CobiT and IT Governance - Elements for building in security from the top, down and the bottom, up

NEbraska CERT Conference 2006

Computer Security and Information Assurance

David Kohrell, PMP®, CISA®, MA, MCRP
david.kohrell@tapuniversity.com
Technology As Promised, LLC
TAPUniversity – www.tapuniversity.com

This presentation was developed using the OpenOffice.org

Session Outline

- A 3 prong exploration of:
  - (1) Does IT Governance (best practices, standards, regulations) really translate into more secured environment?
  - (2) If so what's the cost/benefit?
  - (3) If so does it have to be exclusive domain and delivery of top/down?

Wealth of best practices, standards and regulations exists for shaping corporate and IT governance.

Information Technology Governance, Common objectives for Information and related Technology (CobiT), IS0 17799 to name just a few.

Session Outline Continued

- Do those best practices, standards and regulations translate into a more secured IT and Corporate environment?
- If they do, are they worth the effort and cost involved?
  - Is there a danger of losing agility and market reaction time for the sake of smothering process?
  - Finally even if they do ensure a more secured environment and they are worth the up front cost, how can those best practices, standards and regulations be implemented in a way that supports bottom up engagement as well as top down direction?

Introductions

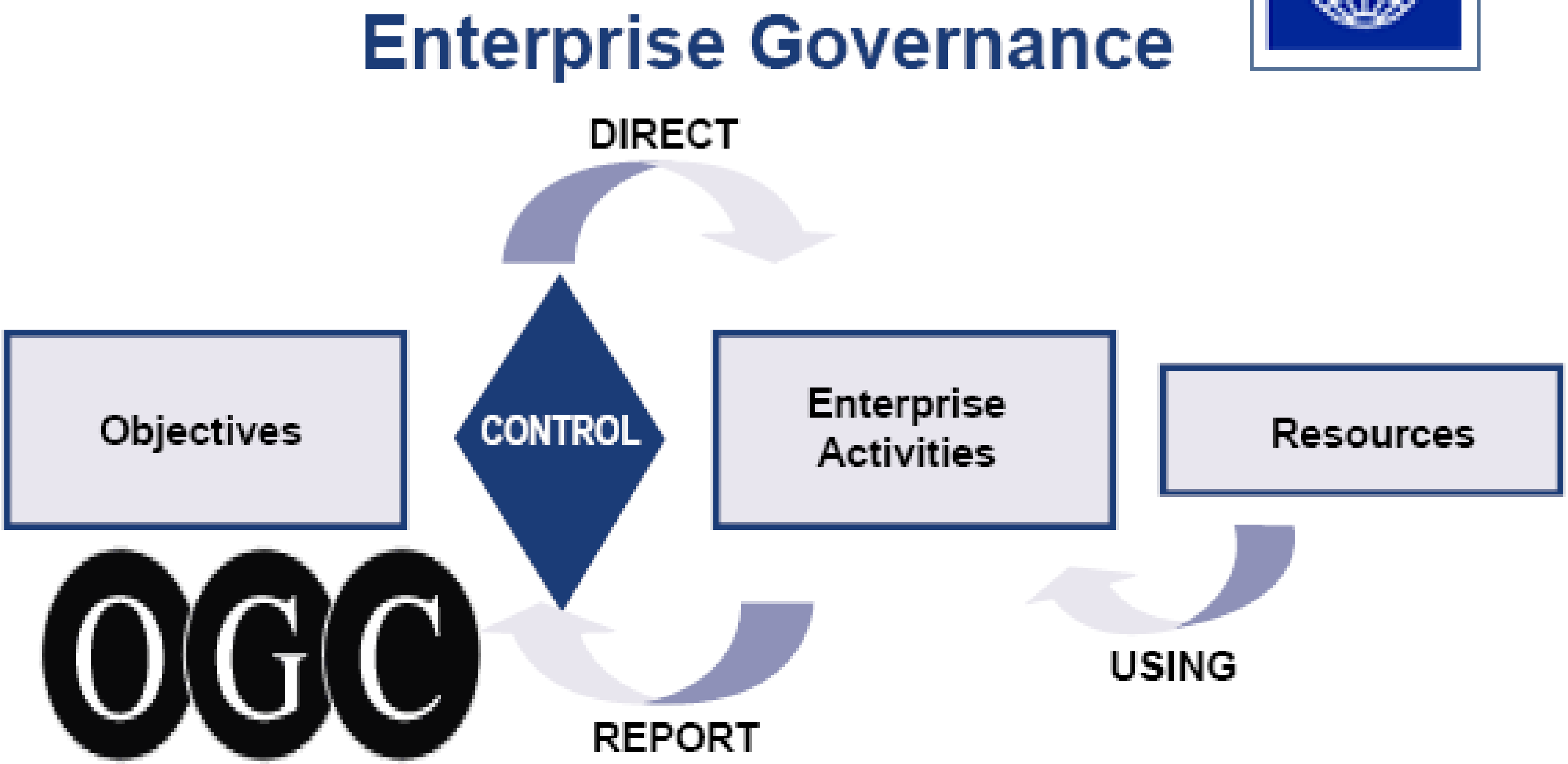
- Organization
- Role or Position
- Experiences
  - Compliance
  - Software Development
  - Security
  - Project Management
- Expectations for this presentation

Ground Rules

- Limit side conversations & mobile interruptions
- This presentation will present some thought provoking ideas and answers to those three questions. The delivery will be candid and audience participation will be encouraged.
- Honorable environment
  - Listen
  - Argue a point, not a person
  - Trust
- Yours:

CobiT – ITIL - ISO

ISO



OGC

Office of Government Commerce

ITIL®

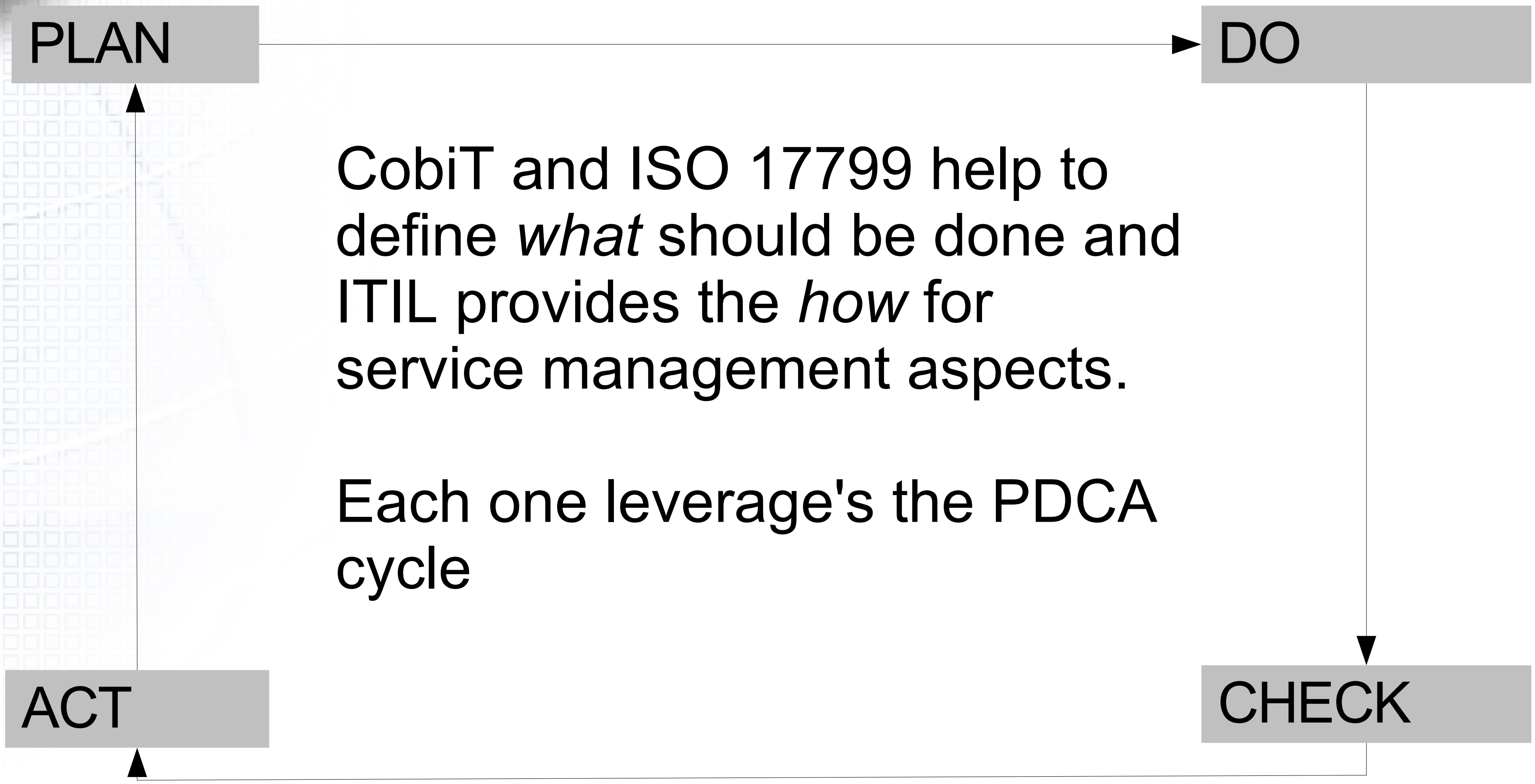
IT Service Management

CobIT – ITIL - ISO

Standards & Best Practice

- What's the difference between a **standard** and a **best practice**?
- What's the difference between a **standard** and a **regulation**?
- What impacts your work world in terms of:
  - **Standards?**
  - **Best practices?**
  - **Regulations?**

CobiT – ISO17799 - ITIL



PLAN

DO

CHECK

ACT

CobiT and ISO 17799 help to define *what* should be done and ITIL provides the *how* for service management aspects.

Each one leverage's the PDCA cycle

See American Society for Quality – http://www.asq.org/pub/quality progress/past/0804/qp0804dias.pdf

Roots

COSO™

COSO

- Due to accounting problems, the National Commission on Fraudulent Financial Reporting that was created in 1985… The results recommended that COSO undertake a project to provide practical, broadly accepted criteria for establishing internal controls and evaluating their effectiveness

CobiT emerged from the COSO practice

http://www.isaca.org &
http://documents.iss.net/marketsolutions/SOXCOSOMatrix.pdf

Mission

- “The CobiT Mission: To research, develop, publicize and promote an authoritative, up-to-date, international set of generally accepted information technology control objectives for day-to-day use by business managers, IT professionals and assurance professionals.”

Source: http://www.isaca.org

What is it

CobiT™

- CobiT ™ is the 'Control objectives for information and related Technology'.
- 34 CobiT IT control objectives:
  - 11 planning and acquisition
  - 6 acquisition and implementation
  - 13 delivery and support
  - 4 monitoring
- Each IT process is supported:
  - 8 to 10 Critical Success Factors
  - 5 – 7 Key Goal Indicators
  - 6 – 8 Performance Indicators

http://www.isaca.org

Using CobiT

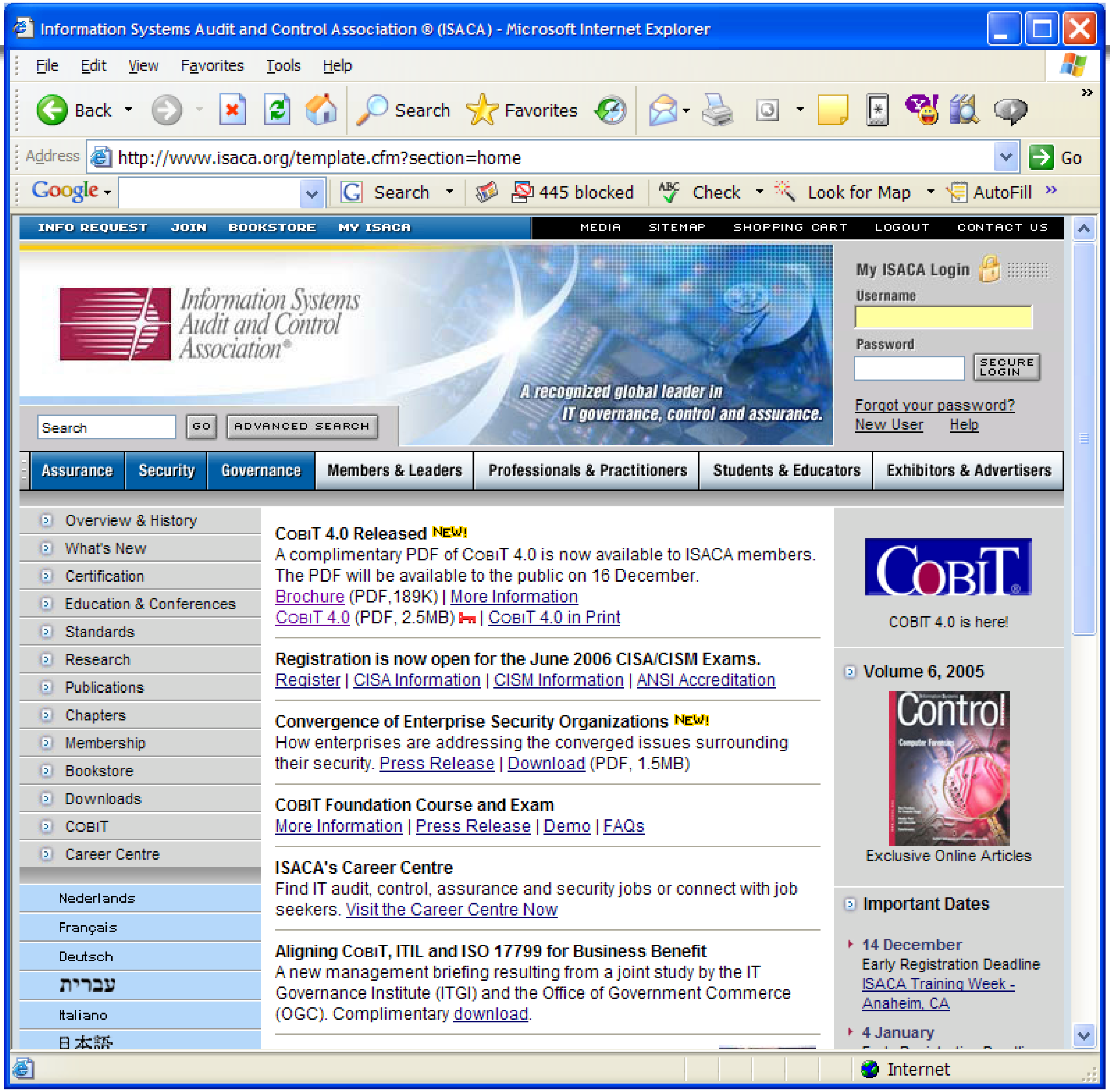
- Manage IT related business risks
  - Business objectives are the basis
  - Select appropriate IT processes and controls from the CobiT Objectives
  - Assess procedures and results with CobiT audit guidelines
- Identify industry models that provide guidance for supporting processes
  - CMMI
  - People CMM
  - ITIL, TickIT, etc

http://www.isaca.org

Who is responsible

CobiT™

- The Information Systems Audit and Control Association (www.isaca.org) through it's Information Technology Governance Institute (ITGI) formed in 1998


Information Systems Audit and Control Association ® (ISACA) - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.isaca.org/template.cfm?section=home Go
Google Search 445 blocked Check Look for Map AutoFill
INFO REQUEST JOIN BOOKSTORE MY ISACA
MEDIA SITEMAP SHOPPING CART LOGOUT CONTACT US
Information Systems Audit and Control Association®
A recognized global leader in IT governance, control and assurance.
My ISACA Login
Username
Password
SECURE LOGIN
Forgot your password?
New User Help
Search GO ADVANCED SEARCH
Assurance Security Governance Members & Leaders Professionals & Practitioners Students & Educators Exhibitors & Advertisers
Overview & History
What's New
Certification
Education & Conferences
Standards
Research
Publications
Chapters
Membership
Bookstore
Downloads
COBIT
Career Centre
Nederlands
Français
Deutsch
עברית
Italiano
日本語
COBIT
COBIT 4.0 is here!
Volume 6, 2005
Control
Exclusive Online Articles
Important Dates
14 December
Early Registration Deadline
ISACA Training Week - Anaheim, CA
4 January
Internet

COBIT 4.0 Released NEW!
A complimentary PDF of COBIT 4.0 is now available to ISACA members. The PDF will be available to the public on 16 December.
Brochure (PDF,189K) | More Information
COBIT 4.0 (PDF, 2.5MB) | COBIT 4.0 in Print

Registration is now open for the June 2006 CISA/CISM Exams.
Register | CISA Information | CISM Information | ANSI Accreditation

Convergence of Enterprise Security Organizations NEW!
How enterprises are addressing the converged issues surrounding their security. Press Release | Download (PDF, 1.5MB)

COBIT Foundation Course and Exam
More Information | Press Release | Demo | FAQs

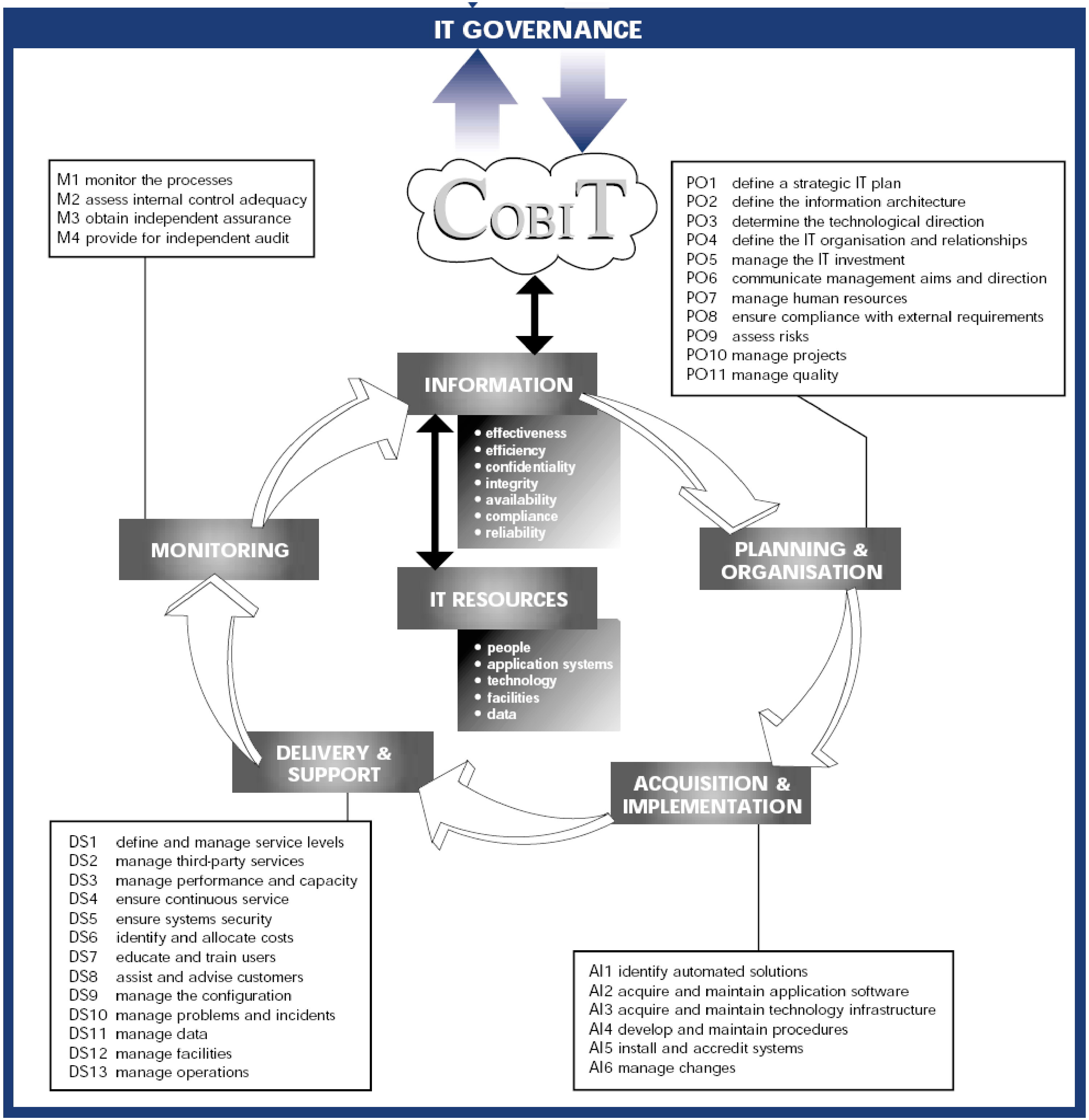
ISACA's Career Centre
Find IT audit, control, assurance and security jobs or connect with job seekers. Visit the Career Centre Now

Aligning COBIT, ITIL and ISO 17799 for Business Benefit
A new management briefing resulting from a joint study by the IT Governance Institute (ITGI) and the Office of Government Commerce (OGC). Complimentary download.

http://www.isaca.org

Lets dig deeper

CobiT™



- effectiveness
- efficiency
- confidentiality
- integrity
- availability
- compliance
- reliability

- people
- application systems
- technology
- facilities
- data

M1 monitor the processes
M2 assess internal control adequacy
M3 obtain independent assurance
M4 provide for independent audit

PO1	define a strategic IT plan
PO2	define the information architecture
PO3	determine the technological direction
PO4	define the IT organisation and relationships
PO5	manage the IT investment
PO6	communicate management aims and direction
PO7	manage human resources
PO8	ensure compliance with external requirements
PO9	assess risks
PO10	manage projects
PO11	manage quality

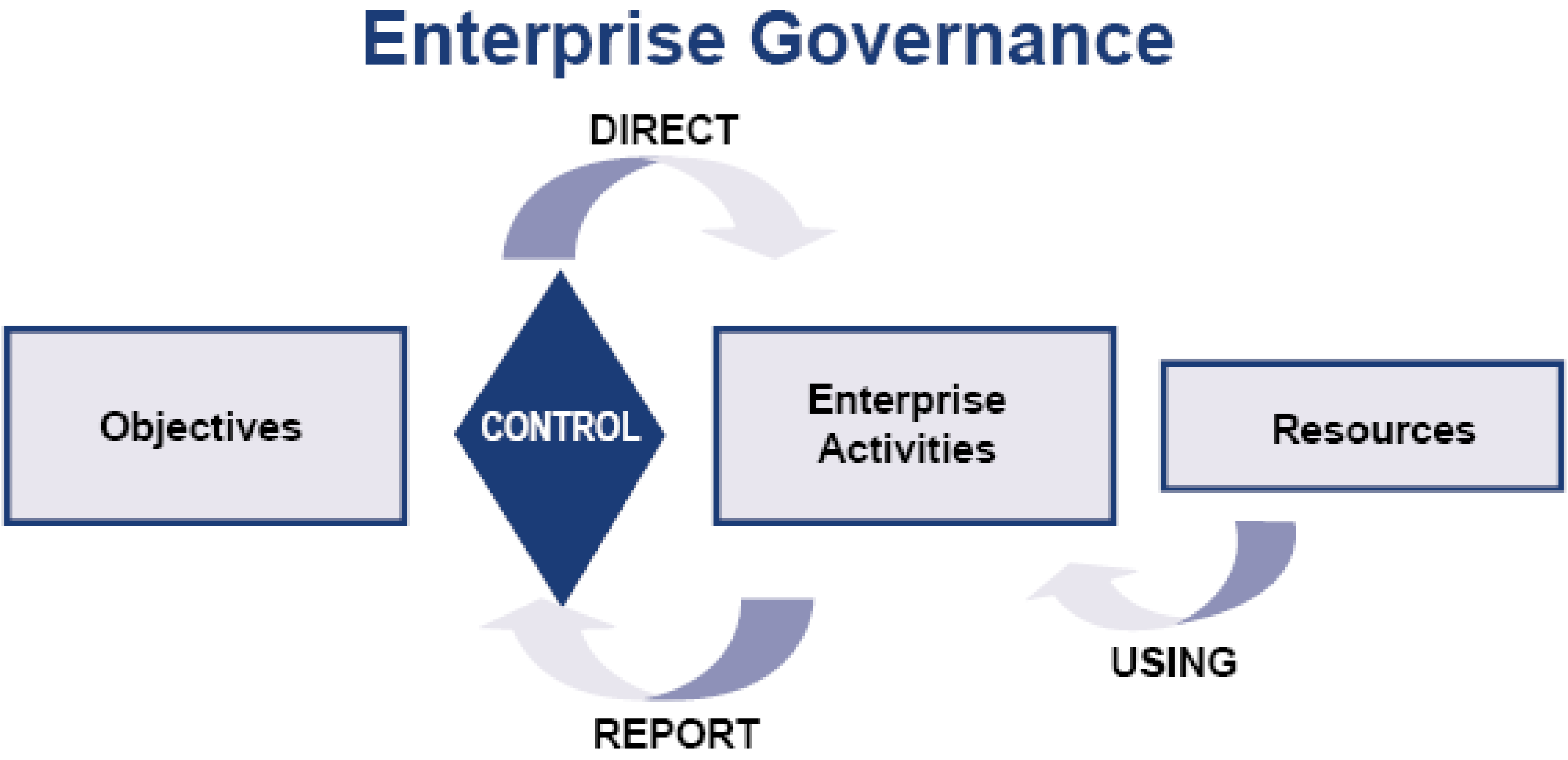
AI1 identify automated solutions
AI2 acquire and maintain application software
AI3 acquire and maintain technology infrastructure
AI4 develop and maintain procedures
AI5 install and accredit systems
AI6 manage changes

DS1	define and manage service levels
DS2	manage third-party services
DS3	manage performance and capacity
DS4	ensure continuous service
DS5	ensure systems security
DS6	identify and allocate costs
DS7	educate and train users
DS8	assist and advise customers
DS9	manage the configuration
DS10	manage problems and incidents
DS11	manage data
DS12	manage facilities
DS13	manage operations

Page 5 from CobiT Executive Summary
http://www.isaca.org

Lets dig deeper

CobiT™



Source: CobiT Executive Summary
http://www.isaca.org

TECHNOLOGY AS PROMISED

Lets dig deeper

CobiT™ 4.0 just released

IT Governance Focus Areas

- **Strategic alignment**

  focuses on ensuring the linkage of business and IT plans, on defining, maintaining and validating the IT value proposition, and on aligning IT operations with enterprise operations.

- **Value delivery**

  is about executing the value proposition throughout the delivery cycle, ensuring that IT delivers the promised benefits against the strategy, concentrating on optimizing costs and proving the intrinsic value of IT.

- **Resource management**

  is about the optimal investment in, and the proper management of, critical IT resources: processes, people, applications, infrastructure and information. Key issues relate to the optimization of knowledge and infrastructure.

- **Risk management**

  requires risk awareness by senior corporate officers, a clear understanding of the enterprise's appetite for risk, transparency about the significant risks to the enterprise, and embedding of risk management responsibilities into the organization.

- **Performance measurement**

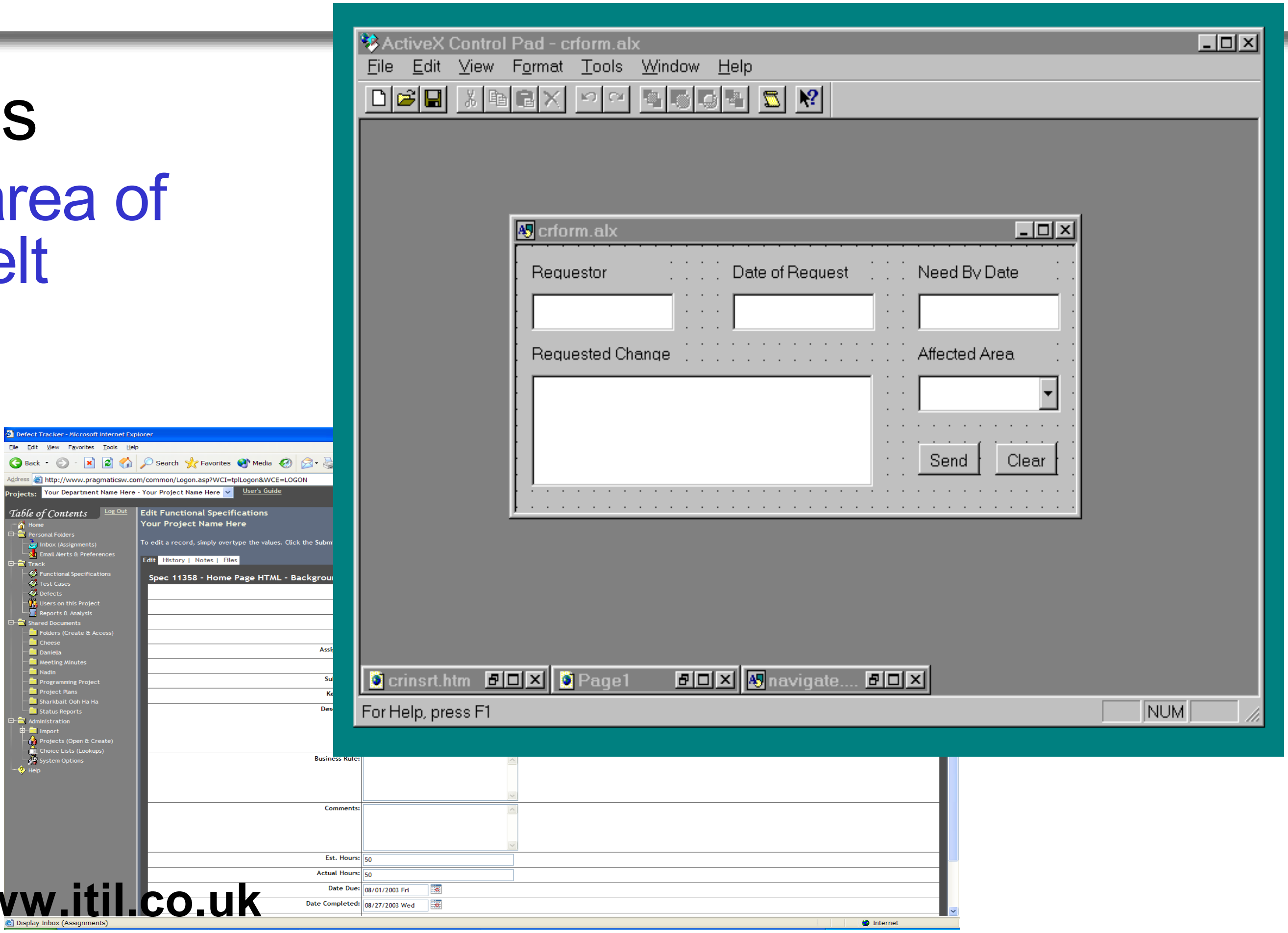
  tracks and monitors strategy implementation, project completion, resource usage, process performance and service delivery, using, for example, balanced scorecards that translate strategy into action to achieve goals measurable beyond conventional accounting.

Source: CobiT 4.0 http://www.isaca.org

ITIL – “how” in services

ITIL®

- IT Operations
  - Emerging area of need and felt pain
  - Supports a Change Request World


Defect Tracker - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Projects:
User's Guide
Table of Contents
Log Out
Edit History | Notes | Files
Internet
ActiveX Control Pad - crform.alx
File Edit View Format Tools Window Help
crform.alx
Send
Clear
crinsrt.htm
Page1
navigate....
NUM

http://www.pragmaticsw.com/common/Logon.asp?WCI=tplLogon&WCE=LOGON

Projects: Your Department Name Here - Your Project Name Here

Table of Contents
- Home
- Personal Folders
  - Inbox (Assignments)
  - Email Alerts & Preferences
- Track
  - Functional Specifications
  - Test Cases
  - Defects
  - Users on this Project
  - Reports & Analysis
- Shared Documents
  - Folders (Create & Access)
  - Cheese
  - Daniella
  - Meeting Minutes
  - Nadin
  - Programming Project
  - Project Plans
  - Sharkbait Ooh Ha Ha
  - Status Reports
- Administration
  - Import
  - Projects (Open & Create)
  - Choice Lists (Lookups)
  - System Options
- Help

Edit Functional Specifications
Your Project Name Here

To edit a record, simply overtype the values. Click the Submi

Spec 11358 - Home Page HTML - Backgrou

Assi

Su

Ke

Des

Business Rule:

Comments:

Est. Hours: 50

Actual Hours: 50

Date Due: 08/01/2003 Fri

Date Completed: 08/27/2003 Wed

Requestor

Date of Request

Need By Date

Requested Change

Affected Area

For Help, press F1

OGC
Office of Government Commerce

ITIL®
IT Service Management

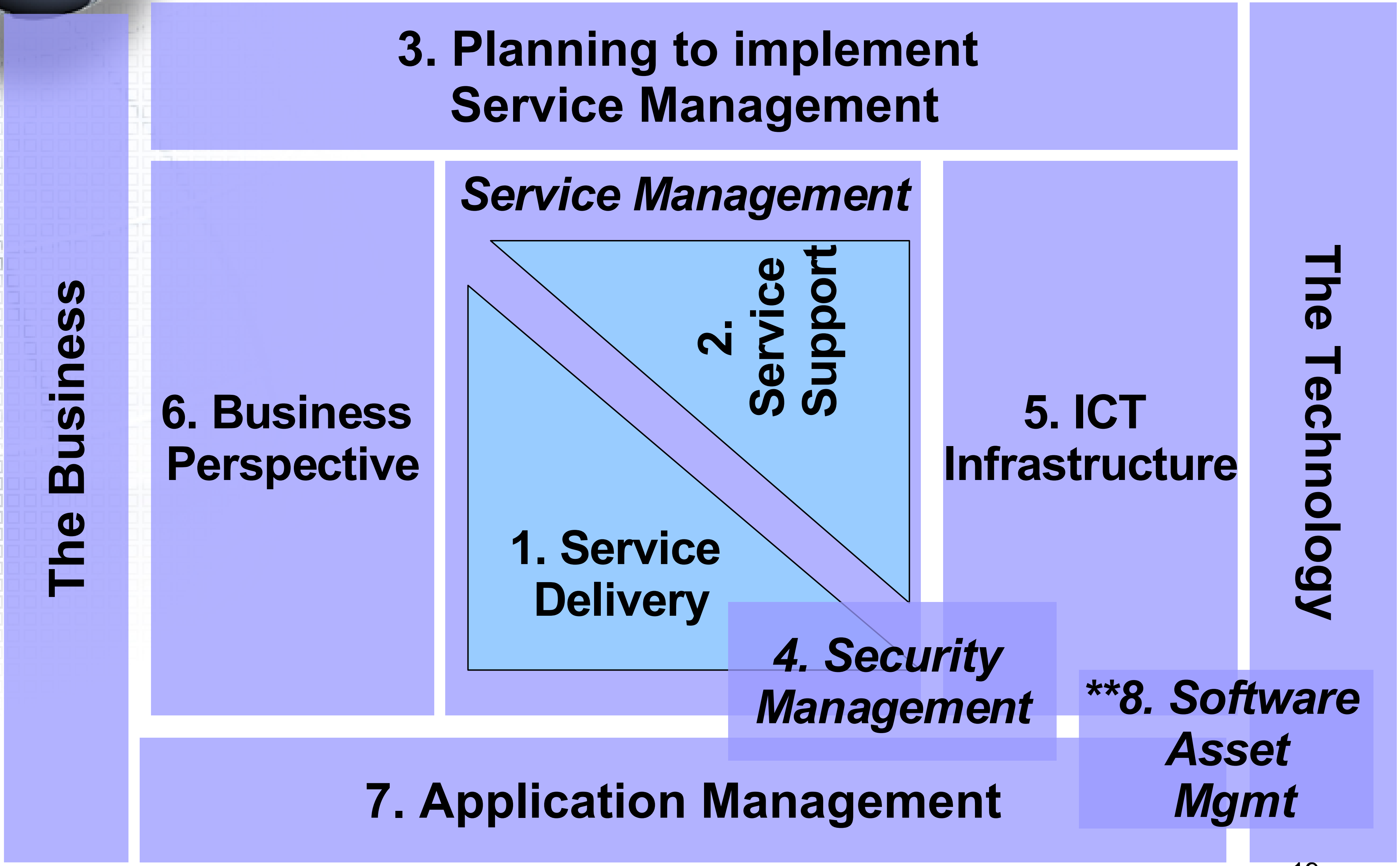
http://www.itil.co.uk
http://www.get-best-practice.co.uk/itilProducts.aspx
http://www.itilcommunity.org
http://www.microsoft.com/mof
http://en.wikipedia.org/wiki/ITIL#Overview_of_the_ITIL_frameworks

ITIL – “how” in services

- The IT Infrastructure Library (ITIL) is a series of eight books which is referred to as the only consistent and comprehensive best practice for IT service management.
- Although published by a governmental body, ITIL is not a standard or regulation. It falls into the realm of ‘best practice’.

Overview

ITIL®



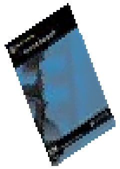
Source: ITIL: Planning to implement Service Management (2002, p 4)

8 books

ITIL®

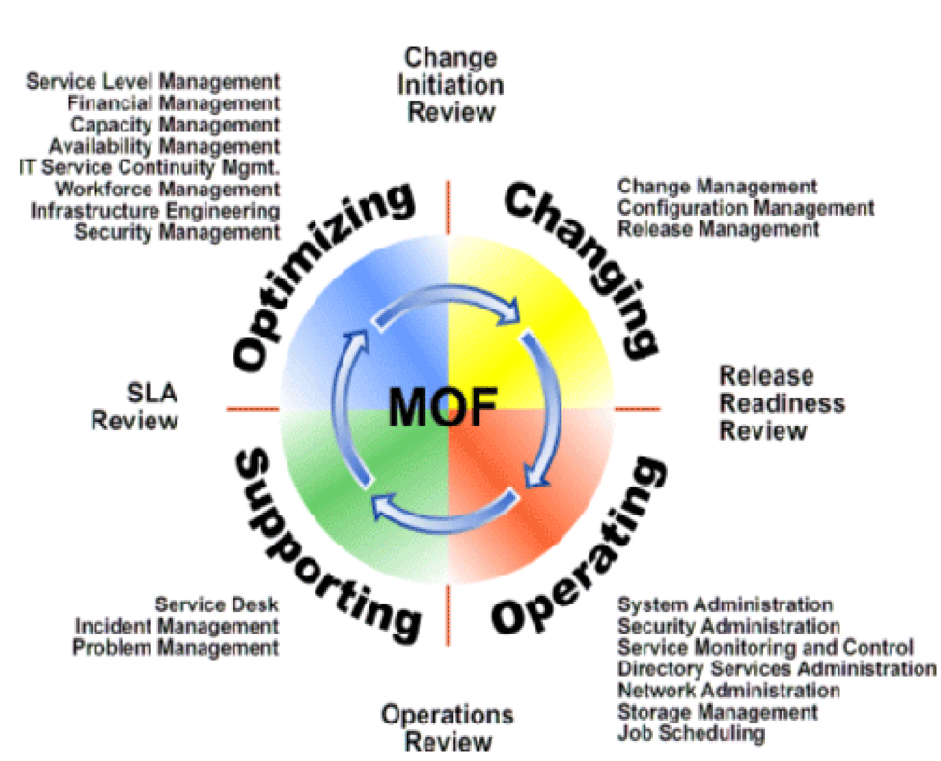
- **Service Delivery**. What services must the data center provide to the business to adequately support it?
  - *IT Financial Management - Capacity Management*
  - *Availability Management - IT Continuity Management*
  - *Service Level Management*
- **Service Support**. How does the data center ensure that the customer has access to the appropriate services?
  - *Change Management - Release Management*
  - *Problem Management - Incident Management*
  - *Configuration Management - Service Desk*
- **Planning to Implement Service Management.**
  - *How to start the changeover to ITIL. It explains the necessary steps to identify how an organization might expect to benefit from ITIL and how to set about reaping those benefits.*
- **Security Management.**

8 books



- **ICT Infrastructure Management**. What processes, organization, and tools are needed to provide a stable IT and communications infrastructure? This is the foundation for ITIL service management processes.
  - *Network Service Management - Operations Management*
  - *Management of local processors* - Systems Management
  - *Computer installation and acceptance*
- **The Business Perspective**. It explains the key principles and requirements of the business organization and operation.
- **Application Management**. How to manage the software development lifecycle,
- **Software Asset Management**.

Microsoft's Operations Framework



- Microsoft's adoption of ITIL began in 2001-02
- It has embraced and amended ITIL

ISO/IEC 17799:2005 –
Components and Sections

ISO
International
Organization for
Standardization

- security policy;
- organization of information security;
- asset management;
- human resources security;
- physical and environmental security;
- communications and operations management;
- access control;
- information systems acquisition, development and maintenance;
- information security incident management;
- business continuity management;
- compliance

http://www.iso.org
http://www.aitp.org/newsletter/2003marapr/article1.htm

ISO/IEC 17799:2005 –

ISO/IEC 17799:2005 establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization:

http://www.iso.org
http://www.aitp.org/newsletter/2003marapr/article1.htm

OK we buy that CobiT, ITIL, ISO blah blah helps secure an environment

- What about (2) and (3) on your 2nd Slide there?
  - (1) CobiT, buzz word parade
  - (2) If so what's the cost/benefit?
  - (3) If so does it have to be exclusive domain and delivery of top/down?

```
10 If Speed - Velocity > 4
20 Then GOTO 80
30 If Speed - Velocity < 4
40 Then GOTO 90
50 If Speed - Velocity > 4
60 AND Police = behind the sign
70 THEN GOTO 100
80 STOP
90 GO
100 RUN
```

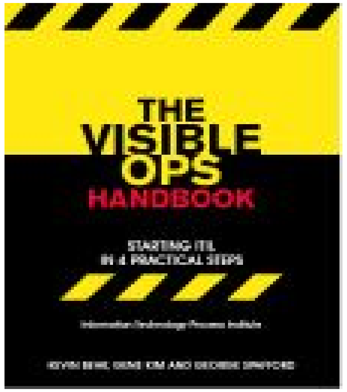
OK we buy that CobiT, ITIL, ISO blah blah helps secure an environment

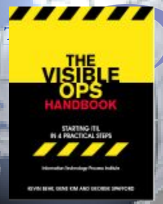
- Cost / Benefit
  - There is a cost of compliance much like the cost of quality
  - If phased in over 18 – 48 months; the cost is far less then the benefits accrued
  - However, if you attempt to 'build the whole elephant' in 1 year, you're costs will exceed benefits by a 3 or 4 to 1 ratio and you'll choke

- Top/Down
  - Top / Down authorization and empowerment
  - Bottom/Up Communication & Wisdom

OK we buy that CobiT, ITIL, ISO blah blah helps secure an environment

- Now for away to phase in over time


THE
VISIBLE
OPS
HANDBOOK
STARTING ITIL
IN 4 PRACTICAL STEPS
Information Technology Process Institute
KEVIN BEHR, GENE KIM AND GEORGE SPAFFORD



Visible Op Handbook

Information Technology Process Institute

http://www.itpi.org/

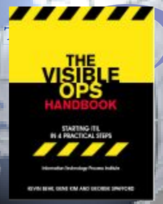
The IT Process Institute (ITPI) is a not for profit organization that exists to support the membership of IT audit, security, and operations professionals.

The IT Process Institute has created a unique three-part methodology designed to create and share results-oriented prescriptive guidance with our members.

* Research - study top performers and identify the causal link between behavior and results.
* Benchmarking - create tools that compare individual organizations to top performers.
* Prescriptive Guidance - share content written to help IT organizations become top performers.

Information Technology Process Institute

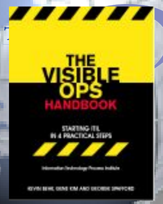
Research - Benchmarking - Prescriptive Guidance


THE VISIBLE OPS HANDBOOK

Visible Op Handbook
Information Technology Process Institute

- Challenges Addressed include Organizations:
  - Where change management processes are viewed as overly bureaucratic and of little value
  - Where people circumvent proper process
  - Where “Cowboy culture” exists that feeds apparent “nimble” behavior results in destructive side effects
  - Where a Pager culture rules and true control is not possible so page someone
  - IT Ops and Security are in reactive mode

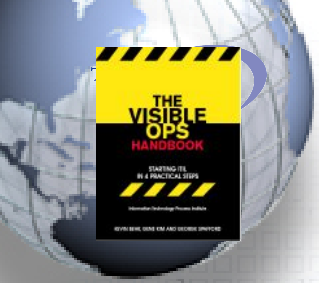
Page 11, Visible Ops Handbook, 2005



Visible Op Handbook

Information Technology Process Institute

- Key Measures
  - MTTR – Mean Time To Repair
  - MTBF – Mean Time Between Failure



Visible Op Handbook

Characteristics of High Performing IT Organizations

- High service levels and availability
- High throughput of effective change
- Higher investment in the IT Lifecycle
- Early and consistent process integration between IT Operations and Security
- Posture of Compliance
- Collaborative working relationship among IT *development*, operations, security and *architecture*
- Low amounts of unplanned work

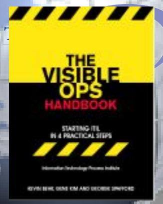
Page 14, Visible Ops Handbook, 2005

Visible Op Handbook

Cultures Common to High Performing IT Organizations

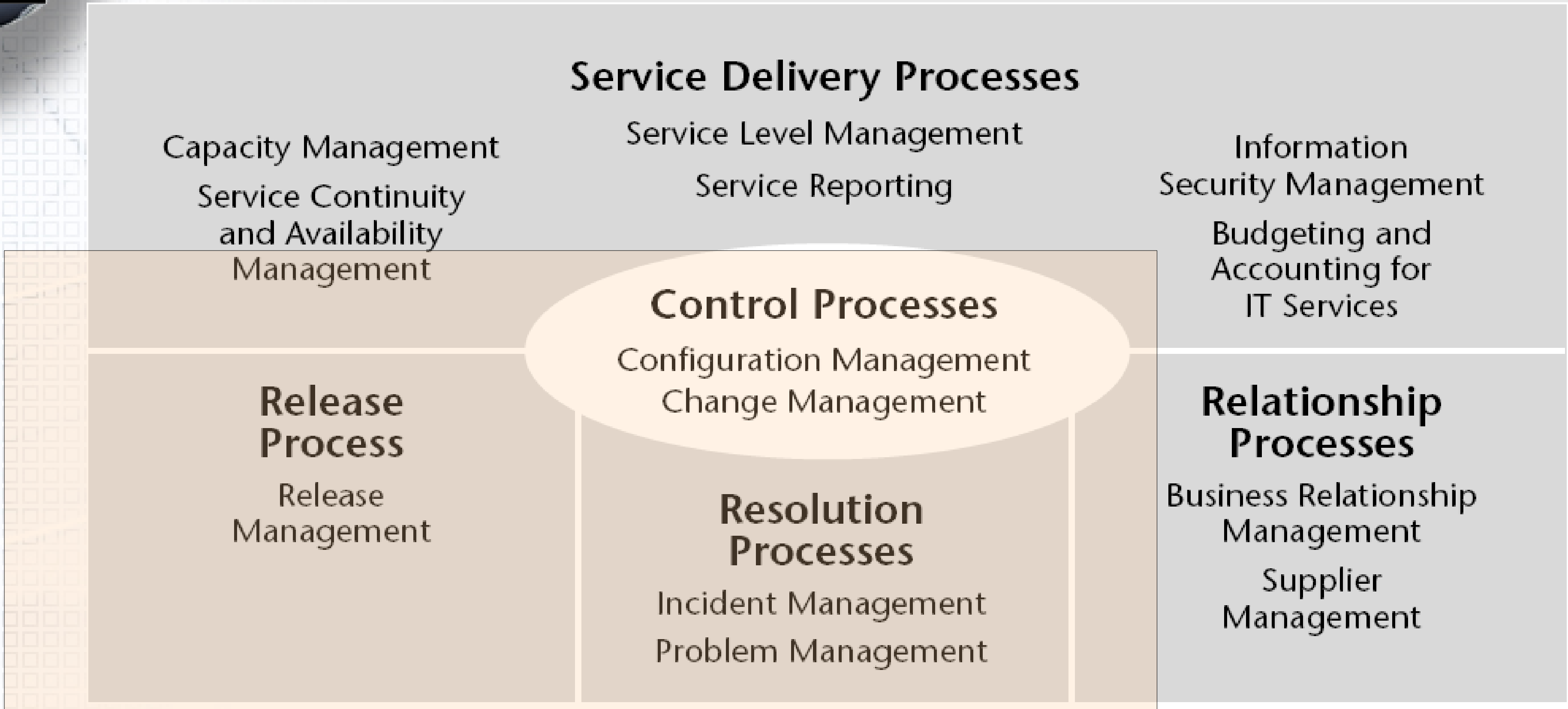
- Culture of change management
- Culture of causality
- Culture of continual improvement

Page 16-17, Visible Ops Handbook, 2005



Visible Op Handbook

ITIL Processes Common to High Performers



Service Delivery Processes

Capacity Management

Service Continuity and Availability Management

Service Level Management

Service Reporting

Information Security Management

Budgeting and Accounting for IT Services

Control Processes

Configuration Management

Change Management

Release Process

Release Management

Resolution Processes

Incident Management

Problem Management

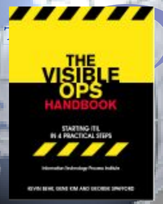
Relationship Processes

Business Relationship Management

Supplier Management

- Release
- Control
- Resolution

Page 19, Visible Ops Handbook, 2005


THE VISIBLE OPS HANDBOOK

STARTING ITIL IN 4 PRACTICAL STEPS

Visible Op Handbook

Implementation Approach

- Definitive Projects
- Ordered
- Catalytic
- Auditable
- Sustaining

Page 16-17, Visible Ops Handbook, 2005

Visible Op Handbook

Four Visible Operations Phases

- Phase 1 – Stabilize the Patient
- Phase 2 - “Catch and Release” and “Find Fragile Artifacts”
- Phase 3 – Establish Repeatable Build Library
- Phase 4 – Enable Continuous Improvement

Page 23-24, Visible Ops Handbook, 2005

Finished!

- We've addressed
  - emerging best practices & standards in CobiT /ITIL/ MOF / ISO17799 / Visible OPS
- What's the next mountain top?
- For an electronic copy of this presentation please go to www.tapuniversity.com and register.
  - You'll be given access to the TAPUniversity Community at no charge as part of this conference. A pdf of this presentation and additional compliance content is located in the TAPUniversity Community