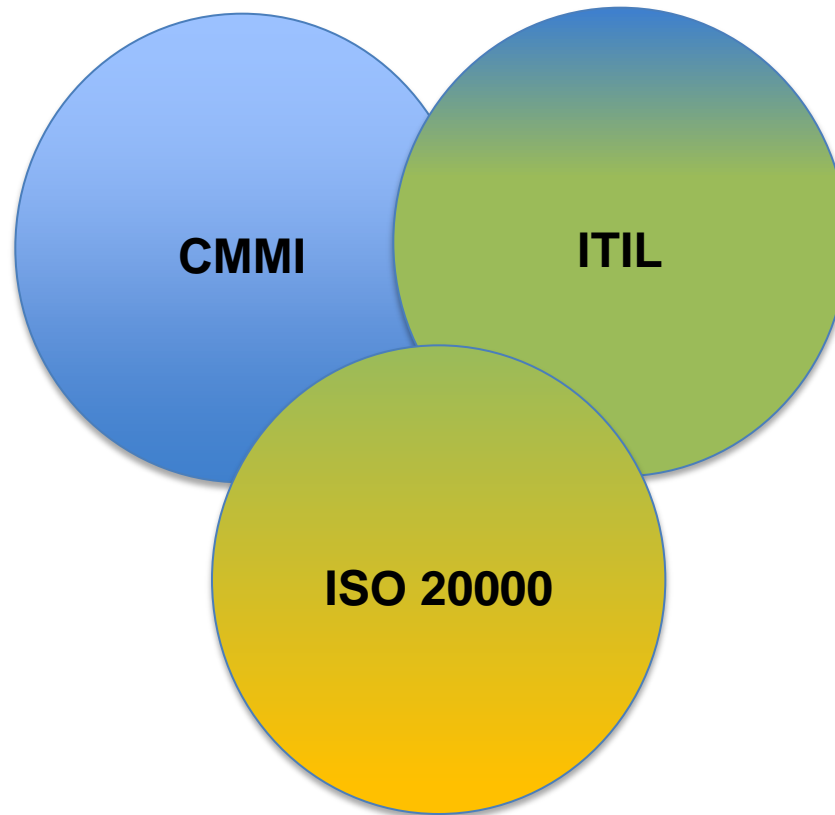


CMMI & Security:

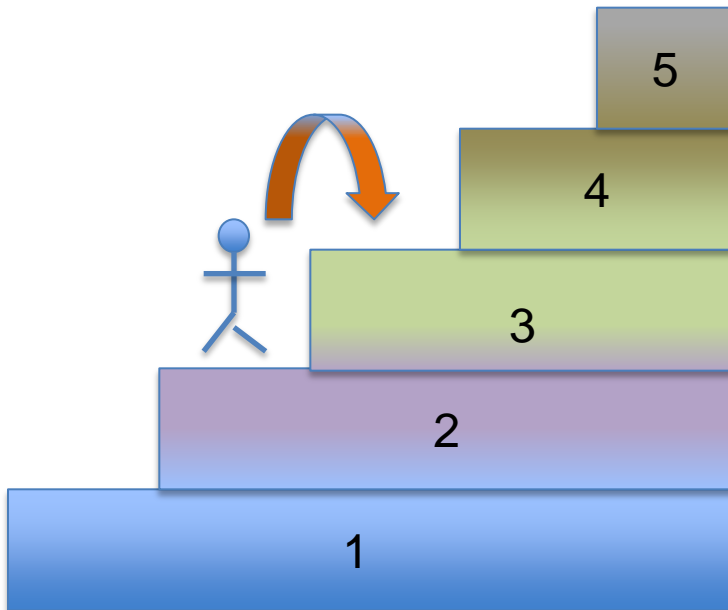
Agenda

- How CMMI fits with Other models
 - ISO 20K & ITIL
 - ISO 27001
 - RMM
 - The complementary fit
- Adding Security to CMMI
 - GPs
 - Pseudo PA
 - Benefits
- Taking it Forward

Improving Service Management



An Improvement Progression



A Road Map of Change



Ensures Stable
Foundations
- The Generic Practices



ISO 20000 & CMMI Mapping

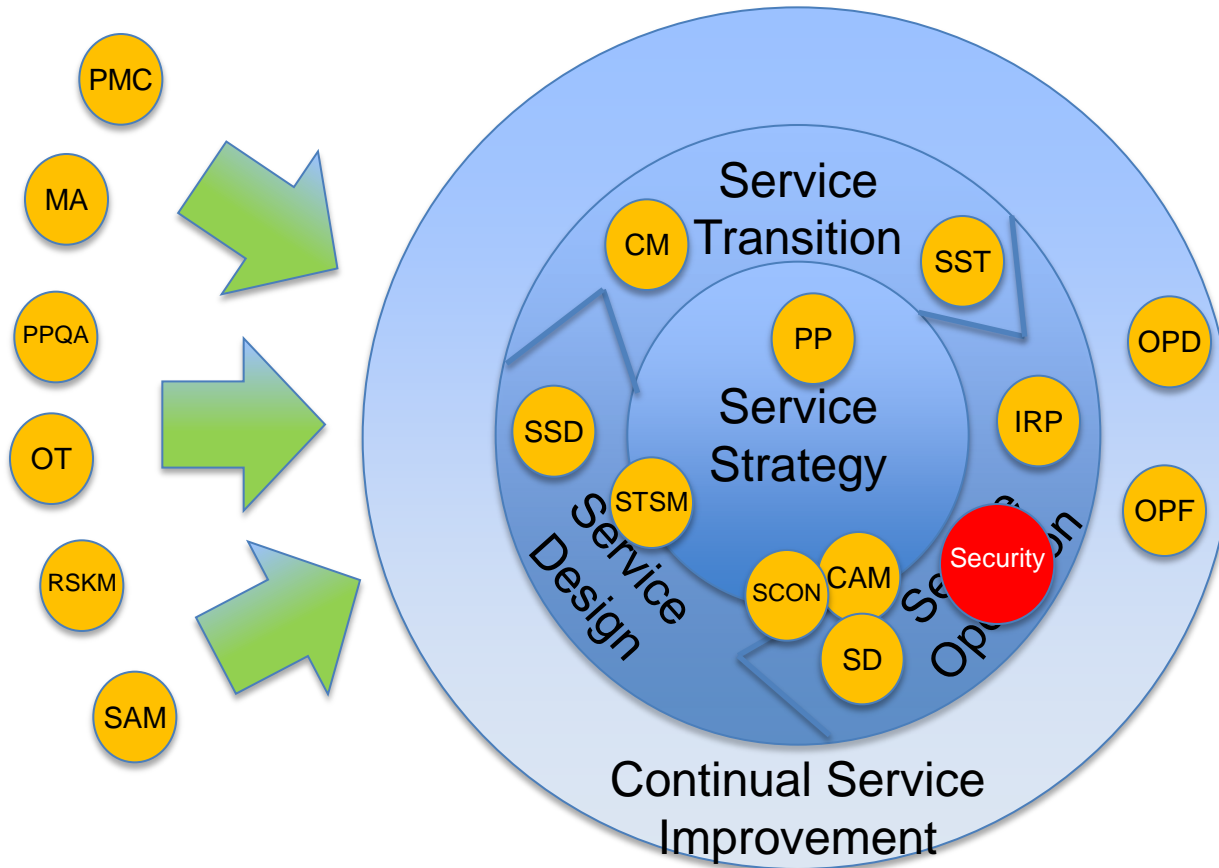
Clause Ref	ISO 20000 Clause Title	CMMI Process Areas / Practices	Coverage
1	Scope		
2	Terms and Definitions		
3	Requirement for a Management System		
3.1	Management Responsibility	REQM, RSKM, PP, PMC (GP2.1, GP2.2, GP2.3, GP2.4)	
3.2	Documentation Requirements	SD, (GP2.1, GP2.2)	
3.3	Competence, Awareness and Training	PP, OT (GP2.5)	
4	Planning and Implementing Service Management		
4.1	Plan Service Management (Plan)	PP, SD, REQM, SSD, SST, PPQA (GP2.2, GP2.3, GP2.4, GP2.9)	
4.2	Implement Service Management and Provide the Services (Do)	PP, PMC, SD	
4.3	Monitoring, Measuring and Reviewing (Check)	PMC, MA, SD, PPQA (GP2.8, GP2.10)	
4.4	Continual Improvement (Act)	PPQA, OPF, <i>OPP, QPM</i> (GP2.1, GP3.1, GP3.2)	
5	Planning and Implementing New or Changed Services	STSM, SSD, SST, REQM, PP, OT (GP2.2, GP2.3, GP2.4, GP2.8)	
6	Service Delivery Processes		
6.1	Service Level Management	SD, (GP2.6, GP2.8)	
6.2	Service Reporting	PMC, MA	
6.3	Service Continuity and Availability Management	SCON, CAM, CM	
6.4	Budgeting and Accounting for IT Services	PP	
6.5	Capacity Management	CAM	
6.6	Information Security Management	?	
7	Relationship Processes		
7.1	General		
7.2	Business Relationship Management	SD, REQM, STSM	
7.3	Supplier Management	SAM	
8	Resolution Processes		
8.1	Background		
8.2	Incident Management	IRP	
8.3	Problem Management	IRP	
9	Control Processes	CM	
9.1	Configuration Management		
9.2	Change Management	SST, CM	
10	Release Process		
10.1	Release Management Process	SST, CM	

Implications

- The fit between CMMI and ISO 20000 is good
- There is potentially more detail in CMMI
 - *What makes a good service management system?*
- **Gap = Security**

Good Fit	
Not Applicable	
Poor or No Fit	

ITIL V3 & CMMI-SVC



CMMI & ITIL

- Good fit
- ITIL Provides “How to”
- CMMI provides Improvement Path

The Need

- Security is already out there
 - ITIL
 - ISO 20000
- Both models are highly compatible with CMMI-SVC
 - ISO 20K
 - Defines the “minimum”
 - What do you need for good Service Management
 - ITIL
 - Lots of “How To” information
 - CMMI-SVC
 - Provides an “improvement trajectory”
 - But it misses the security component

Why Should We Fill the Gap?

- Completeness of Improvement Journey
 - Organisations have business problems to solve that cross model boundaries
 - Framing these issues in a common language helps
- Appraisal/Audit Need
 - Organisations with multiple accreditations are faced with frequent internal audit/appraisal issues
 - One common framework – cuts appraisal/audit costs & minimises disruption to busy front line workers
- Model Completeness
 - Security issues are not “additional” to service delivery
 - They are integral to it

How To Fill The Gap?

- RMM?
 - Lots of great material
 - High specification of how to solve security questions
 - Probably interpreted in some people’s minds as “An Extra Model to adopt!!”
- Services PA
 - Needs Steering Group approval
 - Requires long development period
- CMMI-SVC “Bolt On” Material
 - Quick
 - Seed for further development
 - Small scale addition to existing model

Developing a “Bolt on” for CMMI



- Requirements
 - Needs to work with other CMMI process areas
 - Needs to have fit CMMI architecture
 - Required Components
 - Expected Components
 - Informative Material ?
 - Generic Practices
 - Specific Material

ISO27001 – GP Relationships

Clause Ref	Clause Title	Generic Practice Relationships
4.3	Documentation Requirements	
4.3.1	General	GP2.1, GP2.2
4.3.2	Control of Documents	GP2.6
4.3.3	Control of Records	GP2.6
5	Management Responsibility	
5.1	Management Commitment	GP2.1, GP2.4
5.2	Resource Management	GP2.3
5.2.1	Provision of Resources	GP2.3
5.2.2	Training , Awareness and Competence	GP2.5
6	Internal ISMS Audits	GP2.9
7	Management Review of the ISMS	
7.1	General	GP2.10
7.2	Review Input	GP2.8, GP2.9, GP2.10
7.3	Review Output	GP3.1, GP3.2
8	ISMS Improvement	
8.1	Continual Improvement	GP3.1, GP3.2
8.2	Corrective Action	GP2.9, GP3.1, GP3.2
8.3	Preventive Action	GP2.9, GP3.1, GP3.2

CMMI GP's	Cover
2.1	✓
2.2	✓
2.3	✓
2.4	✓
2.5	✓
2.6	✓
2.7	✗
2.8	✓
2.9	✓
2.10	✓
3.1	✓
3.2	✓

GP Relationship - Conclusions



- ISO 27001 clauses are short statements of requirements
 - There is not much detail
 - No “informative material” – Example work products, etc.
- ISO 27001 – Is less explicit on Stakeholder Management
- Using CMMI GPs would:
 - Further help embed good practice
 - Build upon existing material

Specific Material

- In CMMI the specific goals and practices express what is unique or “makes a difference” about a process area
 - These are the essential ingredients for improving
- Specific Goals
 - What are we trying to achieve?
- Specific Practices
 - What should we do?
- ISO 27001 – Provided a suitable starting place

- Clause 4.2.1 - Establish the Information Security Management System
 - Scope the security system
 - Define an approach to identifying and evaluating security threats
 - Define how to deal with them
 - Obtain management approval for the plans and mechanisms defined

ISO 27001 – Put the ISMS in Place



- Clause 4.2.2 - Implement and Operate the Information Security Management System
 - Instigate a plan to operate the security system
 - Manage the level of threat.
- Clause 4.2.3 - Monitor and Review the ISMS
 - Use ISMS mechanisms to monitor threats
 - Take action to address threats
- Clause 4.2.4 - Maintain and Improve the ISMS
 - Measuring and monitor the system
 - Implement corrections or improvements

Pseudo PA – Basic Structure



- Examination of ISO 27001 provided a nice suggestion of initial content
 - Establish and Maintain a Security Management System
 - Use the Agreed Security Management System to Provide required security
- Under these two strands we can construct statements that look and feel like Practice Statements
 - Ideal for Appraisal Purposes
 - Very valuable for improvement teams constructing an improvement plan
 - One language style, one plan, potentially multiple models engaged

Pseudo PA: Security Management (SM)

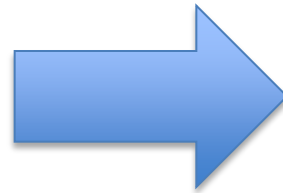


- ESG1 – Establish a Security Management System
 - ESP1.1 Establish Security Objectives
 - ESP1.2 Establish an Approach to Threat Assessment
 - ESP1.3 Identify Security Threats
 - ESP1.4 Evaluate and Prioritize Security Threats
 - ESP1.5 Establish a Security Management Plan
 - ESP1.6 Obtain Commitment to the Security Management Plan

- ESG2 – Provide Security
 - ESP2.1 Operate the Security Management System
 - ESP2.2 Monitor the Security Management System

Framework For Building Upon

Basic Pseudo
PA
Architecture



Ability to
Appraise

But

CMMI is used for more than appraisals

Process Improvement

We need more detail!!

Informative Material

- Informative Material provides:
 - Subpractices
 - Notes
 - Examples
 - Elaborations
 - Example Work Products
 - Etc.
- All these help the implementation of good practice

- **ESP1.2 Establish an Approach to Threat Assessment**

Establish and maintain an approach to assessing vulnerabilities and threats to essential assets.

- *Subpractices*

1. Select methods for assessing security threats
2. Define criteria for evaluating and quantifying security threats.
3. Describe responsibility and resources for evaluating vulnerabilities and threats.

Next Moves

- Pseudo PA has been tested on a number of appraisals
- Challenge to develop more “PA” like substructure
 - Practices
 - Subpractices
 - Example Workproducts
 - GP Elaborations
- We have made a start – but now would like to engage a wider audience to take the discussion forward

Community Feedback/Input

- Should this work be taken further?
- Is the scope useful for improvement?
- What could be done next to make it more credible?
- We would like your comments.
 - cmmi-comments@sei.cmu.edu.

Summary

- ISO20000, ITIL & CMMI all work very well together
- CMMI misses one component in common with the other approaches
 - Security
- ISO 27001 provided a starting point for developing a Pseudo Process Area – SM
- We are seeking community input to develop this pseudo process area further