Getting ready for ISO 27001

How we helped a global financial company use ISO 27001 as a tool rather than a checkbox.

Issue

The client was required to provide ISO 27001 certification annually to their own customers. Her predecessor hadn't taken it seriously, and found an inexpensive and lax audit team to get by year after year. This was causing the new CISO grief for two reasons. The first was it was challenging to honestly stand behind the certification they were getting. The second was that is was enabling bad behavior in IT, which pointed to that certification to justify that barely passable controls were sufficient. She needed IOS to do what it was supposed to, create a systematic way of managing risk.

Action

We worked with the client on bringing in our ISO 27001 expertise to do a true readiness assessment. This assessment would look at the ISO 27001 requirements as typical auditors do, and provide findings that not only highlight control deficiencies, but also areas that miss the intent of the standard. This would not be a checkbox exercise, but highlight how the company can and should use ISO 27001 as intended, to continuously improve your risk processes, tie controls to risk, improve those controls, and have meaningful discussions on risk priority with senior executives and the board.

Impact

The client was expecting a list of control deficiencies to help promote her case for control maturity, but also received some help viewpoints on how to improve risk management to prioritize that work appropriately. This report coupled with deficiencies in other audits has helped shine a light on themes to mature, in a risk-based way, the controls discipline in IT.