

AN INNOVATIVE APPROACH TO TEACHING IT GOVERNANCE, RISK AND CONTROLS

Justin Greis and V. Ramesh

Ernst & Young and Indiana University

Justin.Greis@ey.com and venkat@indiana.edu

1. Summary of Learning Objectives

The objective of the course is to blend practical industry business and technology issues with the rigor of academic analysis in the areas of IT Governance, Risk and Controls. The key objective of this exercise is to enable students to clearly understand the issues in Identity and Access Management (IAM), the link between IAM and Logical Access Controls as well as the factors to consider in making a business case for [and choosing to invest in] IAM in an organization.

The primary challenge lies in making the business case both for and against implementation of Identity and Access Management as a means of addressing both tactical control deficiencies and enablement of key business initiatives. Students are required to prepare both a CIO and CFO perspective and debate the issue in front of a simulated executive board; however, they are not told which side they will be presenting until minutes before the debate begins.

2. Target Audience

Primarily graduate students in Information Systems Master's programs or as a module in an MBA core course. It is also possible to use this in a senior-level undergraduate IS course on Security or Information Assurance. No pre-requisite knowledge is assumed, although some exposure to security, business case analysis and/or control concepts can be helpful.

3. Business Problem

Investment decisions in enterprise automation and control technologies are often made without fully exploring the tangible (i.e. cost savings, revenue generation, etc.) and intangible (i.e. efficiencies, productivity, SLA optimization, etc.) benefits of the investment. Identity and Access Management solutions are typically implemented in response to audit findings/issues as a means of strengthening the control environment yet are rarely linked to the strategic enablers that IAM can offer such as customized customer/vendor portals, workflow, business intelligence, CRM and other organizational drivers. Executives are realizing that controls can be embedded in strategic enabling technology such as IAM in order to achieve compliance, embed governance and enable the business. This exercise is designed to familiarize students with arguments for and against making such an investment. It forces them to think like CFO and CIO in order to defend both the fiscally conservative and technologically progressive positions on the issue.

4. Teaching Notes

The case on IAM is delivered in the following format:

1. Students are assigned a set of reading materials on how to make a case for IAM. They are also introduced to leading practice control frameworks such as COBIT and ISO27001.
2. Two groups (4 – 5 students) are assigned the case and are given the week to prepare positions for and against the investment in IAM, each representing the CIO and CFO respectively.
3. Students must submit a presentation and summary memo for both sides of the debate; but sides are chosen through a coin toss at the beginning of class.

4. The groups make their presentation to the CEO (played by the instructor) and the board of directors (the rest of the class). One group represents the CIO (proponent of IAM), while the other represents the CFO side (opposed to the investment in IAM technology).
5. The groups that are not presenting are given an individual assignment that forces them to gain a good understanding of the core issues in the case. This allows them to be active participants during the Q & A portion of the debate.
6. The instructor serves as both debate moderator and leads the Q&A session after closing arguments have been delivered by both student teams.
7. After the key issues in the case are brought via the debate, the instructor and/or a guest speaker presents key materials around the concept of Identity and Access Management reinforcing the key issues in the case:
 - IAM satisfies both compliance/controls as well as enables strategic objectives of an organization.
 - Benefits of IAM are often cost savings that are difficult to quantify. Strategic benefits of enabling key organizational drivers are even more difficult to measure and quantify.
 - IAM satisfies one of the most fundamental IT governance concepts: identifying the “who has access to what” and thereby embedding accountability in key IT controls.