Pink Tutorial: Standards, Frameworks, Methodologies & Best Practices – Oh My!

George Spalding
Executive Vice President
Pink Elephant

Agenda

- Frameworks
  - ITIL
  - COBIT
  - TOGAF
  - eTOM
  - MOF
- Models
  - CMMI
- Standards
  - ISO
- Quality Programs
  - Six Sigma
- Project Management Methodologies
  - PMI
  - Prince2

Key Frameworks

- ITIL (IT Infrastructure Library)
- COBIT (Control Objectives for Information and related Technologies)
- TOGAF (The Open Group Architecture Framework)
- eTOM (Enhanced Telecom Operations Map)
- MOF (Microsoft Operations Framework)

Framework: ITIL

- IT Infrastructure Library (ITIL)
- Custodian: Office of Government Commerce (OGC) out of the UK
- ITIL v2 (Best Practice Framework) 2001
  - Defines 10 key IT processes; 1 function
- ITIL v3 (Best Practice Framework) 2007
  - Defines 24 key IT processes; 4 functions in a Service Lifecycle
- Individual Certification: Yes
- Organizational Assessment: Yes
- www.itil-officialsite.com

Framework: COBIT

- Control Objectives for Information and related Technologies (COBIT)
- Custodian: IT Governance Institute (ITGI) an offshoot of Information Systems Audit & Control Association (ISACA) out of the US
- Current version: 4.1 (2007)
- Defines 4 Domains, 34 IT processes and hundreds of control objectives
  - Add-on frameworks:
    - Val-IT 2.0 (2008)
    - Risk-IT (2009)
- Individual Certification: Yes
- Organizational Assessment: Yes
- www.isaca.org

Framework: TOGAF

- The Open Group Architecture Framework (TOGAF)
- Custodian: The Open Group (US/UK); Architecture Forum
- Current version is: TOGAF 9 (2009)
- Details a framework for enterprise architecture which provides a comprehensive approach to the design, planning, implementation, and governance of an enterprise information architecture.
- The architecture is typically modeled at four levels or domains: Business, Application, Data, and Technology. A set of foundation architectures are provided to enable the architecture team to envision the current and future state of the architecture.
- Individual Certification: Yes
- Organizational Assessment: Yes
- www.opengroup.org

Framework: eTOM

- Enhanced Telecom Operations Map (eTOM)
- Custodian: TM Forum (US)
- The eTOM defines a business-oriented view of the service provider's enterprise. This view is useful for planners, managers, and strategists who need to view the enterprise in business terms, without immediate concern for the way that these business needs are organized or automated within the business.
- *The Business Process Framework v8.0 also has now embedded direct support for 14 ITIL processes from ISO 20000, creating an integrated solution that encompasses both eTOM and ITIL together.*
- www.tmforum.org

Framework: MOF

- Microsoft Operations Framework (MOF)
- Custodian: Microsoft Corporation (US)
- MOF 4.0 was created to provide guidance across the entire IT life cycle. Completed in early 2008, MOF 4.0 integrates community-generated processes; governance, risk, and compliance activities; management reviews, and Microsoft Solutions Framework (MSF) best practices.
- The guidance in the Microsoft Operations Framework encompasses all of the activities and processes involved in managing an IT service: its conception, development, operation, maintenance, and—ultimately—its retirement.
- Individual Certification: Yes
- Organizational Assessment: Yes
- www.microsoft.com/mof

Model: CMMI

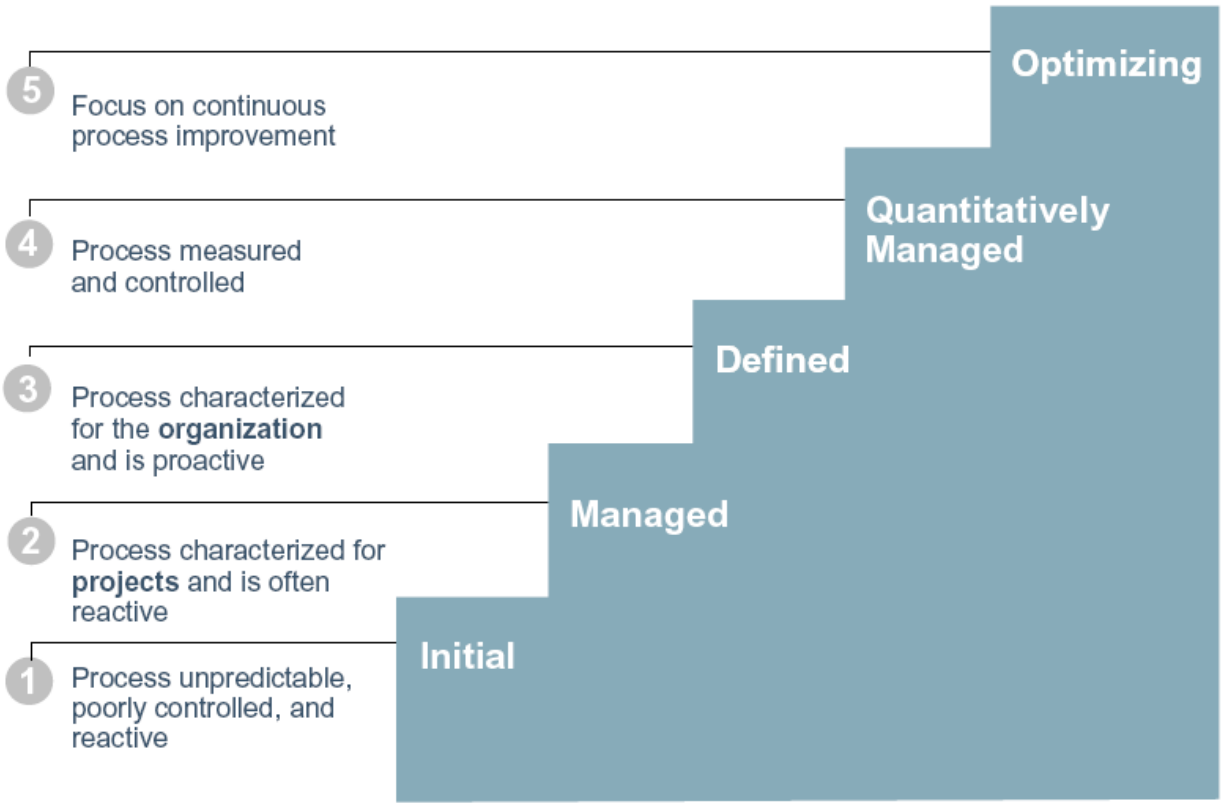
- Capability Maturity Model Integrated (CMMI)
- Custodian – Software Engineering Institute (SEI) of Carnegie Mellon University out of the US
- Details 16 shared processes and differing discreet processes for each of the 3 areas.
- Current version: CMMI v1.2 (2008)
  - CMMI-DEV (CMMI for Development)
  - CMMI-SVC (CMMI for Services)
  - CMMI-ACQ (CMMI for Acquisition)
- Details 5 levels of process maturity
- Individual Certification: No
- Organizational Assessment: Yes
- www.sei.cmu.edu/cmmi

Maturity Levels

Carnegie Mellon
Software Engineering Institute

CMMI

The Maturity Levels



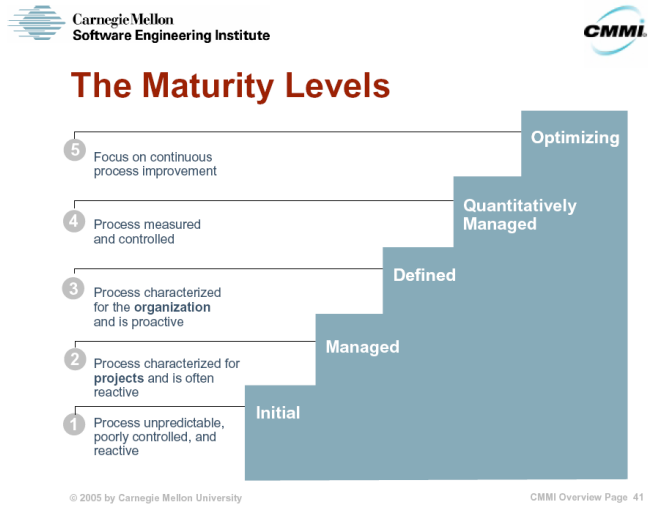
CMMI Overview Page 41

Maturity Levels

Used by:

- ITILv3
- COBIT
- CMMI

To measure the maturity of any process



Standards

- ISO/IEC 20000:2005 (IT Service Management)
- ISO/IEC 27001:2005 (Information Security Req.)
- ISO/IEC 27002:2005 (Information Security Mgt.)
- ISO/IEC 38500:2008 (IT Governance)

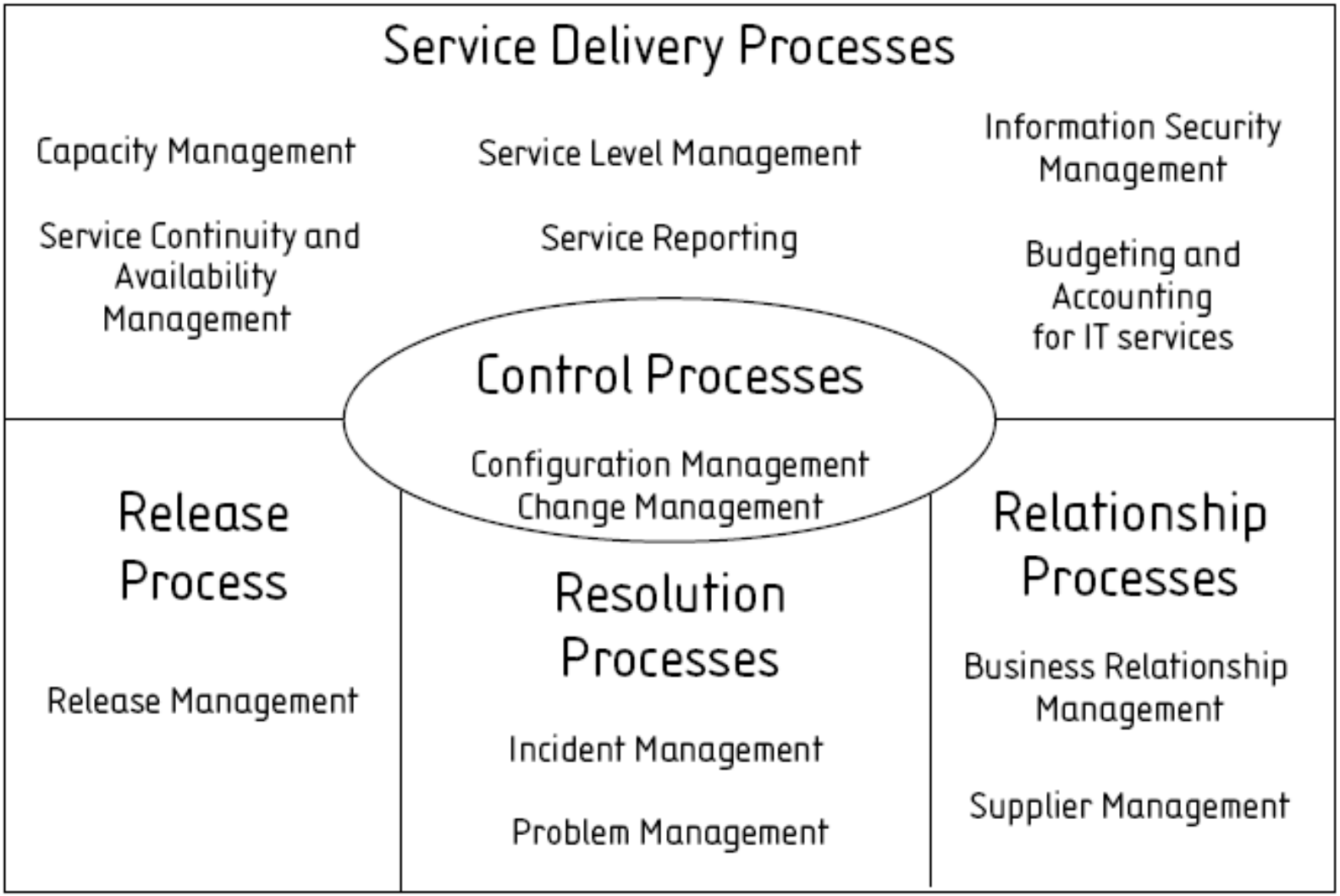
- Custodian:
  - ISO, the International Organization for Standardization
  - IEC, the International Electrotechnical Commission
  - Geneva, Switzerland

- Standards evolve and change just like everything else
- In the ISO, years are used instead of version numbers and revision and document control is stringent
- A published ISO version is in place for at least 3 years

Standard: ISO/IEC 20000:2005

- ISO/IEC 20000 is the first worldwide standard targeted at IT Service Management. It describes an integrated set of management processes for the effective delivery of services to the business and its customers.
- ISO/IEC 20000 consists of two parts:
  - ISO/IEC 20000-1:2005
    - Formal Specification and defines the requirements for an organization to deliver managed services of an acceptable quality for its customers.
  - ISO/IEC 20000-2:2005
    - Code of Practice, describes the best practices for Service Management processes within the scope of ISO/IEC 20000-1. The code of Practice will be of particular use to organizations preparing to be audited against ISO/IEC 20000 or planning service improvements.
- Individual Certification: Yes
- Organization Assessment: Yes
- www.iso.org

ISO 20000 Service Management Processes



Standard: ISO/IEC 20000:2005

- Adoption: 441 organizations in 40 countries
- What's Next for ISO 20000?
  - Part 1: Redeveloped to align more closely with ITILv3 (2011)
  - Part 2: Updated with Part 1 (2012)
  - Part 3: Guidance for scoping and applicability (2010)
  - Part 4: Process Reference Model (2010)
  - Part 5: Exemplar implementation plan for ISO/IEC 20000 (2010)

  - ISO/IEC 15504 (SPICE) Part 8 will be the Process Assessment Model for ISO/IEC 20000

Standard: ISO/IEC 27001

- ISO/IEC 27001:2005
- Information Security Management System for bringing Information Security under explicit management control
- ISO/IEC 27001 requires that management:
  - Systematically examines the organization's information security risks, taking account of the threats, vulnerabilities and impacts;
  - Designs and implements a coherent and comprehensive suite of information security controls and/or other forms of risk treatment (such as risk avoidance or risk transfer) to address those risks that it deems unacceptable; and
  - Adopts an overarching management process to ensure that the information security controls continue to meet the organization's information security needs on an ongoing basis.

Standard: ISO/IEC 27002:2005

- ISO/IEC 27002:2005
- A “code of practice” for Information Security Management
- Used to be ISO 17799 (was renamed in 2007)
- ISO/IEC 27002 provides best practice recommendations on information security management for use by those who are responsible for initiating, implementing or maintaining Information Security Management Systems (ISMS). Information security is defined within the standard in the context of the C-I-A triad:
  - *the preservation of confidentiality (ensuring that information is accessible only to those authorized to have access), integrity (safeguarding the accuracy and completeness of information and processing methods) and availability (ensuring that authorized users have access to information and associated assets when required)*.

Standard: ISO/IEC 38500:2008

- ISO 38500 is the first international standard for IT Governance
- “Corporate governance of information technology” standard, provides a framework for effective governance of IT to assist those at the highest level of organizations to understand and fulfill their legal, regulatory, and ethical obligations in respect of their organizations’ use of IT.
- ISO/IEC 38500 is applicable to organizations from all sizes, including public and private companies, government entities, and not-for-profit organizations. This standard provides guiding principles for directors of organizations on the effective, efficient, and acceptable use of Information Technology (IT) within their organizations. It is organized into three prime sections, specifically, Scope, Framework and Guidance
- Derived from AS 8015 (Australia)
- The framework comprises definitions, principles and a model. It sets out six principles for good corporate governance of IT:
  - Responsibility
  - Strategy
  - Acquisition
  - Performance
  - Conformance
  - Human behavior

International Organization for Standardization

- **www.iso.org**
- ISO is a network of the national standards institutes of 156 countries, on the basis of one member per country, with a Central Secretariat in Geneva, Switzerland, that coordinates the system.
- ISO is a non-governmental organization: its members are not, as is the case in the United Nations system, delegations of national governments. Nevertheless, ISO occupies a special position between the public and private sectors. This is because, on the one hand, many of its member institutes are part of the governmental structure of their countries, or are mandated by their government. On the other hand, other members have their roots uniquely in the private sector, having been set up by national partnerships of industry associations.

ISO Member Organizations

- **Relevant ISO Members:**
  - US – ANSI (American National Standards Institute)
  - CA – SCC (Standards Council of Canada)
  - MY – DSM (Department of Standards Malaysia)
  - SG – SPRING SG (Standards, Productivity and Innovation Board - Singapore)
  - MX – DGN (Dirección General de Normas - Mexico)
  - UK – BSI (British Standards Institution)
  - NL – NEN (Nederlands Normalisatie-instituut - Netherlands)
  - ZA – SABS (South African Bureau of Standards)
  - AU – SA (Standards Australia)
  - NZ – SNZ (Standards New Zealand)
  - JP – JISC (Japanese Industrial Standards Committee)
  - CN – SAC (Standardization Administration of China)
  - etc

Quality Programs

- Six Sigma
- Malcolm Baldrige
- EFQM
- TQM
- Zero Defects

Quality Program: Six Sigma

- Developed by Motorola in 1986
- Custodian: No one really, Motorola, Inc. in US owns the Six Sigma copyright & trademark
- Often combined with LEAN manufacturing methods to create LEAN Six Sigma
- Intense focus on processes
- Six Sigma is achieved when we reach 99.99966% accuracy
- Individual Certification: Yes
- Organizational Assessment: Yes
- www.isixsigma.com

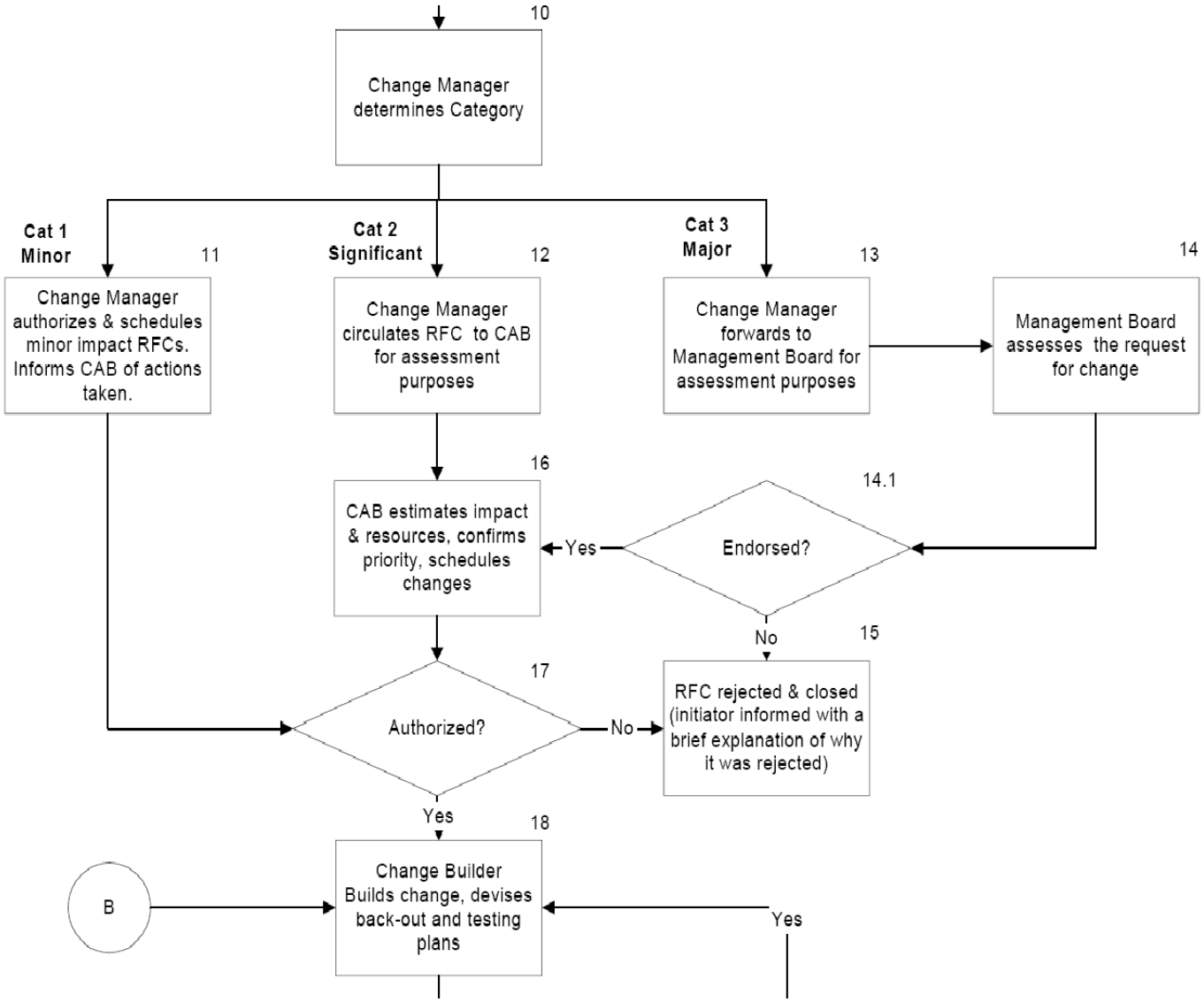
Six Sigma (TQM on Steroids)

- Six Sigma at many organizations simply means a measure of quality that strives for near perfection. Six Sigma is a disciplined, data-driven approach and methodology for eliminating defects (driving towards six standard deviations between the mean and the nearest specification limit) in any process -- from manufacturing to transactional and from product to service.
- The statistical representation of Six Sigma describes quantitatively how a process is performing. ***To achieve Six Sigma, a process must not produce more than 3.4 defects per one million opportunities.*** A Six Sigma defect is defined as anything outside of customer specifications. A Six Sigma opportunity is then the total quantity of chances for a defect.

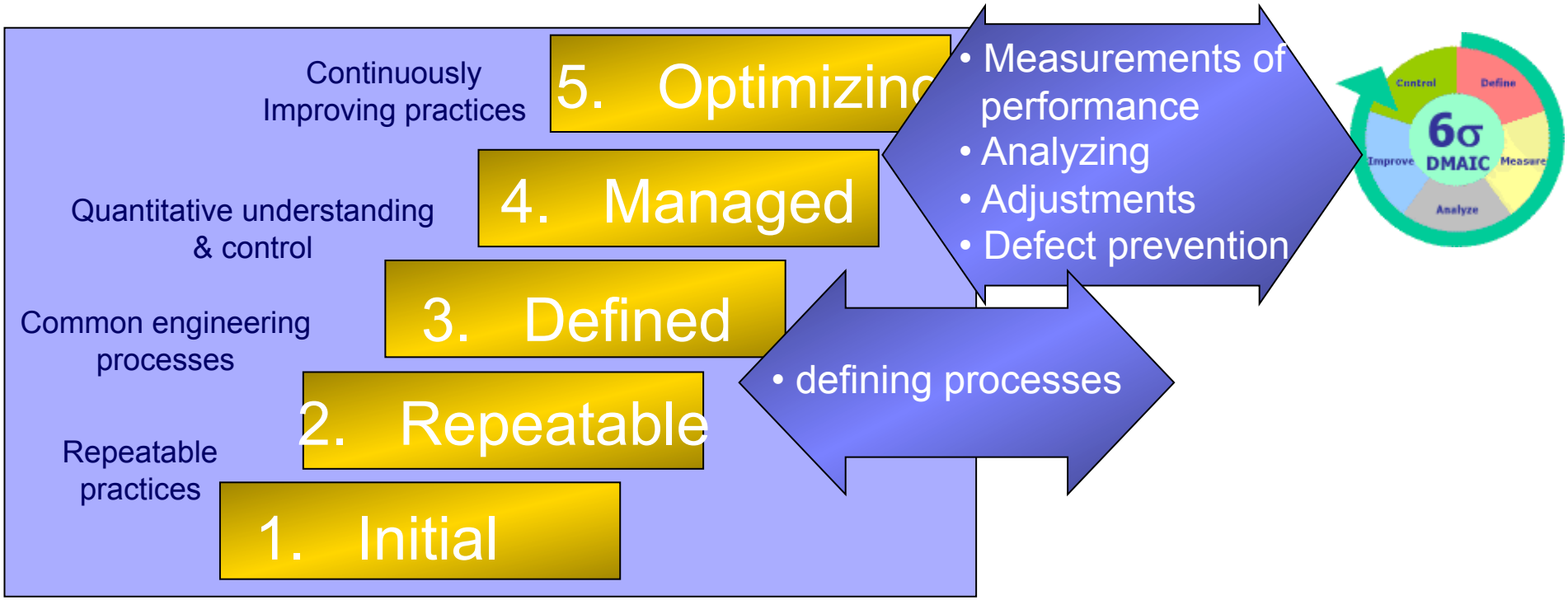
Six Sigma (TQM on Steroids)

- There are two Six Sigma sub-methodologies: DMAIC and DMADV.
- The Six Sigma DMAIC process (define, measure, analyze, improve, control) is an improvement system for existing processes falling below specification and looking for incremental improvement.
- The Six Sigma DMADV process (define, measure, analyze, design, verify) is an improvement system used to develop new processes or products at Six Sigma quality levels. It can also be employed if a current process requires more than just incremental improvement.
- Both Six Sigma processes are executed by Six Sigma Green Belts and Six Sigma Black Belts, and are overseen by Six Sigma Master Black Belts.

Opportunities for errors?



CMMI & Six Sigma



❖ If an organization is truly a CMM Level 5 organization, it is also in spirit, if not in fact, a Six Sigma organization.

❖ Conversely, a true Six Sigma organization is in spirit, if not in fact, a CMM Level 5 organization.

❖ **In each case, processes must be defined, data must be collected, and data used quantitatively to improve the processes.**

ITIL, CMMI & Six Sigma

- **ITIL** defines the processes and shows us “how” to achieve higher levels of integration and maturity
  - **“Success”** in ITIL is integration and efficiency
  - “Goal” is higher availability, reliability and stability
- **CMMI** provides the model and the rough scale of measurement
  - Defines maturity in terms of whether or not processes have been defined, implemented, documented and consistently used
  - "**Success**" in CMMI is moving up the scale.
  - “Goal” is improve quality of product by improving the processes used to build it
- **Six Sigma** may be viewed as the verification element (to forecast and validate improvement) and the "why" (establishing and proving the business case for improvement projects).
  - "**Success**" in Six Sigma is bottom line business benefit.
  - “Goal” reduce defects to a statistical level

Language is also Important

- “Wipro is the first software services company in the world to be assessed at SEI CMM level 5 - the highest maturity level for any software process. We achieved CMMI level 5 certification in June, 1999….”
- SCAMPI (Standard CMMI Appraisal Method for Process Improvement) Assessment
- ITIL-Compatible vs. ITIL-Certified vs. ITIL-Compliant
- ISO 20000-Certified

Project Management Methodogies

- PMI
- Prince2

Project Management: PMBOK

- Project Management Body of Knowledge (PMBOK)
- Custodian: Project Management Institute (PMI) in US
- Established in 1969
- Focused on projects of any kind, not IT specific
- Currently over 60% of the membership work in IT
- Over 300,000 credentials issued worldwide
- Individual Certification: Yes
- Organizational Assessment: Yes
- www.pmi.org

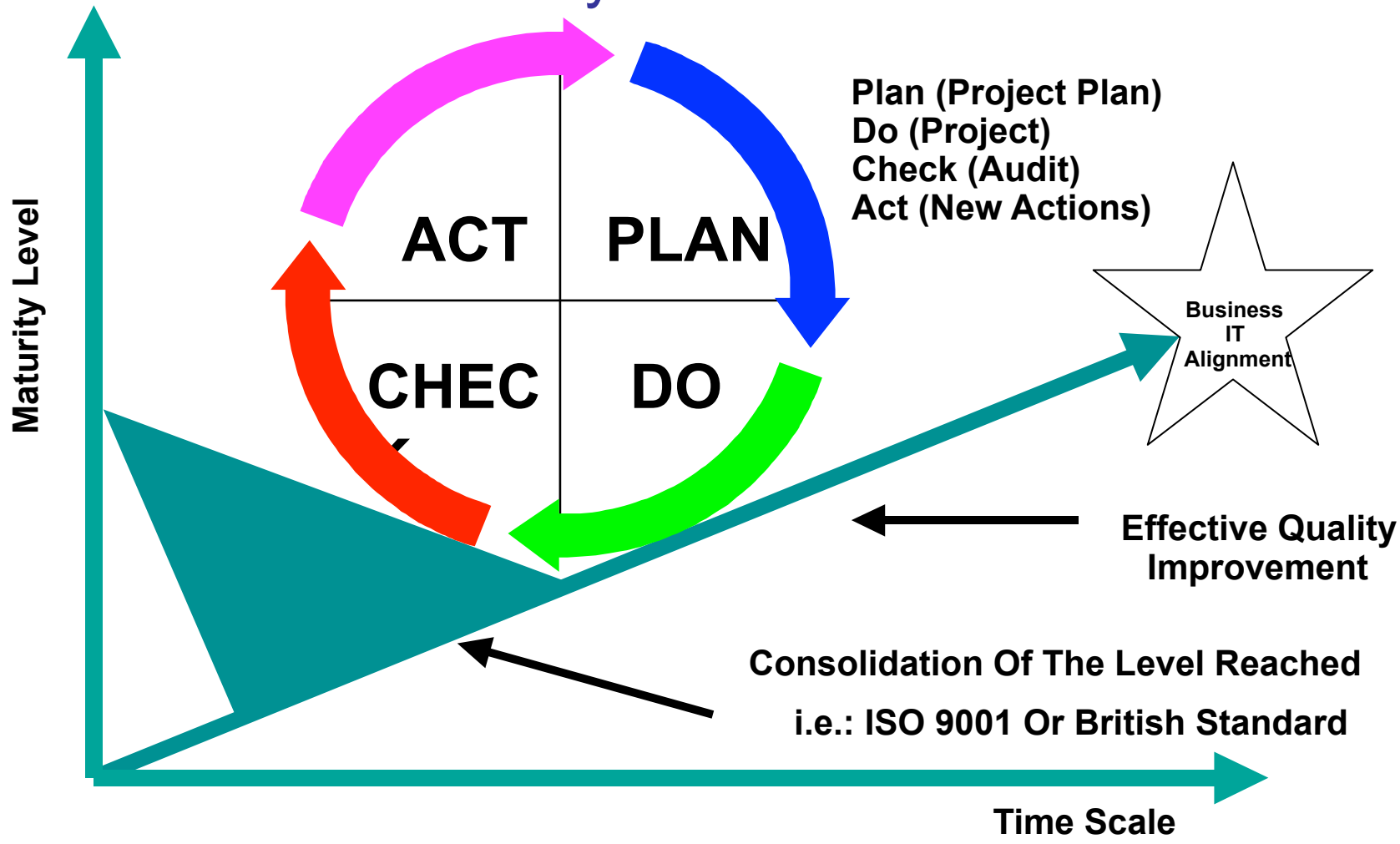
Project Management: Prince2 2009

- PRojects IN Controlled Environments v2
- Custodian: Office of Government Commerce (UK)
- Just updated/refreshed in 2009
- While not IT specific it works well in managing IT projects
- Individual Certification: Yes
- Organizational Assessment: Yes
- www.prince-officialsite.com

So now what?

The Deming Cycle

Continuous Quality Control & Consolidation



Plan-Do-Check-Act

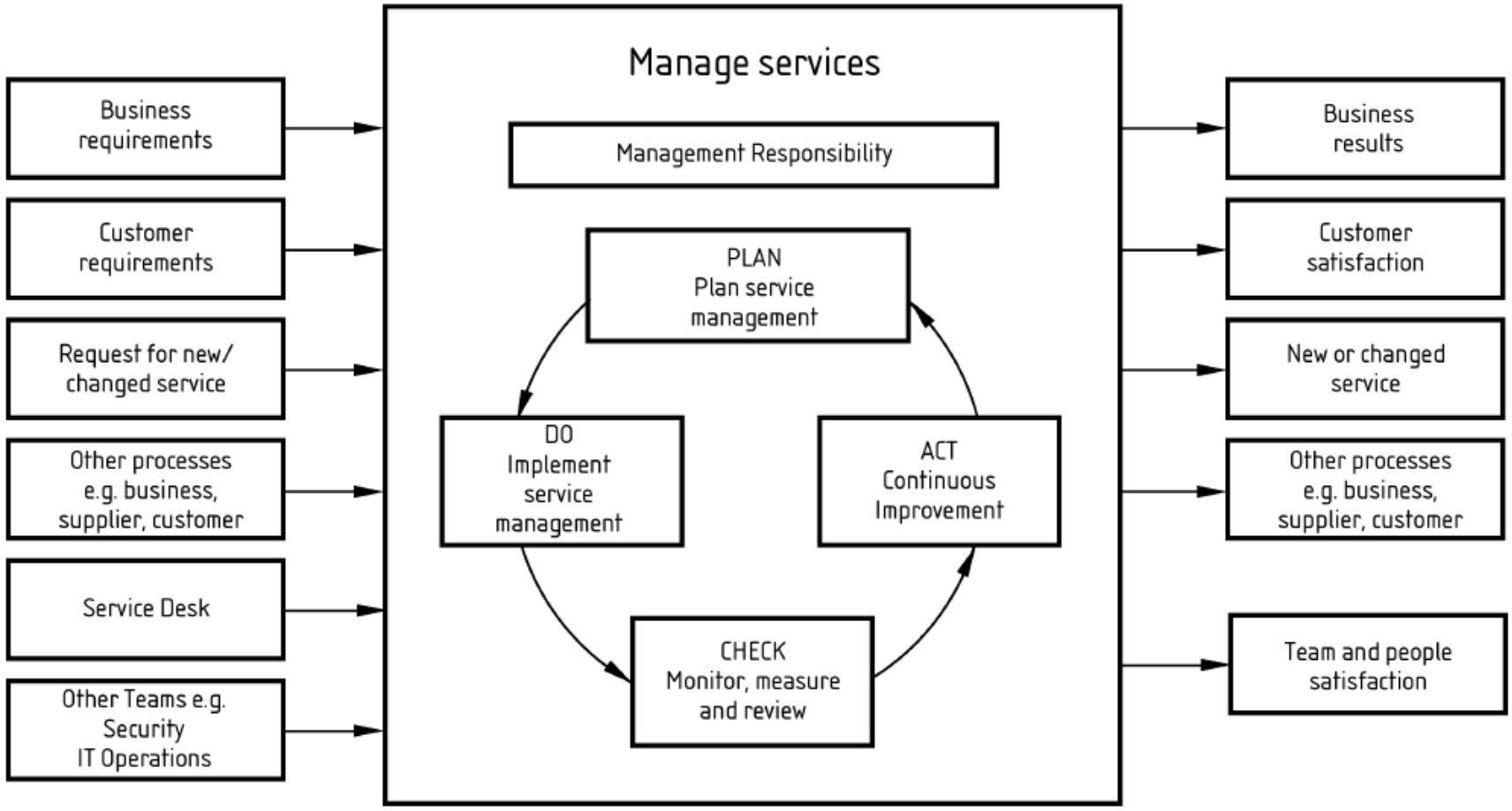


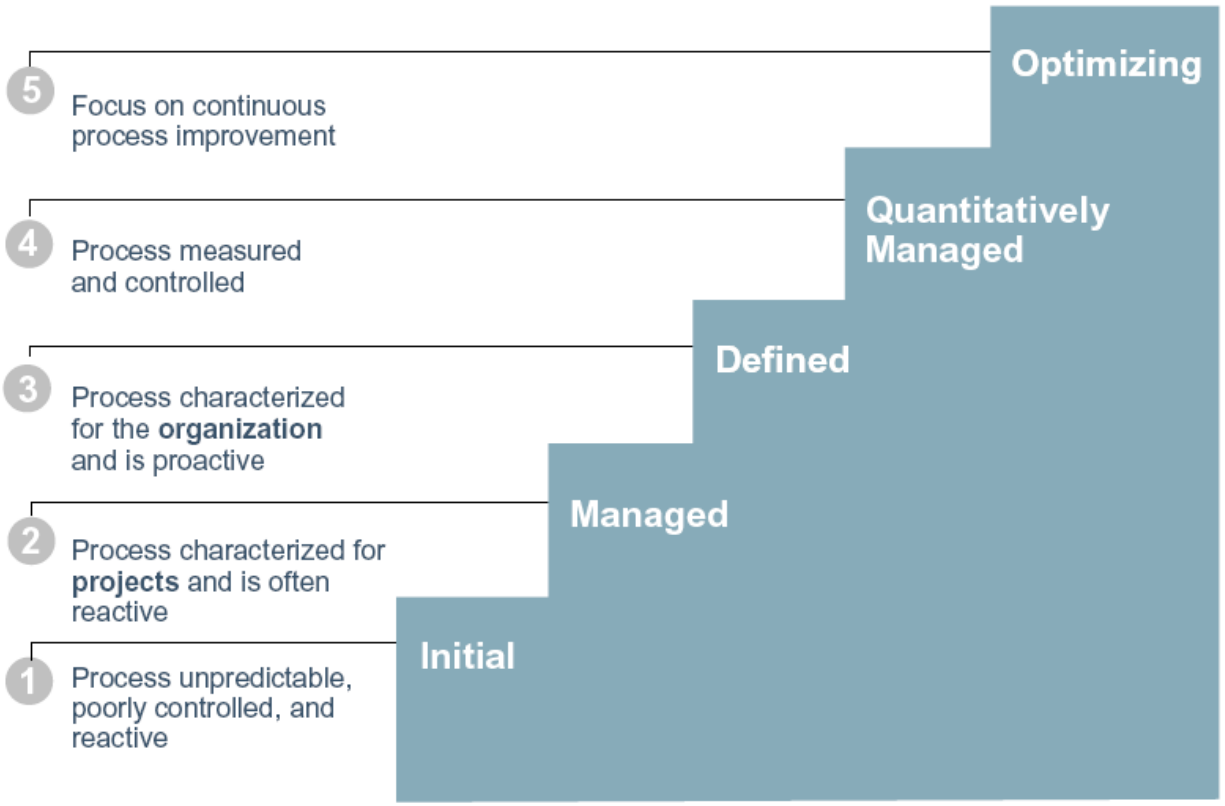
Figure 1 — Plan-Do-Check-Act methodology for service management processes

Maturity Levels

Carnegie Mellon
Software Engineering Institute

CMMI

The Maturity Levels



When is my ITSM Implementation good enough?

- Every framework/model is focused on the reality that every process should be:
  - Consistent
  - Documented
  - Repeatable
  - Auditable
- In other words, the process is well-defined and we are in “control” of the process
- “Control” or “Defined” is equal to SEI’s Capability Maturity Model, Level 3

Pink Perspective
December 2009

David Ratcliffe
President
Pink Elephant
david.ratcliffe@pinkelephant.com
http://blogs.pinkelephant.com/president

George Spalding
Executive Vice President
Pink Elephant
g.spalding@pinkelephant.com