Implementing IT Governance Using COBIT, ITIL & Six Sigma

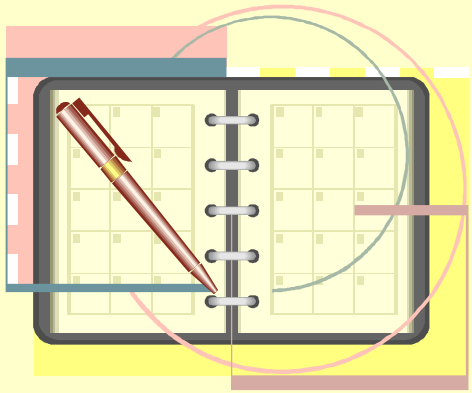
Peter T. Davis, CISA, CISSP, CDP,
CMA, CSP, I.S.P., CNA, CMC, CCNA, CWNA,
CISM, COBIT Foundation Certificate, ITIL
Foundation Certificate, ISSPCS, PMP, SSGB
ptdavis@pdaconsulting.com
www.pdaconsulting.com
(v) 416-907-4041
(f) 416-907-4851

Peter T. Davis

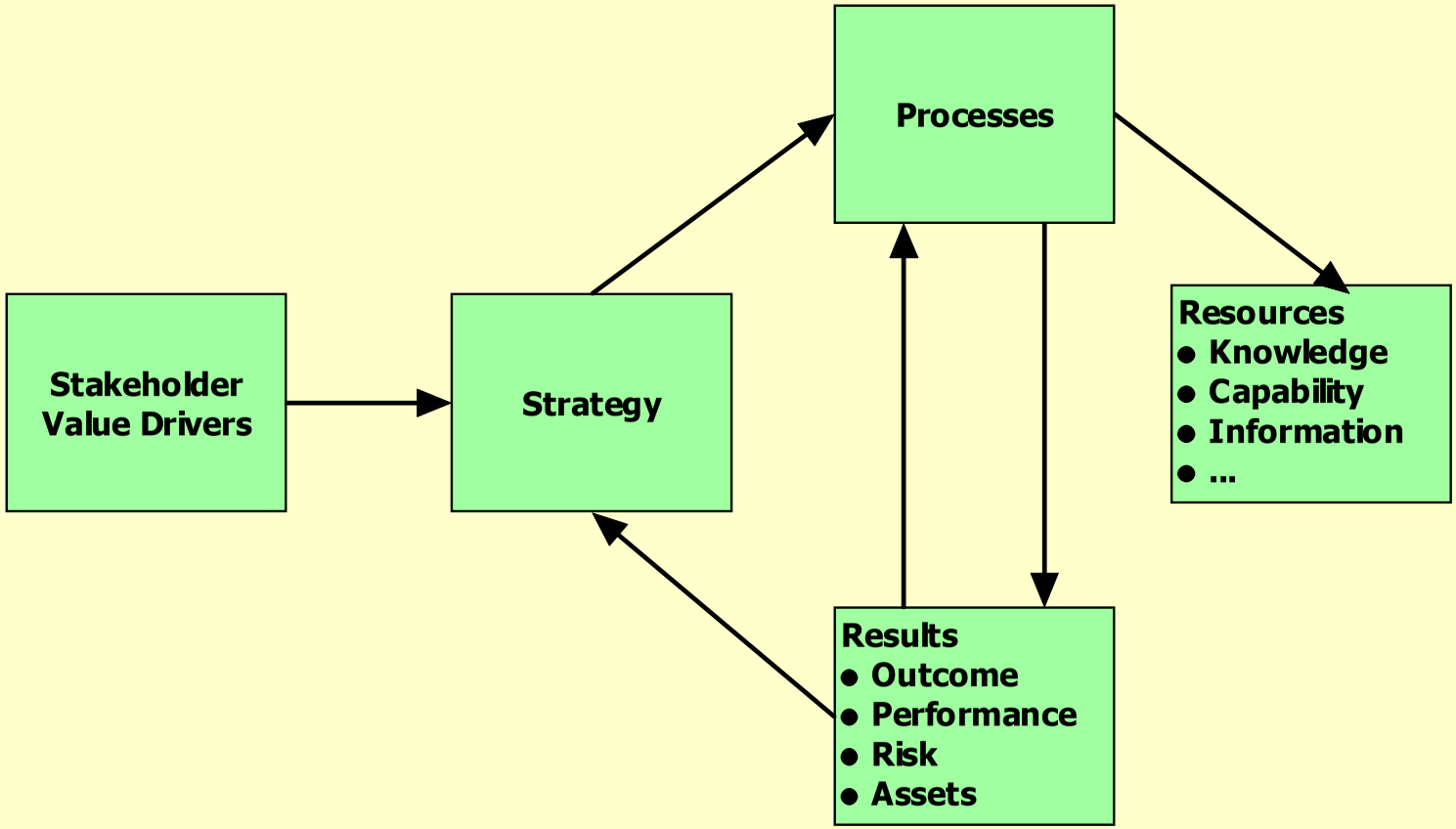
- IT Governance consulting
- CISA, CISSP, CSP, CMA, ISP, CNA, CMC, CCNA, CWNA, CISM, COBIT Foundation, ITIL Foundation, Accredited COBIT Trainer, PMP, SSGB
- 27 years IT security and audit experience
- Authored/co-authored 12 books
- *International Who's Who of Professionals*
- COBIT, ITIL, CISM and CISSP trainer

Agenda

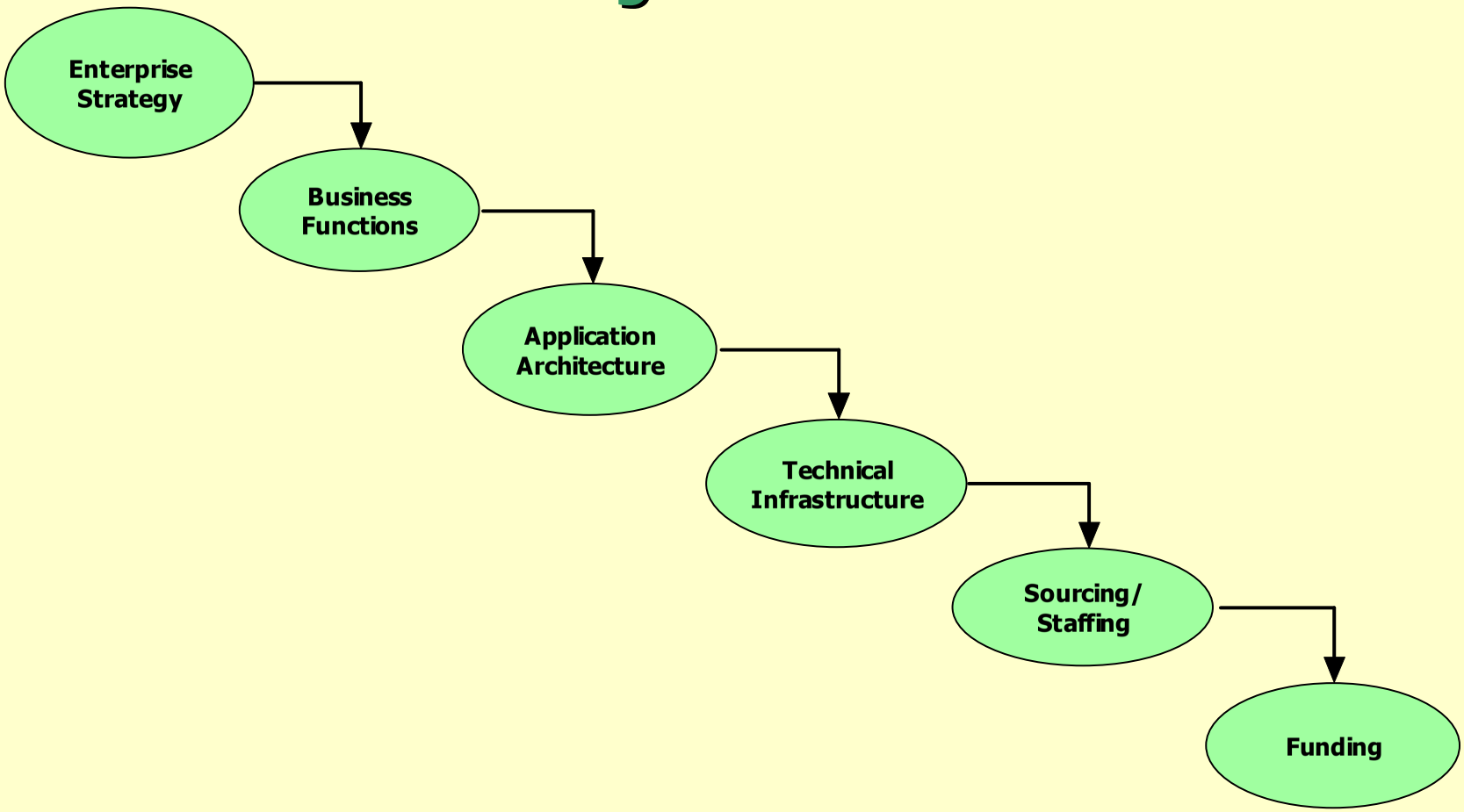
- What is IT Governance?
- What are the various methodologies?
- How do they fit in?
- How do we use them?



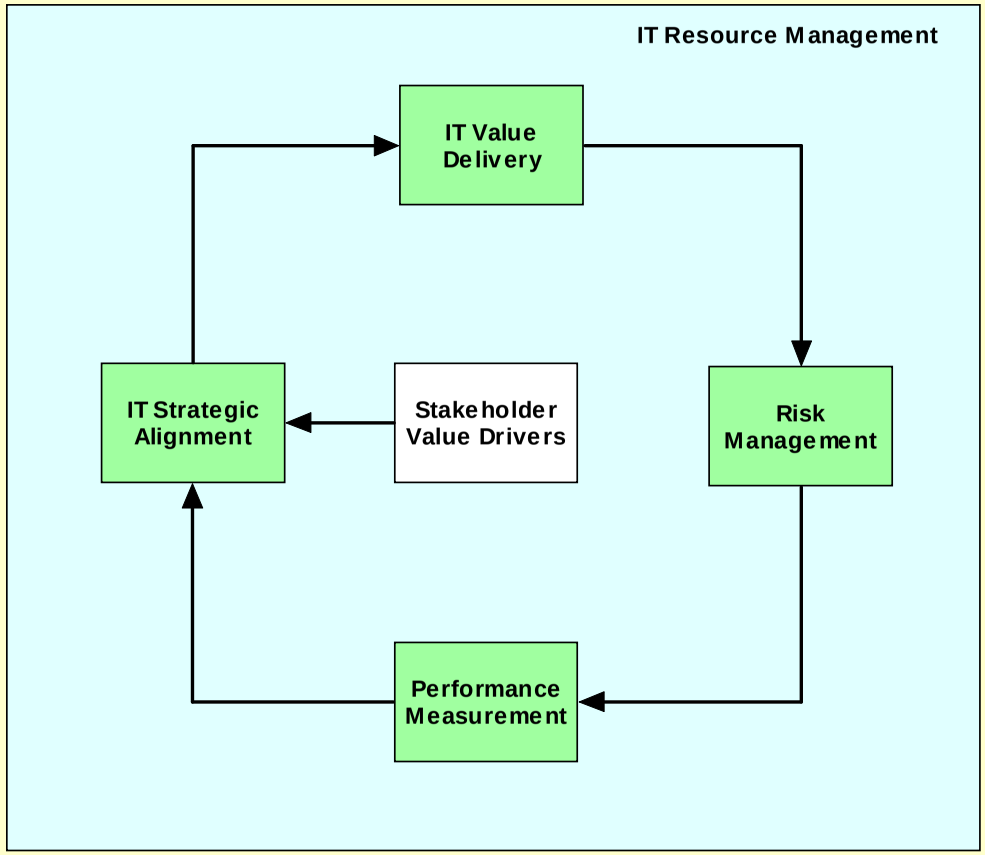
IT Governance Process



IT Supporting Strategic Objectives



Focus Areas of IT Governance



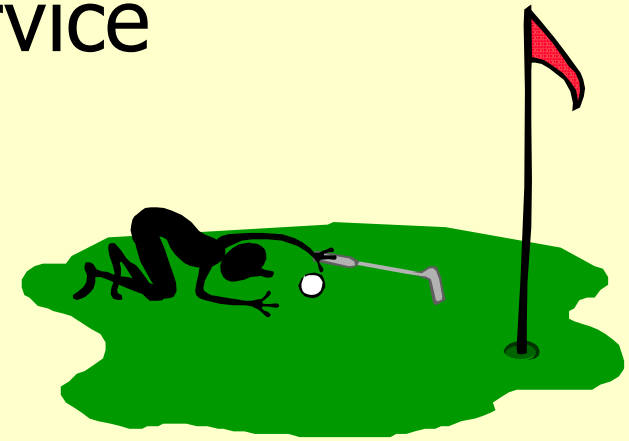
aka Scope of IT Governance

IT Governance

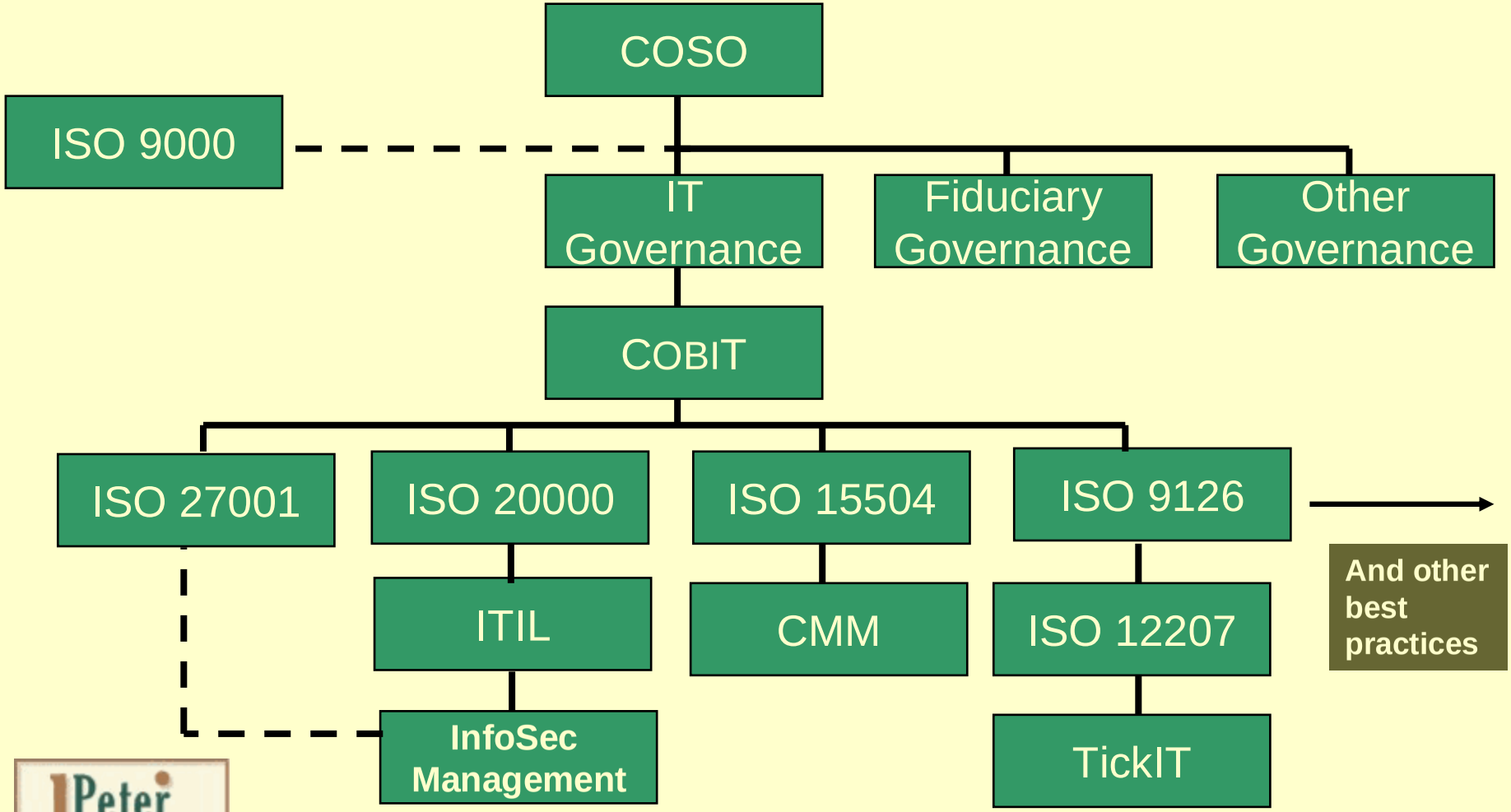
- **Ensures:**
  - Joint responsibility for planning and executing IT in the business
  - Clearer understanding by all of objectives and expectations
  - Clearer visibility of issues and priorities
  - Transparency and better comprehension of IT activities and performance

IT Governance Delivers

- Alignment of IT with business needs
- Improved value delivery (operational and project)
- Optimized costs
- Management of IT-related risks
- Improved Quality of Service



Enterprise Governance Models

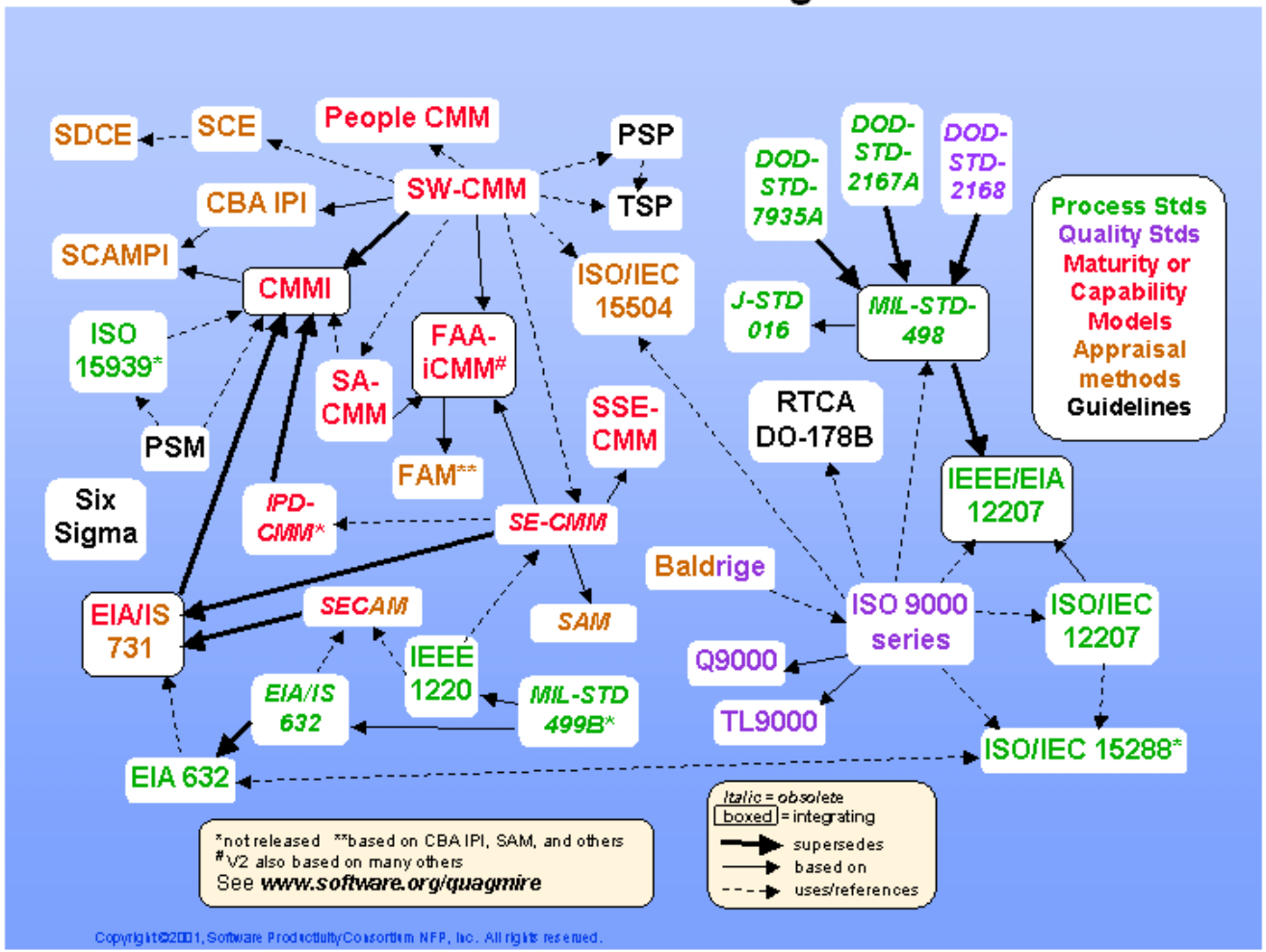


To Join / Login Info
About
Members & Affiliates
News
Training & Events
Products & Services
GSA Services
Case Histories

Member Forum
Exec. Round Table
Product Overviews
Product Websites
Standards Activities
Recent Papers
Digital Library
SITC
Telework Consortium
Other Sites of Interest

Contact Us
Site Map
Careers
Directions, Hotels, & Area Dining

The Frameworks Quagmire

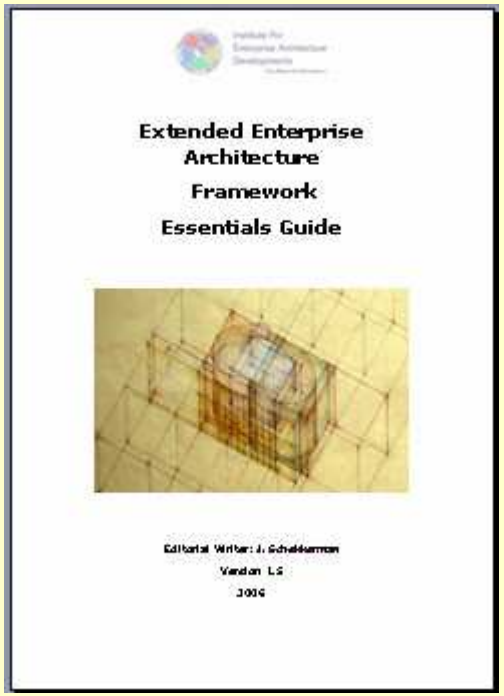


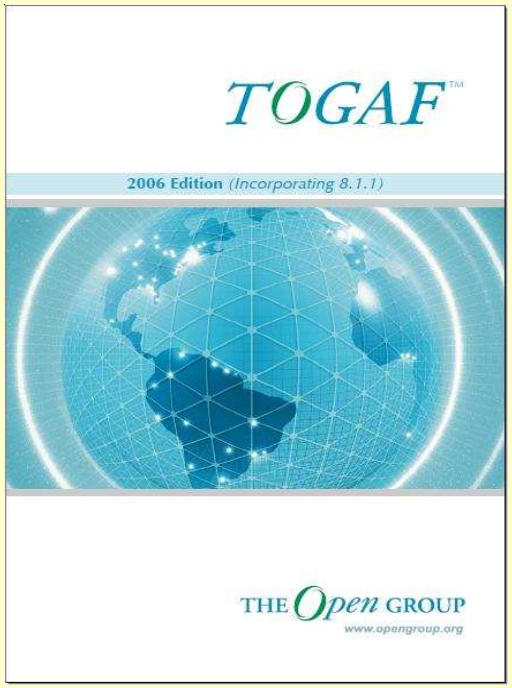
Numerous standards and process models apply to the software development industry. The Systems and Software Consortium has studied frameworks that are relevant to companies building software-intensive systems. The Frameworks Quagmire documents the results of this research. Additional information is available by clicking on the frameworks in the graphic below. In addition, Consortium members may take a course that describes the relationships, similarities, and differences among maturity models, technical and quality standards, and contractor selection vehicles. Members may also download our Quagmap tool (login required), designed to help organizations compare their existing processes and capabilities with various frameworks to determine the degree of compliance.

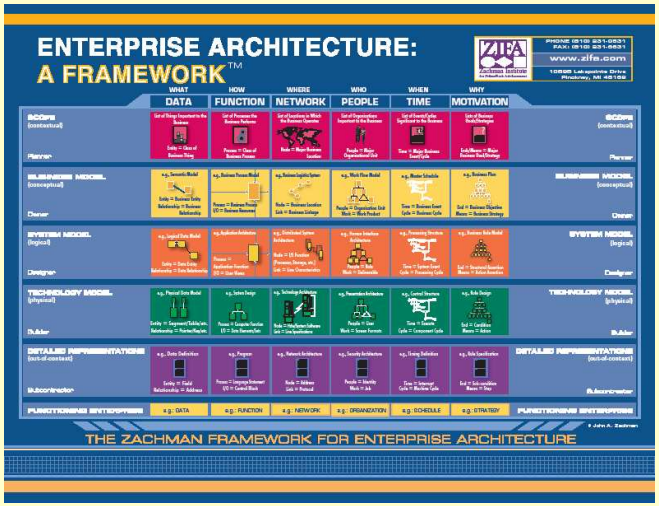
The Technical Staff at the Consortium is interested in any questions or comments that you may have.

Please contact: Sarah Sheard 703-742-7106

E2AF, TOGAF and Zachman







Security Architecture Models

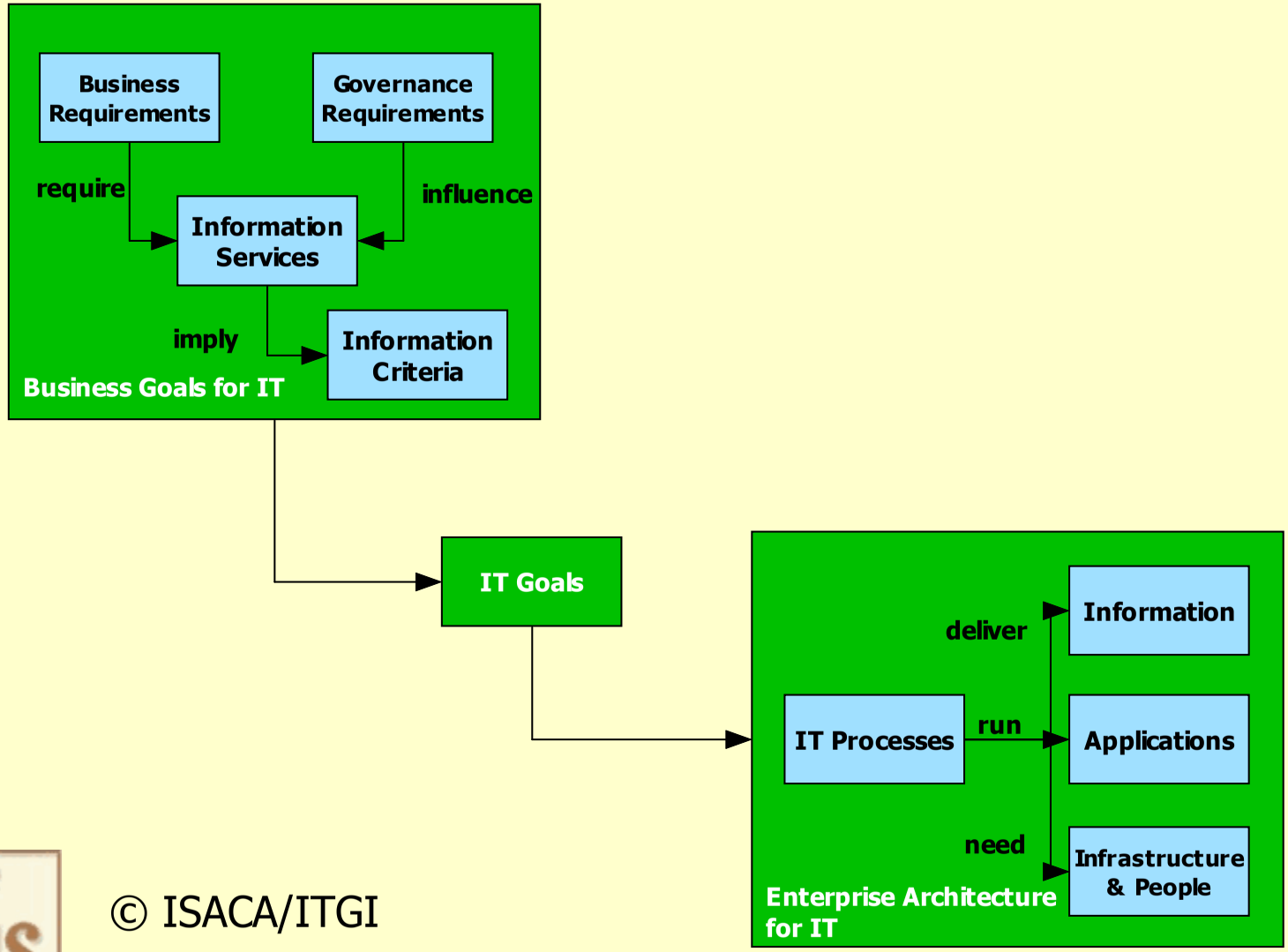
- ISO 7498-2: http://www.iso.ch/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=14256
- Moriconi, Xiaolei and Riemenschneider Methodology: http://citeseer.ist.psu.edu/moriconi97secure.html
- NIST Special Publication 800-27: http://csrc.nist.gov/publications/nistpubs/
- SABSA: http://www.sabsa.org/
- Whitman & Mattford Methodology: http://www.amazon.com/Principles-Information-Security-Michael-Whitman/dp/0619216255/sr=8-1/qid=1168271358/ref=sr_1_1/105-8440691-5565264?ie=UTF8&s=books

Frameworks Compared

Category	Type	Examples
IT Governance	Focus on how to manage information and information and communications technology efficiently and effectively	COBIT, Val IT
Information Management	Focus on how to perform and organize IT management, such service delivery and support	Generic Framework for Information Management, ITIL
Quality Management	Focus on quality standards, applied to specific IT domains	ISO 9000, ISO 20000, ISO 27001
Quality Improvement	Focus on improvement of processes or performance	IT BSC, ITS-CMM, Six Sigma
Project Management	Focus on portfolio, program and project management	MSP, PMBOK, PRINCE2
Risk Management	Focus on identifying and managing risk	M_o_R, OCTAVE, FIRM

Let's focus here, and here, and here

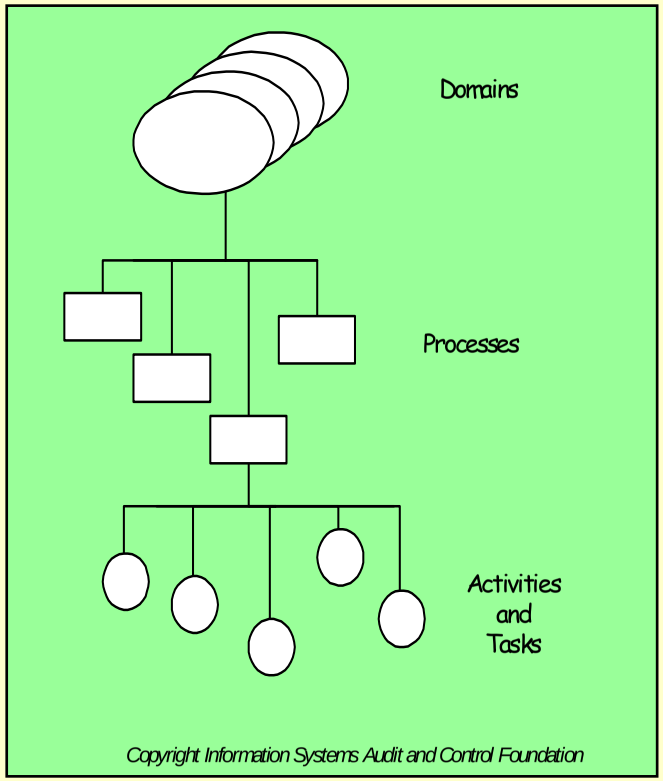
COBIT 4.1 Focus



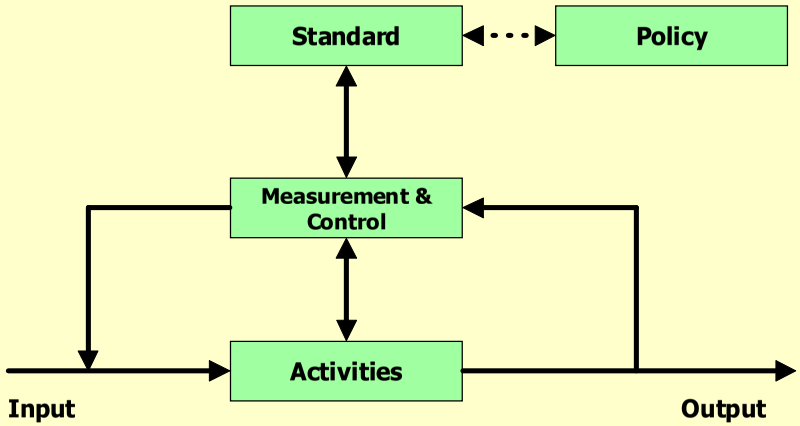
© ISACA/ITGI

COBIT Structure

- Four DOMAINS:
  - Plan & Organize
  - Acquire & Implement
  - Deliver & Support
  - Monitor & Evaluate
- The DOMAINS consist of 34 IT processes



Process



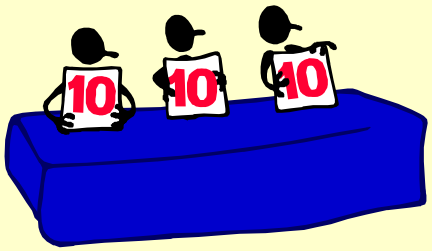
- A **process** is a logically related series of activities intended to contribute towards reaching a defined objective
- Process Owner responsible for process results
- Process Manager responsible for realization and structure of the process and reports to PO
- Process Operatives responsible for defined activities and reports to PM
- Standards = KPI
- Processes described using procedures and work instructions

COBIT Domains	
Plan and Organize	**Deliver and Support**
PO1 Define a strategic IT plan	DS1 Define and manage service levels
PO2 Define the information architecture	DS2 Manage third-party services
PO3 Determine technological direction	DS3 Manage performance and capacity
PO4 Define the IT processes, organization and relationships	DS4 Ensure continuous service
PO5 Manage the IT investment	DS5 Ensure systems security
PO6 Communicate management aims and directions	DS6 Identify and allocate costs
PO7 Manage IT human resources	DS7 Educate and train users
PO8 Manage quality	DS8 Manage service desk and incidents
PO9 Assess and manage risks	DS9 Manage the configuration
PO10 Manage projects	DS10 Manage problems
Acquire and Implement	DS11 Manage data
AI1 Identify automated solutions	DS12 Manage the physical environment
AI2 Acquire and maintain application software	DS13 Manage operations
AI3 Acquire and maintain technology infrastructure	**Monitor and Evaluate**
AI4 Enable operation and use	ME1 Monitor and evaluate IT performance
AI5 Procure IT resources	ME2 Monitor and evaluate internal control
AI6 Manage changes	ME3 Ensure regulatory compliance
AI7 Install and accredit solutions and changes	ME4 Provide IT Governance

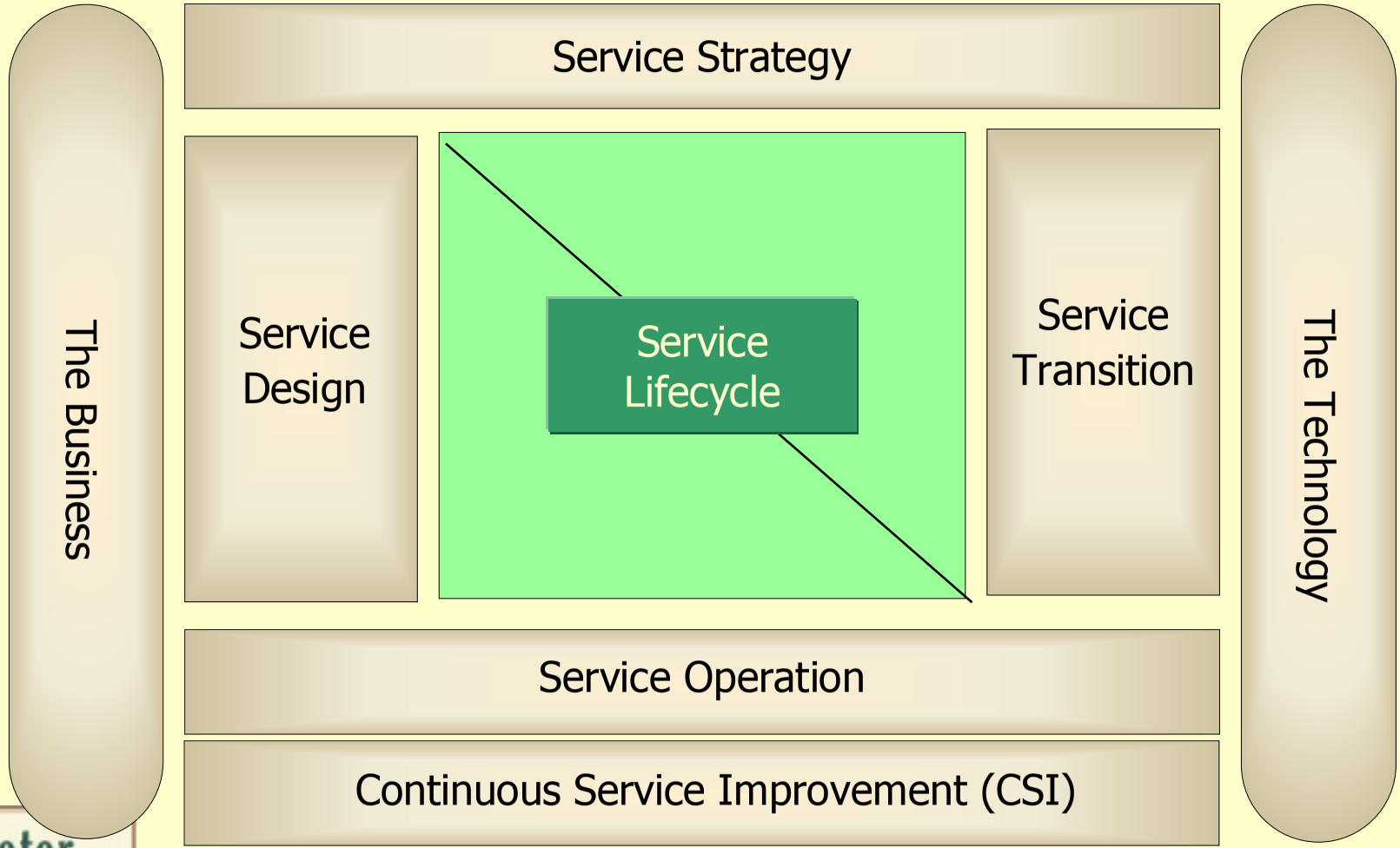
Let's focus here

KGIs

- Amount of user satisfaction with first-line support (service desk or knowledge base)
- Percent of incidents resolved within an agreed-upon/acceptable period of time

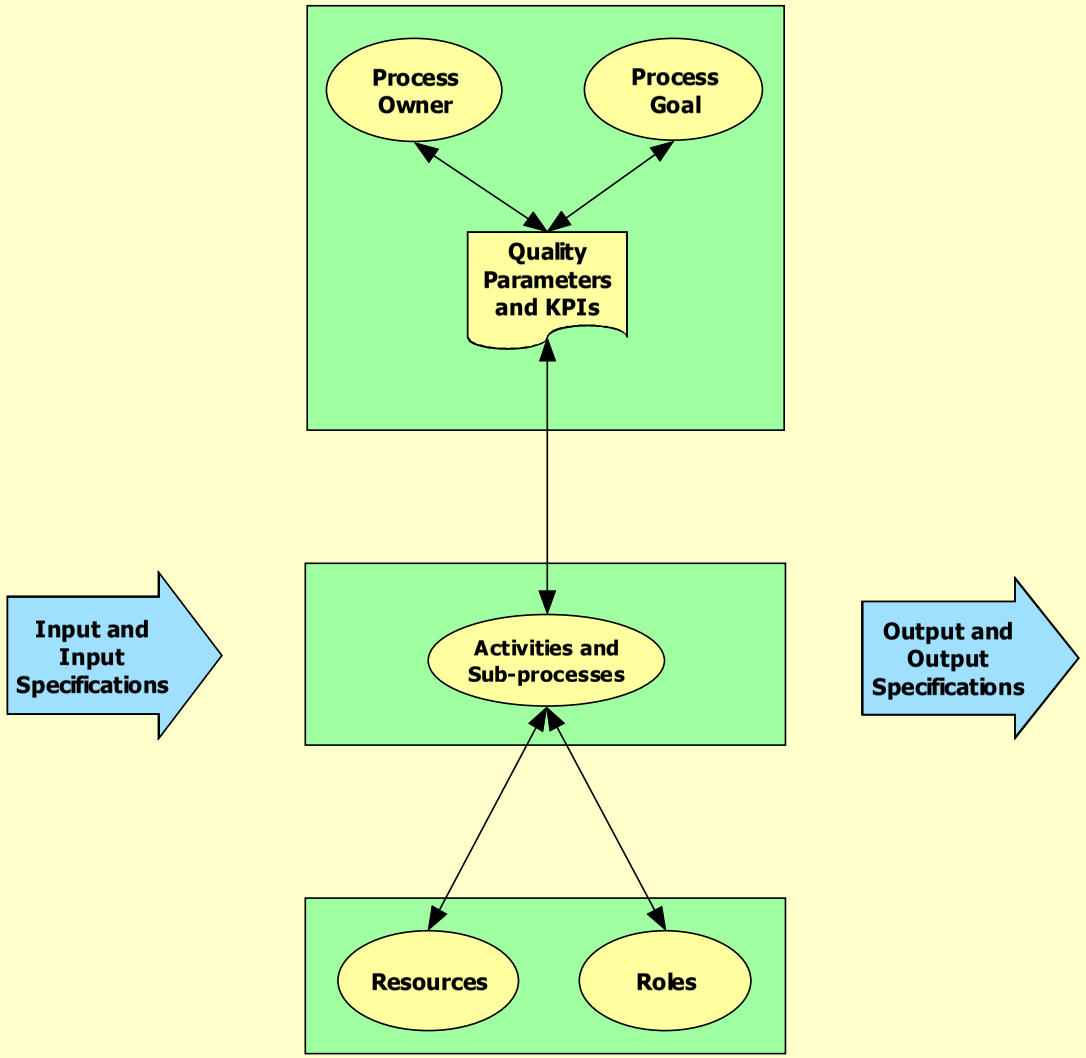


ITIL v3 Model

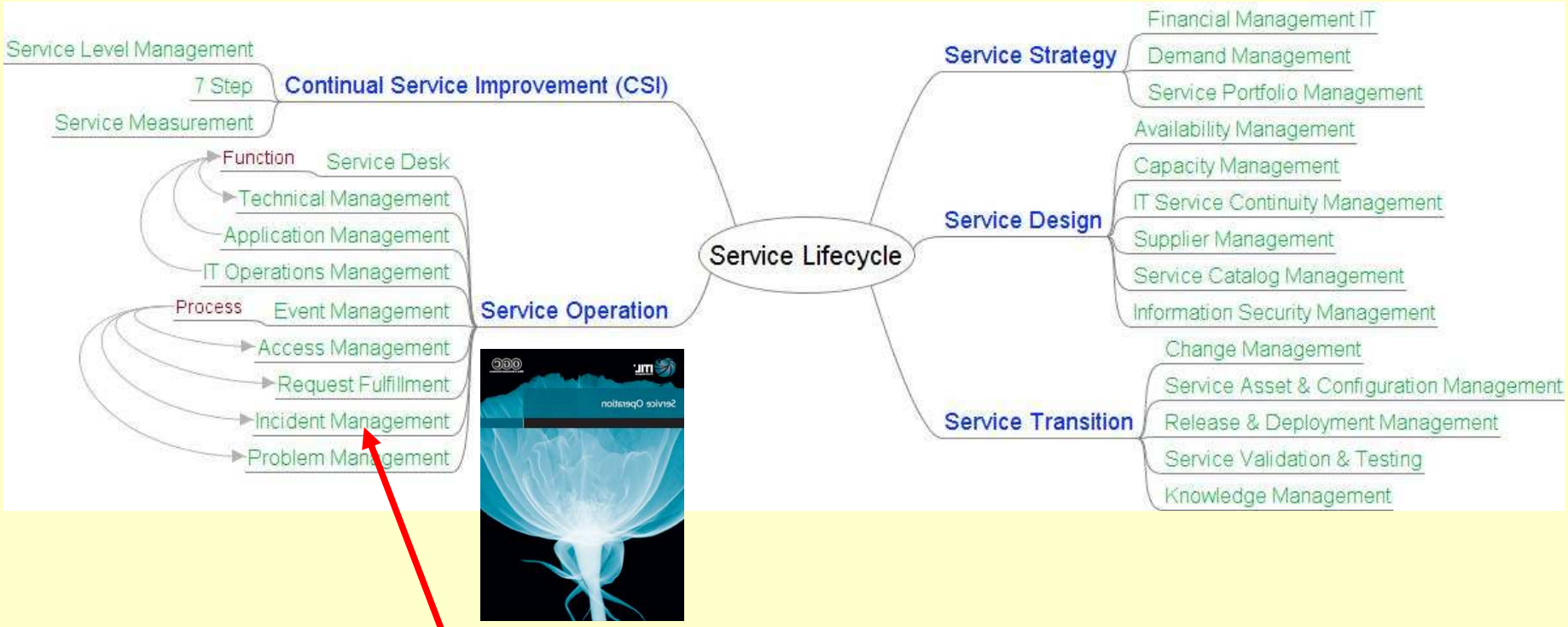


Source: TAOS

Generic ITIL Model

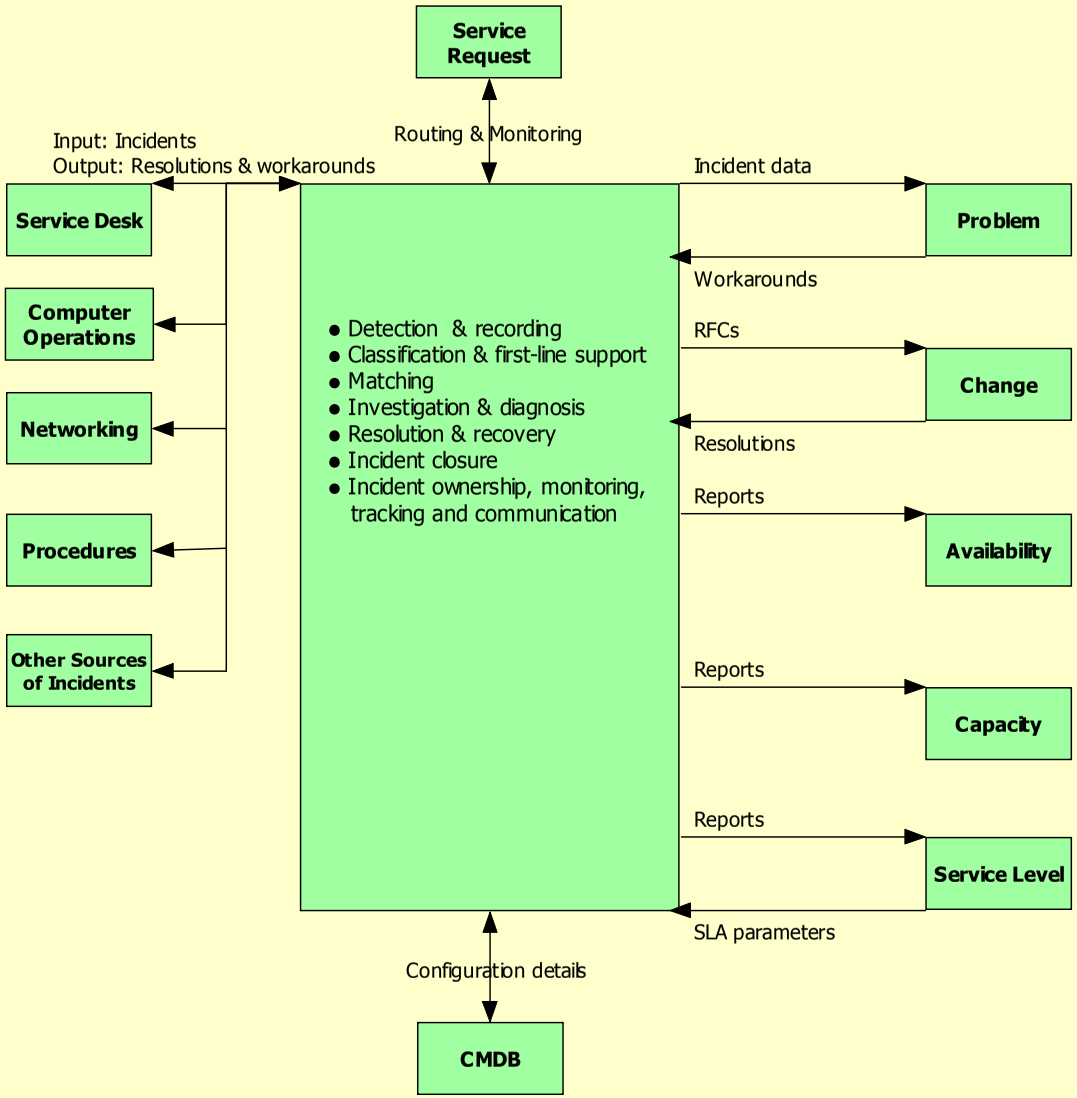


ITIL v3 Service Lifecycle



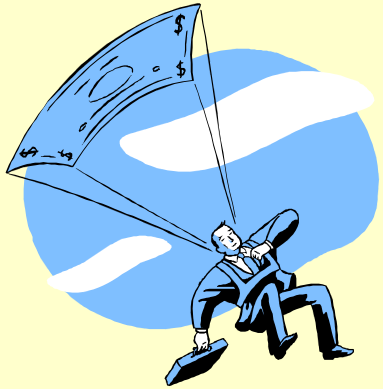
Let's focus here

Incident Management Process



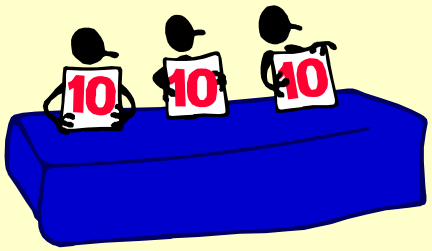
Benefits

- Reduction in volume of Incidents
- Improved IT service quality
- Better first time fix rate at service desk
- Permanent solutions
- Improved organization learning and awareness



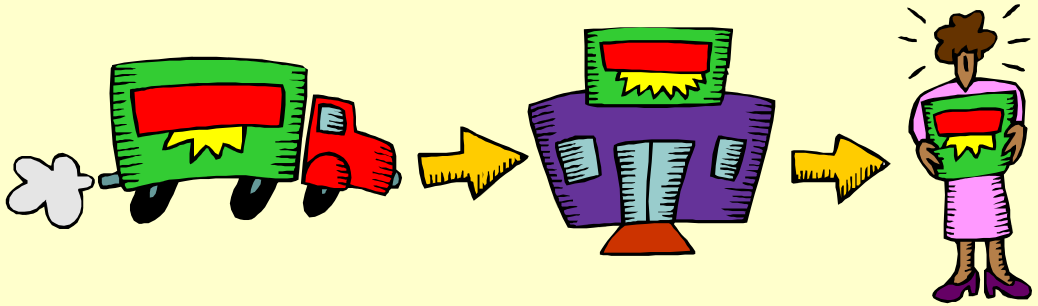
KPIs

- # of incidents per time period / category / priority level
- Incident resolution performance against service levels
- # of closed incidents per time period
- # incidents resolved without visiting the user
- # of incidents resolved within SLA targets
- # of incidents resolved by 1st line support
- Average support cost/incident
- Total number of Incidents
- Percentage of Incidents resolved within SLA
- Percentage of Incidents resolved first call



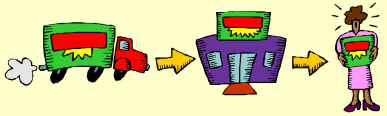
"Eighty-five percent of the reasons for failure to meet customer expectations are related to deficiencies in systems and processes …"

W. Edwards Deming



- "If you can't measure it, you can't manage it"
- "If you can't measure it, you can't manage it; and you can't manage it if you are not measuring it." *Rudy Giuliani, former NYC Mayor*
- "You've got to be very careful if you don't know where you're going, because you might not get there." *Yogi Berra, former NY Yankee*

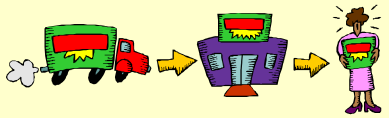
Processes



- Everything we do can be considered a process or part of a process
- Every process can be characterized by:
  - Average performance
  - Variation
- Processes are performing optimally when the result of the process is at the expected value (meaning there is minimal variation)

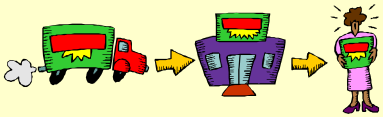
Process Improvement

- You must measure and monitor IT activities, otherwise it's not possible to govern IT and ensure alignment, value delivery, risk management, and effective use of resources
- Effective metrics should be defined and approved by stakeholders
- Metrics can then be tracked by using performance scorecards



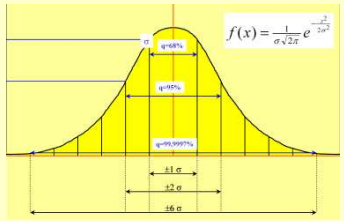
Stages of Process Improvement

- Starting with chaos (or ad hoc)
  - First a **process** must be put in place
  - Then the process must be **controlled** (made stable)
  - Finally the process must be **improved** (reduce variation)
- Need to know where you are: different tools at each stage

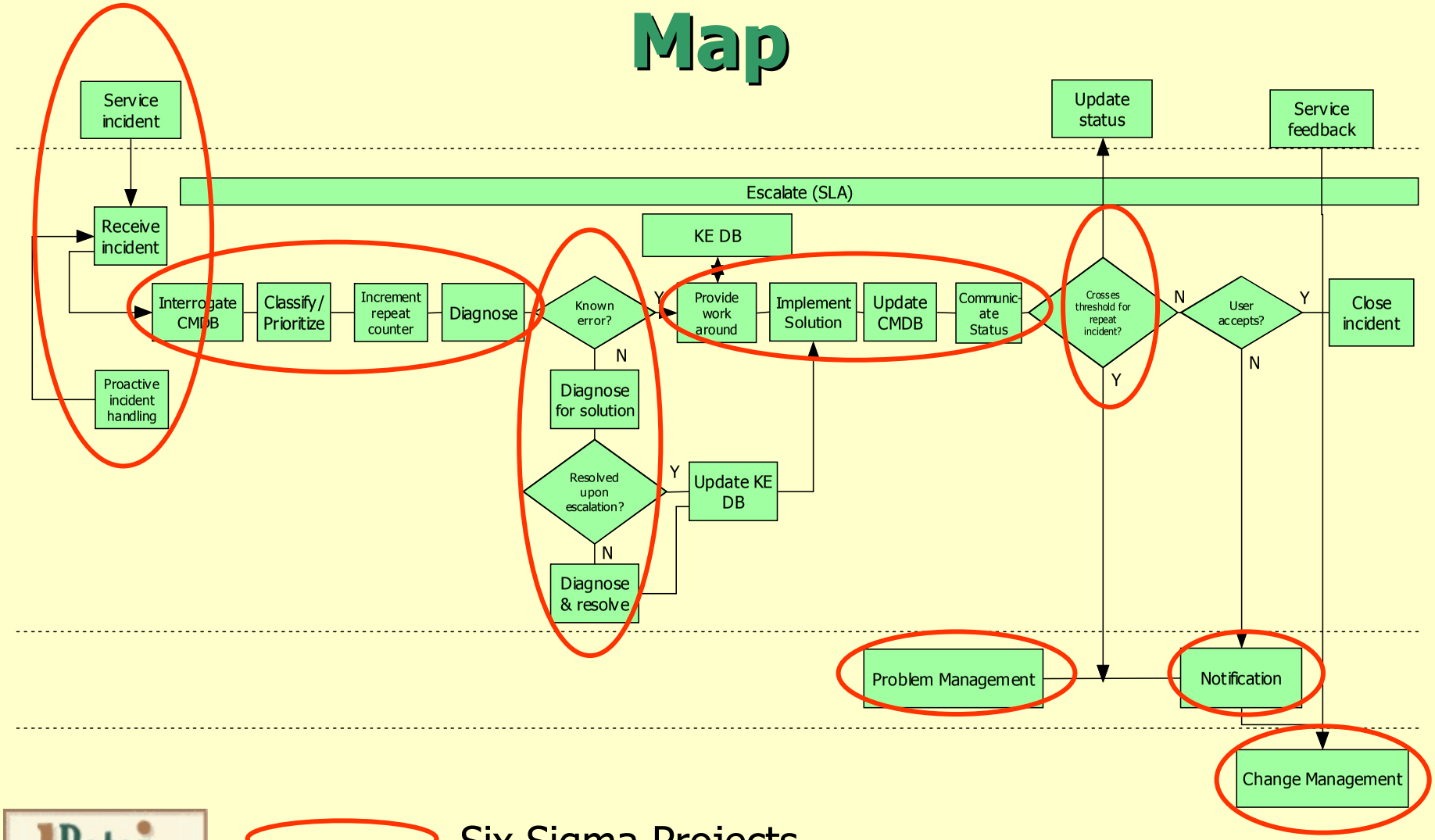


What is Six Sigma?

- A statistical measure of variation
- Full Six Sigma equals 99.9997% accuracy (3.4 DPMO)
- Methodology for improving key processes
- A "tool box" of quality and management tools for problem resolution
- A business philosophy focusing on continuous improvement
- An organized **process** (DMAIC) for structured analysis of data

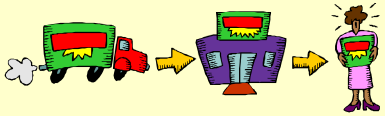


Incident Management Process Map



Six Sigma Projects

Stable Process



- When only normal (common cause) variation is present in a process, it is said to be **stable** (its entitlement)
- Stable processes are **predictable**: predict future based on past for a stable process
- Stable processes are in **(statistical) control**
- Stable processes have a **known process capability** (sigma level)
- Process capability is made up of **people, process and technology**

IT Governance Action Plan

1. Adopt a governance organizational framework
2. Align IT strategy with business goals
3. Understand/define the risks
4. Define target areas
5. Analyze current capability and identify gaps
6. Develop improvement strategies
7. Measure results
8. Repeat on a regular basis

Summary

- To combat entropy, implement an IT Governance framework
- Standards overlap
- Use tools like the CCI (previously the UCP)
- Work on processes not solutions
- Develop an action plan

Contact Information

Peter T. Davis
Principal
Peter Davis+Associates
ptdavis@pdaconsulting.com
http://www.pdaconsulting.com
Voice: 416-907-4041
Fax: 416-907-4851
Skype: ptdavis416

Additional Resources

- http://www.goal-setting-guide.com/smart-goals.html
- http://www.hhs.gov/ocr/hipaa/
- http://www.iec.org/
- http://www.isaca.org/cobit
- http://www.iso.org
- http://www.itcinstitute.com/cci/
- http://www.itgi.org
- http://www.itpi.org
- http://www.itsmf.com
- http://www.oceg.org
- http://www.pdaconsulting.com
- http://www.sse-cmm.org
- http://survey.cxo.com/surveys/csoec_kk_raci_12_02.htm