My thoughts on the ISG Framework:

I thought the whole document was well organized and very detailed. I really like the IDEAL model they laid out on page 7 of the document. I personally never heard of that and it looked to be practical and could apply to many situations.

The IDEAL model was developed by Carnegie Mellon University Software Engineering Institute and is an organizational improvement model that serves as a roadmap for initiating, planning and implementing improvement actions (ISG Framework pg 7). The IDEAL model has five phases, initiating, diagnosing, establishing, acting, and learning. Below is the main point of each phases (ISG Framework pg 7, table 1):

Initiating - Lay the groundwork for a successful improvement effort

Diagnosing - Determine where you are relative to where you want to be

Establishing - Plan the specifics of how you will reach your destination

Acting - Do the work according to the plan

Learning - Learn from the experience and improve your ability to adopt new improvements

The ISG Framework spells out 12 core principles that the framework was built upon. All twelve are located on page 2 of the frame work. The first principle is that the CEO or high level executive should receive and review an annual information security report. The report should be reviewed with staff and represented to the board of directors. Some of the other principals include implementing incident response procedures and implement policies and procedures based on risk assessment. It also calls for security awareness and training for all personnel. Organizations should have an operations continuity plan that has been established and tested. Organizations should also use security best practices when measuring information security performance.

I can see even the smallest organization all the way up to a large organization being able to adopt these.

I like how this framework gives responsibility and accountability to all levels of an organization from the employee to the board of directors.

The forms you can use to evaluate your dependency on IT looked to be well developed.

I agree with their assessment of what would need done to make this framework work in education. The only problem I see is that many institutions don’t have a centralized office that would apply this framework. Maybe they should address that aspect because with larger institutions, often, their IT staff are decentralized and might be assigned to different Schools, Departments with little collaboration.

This document provides everything you need to utilize this framework. This makes it so a user doesn’t need to track down other documents for reference.

It will be interesting to see if this framework is adopted by DoD and the corporate world. It is very straight forward and easy to follow and apply.

Daniel Bennett

IT Security Analyst

Security+