getting rid of these pesky risks. Maintaining the SOA is a vital point that you need to follow so that you know what to do and can share to others what to do if they encounter there risks and what they can do to deplete the risks. If more and more people are aware of the SOA, then risk management can become a strong front of the company.

Ciunci, M. (2020, May 19). 6 Steps to Develop Your Statement of Applicability. Retrieved July 09, 2020, from https://www.ispartnersllc.com/blog/6-steps-develop-statement-of-applicability/