It struck me as I went through the document that this was very similar in design to the recent Financial and IT Audit process that I recently went through this year at my previous college in Red Deer, Alberta, Canada. As part of the office of Auditor's General requirements, we, in IT, performed a comprehensive risk assessment, detailed change management plan, dictionary of policies and procedures, access and job responsibility lists and a service catalog listing all IT services and risk mitigation information.

In reviewing the document further, the ISG framework would definitely help with the process that we went through last fall. Since the attached spreadsheet shows you the COBIT framework items that we had to address, I'm sure you can see how the IDEAL model from CMU blends in nicely. A standards-based, scalable model like this easily gets people in the right frame of mind to work together to develop the final governance policies and procedures. One other item mentioned in this document was the necessity of preparing and carrying out a comprehensive security awareness program.

I think Recommendation 4 really hits this topic on the head. Having the College endorse ISG framework and making it part of the financial and IT audit process really established the ISG as a part of the corporate governance compliance package.

The assessment tool was also spot on with the four sections clearly spelling out for your executive team exactly why we are doing what we are doing. Demonstrating the dependency on IT (from a financial standpoint) and then relating it to the amount of services performed and the risk involved in losing any of those services (through the service catalog) quickly brings the importance of this governance effort into reality. When you start to bring in the people and policies you have for guaranteeing the security of the information, the network and the systems, the executive team, while the external audit process is being performed, pays attention. In the long run, perhaps not all schools are able to do everything required to appease the auditors BUT a concerted effort is ensured if the list of items is obvious and the achievable items are simple and clear.

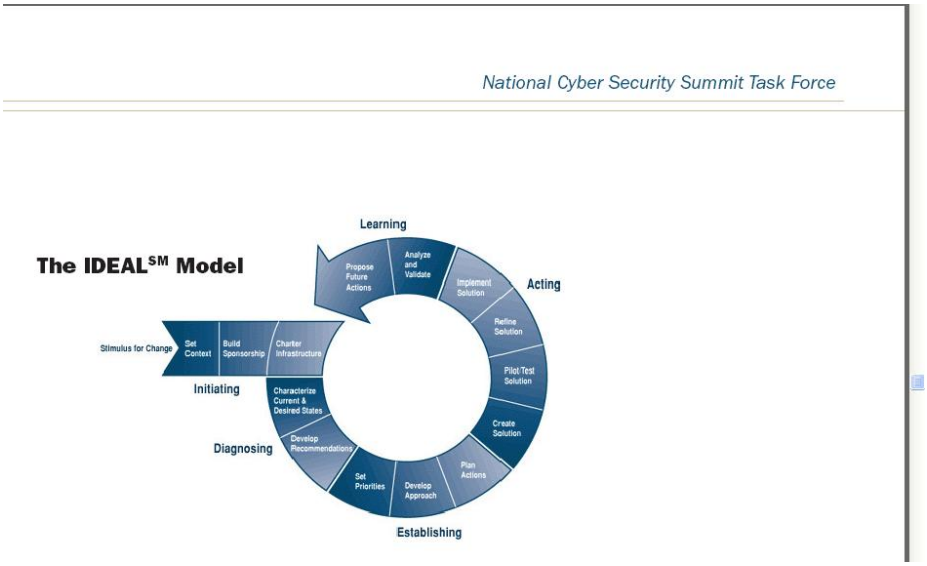
The part of this document I appreciated the most and will utilize in the future was the listing of responsibilities for Boards and Trustees, the senior executive, the executive team members, senior managers and finally all employees and users. Getting the entire organizational unit security program together was a daunting task (over eight months of preparation and collection of information) because there were so many elements and so many people involved. However having the independent auditor really helped because everyone gave this due attention.

This chart would have been helpful and so is a very good guide for anyone trying to establish the 'whys" of what we are trying to accomplish.

Information Security Governance

Responsibilities	Functional Role Examples
• Oversee overall "Corporate Security Posture" (Accountable to Board) • Brief board, customers, public	• Chief Executive Officer
• Set security policy, procedures, program, training for Company • Respond to security breaches (investigate, mitigate, litigate) • Responsible for independent annual audit coordination	• Chief Security Officer • Chief Information Officer • Chief Risk Officer • Department/Agency Head
• Implement/audit/enforce/assess compliance • Communicate policies, program (training)	• Mid-Level Manager
• Implement Policy, Report security vulnerabilities and breeches	• Enterprise Staff/Employees

I also thought this diagram was useful in showing the various phases of this project.



Using a simple chart with High-Moderate-Low (Red-Yellow-Green) rankings for risks of every component was extremely valuable when presenting to the executive team. It made the entire report much more easily interpreted and brought more reality to the process. Another element that the service catalog enabled was identifying key information systems and business owners throughout the College who had a stake in preserving data, ensuring its safety and viability and evaluating how business would occur without it.

In closing, I thought this was a great document to reflect some of the processes and tasks that had to be accomplished during that financial IT audit. For the college it was a very valuable experience. For IT, though at times it was a pain, it also provided some guidance on areas where we thought we had done due diligence but discovered wholes. Above all, it standardized everything we did and applied written policies to those areas where standard operating procedure was understood.

Attached please find the spreadsheet that was our deliverable for this audit.