



Not another audit!
How solving the multi model
problem can save you money

Kieran Doyle
T: +441748 821824
M: +447971222160
E: kieran.doyle@lamri.com

Agenda






- The Challenge
- An Example Approach
- Experiences & Lessons Learned



THE CHALLENGE

The Specific Customer Challenge



- Baseline the current process capability of our organisation 
- Run a CMMI Services Appraisal 
- We are also using ITIL/ISO 20000
- Include Security in the scope of the Appraisal
- One appraisal event to: 
 - Keep Down Costs
 - Reduce schedule impacts
 - Avoid Duplication – Its always the same people involved!

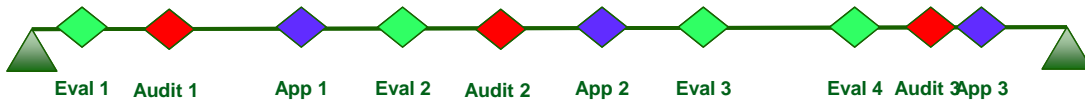
Can we possibly run one appraisal and hit multiple models?

The Wider Business Problem



Company X – Business Process Improvement

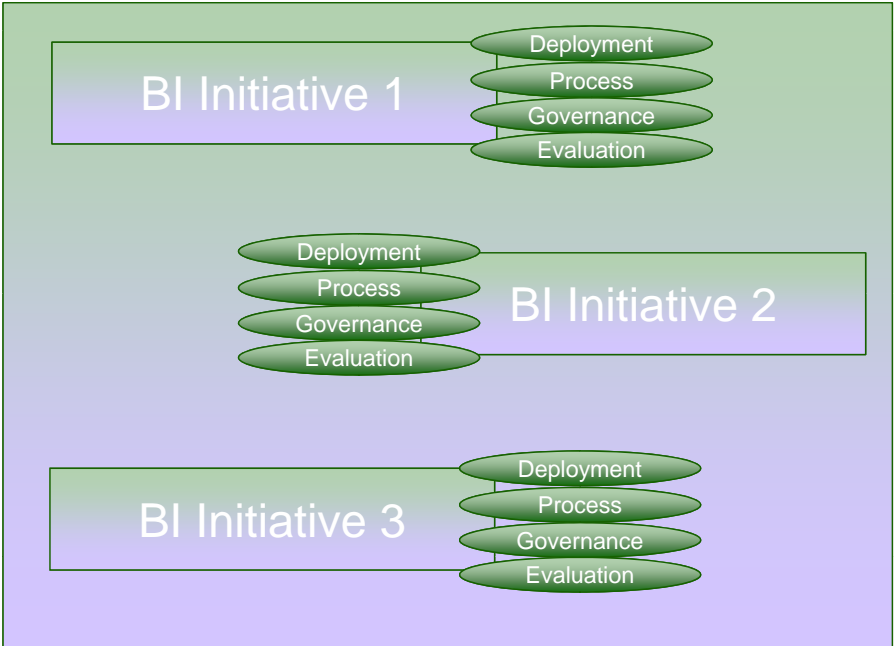
Additional Customer Requirements (E.g. ISO 15 505, SPICE, T9000, etc.)



The Wider Business Problem



Company X – Business Process Improvement





AN EXAMPLE APPROACH: WHAT I DID

Background



- Many Organisations looking at CMMI for Services have already looked at or used ISO 20000.
- ISO 20000 is a standard for the requirements of an IT service management system. It can complement CMMI for services, or vice versa.
- ISO 20000 also works very well with ITIL
- But ISO 20000 does not provide a way to measure improvement ...
- CMMI-SVC also covers many of the areas that ISO 20K

Mapping ISO 20000 Clauses to CMMI-SVC



ISO 20000 Clauses		CMMI-ISO20000 Coverage
Index	Title	
3	Requirements for a Management System	
3.1	Management Responsibility	■
3.2	Documentation Requirements	■
3.3	Competence, awareness and training	■
4	Planning & Implementing Service Management	
4.1	Plan Service Management	■
4.2	Implement Service Management and provide services	■
4.3	Monitoring, measuring and reviewing	■
4.4	Continual Improvement	■
5	Planning and Implementing new or changed services	■
6	Service Delivery Process	
6.1	Service Level Management	■
6.2	Service Reporting	■
6.3	Service Continuity & Availability Management	■
6.4	Budgeting and Accounting for IT Services	■
6.5	Capacity Management	■
6.6	Information Security Management	■
7	Relationship Processes	
7.2	Business Relationship Management	■
7.3	Supplier Management	■
8	Resolution Processes	
8.2	Incident Management	■
8.3	Problem Management	■
9	Control Processes	
9.1	Configuration Management	■
9.2	Change Management	■
10	Release Process	
10.1	Release Management Process	■

CMMI-SVC provides almost complete coverage of ISO 20000 clauses

Situation



- As part of “baselining” the processes we want to run an appraisal event
- The overlap between CMMI-SVC and ISO 20000 is good
- So **One Event** could realistically give us all the improvement information we need, except

Security

- How therefore can we keep the one appraisal event and still cover this issue?

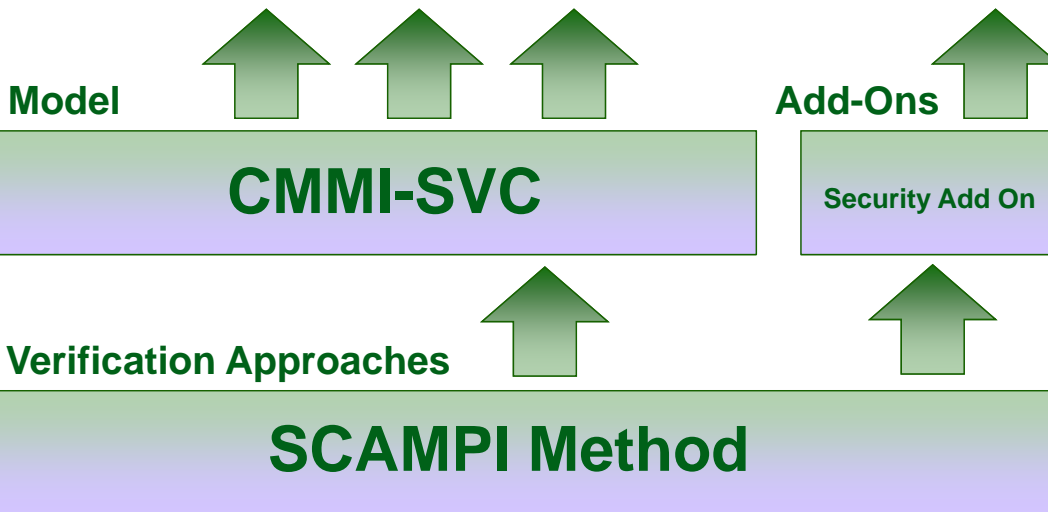


“AUGMENTING” CMMI-SVC

Approach



Process Requirements



The Need for A Reference Framework



- The power of SCAMPI Appraisals lies in:
 - Collaborative Approach
 - Internal & External team participation
 - Focus on business objectives – not just conformance
 - Objective Evidence – particularly prior collection in verification mode
 - Rules of Characterisation
- All these need a Reference Framework to hang off
- So to include Information Security in our CMMI-SVC appraisal we need something similar to focus the appraisal activities.

What could we use as an Information Security reference framework?

ISO 27001:2005 – In Outline



- Defines the requirements for an Information Security Management System (ISMS)
- The most pertinent sections are as follows:
 - Clause 4 – Information Security Management System (ISMS)
 - 4.1 General Requirements
 - 4.2.1 Establish the ISMS
 - 4.2.2 Implement and Operate the ISMS
 - 4.2.3 Monitor and Review the ISMS
 - 4.2.4 Maintain and Improve the ISMS
 - 4.3 Documentation Requirements
 - Clause 5 Management Responsibility
 - Clause 6 Internal ISMS Audits
 - Clause 7 Management Review of the ISMS
 - Clause 8 ISMS Improvement
 - 8.1 Continual Improvement
 - 8.2 Corrective Action
 - 8.3 Preventive Action
 - Annex A - Control Objectives and Controls

CMMI Generic Practices and ISO 27001



- Examining the ISO 27001 clauses we find that there are overlaps between some of the clauses and certain CMMI Generic Practices (GP)

- Clause 4.2.2 Implement & Operate the ISMS Also covers planning its implementation (GP2.2)
- Clause 4.3 Documentation Requirements Aspects of policy (GP2.1) & configuration control (GP2.6)
- Clause 5 Management Responsibility More aspects of policy (GP2.1) Provision of resources (GP2.3) Assigning Responsibility (GP2.4) Training (GP2.5)
- Clause 6 Internal ISMS Audits Conformance to the standard (GP2.9)
- Clause 7 Management Review of ISMS Very akin to GP2.10, but also may require some aspects of GP2.8.
- Clause 8 ISMS Improvement Ensures implementation of improvements from GP2.9 like behaviour. But also has some flavour of GP3.2

This indicates



- We could use the CMMI-SVC **GPs** to appraise some of the requirements for a IT Security Management System.
- We could use the typical Practice Implementation Indicator (PII) approach to collect and analyse data.
- Missing GPs – GP2.7 ?
 - Reading between the lines of some other clauses this is also there.
 - But not as explicitly.
 - Looking for this in a way that is compatible with the CMMI would however be advantageous to the organisation.

But what about ISMS specific material?

Specific ISMS Requirements



- Exploring ISO 27001 – Clause 4.2 Establishing and Managing the ISMS poses some useful material.
- The four sub-clauses summarise what is required for an effective ISMS
 - 4.2.1 – Establish the ISMS
 - 4.2.2 – Implement and Operate the ISMS
 - 4.2.3 – Monitor and Review the ISMS
 - 4.2.4 – Maintain and Improve the ISMS

4.2.1 – Establish the ISMS (Part 1)



- Define the scope of the security system
- Define ISMS policies – based on the nature, and context of the organisation.
- Define a risk assessment approach
 - What methodology is used for assessing security risks?
 - What criteria do we use for identifying the acceptable level of security risks?
- Identify the Security Risks
 - What assets may be threatened? How?
 - What vulnerabilities exist?
- Analyse and Evaluate the Security Risks
 - Probability & impact, etc.

4.2.1 – Establish the ISMS (Part 2)



- Evaluate options for treatment of risks
 - What sort of controls could/should we apply?
 - Annex A provides a comprehensive checklist identifying a range of control objectives and potential control mechanisms
 - E.g.
 - Objective – To ensure that information receives an appropriate level of protection
 - Control - Classification guidelines, etc.
- Select control objectives and controls for treating risks
- Obtain management approval of any remaining threats
- Obtain management authorisation for the ISMS.

4.2.2 – Implement and Operate the ISMS



- This clause deals with planning how we will actually put the ISMS into action.
- It covers:
 - Identifying management action, resources, responsibilities and priorities
 - How to implement the selected threat control mechanisms
 - Defining how we measure the effectiveness of the selected control mechanisms
 - How will we manage the operation of ISMS and its resources?
- But it also deals with putting this plan into action.

4.2.3 – Monitor and Review the ISMS



- This clause deals with checking that the ISMS is in place and operates effectively
 - i.e. it captures or prevents security threats
- It requires:
 - Monitoring attempted and successful security breaches
 - What do we learn from them?
 - Are the security activities being done according to plan
 - Conducting ISMS audits
 - Identifying necessary actions and updates to security plans (I.e. corrective actions)
 - Re-visiting the risk/threat assessments as required

4.2.4 – Maintain and Improve the ISMS



- This clause deals with:
 - Implementing corrective actions
 - Implementing improvements to the ISMS
 - Communicating actions and improvements
 - Making sure that the improvements are done and that they are successful (achieve their objective)

Information Security Components of a PII



- From a point of view of using a SCAMPI to examine Information Security, these requirements of an ISMS could be **codified** as practices.
- Implementation Data could then be collected against each security “practice” in the same vein as for CMMI Process Areas
- The Security appraisal could be run in parallel with appraisal of the CMMI Process Areas

Security “Practices”



- Two main “blocks” of practices were identified:
 - Establishing and Maintaining the Information Security System
 - Mainly guided by the information in Clause 4.2.1 and involved:
 1. Identify the scope and objectives of the ISMS
 2. Specify the approach to identifying and assessing ISMS threats
 3. Identify, analyse and evaluate ISMS threats
 4. Obtain commitment for the ISMS from all relevant stakeholders
 - Provide Information Security using the agreed ISMS
 - These are drawn mainly from the other three clauses
 1. Implement and operate the agreed ISMS
 2. Monitor and review the ISMS
 3. Maintain and improve the ISMS

Security PIID – An Extract



Goal ID	Practice ID	Evidence Comments	Document Title / Interview Session	Direct	Indirect	Affirmation	Service 1	Service 2	Service 3	Service 4	Service 5	Service 6	Review Comments
A		<i>An information security system is established and maintained.</i>											
	1	Identify the scope and objectives for the information security system.											
	2	Identify the approach to identifying and assessing information security threats.											
	3	Identify, analyse and evaluate information security threats.											
	4	Select options for treating information security threats relevant to the project's threat control objectives.											
	5	Obtain commitment to the project's information security system from all relevant stakeholders.											
B		<i>Information security is provided according to the agreed objectives.</i>											
	1	Implement and operate the agreed information security system.											
	2	Monitor and review the information security system											
	3	Maintain and improve the information security system.											
GG2		<i>Institutionalize a Managed Process</i>											
	GP2.1	Establish and maintain an organizational policy for planning and performing the process.											



EXPERIENCES & LESSONS LEARNED

Experiences



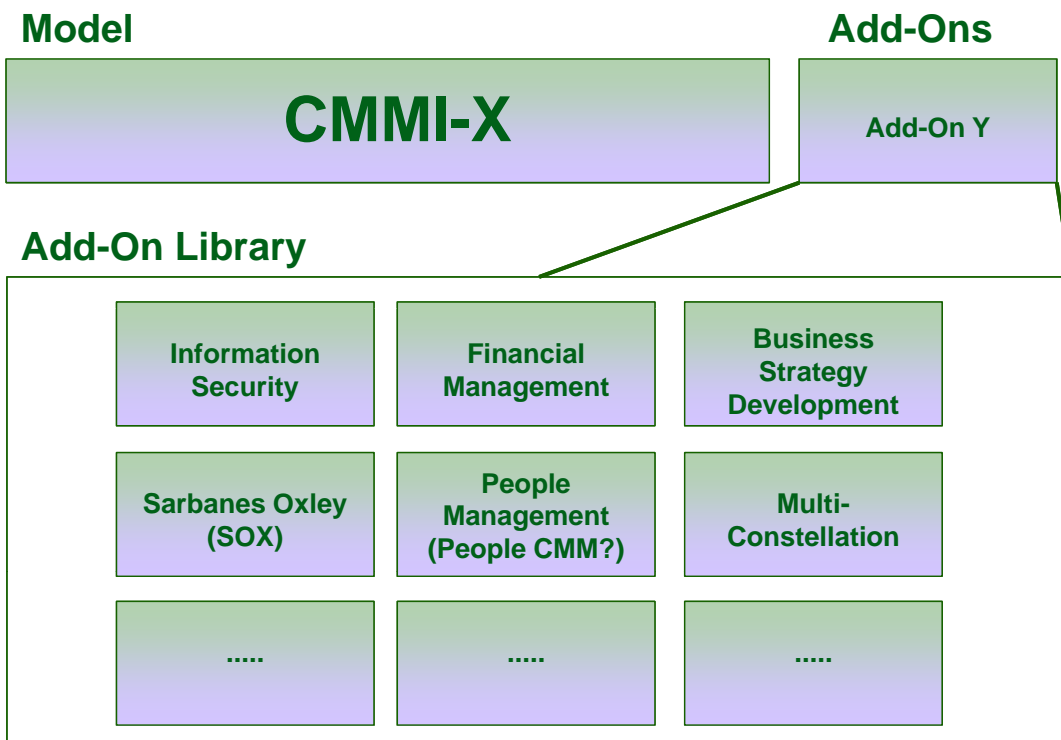
- The approach was trialled in a CMMI-SVC SCAMPI Class B appraisal.
 - All ML2 PAs + IRP, SCON, SST, OPF + Information Security
 - Data was collected in advance for all PAs + Information Security
 - Normal SCAMPI approach was used
 - Characterisation (RAG) was applied to Security “Practices”
 - In the Findings Presentation, security results were presented separately as non-CMMI findings
- Result
 - Organisation obtained improvement data pertinent to its ISMS
 - In similar vein to improvement data for CMMI PA’s
 - Integrated improvement effort that covers all aspects of process important to the organisation

Lessons Learned

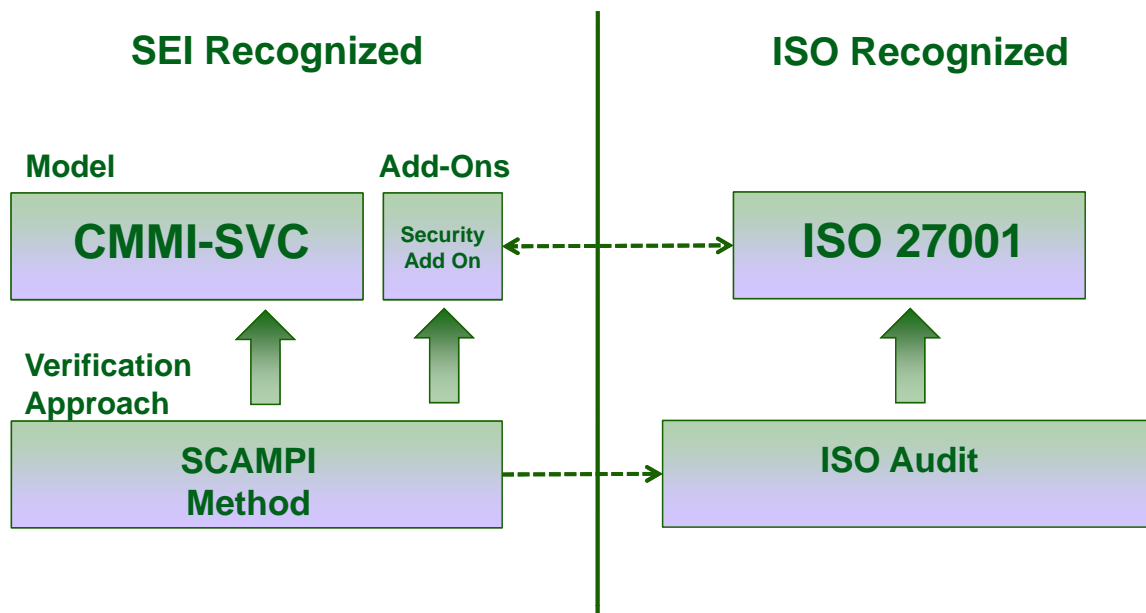


- Granularity of Security “Practices” may currently be too high.
 - The current PIID statements may miss out on some important aspects
 - E.g. PIID statement B2 & ISO clause 4.2.3 – Monitor and review the ISMS
 - There are various aspects of what ought to be monitored.
 - Perhaps a single PIID statement might not cover all appropriate aspects.
 - Splitting the practice may be needed.

Going Forward?



Certification?

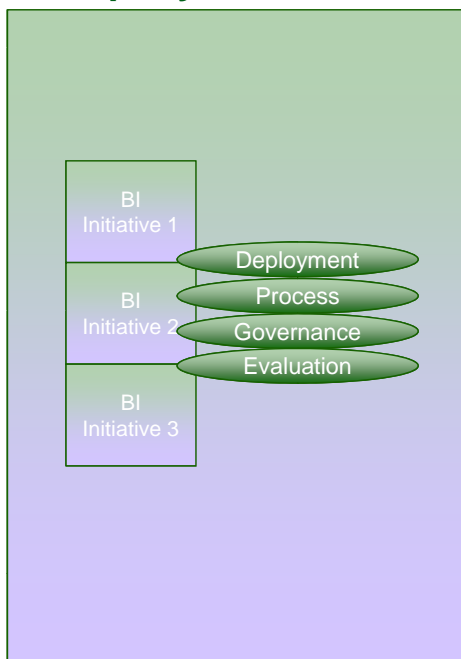


Perhaps by “dint of history” the SCAMPI Method may be accepted as a means of indicating likely certification.

The real opportunity



Company X



- Opportunity to rationalise deployment, process, governance and evaluation – saving resources and reducing “process user” confusion
- Increases business focus
- Enables focusing of improvement skill sets to ensure you get the best return

In conclusion - 1



- Multiple Models introduce multiple process requirements
- They may all complement each other (e.g. CMMI-SVC, ITIL & ISO20000)
- Working out where you are with all of them can be expensive and time consuming
- We looked at one specific example
- Using ISO 27001 as a basis we have constructed a means for including Security in SCAMPI appraisals
- This is **NOT** a CMMI-SVC Process Area
- But it does allow an important aspect of managing IT Services to be included in the process improvement journey using CMMI & SCAMPI.

In conclusion - 2



- We could extend this approach into other areas
- Thinking about the models in an integrated manner, provides the opportunity to streamline the:
 - Process Deployment
 - Process Development
 - Process Governance
 - Process Evaluation
- It focuses the Business Improvement Initiative(s) on Getting Things Done



Q&A



