Combining multiple standards equals Staying on Target!
What is a Control?

- Controls are mechanisms that keep IT in check in terms of delivering value and managing risk.
  - *IT controls are like the brakes on a car. Not only do they serve to stop the car and keep it under control, they enable the driver to actually go faster and still remain safe.* (Stephen Katz, former CISO of Citibank)

- The perspective that IT and management must have these days:
  - Controls aren't a necessary evil mandated by regulation or by the Information Security department
  - Controls not only are a necessity, but will generate positive results when done correctly
People reject adopting a formal change management process because they fear it will slow down implementation of changes -- yet they don't stop and look at the delusion of speed. Yes, the changes are getting slammed in. However, how many of those changes fail during installation or go on to create incidents and problems?

Anyone with experience in enterprise-level IT management or support will tell you that uncontrolled changes cause problems to the overall IT environment with great frequency.
What Is A Control Framework?

- Essentially, a framework is a collection of controls organized to highlight what needs to be done at various levels of the organization.
  - An outline that tells what should be done but not how to do it.
- Never forget that because organizations differ, their control needs also will differ.
  - For example, all groups need change management if they wish to ensure stability, but how it is implemented will depend on the enterprise.
If a Control Framework Doesn’t Tell Us “How To” then What Does?

● There are three bodies of knowledge that are the de facto standard for answering this question and that are the basis of this presentation:
  – ISO 27001/17799
  – ISO 20000/ BS 15000 (ITIL)
  – COBIT
● COBIT does not include process steps and tasks because it is an Audit control and management framework rather than a process framework.
  – COBIT focuses on what an enterprise needs to do, not how it needs to do it.
  – COBIT “standards” are necessary for establishing an integrated process approach to InfoSec.

● ITIL (IT) and ISO 27001/17799 (InfoSec) provide the “how to” and the process framework.
• ITIL and ISO 27001/17799 covers specific areas which, when mapped to the COBIT framework, provide an environment of Good Computing and establishes a strong Trusted Computing Base.

• COBIT can be used at the highest level of IT governance to provide an overall control framework based on an IT process model that is intended to generically suit every organization.
Why Does the UCI T Office of Information Security Care About IT Service Support and Delivery?

- We can demonstrate repeatedly that change management is a foundation control for both security and availability, yet we still run into arguments from people who don't understand the causal link between their actions and problems on IT systems.
- Human error is the largest error factor.
- Research has shown that 80% of problems arise from human actions if left unmanaged.

(George Spafford, Pepperweed)
Why Does the UCI Office of Information Security Care About ITIL_ISO 27001/17799 or COBIT?

- IT best practices have become significant due to a number of factors:
  - Business managers and Board of Trustees demanding better returns from IT investments, i.e., that IT delivers what the business needs to enhance stakeholder value
  - Concern over the generally increasing level of IT expenditure
  - The need to meet regulatory requirements for IT controls in areas such as privacy and financial reporting; e.g., HIPAA, PCI, SOX, and FERPA
  - The selection of service providers and the management of service outsourcing and acquisition
  - Increasingly complex IT-related risks, such as network security
Enterprises that want to put their ITIL program into the context of a wider control and governance framework should use COBIT. (ITSGI White Paper, 2006)
The effective use of best practices can help to avoid re-inventing wheels, optimize the use of scarce IT resources and reduce the occurrence of major IT risks, such as:

- Project failures
- Wasted investments
- Security breaches
- System crashes
- Data Compromise
- Failures by service providers to understand and meet customer requirements
Summary

● Every organization needs to tailor the use of standards and practices to suit its individual requirements.

● All three of the ones presented can play a very useful part
  - COBIT in helping to define what should be done
  - ITIL and ISO 27000/17799 in providing the how to do it.
Examples of complementary elements between ITIL, COBIT, and ISO 27001/17799 are:

- Incident management. Defined as an ITIL service support process, it has an ISO complement in case of security incidents as well as a COBIT delivery and support chapter.
- Problem management. The COBIT delivery and support chapter defines incident and problem management processes that complement the ITIL problem management process.
- Change, configuration, and release management. These ITIL processes have a direct complement in COBIT’s change management and configuration changes section as well as in ISO 27001/17799’s operational change control, controls against viruses, and third-party security requirements.

COBIT and ISO also provide guidance, key indicators, and controls for the definition of Service-Level Agreements, capacity planning, availability management, and business continuity, which complement ITIL service delivery processes.
ITIL, COBIT, and ISO are good sources of inspiration. When it comes to process improvements, the tried and true is difficult to beat. But a single source of information may not be enough. Combining elements of at least these three major frameworks will broaden the scope of the resulting process and improve its quality.

(Jean-Pierre Garbani with Laura Koetzle and Thomas Powell, 2006)