Applicazioni del CMMI© : Information Technology e Sicurezza

Software Engineering Institute
Carnegie Mellon University

Enrico Viola, CISA, CMMI Appraiser
viola@eclat-web.com

Applicazioni del CMMI
Agenda :

- ✓ Introduzione : uso dei modelli; i modelli di maturità
- ✓ I modelli per l’IT
- ✓ Il CMMI per l’IT : motivazioni, benefici, difficoltà da superare
- ✓ La sicurezza : modelli di riferimento
- ✓ Utilizzo del CMMI per soddisfare gli obiettivi di sicurezza
- ✓ Considerazioni finali

I modelli

“All models are wrong, but some are useful.”

– George Box

I modelli

Un modello è utile
- Per individuare obiettivi e priorità, e per “riassumere” le migliori pratiche in una guida che assicuri processi stabili, performanti e maturi
- Come guida per il miglioramento

Un modello utile fornisce
- Un punto di partenza
- I benefici dell’esperienza di chi lo ha generato
- Un linguaggio ed una visione condivisi
- Uno strumento per stabilire le priorità

Modello di Maturità

- E' un insieme strutturato di elementi che descrive le caratteristiche di **processi efficaci** (*in base all'esperienza delle organizzazioni che hanno predisposto il modello*)
- Fornisce
  - Un punto di partenza e degli **stati "obiettivo"**
  - L'esperienza della comunità che lo ha prodotto
  - Un linguaggio comune ed una visione condivisa
  - Un metodo per determinare le priorità
  - Un modo per definire il significato di "miglioramento" per l'organizzazione
- Può essere utilizzato per confrontare organizzazioni diverse

I modelli di maturità

Software CMM	staged	software development
System Engineering CMM	continuous	system engineering
System Engineering Capability Model	continuous	system engineering
Software Acquisition CMM	staged	software acquisition
System Security Engineering CMM	continuous	security engineering
Personal Software Process	staged	individual software development
FAA-iCMM	continuous	software engineering, systems engineering, and acquisition
IPD-CMM	hybrid	integrated product development
People CMM	staged	workforce
SPICE Model	continuous	software development

CMMI

CAPABILITY

*quanto è **adeguato** un processo per gli scopi per cui è stato definito?*

MATURITY

*quanto è **consolidato** il suo uso all’interno dell’Azienda?*

MODEL

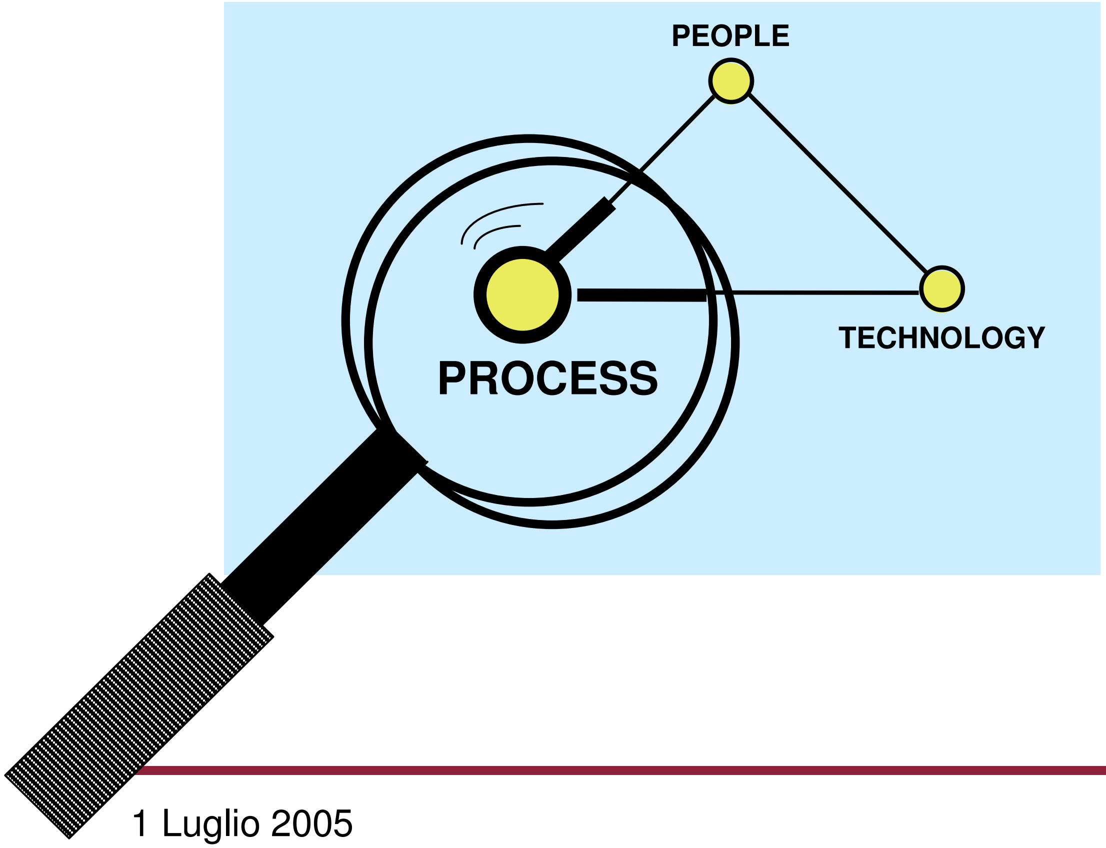
***Insieme** di descrizioni **di processi** da adattare alle diverse realtà aziendali*

INTEGRATION

*Una struttura predisposta all’integrazione di **più discipline** (SW, Systems Engineering, Supplier Sourcing, IPPD)*

CMMI

Focalizza l'attenzione sul concetto di PROCESSO



"La qualità di un prodotto è determinata principalmente dalla qualità dei processi di sviluppo, produzione e manutenzione"

Dai principi del TQM (Shewhart, Juran, Deming, Humphrey.

Il modello CMM Integration^{SM}

✓Raggruppa i processi in 25 aree (***Process Area***) che coprono un largo spettro delle attività aziendali relative ad alcune Discipline

✓Le Process Area appartengono a quattro categorie:

- **Process management**
- **Project management**
- **Engineering**
- **Support**

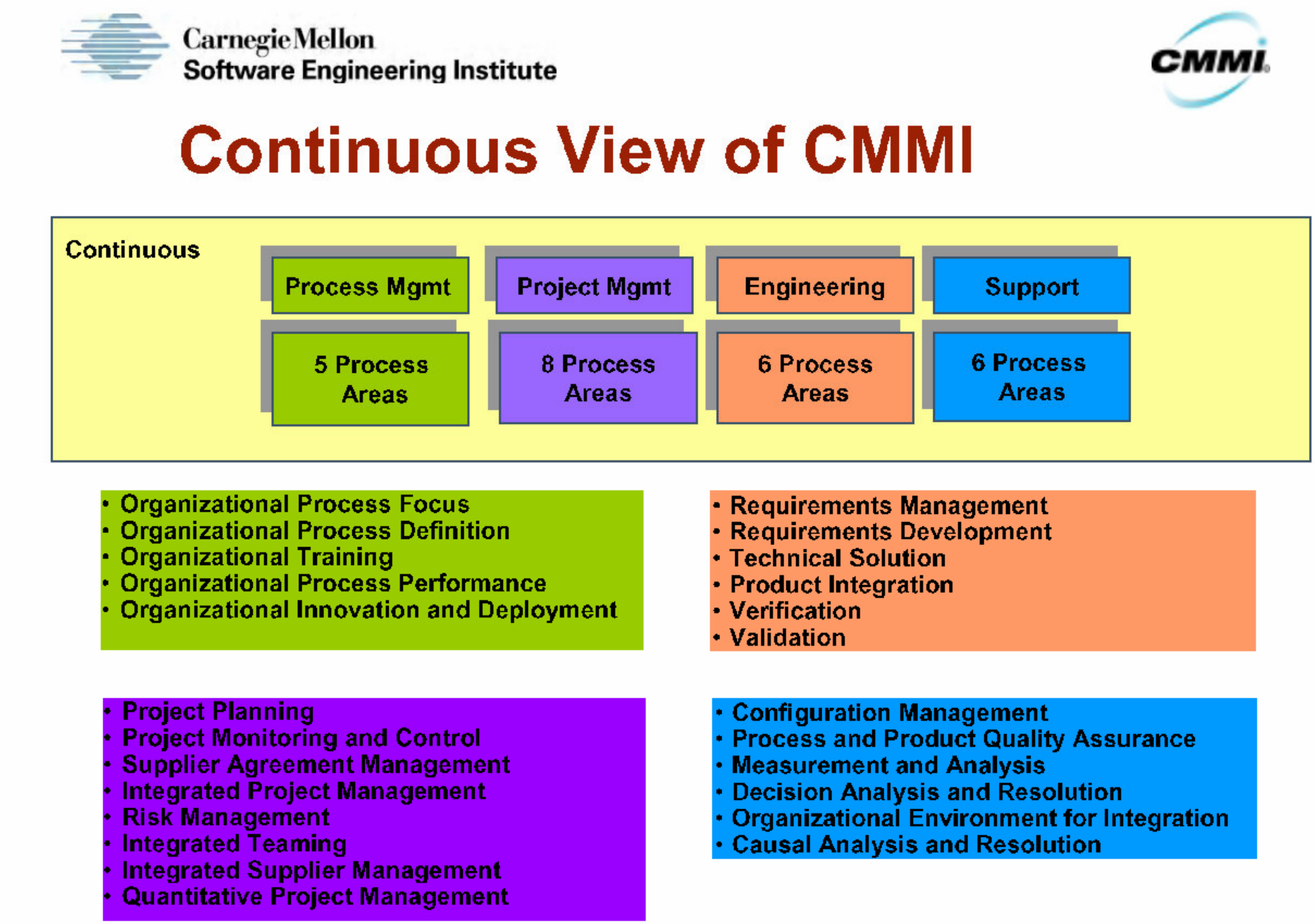
✓Costituisce l'infrastruttura per l'inserimento dei processi relativi ad altre discipline

Caratteristiche del modello

- ✓ Per ciascuna area di processo il CMMI fornisce una struttura unica composta da:
  - ***Obiettivi (Goal) da soddisfare***
  - ***Pratiche per soddisfarli***
  - ***Livelli di evoluzione dei processi dell’area (Capability)***

  Gli obiettivi sono di due tipi:
  - ***Specifici dell’area di processo***
  - ***Comuni a tutte le aree di processo***
- ✓ Obiettivi e pratiche specificano i requisiti di processi di provata efficacia, lasciando alle Organizzazioni il compito di soddisfare agli stessi nei modi più appropriati

I modelli per l'IT : CMMI



Carnegie Mellon
Software Engineering Institute

CMMI

Continuous View of CMMI

Continuous

Process Mgmt	Project Mgmt	Engineering	Support
5 Process Areas	8 Process Areas	6 Process Areas	6 Process Areas

- Organizational Process Focus
- Organizational Process Definition
- Organizational Training
- Organizational Process Performance
- Organizational Innovation and Deployment

- Project Planning
- Project Monitoring and Control
- Supplier Agreement Management
- Integrated Project Management
- Risk Management
- Integrated Teaming
- Integrated Supplier Management
- Quantitative Project Management

- Requirements Management
- Requirements Development
- Technical Solution
- Product Integration
- Verification
- Validation

- Configuration Management
- Process and Product Quality Assurance
- Measurement and Analysis
- Decision Analysis and Resolution
- Organizational Environment for Integration
- Causal Analysis and Resolution

I livelli di Capability

Ciascuna Process Area prevede 6 livelli di Capability che vengono conseguiti mettendo in pratica attività via via più evolute

5 Optimizing

4 Quantitatively Managed

3 Defined

2 Managed

1 Performed

0 Incomplete

Le Process Areas ordinate per Livelli di Maturità

Livello	Focus	Process Area
5 Optimizing	*Continuous process improvement*	Organizational Innovation and Deployment
		Causal Analysis and Resolution
4 Quantitatively Managed	*Quantitative management*	Organizational Process Performance
		Quantitative Project Management
3 Defined	*Process standardization*	Requirements Development
		Technical Solution
		Product Integration
		Verification
		Validation
		Organizational Process Focus
		Organizational Process Definition
		Organizational Training
		Integrated Project Management
	(SS)	Integrated Supplier Management
		Risk Management
		Decision Analysis and Resolution
	(IPPD)	Organizational Environment for Integration
	(IPPD)	Integrated Teaming
2 Managed	*Basic project management*	Requirements Management
		Project Planning
		Project Monitoring and Control
		Supplier Agreement Management
		Measurement and Analysis
		Process and Product Quality Assurance
		Configuration Management
1 Initial		

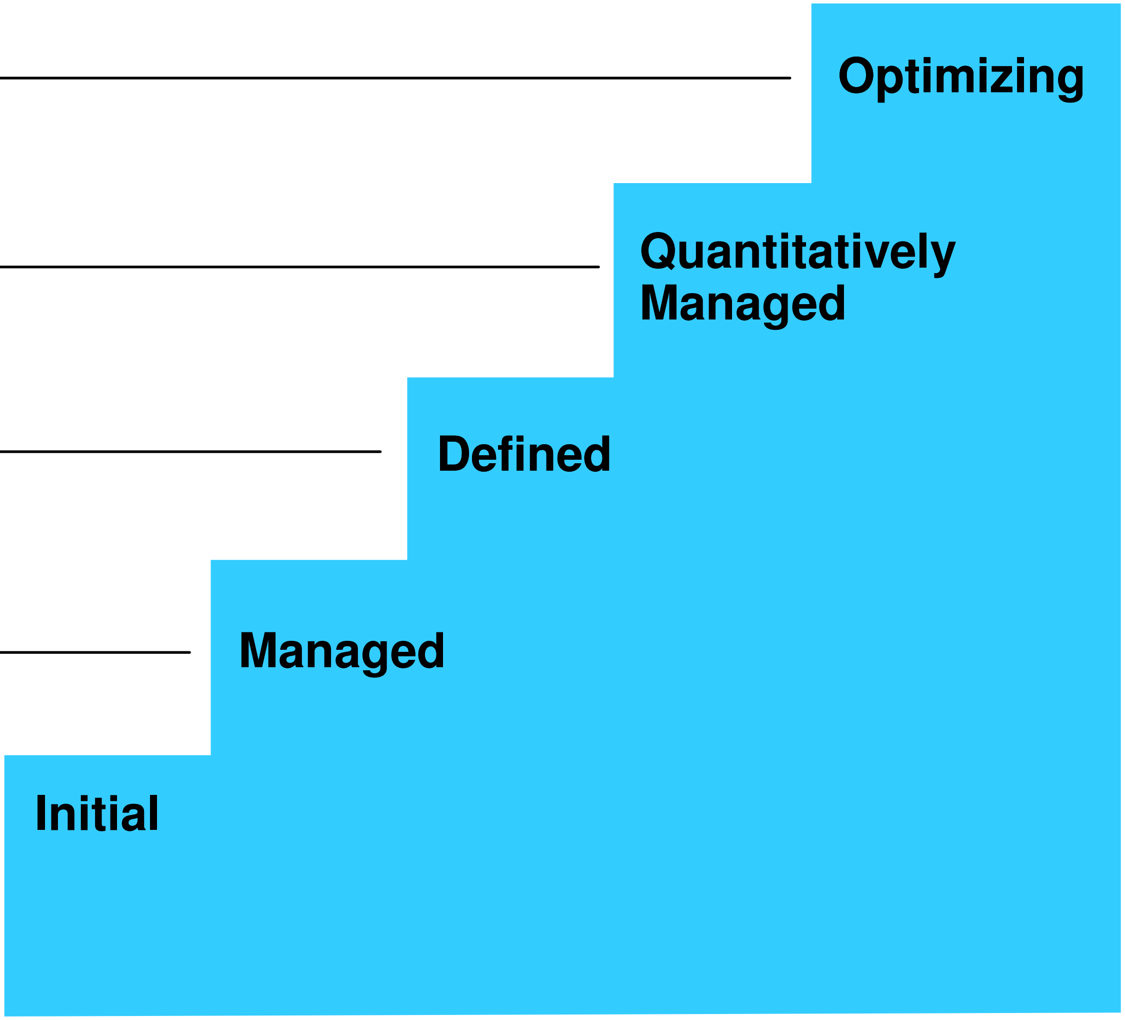
CL3

CL3

CL3

CL2

I 5 livelli di maturità (nel modello Staged)



5 **Focus on process improvement**

4 **Process measured and controlled**

3 **Process characterized for the organization and is proactive**

2 **Process characterized for projects and is often reactive**

1 **Process unpredictable, poorly controlled and reactive**

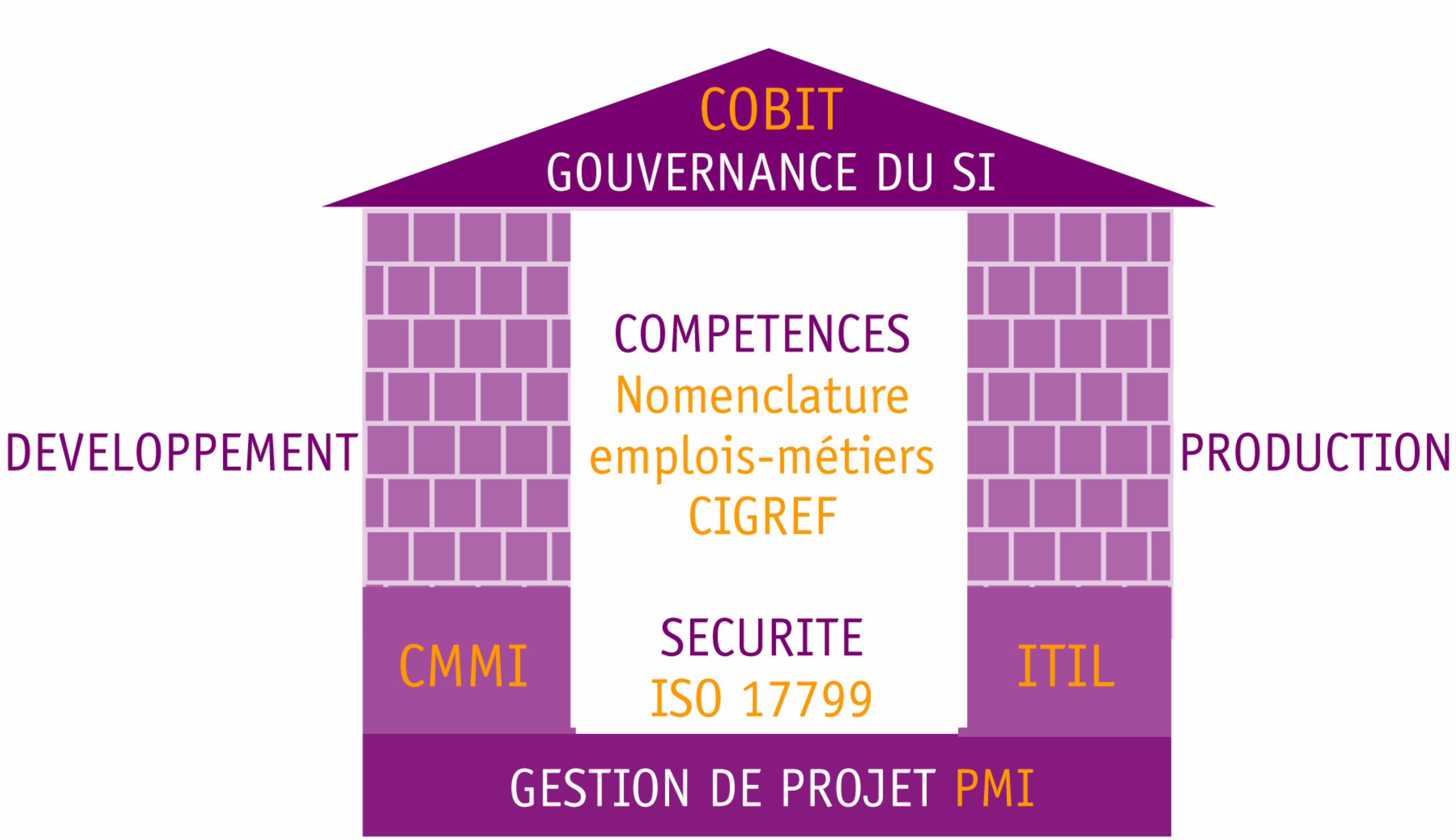
I modelli per l’IT

- ✓ COBIT
- ✓ ITIL – Information Technology Infrastructure Library di OCG (British Office of Government)
- ✓ I modelli per la gestione delle singole discipline (ad esempio, per la sicurezza, BS7799, ISO/IEC 13335 , SSE-CMM, NIST 800-14)
- ✓ CMMI ??

I modelli per l'IT : ITIL

- ✓ è un insieme di template e "Best Practice" indirizzate a migliorare ed a rendere più efficace ed efficiente la gestione dei servizi erogati dell'Organizzazione IT
- ✓ ITIL consiste in una serie di libri che descrivono delle linee guida su come fornire, gestire e controllare la qualità dei servizi IT, e su come adattare ed integrare le risorse umane e strutturali per supportare l'IT.
- ✓ Esistono ad oggi sette libri delle "Best Practices" ITIL :
  - ⇨ *Service Support*
  - ⇨ *Service Delivery*
  - ⇨ *Planning to Implement Service Management*
  - ⇨ *Application Management*
  - ⇨ *ICT Infrastructure Management*
  - ⇨ *Security Management*
  - ⇨ *The Business Perspective (non ancora pubblicato – autunno 2004)*

La « visione ITIL » (itSMF Francia)



Fonte : presentazione ***it*SMF France**

I modelli per l’IT : CMMI ?

- ✓ **Punti di forza :**
  - ✓ E’ riconosciuto come eccellente per lo sviluppo del software
  - ✓ E’ stato integrato per alcuni aspetti rilevanti : Sicurezza (SSE-CMM), Safety (+SAFE)
  - ✓ Consentirebbe di condividere i metodi e i contenuti degli audit
  - ✓ E’ sicuramente “compliant” con le norme ISO
  - ✓ E’ orientato ai processi, quindi facilmente adattabile (dice “cosa” fare, non “come” farlo)
  - ✓ E’ sostenuto e continuamente alimentato dalle esperienze di numerose aziende

- ✓ **Riflessioni :**
  - ⇨ Ci sono modelli specifici, facilmente integrabili, anch’essi conformi alle norme ISO
  - ⇨ I metodi di audit si assomigliano tutti

I modelli per l’IT : CMMI

Requisiti

- ✓ Orientamento ai processi dell’organizzazione e del reparto IT
- ✓ Prevalenza dei metodi sui tools
- ✓ Cultura della misura
- ✓ Focus sui dati (*il miglioramento dei processi è attuato attraverso la rilevazione, la comprensione e l’utilizzo di dati di progetti, qualità, testing, …)*

I modelli per l’IT : CMMI

Caratteristiche

✓il CMMI è prima di tutto un **MODELLO PER IL MIGLIORAMENTO DEI PROCESSI**, non solo un modello di valutazione

✓ Il concetto di “maturità” è riferito all’intera organizzazione, non al singolo processo (per il quale è definito il concetto di “capability”)

✓ Le pratiche sono articolate per livello di capability, è quindi molto semplice definire un percorso di evoluzione

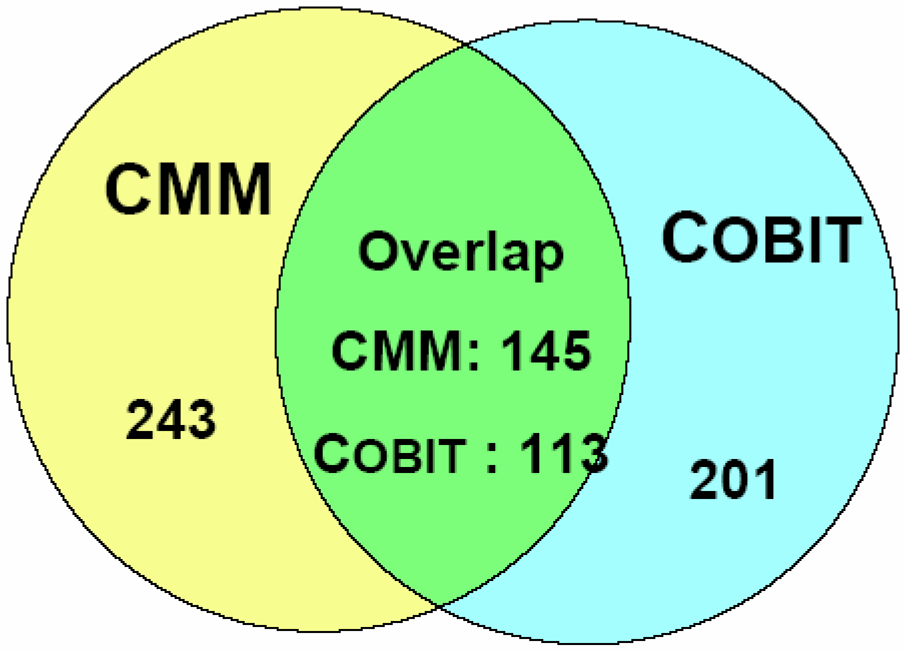
I modelli per l'IT : CMMI

Caratteristiche

- ✓L'estensione a discipline diverse da quelle "di origine" avviene normalmente attraverso la definizione di aree di processo SPECIFICHE

Domanda : Ha senso farlo nel momento in cui c'è già un modello specifico come COBIT ?

COBIT e CMMI



CMM

243

Overlap

CMM: 145

COBIT : 113

COBIT

201

44 Reference Practices
484 Cross-connects

CMM: Practices and Goals

COBIT: Detailed Control Objectives

Fonte : Teraquest

COBIT e CMMI

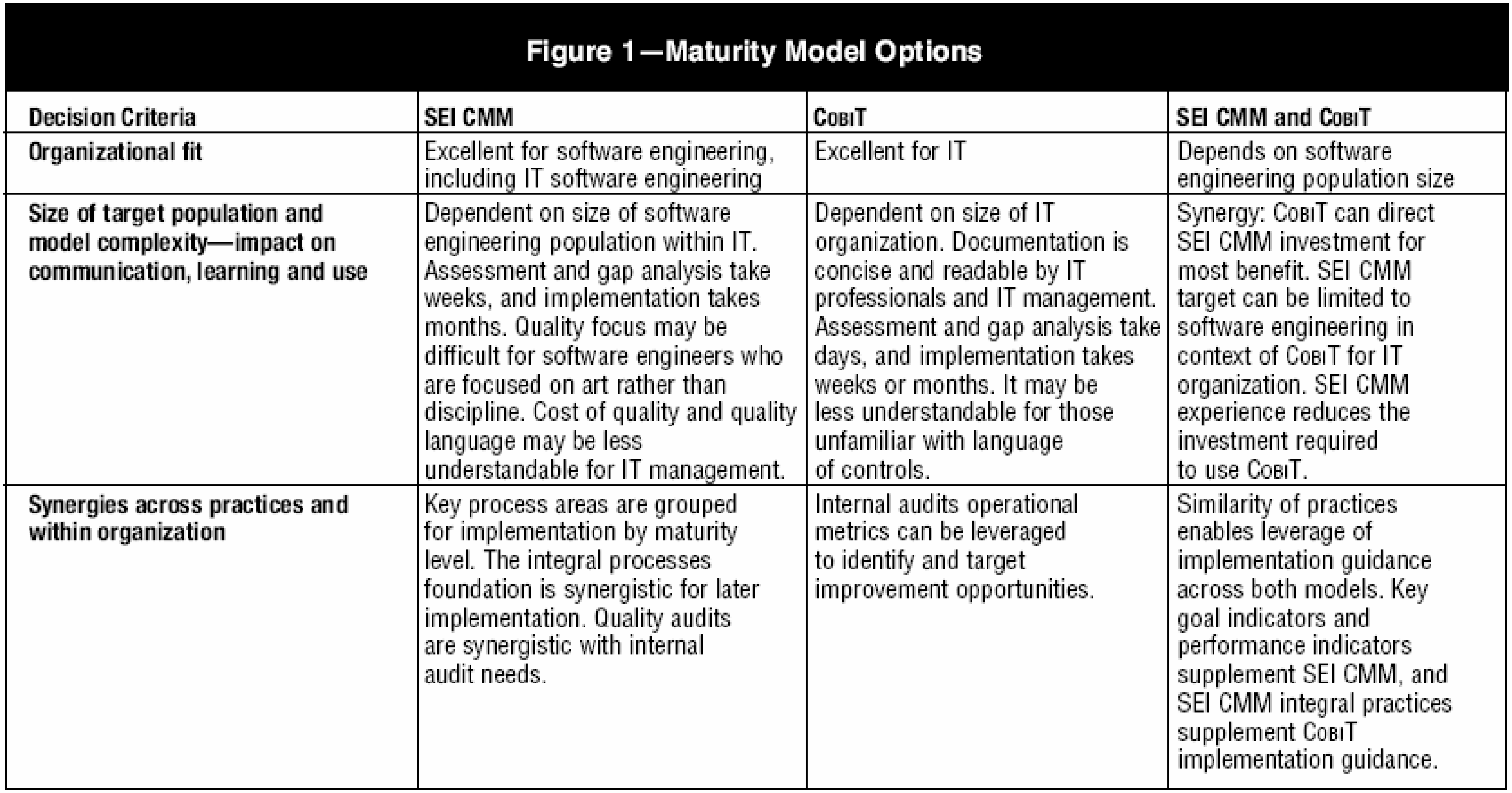


Figure 1—Maturity Model Options

Decision Criteria	SEI CMM	CobiT	SEI CMM and CobiT
Organizational fit	Excellent for software engineering, including IT software engineering	Excellent for IT	Depends on software engineering population size
Size of target population and model complexity—impact on communication, learning and use	Dependent on size of software engineering population within IT. Assessment and gap analysis take weeks, and implementation takes months. Quality focus may be difficult for software engineers who are focused on art rather than discipline. Cost of quality and quality language may be less understandable for IT management.	Dependent on size of IT organization. Documentation is concise and readable by IT professionals and IT management. Assessment and gap analysis take days, and implementation takes weeks or months. It may be less understandable for those unfamiliar with language of controls.	Synergy: CobiT can direct SEI CMM investment for most benefit. SEI CMM target can be limited to software engineering in context of CobiT for IT organization. SEI CMM experience reduces the investment required to use CobiT.
Synergies across practices and within organization	Key process areas are grouped for implementation by maturity level. The integral processes foundation is synergistic for later implementation. Quality audits are synergistic with internal audit needs.	Internal audits operational metrics can be leveraged to identify and target improvement opportunities.	Similarity of practices enables leverage of implementation guidance across both models. Key goal indicators and performance indicators supplement SEI CMM, and SEI CMM integral practices supplement CobiT implementation guidance.

Fonte : ISACA

I modelli per l'IT : CMMI

- ✓CMMI e COBIT sono complementari
  - Non ci sono casi di evidente contraddizione
  - ognuno copre aree non gestite dall'altro
- ✓CMMI è focalizzzato sul miglioramento (come posso fare meglio le singole attività?)
- ✓COBIT è orientato al controllo *(come sto lavorando ora?)*
- ✓COBIT è sicuramente integrabile all'interno del framework CMMI per le organizzazioni IT

I modelli per l'IT : CMMI

Using COBIT and SEI CMM to Lead Process Improvement

Recommended steps include:

1. **Identify opportunities for improvement.** The opportunities could be identified by looking at internal audit findings mapped to COBIT control objectives and a COBIT assessment and/or benchmark.
2. **Evaluate the expected benefit from the improvement.** The COBIT key goal indicators and the “why do it” statement from COBIT can be used if process measures are not already available.
3. **Use correlations and mapping of SEI CMM key practices to COBIT control objectives** to identify control objectives that are met and strengthened using SEI CMM practices. COBIT control objective correlation to SEI CMM practices indicate where the SEI CMM KPAs have a higher probability of giving more accurate and precise guidance than using COBIT alone.

Fonte : ISACA

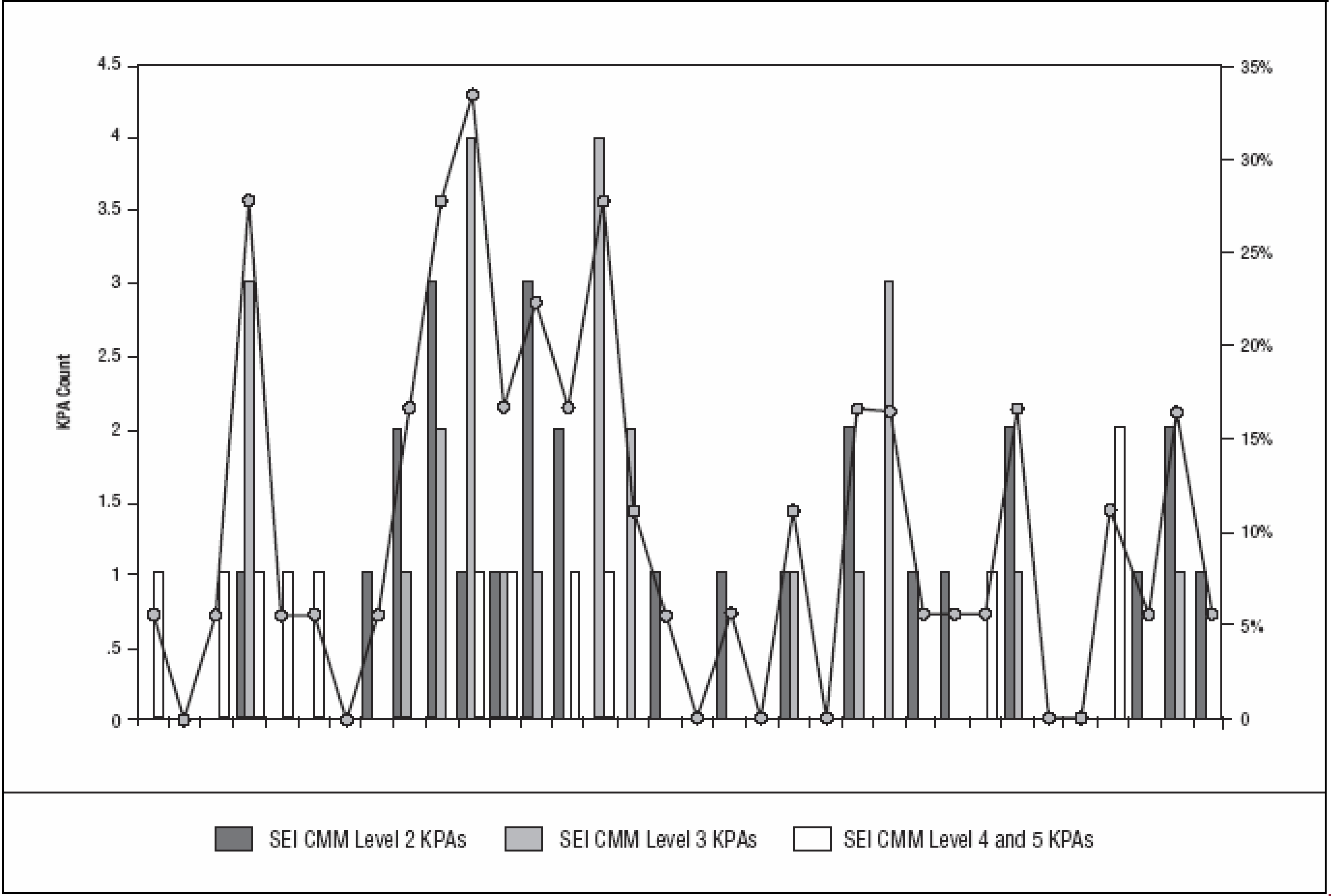
I modelli per l'IT : CMMI

4. **Decide whether the expected benefit justifies a full SEI CMM assessment** if not already available.
5. **Base the implementation strategic and tactical plans on assessed opportunities linked to best practices**. Set goals and milestones to reach an IT-wide balanced maturity level. Establish priorities for processes to improve based on the desired improvement and the planning and monitoring processes to create the feedback loops foundational to sustaining performance and generating additional opportunities.

Fonte : ISACA

I modelli per l’IT : CMMI

Figure 4—CobiT and SEI CMM Correlation



Fonte : ISACA

I modelli per la sicurezza : SSE-CMM

- ✓L’estensione del CMMI a discipline diverse da quelle “di origine” avviene normalmente attraverso la definizione di aree di processo SPECIFICHE
- ✓ nel caso della sicurezza è stato creato un nuovo modello (da parte della FAA e del DoD ed attualmente seguito da ISSEA-International Systems Security Engineering Association) :

SSE-CMM   Systems Security Engineering CMM

I modelli per la sicurezza : SSE-CMM

- ✓ Descrive le caratteristiche essenziali del processo di “security engineering” di una organizzazione.
- ✓ La versione 2.0 è stata recepita dalla ISO nella norma ISE/IEC 21827
- ✓ Comprende un metodo specifico per la valutazione (SSE-CMM Appraisal Method)
- ✓ E’ una collezione delle migliori “pratiche” di ingegneria della sicurezza
- ✓ E’ un modello basato sui processi,finalizzato al loro miglioramento

Security Engineering

Security engineering is an evolving discipline. As such, a precise definition with community consensus does not exist today. However, some generalizations are possible.

Some goals of security engineering are to:

- Gain understanding of the security risks associated with an enterprise
- Establish a balanced set of security needs in accordance with identified risks
- Transform security needs into security guidance to be integrated into the activities of other disciplines employed on a project and into descriptions of a system configuration or operation
- Establish confidence or assurance in the correctness and effectiveness of security mechanisms
- Determine that operational impacts due to residual security vulnerabilities in a system or its operation are tolerable (acceptable risks)
- Integrate the efforts of all engineering disciplines and specialties into a combined understanding of the trustworthiness of a system

I modelli per la sicurezza : SSE-CMM

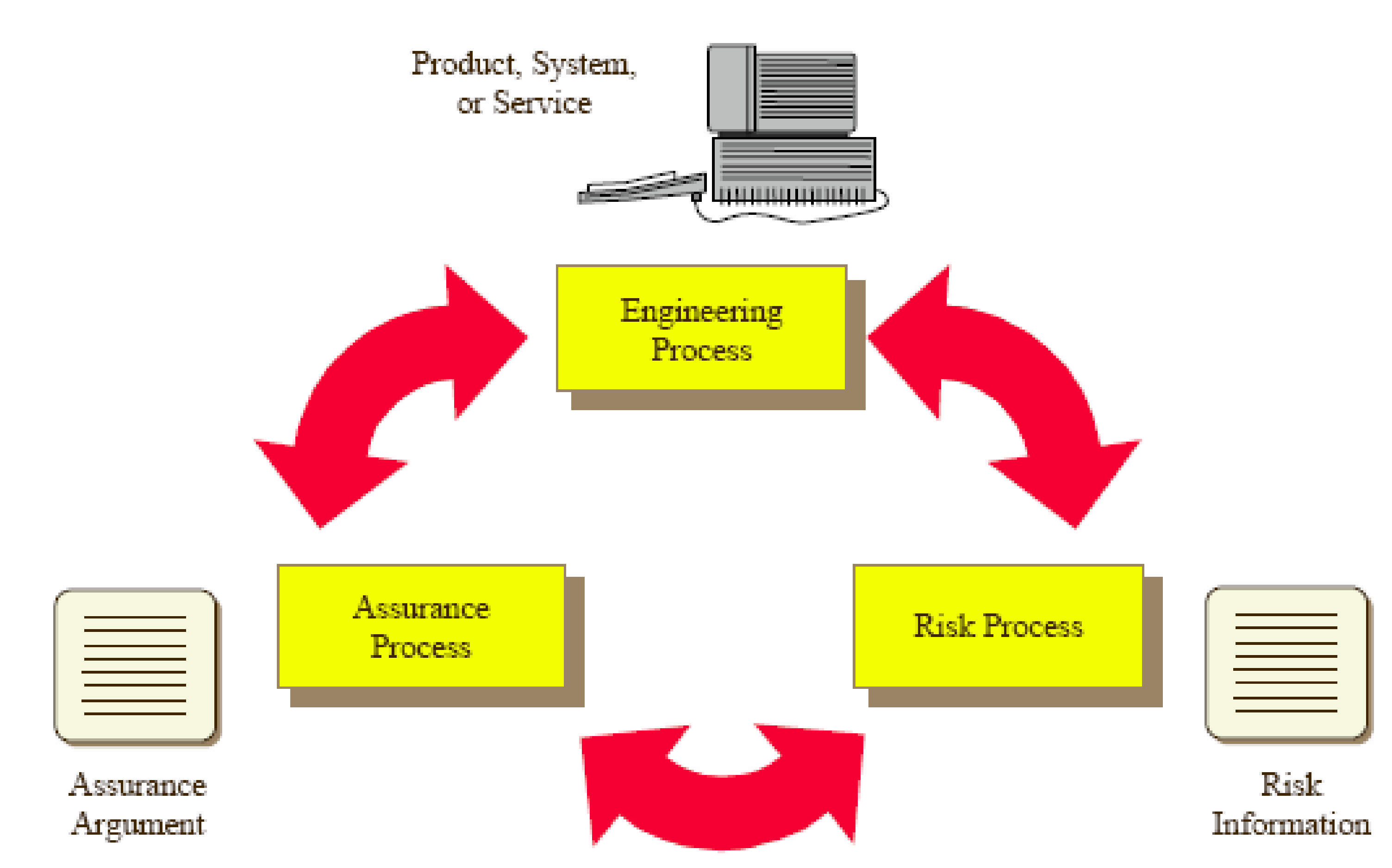
Il modello è utilizzato per :

- valutare le attività di “ingegneria della sicurezza” di un’organizzazione e per definirne I miglioramenti.
- valutare la “capability” dei fornitori di prodotti e servizi di sicurezza.
- formalizzare gli standard di ingegneria della sicurezza di una organizzazione.

SSE-CMM : risultati attesi

- PREDICIBILITA' DEI PROCESSI : come in tutti i CMM, il miglioramento è basato sulla misura
- CONTROLLO : il miglioramento del livello di "capability" genera un miglior controllo
- MIGLIORAMENTO DELL'EFFICACIA DEI PROCESSI

SSE-CMM : 3 aree



SSE-CMM : 2 dimensioni

1. DOMAIN :

consiste nell’insieme di “pratiche” (*dette “base practices”)* che nel loro insieme definiscono la “ingegneria della sicurezza”

2. CAPABILITY :

Contiene pratiche (*dette “generic practices”)* riferite al “process management” ed alla “institutionalization capability”

Sono attività che si possono riferire a qualsiasi processo

Indicano la “capability” dell’organizzazione nell’attuare un determinato processo

le “BASE PRACTICES”

- **Sono 129 organizzate in 22 “process area”**

  le prime 68, riferite ad 11 aree, sono le principali per l’ingegneria della sicurezza

  - PA01 Administer Security Controls
  - PA02 Assess Impact
  - PA03 Assess Security Risk
  - PA04 Assess Threat
  - PA05 Assess Vulnerability
  - PA06 Build Assurance Argument
  - PA07 Coordinate Security
  - PA08 Monitor Security Posture
  - PA09 Provide Security Input
  - PA10 Specify Security Needs
  - PA11 Verify and Validate Security

le “BASE PRACTICES”

le altre 61 (afferenti ad altre 11 process area) si riferiscono al progetto ed all’organizzazione

- PA12 – Ensure Quality
- PA13 – Manage Configuration
- PA14 – Manage Project Risk
- PA15 – Monitor and Control Technical Effort
- PA16 – Plan Technical Effort
- PA17 – Define Organization’s Systems Engineering Process
- PA18 – Improve Organization’s Systems Engineering Process
- PA19 – Manage Product Line Evolution
- PA20 – Manage Systems Engineering Support Environment
- PA21 – Provide Ongoing Skills and Knowledge
- PA22 – Coordinate with Suppliers

le “BASE PRACTICES”

PA01: Administer Security Controls

Goal 1 Security controls are properly configured and used.

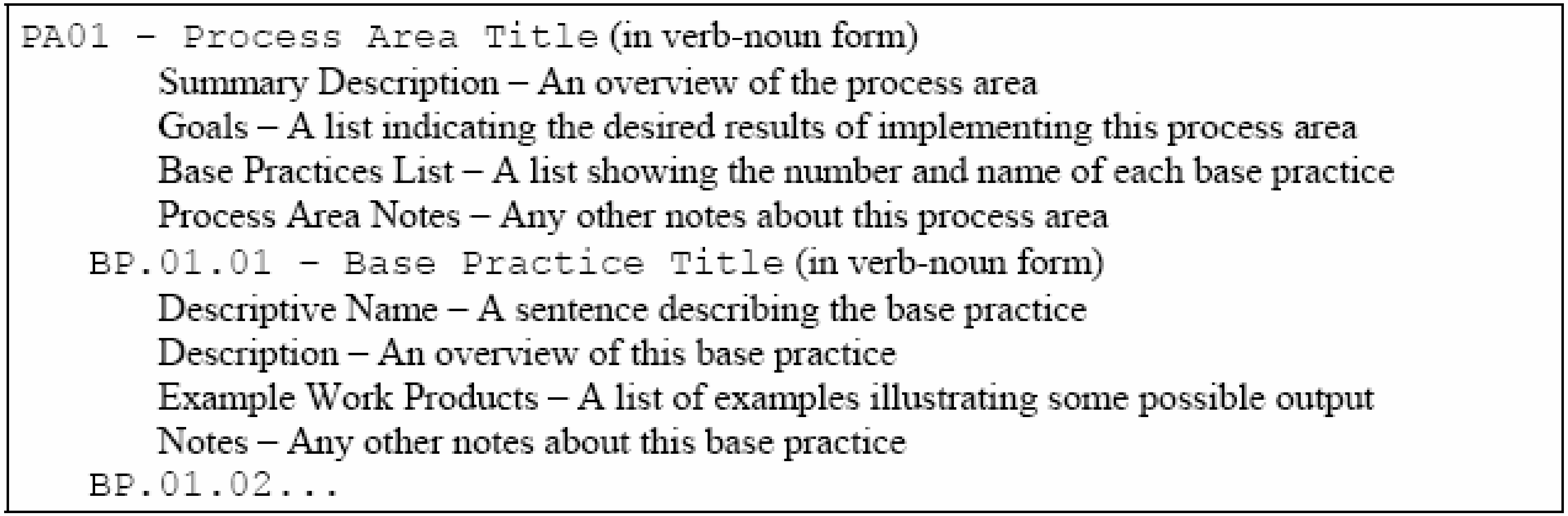
BP.01.01 Establish responsibilities and accountability for security controls and communicate them to everyone in the organization.

BP.01.02 Manage the configuration of system security controls.

BP.01.03 Manage security awareness, training, and education programs for all users and administrators.

BP.01.04 Manage periodic maintenance and administration of security services and control mechanisms.

le “BASE PRACTICES”



PA01 - Process Area Title (in verb-noun form)
- Summary Description – An overview of the process area
- Goals – A list indicating the desired results of implementing this process area
- Base Practices List – A list showing the number and name of each base practice
- Process Area Notes – Any other notes about this process area

BP.01.01 - Base Practice Title (in verb-noun form)
- Descriptive Name – A sentence describing the base practice
- Description – An overview of this base practice
- Example Work Products – A list of examples illustrating some possible output
- Notes – Any other notes about this base practice

BP.01.02...

Figure 6.1 - Process Area Format

le “BASE PRACTICES”

PA01 – Administer Security Controls

Summary Description

The purpose of Administer Security Controls is to ensure that the intended security for the system that was integrated into the system design, is in fact achieved by the resultant system in its operational state.

Goals

- Security controls are properly configured and used.

Base Practices List

BP.01.01 Establish responsibilities and accountability for security controls and communicate them to everyone in the organization.
BP.01.02 Manage the configuration of system security controls.
BP.01.03 Manage security awareness, training, and education programs for all users and administrators.
BP.01.04 Manage periodic maintenance and administration of security services and control mechanisms.

Process Area Notes

This process area addresses those activities required to administer and maintain the security control mechanisms for a development environment and an operational system. Further this process area helps to ensure that, over time, the level of security does not deteriorate. The management of controls for a new facility should integrate with existing facility controls.

le “BASE PRACTICES”

BP.01.01 – Establish Security Responsibilities

Establish responsibilities and accountability for security controls and communicate them to everyone in the organization.

Description

Some aspects of security can be managed within the normal management structure, while others require more specialized management.

The procedures should ensure that those charged with responsibility are made accountable and empowered to act. It should also ensure that whatever security controls are adopted are clear and consistently applied. In addition, they should ensure that whatever structure is adopted it is communicated, not only to those within the structure, but also the whole organization.

Example Work Products

- An organizational security structure chart – identifies the organization members related to security and their role.
- Documents describing security roles – describes each of the organizational roles related to security and their responsibilities.
- Documents describing security responsibilities – describes each of the security responsibilities in detail, including what output is expected and how it will be reviewed and used.
- Documents detailing security accountabilities – describes who is accountable for security related problems, ensuring that someone is responsible for all risks.
- Documents detailing security authorizations – identifies what each member of an organization is allowed to do.

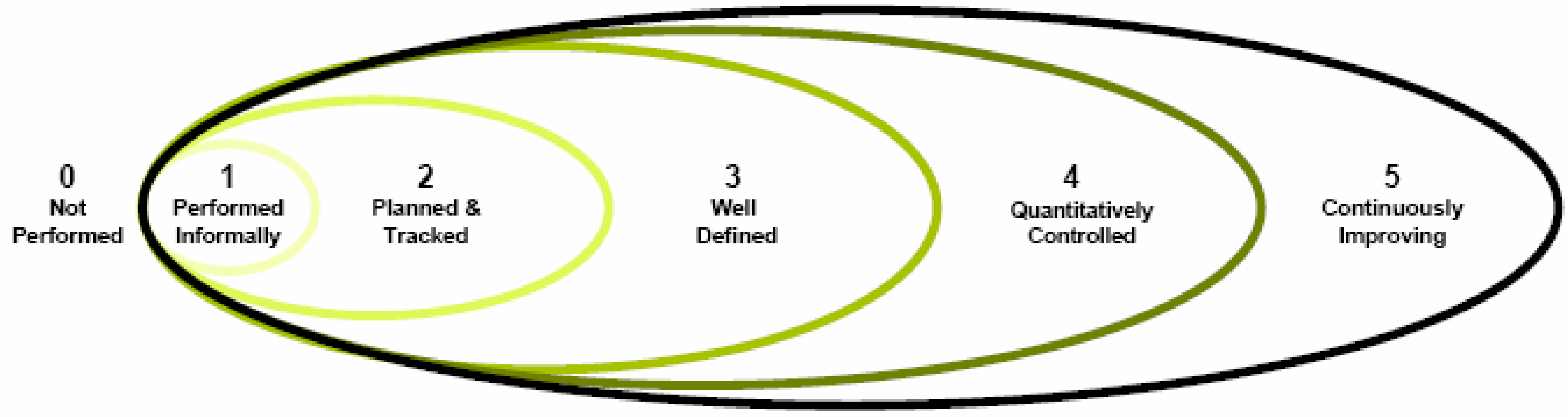
Notes

Some organizations establish a security engineering working group which is responsible for resolving security related issues. Other organizations identify a security engineering lead who is responsible for making sure that the security objectives are attained.

le “GENERIC PRACTICES”

- Sono attività che si possono riferire a qualsiasi processo
- Indicano la “capability” dell’organizzazione nell’attuare un determinato processo
- Sono raggruppate logicamente in “common features”, a loro volta organizzate in “livelli di capability”

I “CAPABILITY LEVELS”



Base practices performed	Committing to perform Planning performance Disciplined performance Tracking performance Verifying performance	Defining a standard process Tailoring standard process Using data Perform a defined process	Establishing measurable quality goals Determining process capability to achievegoals Objectively managing performance	Establishing quantitative process effectiveness goals Improving process effectiveness

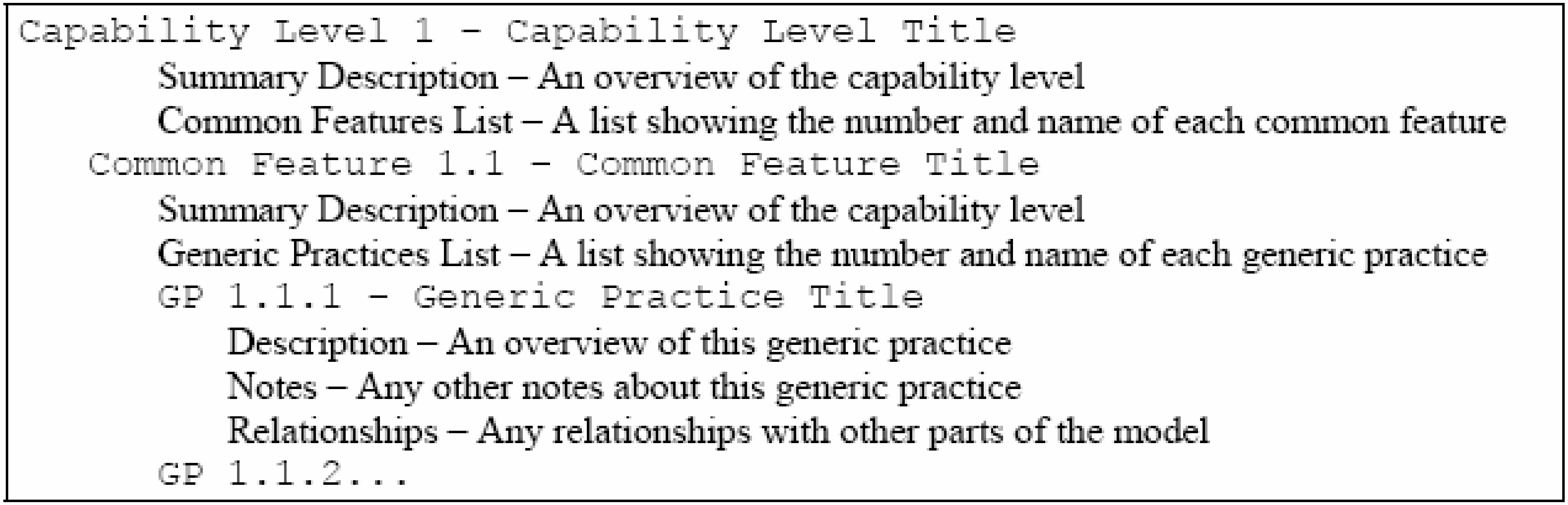
le “GENERIC PRACTICES”

- **Capability Level 1 - Performed Informally**
  - ***Common Feature 1.1 – Base Practices Are Performed***
    - GP 1.1.1 – Perform the Process
- **Capability Level 2 - Planned and Tracked**
  - ***Common Feature 2.1 – Planning Performance***
    - GP 2.1.1 – Allocate Resources
    - GP 2.1.2 – Assign Responsibilities
    - GP 2.1.3 – Document the Process
    - GP 2.1.4 – Provide Tools
    - GP 2.1.5 – Ensure Training
    - GP 2.1.6 – Plan the Process
  - ***Common Feature 2.2 – Disciplined Performance***
    - GP 2.2.1 – Use Plans, Standards, and Procedures
    - GP 2.2.2 – Do Configuration Management
  - ***Common Feature 2.3 – Verifying Performance***
    - GP 2.3.1 – Verify Process Compliance
    - GP 2.3.2 – Audit Work Products
  - ***Common Feature 2.4 – Tracking Performance***
    - GP 2.4.1 – Track with Measurement
    - GP 2.4.2 – Take Corrective Action

le "GENERIC PRACTICES"

- **Capability Level 3 - Well Defined**
  - ***Common Feature 3.1 – Defining a Standard Process***
    - GP 3.1.1 – Standardize the Process
    - GP 3.1.2 – Tailor the Standard Process
  - ***Common Feature 3.2 – Perform the Defined Process***
    - GP 3.2.1 – Use a Well-Defined Process
    - GP 3.2.2 – Perform Defect Reviews
    - GP 3.2.3 – Use Well-Defined Data
  - ***Common Feature 3.3 – Coordinate Practices***
    - GP 3.3.1 – Perform Intra-Group Coordination
    - GP 3.3.2 – Perform Inter-Group Coordination
    - GP 3.3.3 – Perform External Coordination
- **Capability Level 4 - Quantitatively Controlled**
  - ***Common Feature 4.1 – Establishing Measurable Quality Goals***
    - GP 4.1.1 – Establish Quality Goals
  - ***Common Feature 4.2 – Objectively Managing Performance***
    - GP 4.2.1 – Determine Process Capability
    - GP 4.2.2 – Use Process Capability
- **Capability Level 5 - Continuously Improving**
  - ***Common Feature 5.1 – Improving Organizational Capability***
    - GP 5.1.1 – Establish Process Effectiveness Goals
    - GP 5.1.2 – Continuously Improve the Standard Process
  - ***Common Feature 5.2 – Improving Process Effectiveness***
    - GP 5.2.1 – Perform Causal Analysis

le “GENERIC PRACTICES”



Capability Level 1 - Capability Level Title

Summary Description – An overview of the capability level

Common Features List – A list showing the number and name of each common feature

Common Feature 1.1 - Common Feature Title

Summary Description – An overview of the capability level

Generic Practices List – A list showing the number and name of each generic practice

GP 1.1.1 - Generic Practice Title

Description – An overview of this generic practice

Notes – Any other notes about this generic practice

Relationships – Any relationships with other parts of the model

GP 1.1.2...

Figure 5.1 - Capability Level Format

le “GENERIC PRACTICES”

Capability Level 2 – Planned and Tracked

Summary Description

Performance of the base practices in the process area is planned and tracked. Performance according to specified procedures is verified.

Work products conform to specified standards and requirements.

Measurement is used to track process area performance, thus enabling the organization to manage its activities based on actual performance.

The primary distinction from Level 1, Performed Informally, is that the performance of the process is planned and managed.

Common Features List

This capability level comprises the following common features:

- Common Feature 2.1 – Planning Performance
- Common Feature 2.2 – Disciplined Performance
- Common Feature 2.3 – Verifying Performance
- Common Feature 2.4 – Tracking Performance

LE ”COMMON FEATURES”

GP 2.1.1 – Allocate Resources

Description

Allocate adequate resources (including people) for performing the process area.

Notes

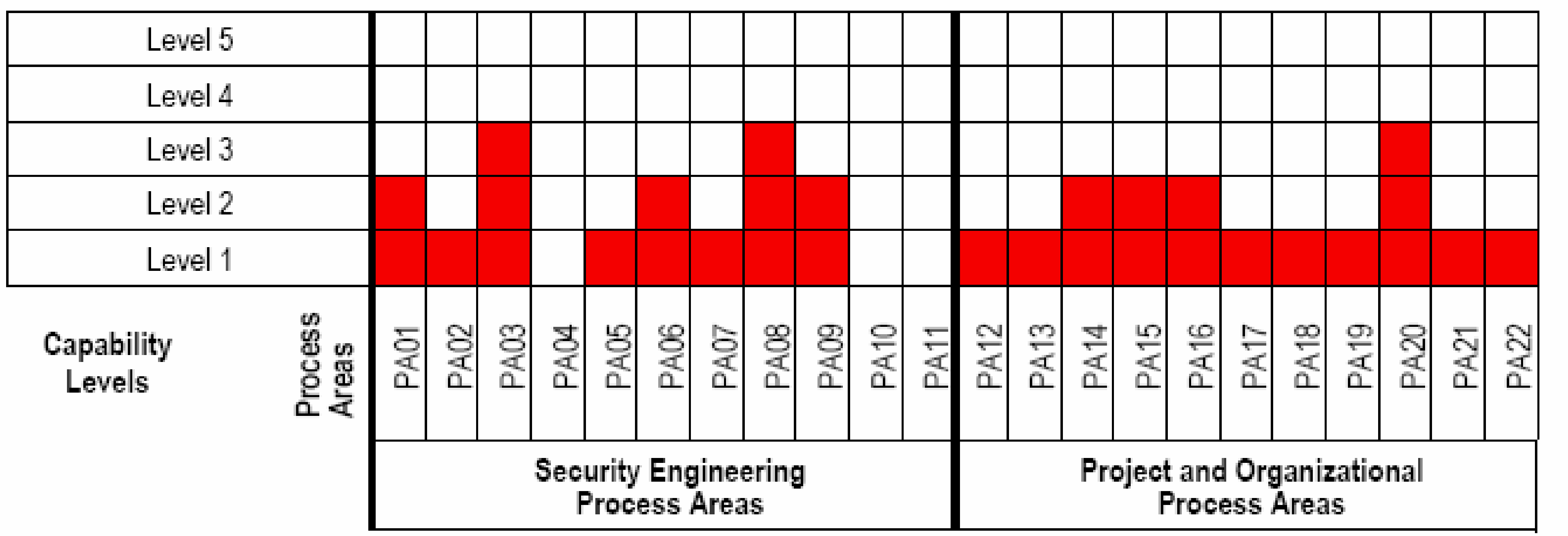
None.

Relationships

Identification of critical resources is done in process area PA16 Plan Technical Effort.

Common Features / Process Areas	PA01 – Administer Security Controls	PA02 – Assess Impact	PA03 – Assess Security Risk	PA04 – Assess Threat	PA05 – Assess Vulnerability	PA06 – Build Assurance Argument	PA07 – Coordinate Security	PA08 – Monitor Security Posture	PA09 – Provide Security Input	PA10 – Specify Security Needs	PA11 – Verify and Validate Security	PA12 – Ensure Quality	PA13 – Manage Configuration	PA14 – Manage Project Risk	PA15 – Monitor and Control Technical Effort	PA16 – Plan Technical Effort	PA17 – Define Org. Systems Eng. Process	PA18 – Improve Org. Systems Eng. Process	PA19 – Manage Product Line Evolution	PA20 – Manage Systems Eng. Support Env.	PA21 – Provide Ongoing Skills and Knldge	PA22 – Coordinate with Suppliers
5.2 Improving Proc. Effectiveness																						
5.1 Improving Org. Capability																						
4.2 Objectively Managing Perf.																						
4.1 Establish Meas. Quality Goals																						
3.3 Coordinate Practices																						
3.2 Perform the Defined Process																						
3.1 Defining a Standard Process																						
2.4 Tracking Performance																						
2.3 Verifying Performance																						
2.2 Disciplined Performance																						
2.1 Planned Performance																						
1.1 Base Practices Are Performed																						
	Security Engineering Process Areas											**Project and Organizational Process Areas**										

La CAPABILITY



Capability Levels / Process Areas	PA01	PA02	PA03	PA04	PA05	PA06	PA07	PA08	PA09	PA10	PA11	PA12	PA13	PA14	PA15	PA16	PA17	PA18	PA19	PA20	PA21	PA22
Level 5																						
Level 4																						
Level 3			🟥					🟥												🟥		
Level 2	🟥		🟥			🟥		🟥	🟥					🟥	🟥	🟥				🟥		
Level 1	🟥	🟥	🟥		🟥	🟥	🟥	🟥	🟥			🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥
	Security Engineering Process Areas											Project and Organizational Process Areas										

Figure 4.2 - Determining Process Capability

riferimenti

- www.issea.org
- www.sse-cmm.org