

## **SSE-CMM LEVEL 4 -- A CASE STUDY**

**Pam Feldpusch and Barry Stoll (Eagle Alliance)**  
pfeldpus@csc.com / bstoll@csc.com

In 2001, Eagle Alliance was presented with a rare opportunity; a new organization, with a group specifically assigned to the task of systems security, and a management committed to “doing it right” from the start.

One requirement of the Eagle Alliance contract was to attain Level 3 of the Systems Security Engineering Capability Maturity Model (SSE-CMM). With that requirement as a guide, the new Information Systems Security Group (ISSG) made the decision to base its structure and processes on the framework and principles of SSE-CMM.

The SSE-CMM is a standard metric for security engineering practices describing the essential characteristics required for the success of an organization's security engineering.

**SSE-CMM**  
SYSTEMS SECURITY ENGINEERING - CAPABILITY MATURITY MODEL

With the implementation of these characteristics, an organization assures the security of their technology systems.

The model requires established processes based on the best existing practices of the security engineering community, and measures compliance by increasing levels of maturity from 1 to 5. The maturity of each level is simply represented as:

- Level 1 – Performed Informally
- Level 2 – Planned and Tracked
- Level 3 – Well Defined
- Level 4 – Quantitatively Controlled
- Level 5 – Continuously Improving

Early on, two members of the ISSG attended SSE-CMM training sponsored by the International System Security Engineering Association (ISSEA). This training concluded with an exam, and issuance of a certificate for Entry-Level SSE-CMM Appraiser.



The first goal for the two appraisers (hereafter referred to as the “SSE-CMM Team”) was to conduct a SSE-CMM self-appraisal. The SSE-CMM Appraisal Methodology (SSAM) recognizes the validity of the self-appraisal approach.

With the SSAM as a guide, the SSE-CMM Team proceeded to select Process Areas (PAs) relative to the work assigned to the ISSG. The 22 possible PAs are grouped into 11 for Security and 11 for Project & Organizational. The ISSG selected a subset of 13 PAs representing all 11 from Security and 2 from Project & Organizational that specifically deal with Security. The SSE-CMM Team determined that the remaining 9 PAs from Project & Organizational were best addressed in the ISO 9001:2000 efforts. The ISSG Management approved these PAs for the self-appraisal:

- PA01 – Administer Security Controls: *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.*

**SSE-CMM LEVEL 4 -- A CASE STUDY**  
**Pam Feldpusch and Barry Stoll (Eagle Alliance)**  
pfeldpus@csc.com / bstoll@csc.com

- PA02 – Assess Impact: *Identify impacts that are of concern with respect to the system and to assess the likelihood of the impacts occurring.*
- PA03 – Assess Security Risk: *Identify the security risks involved with relying on a system in a defined environment.*
- PA04 – Assess Threat: *Identify security threats and their properties and characteristics.*
- PA05 – Assess Vulnerability: *Identify and characterize system security vulnerabilities.*
- PA06 – Build Assurance Argument: *Clearly convey that the customer's security needs are met.*
- PA07 – Coordinate Security: *Ensure that all parties are aware of and involved with security engineering activities.*
- PA08 – Monitor Security Posture: *Ensure that all breaches of, attempted breaches of, or mistakes that could potentially lead to a breach of security, are identified and reported.*
- PA09 – Provide Security Input: *Provide system architects, designers, implementers, or users with the security information they need.*
- PA10 – Specify Security Needs: *Explicitly identify the needs related to security for the system.*
- PA11 – Verify and Validate Security: *Ensure that solutions are verified and validated with respect to security.*
- PA17 – Define Organization's Systems (Security) Engineering Process: *Create and Manage the organization's standard security engineering processes, which can subsequently be tailored by a project to form the unique processes that it will follow in developing its systems or products.*
- PA18 – Improve Organization's Systems (Security) Engineering Process: *Gain competitive advantage by continuously improving the effectiveness and efficiency of the security engineering processes used by the organization.*

These are the PAs identified as being addressed by the Eagle Alliance ISO 9001:2000 efforts, and therefore are not addressed by this SSE-CMM self-appraisal:

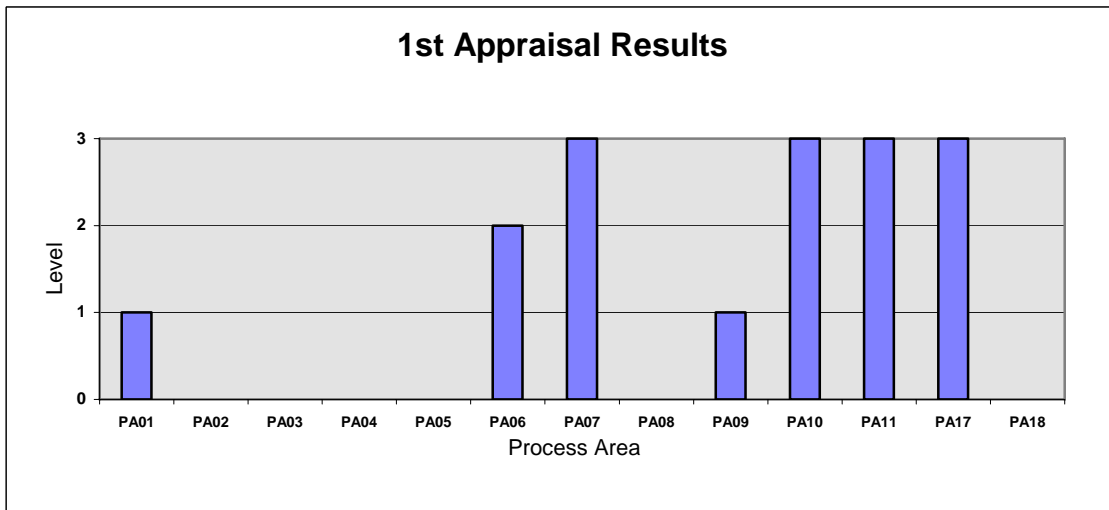
- PA12 – Ensure Quality
- PA13 – Manage Configuration
- PA14 – Manage Project Risk
- PA15 – Monitor and Control Technical Effort
- PA16 – Plan Technical Effort
- PA17 – Define Organization Systems Engineering Process
- PA18 – Improve Organization Systems Engineering Process
- PA19 – Manage Product Line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

# SSE-CMM LEVEL 4 -- A CASE STUDY

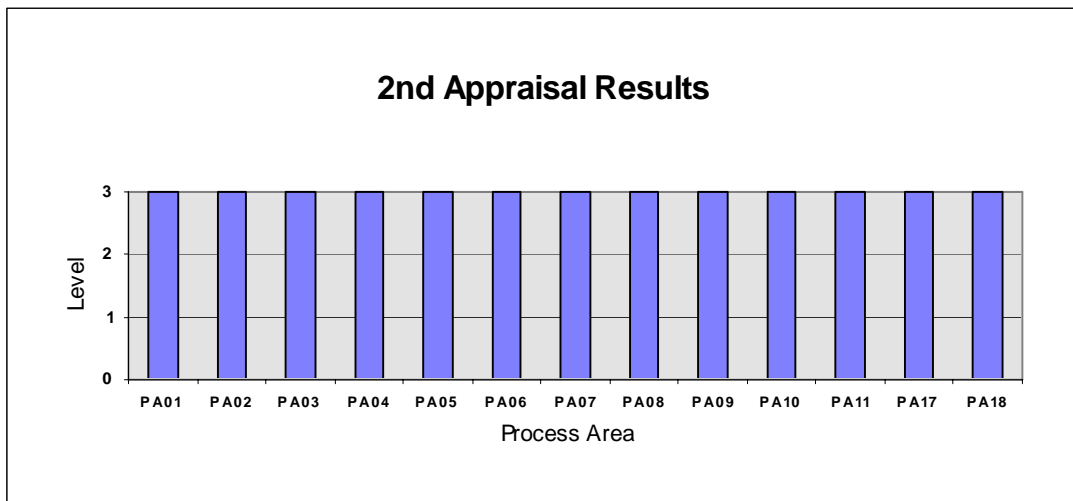
Pam Feldpusch and Barry Stoll (Eagle Alliance)  
pfeldpus@csc.com / bstoll@csc.com

Next, the SSE-CMM Team identified the associated practitioners for the Process Areas, and using the SSAM questionnaires, the initial self-appraisal was conducted. Responses from all questionnaires were tracked in a customized Data Tracking Spreadsheet (DTS) providing a subjective analysis of the data with a resulting calculated maturity level. In addition, all evidence was gathered, stored in a locked file and cataloged in an Evidence Tracking Spreadsheet (ETS) as a record of the self-appraisal.

The burgeoning ISSG anticipated the January 2003 report to reflect “immature” results, and in fact there were areas at each of the maturity levels of 0, 1, 2, and 3.



The ISSG used these results to develop and conduct a comprehensive remediation effort, and allowed time for at least six months of “maturing”, as recommended by the SSAM. A second self-appraisal was conducted, updated responses from all questionnaires were tracked, and changes to evidence were gathered and cataloged. The September 2003 second self-appraisal report indicated that the ISSG was operating at Level 3 in all PAs.





## SSE-CMM LEVEL 4 -- A CASE STUDY

Pam Feldpusch and Barry Stoll (Eagle Alliance)  
pfeldpus@csc.com / bstoll@csc.com

The ISSG management concurred with the SSE-CMM Team that the ISSG responsibilities fall into three primary *Business Functions*:

- **Certification** covering both the certification of systems being built, as well as the tracking and completion of certification training for system and network administrators
- **Implementation** including system security engineering and integration
- **Monitoring** for the 24x7 monitoring of security systems

The SSE-CMM Team realized they could draw upon previous SSE-CMM efforts, as well as Eagle Alliance efforts, for the Quantitative Controls and Quality Goals.

*Quantitative Controls* reflect how well controls over daily activities within each *Business Function* affect the outcome of associated work products. Metrics from such activities were identified in these existing measurements:

- **Service Level Agreements (SLAs)** assigned to the ISSG from the contract between Eagle Alliance and the Client. Each Business Function has at least one SLA.
- **Process Improvement Measures (PIMs)** developed as a result of an Eagle Alliance ISO 9001:2000 Quality Management Council initiative. The ISSG must establish measures beyond SLAs to assess the effectiveness of existing procedures.
- **ISO 9001:2000** internal and external audits. Eagle Alliance is ISO Certified as required by contract, and the results of audits are also measurements of the effectiveness of existing procedures.
- **SSE-CMM Level 3 Self-Appraisals** which will continue to be conducted at least every 18 months. They provide continual feedback on the ISSG's compliance with SSE-CMM requirements.
- **SSE-CMM Level 4 Self-Appraisals** which will be conducted going forward. They will provide objective feedback as to whether the inputs and outputs of the Level 4 tools are valuable.

*Quality Goals* are meant to reflect the bigger picture. They are tied to the business goals of the ISSG, and can be used to manage the *Business Functions*.

- **Award Factors** are generated from periodic customer award documents required by the contract.
- **Service Credits** are numerical penalties assigned to the missing of any SLAs, with each SLA having a unique penalty structure.
- **Client Satisfaction Surveys** are conducted by the Eagle Alliance Customer Relations Office, consisting of both face-to-face interviews as well as on-line surveys.

**SSE-CMM LEVEL 4 -- A CASE STUDY**  
**Pam Feldpusch and Barry Stoll (Eagle Alliance)**  
pfeldpus@csc.com / bstoll@csc.com

Keeping with the initial focus, the SSE-CMM Team could begin to see that the metrics of the *Quantitative Controls* (e.g. SLAs, audits) should influence or impact the measurements of the *Quality Goals* (e.g. Client Awards and Surveys). Now the factors needed to be tracked and each one relatively and objectively represented.

The SSE\_CMM Team devised a numeric structure to represent each of the *Quantitative Control* and *Quality Goal* metrics, normalized to a common scale. This valuation process resulted in a scale that ranged from 60 to 100, and each metric was analyzed so it could be represented by a number within that range. For example, an audit resulting in no Corrective Actions would result in a score of 100. If the audit reported 1 Corrective Action it would have resulted in a score of 90, and if the audit had reported 5 Corrective Actions, the resulting score would have been 60 – the worse the resulting score could ever be. (This was a refinement the SSE-CMM Team made over time as they realized a scale of 0 to 100 yielded results that were too wildly fluctuating to be able to make reasonable sense.)

Again, as in Level 3, a spreadsheet tool was developed to track all of the metrics. In addition, the spreadsheet data was linked to several bar charts for additional analysis. Each factor for each *Business Function* was listed, and the spreadsheet allowed for monthly postings. Where a factor was not applicable, an “X” was posted and it did not factor in spreadsheet calculations. Each month, each *Business Function*, etc., was averaged. As enough historical data was posted, each 4-month period was averaged. Because minor fluctuations are sometimes introduced into the data (which may not indicate a true change, but rather a one-time anomaly), the 4-month averages give a more realistic view of a complex system. The SSE-CMM Team optimistically anticipated the spreadsheet data would indicate a consistent relationship emerging between *Qualitative Controls* and *Quality Goals*, confirming they were measuring the correct metrics; by controlling *Qualitative Controls* the ISSG could control its *Quality Goals*. Over a period of one year, that relationship clearly emerged. The following is a condensed and “sanitized” version of the ISSG Level 4 Tracking Spreadsheet.

**SSE-CMM LEVEL 4 -- A CASE STUDY**  
**Pam Feldpusch and Barry Stoll (Eagle Alliance)**  
 pfeldpus@csc.com / bstoll@csc.com

	Period 1	Feb-05	Mar-05	Apr-05	May-05	Period 2	Jun-05	Jul-05	Aug-05	Sep-05	Period 3
<b>CERTIFICATION</b>											
<b>Quantitative Controls</b>											
SLA 1.1 Certification Requests	100.0	100	100	100	100	100.0	100	100	100	100	100.0
SLA 2.1 Configuration Assessment	100.0	100	80	100	100	95.0	100	100	100	100	100.0
SLA 4.1 ISS Certification (Tier 1)	88.0	100	100	100	97.1	99.3	98.7	98.7	98.7	98.7	98.7
PIM 1 Track Concurrence Delays	100.0	100	100	100	100	100.0	100	100	100	100	100.0
PIM 5 Track Configuration Assessment	X	X	X	X	X	X	X	100	100	100	100.0
ISO 9001 Internal Audit CARs	85.0	80	80	80	80	80.0	80	80	100	100	90.0
ISO 9001 External Audit CARs	80.0	80	80	80	100	85.0	100	100	100	100	100.0
SSE-CMM Level 3 Appraisal	100.0	100	100	100	100	100.0	100	100	100	100	100.0
SSE-CMM Level 4 Appraisal	X	X	X	X	X	X	X	X	X	X	X
<b>Total</b>	<b>86.3</b>	<b>89.8</b>	<b>89.2</b>	<b>92.0</b>	<b>91.2</b>	<b>90.6</b>	<b>92.0</b>	<b>92.9</b>	<b>95.6</b>	<b>95.6</b>	<b>94.2</b>
<b>Quality Goals</b>											
Award Factor	79.0	79	79	79	79	79.0	79	79	79	79	79.0
Achievement / Weakness Ratio	76.3	80	80	80	80	80.0	80	80	80	80	80.0
Service Credits	100.0	100	95	100	100	98.8	100	100	100	100	100.0
Customer Survey Grade (APAR)	78.5	81	81	87	87	84.0	89	89	89	89	89.0
Customer Survey Ratio (CPAR)	78.8	84	84	84	88	85.0	88	88	88	93	89.3
<b>Total</b>	<b>82.5</b>	<b>84.8</b>	<b>83.8</b>	<b>86.0</b>	<b>86.8</b>	<b>85.4</b>	<b>87.2</b>	<b>87.2</b>	<b>87.2</b>	<b>88.2</b>	<b>87.5</b>
<b>IMPLEMENTATION</b>											
<b>Quantitative Controls</b>											
SLA 4.1 ISS Certification	75.2	96.3	96.3	97.3	78.8	92.2	91.2	91.7	95.6	98.5	94.3
PIM 4 Security Product Testing	96.5	97	98	98	98	97.8	98	99	99	99	98.8
ISO 9001 Internal Audit CARs	95.0	100	100	100	60	90.0	60	60	60	60	60.0
ISO 9001 External Audit CARs	80.0	80	80	80	100	85.0	100	100	100	100	100.0
SSE-CMM Level 3 Appraisal	100.0	100	100	100	100	100.0	100	100	100	100	100.0
SSE-CMM Level 4 Appraisal	X	X	X	X	X	X	X	X	X	X	X
<b>Total</b>	<b>87.5</b>	<b>94.7</b>	<b>94.9</b>	<b>95.1</b>	<b>87.4</b>	<b>93.0</b>	<b>89.8</b>	<b>90.1</b>	<b>90.9</b>	<b>91.5</b>	<b>90.6</b>
<b>Quality Goals</b>											
Award Factor	79.0	79	79	79	79	79.0	79	79	79	X	79.0
Achievement / Weakness Ratio	16.8	67	67	67	65	66.5	65	65	65	X	65.0
Service Credits	100.0	100	100	100	100	100.0	100	100	100	100	100.0
Customer Survey Grade (APAR)	78.0	81	82	87	87	84.3	89	89	89	89	89.0
Customer Survey Ratio (CPAR)	77.5	79	79	79	83	80.0	83	83	83	85	83.5
<b>Total</b>	<b>70.3</b>	<b>81.2</b>	<b>81.4</b>	<b>82.4</b>	<b>82.8</b>	<b>82.0</b>	<b>83.2</b>	<b>83.2</b>	<b>83.2</b>	<b>91.3</b>	<b>85.2</b>
<b>MONITORING</b>											
<b>Quantitative Controls</b>											
SLA 5.1 Sec Event Reporting	100.0	99	99.5	99	100	99.4	100	99.6	98.8	100	99.6
SLA 5.2 Sec Incident Resolution	99.5	100	100	99	100	99.8	100	100	100	100	100.0
PIM 2 Security Incident Reporting	100.0	99	98	94	100	97.8	100	99	96	100	98.8
PIM 3 Anti-Virus dat.file Pushout	41.2	39.6	63.3	64	60.8	56.9	64	66.1	64.5	65.6	65.1
ISO 9001 Internal Audit CARs	95.0	100	100	100	100	100.0	80	80	80	80	80.0
ISO 9001 External Audit CARs	80.0	80	80	80	100	85.0	100	100	100	100	100.0
SSE-CMM Level 3 Appraisal	100.0	100	100	100	100	100.0	100	100	100	100	100.0
SSE-CMM Level 4 Appraisal	X	X	X	X	X	X	X	X	X	X	X
<b>Total</b>	<b>87.0</b>	<b>88.2</b>	<b>91.5</b>	<b>90.9</b>	<b>94.4</b>	<b>91.3</b>	<b>92.0</b>	<b>92.1</b>	<b>91.3</b>	<b>92.2</b>	<b>91.9</b>
<b>Quality Goals</b>											
Award Factor	79.0	79	79	79	79	79.0	79	79	79	X	79.0
Achievement / Weakness Ratio	50.0	50	50	50	55	51.3	55	55	55	55	55.0
Service Credits	100.0	100	100	97	100	99.3	100	100	100	100	100.0
Customer Survey Grade (APAR)	78.3	81	81	87	87	84.0	89	89	89	89	89.0
Customer Survey Ratio (CPAR)	77.8	80	80	80	95	83.8	95	95	95	91	94.0
<b>Total</b>	<b>77.0</b>	<b>78.0</b>	<b>78.0</b>	<b>78.6</b>	<b>83.2</b>	<b>79.5</b>	<b>83.6</b>	<b>83.6</b>	<b>83.6</b>	<b>83.8</b>	<b>83.6</b>
<b>QUANTITATIVE CONTROL AVERAGE</b>	<b>86.9</b>	<b>90.9</b>	<b>91.9</b>	<b>92.7</b>	<b>91.0</b>	<b>91.6</b>	<b>91.3</b>	<b>91.7</b>	<b>92.6</b>	<b>93.1</b>	<b>92.2</b>
<b>QUALITY GOAL AVERAGE</b>	<b>76.6</b>	<b>81.3</b>	<b>81.1</b>	<b>82.3</b>	<b>84.3</b>	<b>82.3</b>	<b>84.7</b>	<b>84.7</b>	<b>84.7</b>	<b>87.8</b>	<b>85.4</b>

Following the general guideline from the SSAM, the ISSG knew to track data and wait at least six months for the collection to 'mature'. Over that time, some measurement types were modified, and some metric valuations were adjusted. Immediately, the SSE-CMM Team began to realize the benefits of having all of the ISSG metrics pulled together into one tool. The tool can be used to easily spot a struggling *Quantitative Control*, identify the related procedure, evaluate the issues, and seek changes as needed. Ideally, this action can be done before a significant impact on the *Quality Goals*.

**SSE-CMM LEVEL 4 -- A CASE STUDY**  
**Pam Feldpusch and Barry Stoll (Eagle Alliance)**  
[pfeldpus@csc.com](mailto:pfeldpus@csc.com) / [bstoll@csc.com](mailto:bstoll@csc.com)

The SSE-CMM Team, over time, came to understand that while achieving Level 4 is not the one-time meeting of a goal, nor the mere collection of data. Likewise, operating at Level 4 is not the meeting of goals over time. Operating at Level 4 is putting measurements into action, quantitatively understanding process capabilities, and better controlling performance.

The ISSG again, as in Level 3, sought and received outside validation from an expert third party. Eagle Alliance's ISSG officially declared SSE-CMM Level 4 in March of 2006. While this was not a requirement of the contract as was Level 3, the achievement was still announced to the Client, and it was highly acknowledged by CSC's GSS (Global Security Solutions), and ESI (Enforcement, Security, and Intelligence) Divisions.

Of course, as soon as Level 4 was declared, Eagle Alliance management immediately requested the plan for achieving Level 5. Level 5 will use the same data, but allow for trend analysis and a look forward in an effort to detect expected deviations, so that pre-emptive actions can be taken.

Thankfully, there is no Level 6 ... *yet*.

For additional information about SSE-CMM, visit [www.sse-cmm.org](http://www.sse-cmm.org). For more about ISSEA, visit [www.issea.org](http://www.issea.org).