



Case Study

On

SSE-CMM Assessment

Dated 27th Jan 2005
Version 0.8

American Subsidiary:
Renaissance Information Technology Inc.
Chicago, Illinois

JV's and Branches:
Germany, Australia, Malaysia
Saudi Arabia, Oman, Kuwait
UAE and Bahrain

Global Head Quarters:
#14 El Dorado, 80 Feet Road
Indiranagar 1st Stage
Bangalore 560038
Karnataka, India

Telephone: +91 80 5213190
Video: +91 80 5209320
Fax: +91 80 5213191
URL: www.renaissance-it.com

Revision History

Date	Version	Description	Author
14 th Jan 2005	0.1	Draft version	M N Sudarshan / Manish P
17 th Jan 2005	0.2	Added V&V details	Surender Nath Indarapu
19 th Jan 2005	0.3	Updated the business needs and process details	Manish / Zafar / Surender
20 th Jan 2005	0.4	Updated with the current assessment details	Manish / Zafar / Surender
20 th Jan 2005	0.5	Reviewed and added details of SRIT intro and CMMi initiatives	Dr. Madhu Nambiar
21 st Jan 2005	0.6	Updated and added details section 9	Surender Nath Indarapu
24 th Jan 2005	0.7	Section 5 ,6.4 and 8 were modified for minor corrections	Shaini Varghese
24 th Jan 2005	0.7	Page 12 , Section 9.4 was modified for minor corrections	Zafrulla Khan
27 th Jan 2005	0.8	Reviewed and updated as per Dr's mail	Surender Nath Indarapu
27 th Jan 2005	0.8	Final Review Done, No changes suggested	Shaini / Zafrulla

Table of Contents

1.	About SRIT	4
2.	Our Development Methodology - Rational Unified Process	5
3.	Specific initiatives	5
3.1	CMM Specific	6
3.2	Others	6
4.	Status of various process models	6
4.1	CMM Specific	6
4.2	Others	6
4.3	Our CMMi & Six Sigma Integrated Program	6
5.	Pilot on SSE-CMM	6
5.1	Result of the SSE-CMM Pilot Assessment	7
5.2	Lessons Learnt from the SSE-CMM Pilot Assessment	7
6.	SSE-CMM Implementation and Assessment	8
6.1	Type of Assessment	8
6.2	Appraisal Team Members	8
6.3	About the project Assessed	9
7.	Assessment Model	9
7.1	Initiating Phase	9
7.2	Diagnosing Phase	10
7.3	Establishing Phase	10
7.4	Acting Phase	10
7.5	Learning Phase	10
8.	Certification	11
9.	Flow of activities for SSE-CMM process implementation	11
9.1	Assessing the Risk	11
9.2	Evolving security processes	11
9.3	Security Process Compliance checks	11
9.4	Others	12
10.	Assessment on SSE-CMM	12
10.1	Result of the Assessment	12
10.2	Lessons Learnt from the SSE-CMM Assessment	13
11.	For further queries	14
12.	References	15

1. About SRIT

SRIT is an integral part of the \$210 million, 29-yr old, 5000 people SOBHA group. While \$210 million is the annual turnover, the market capitalization is in excess of US\$1billion.

At Sobha Renaissance Information Technology Private Ltd (SRIT), we operate full-fledged Software ODC's for major corporations like Baxter (a fortune 250 American Company) as also conglomerates like Cable & Wireless Plc / Bahrain Telecommunications Company (Batelco-Bahrain), TUV Rheinland of Germany, Japan, Spain, China, Taiwan &, America & UK. Among the prestigious Companies that got enlisted as an ODC partner during the year 2004 was, **BCG**. Among seven Companies BCG conducted due-diligence on, SRIT got selected as BCG's ODC partner in India.

Quality has been a cornerstone of SRIT's culture. SRIT's Methodologies, Systems & Processes are world class; in that,

- SRIT is **one of the 50** Software Development & IT Companies in India assessed at SEI-CMM Level 5 by the Carnegie Melon University's Software Engineering Institute.
- One of the few Companies in India assessed / rated at PCMM Level 5 (**12th globally**). (PCMM L5 is the highest rating in People Capability Maturity Model as assessed by Carnegie Melon University's Software Engineering Institute).
- One of the **4 or 5** Companies in India who have begun practicing Six Sigma integrated with CMMi Level 5
- **7th** Corporation in India assessed and certified by British Standards Institute (BSI) for BS7799 in the areas of Information Security, Vulnerability Assessments, Risk Management, Disaster Recovery Planning & Business Continuity Planning.
- **1st** Company assessed & rated by BSI (as per authorization of Mr. John Hopkinson) at the highest maturity level for all the 22 PA's in regard to Systems Security Engineering-Capability Maturity Model (SSE-CMM).

SRIT takes pride in stating that the one differentiator with SRIT is, consistently delivering highest quality ahead of the committed time within the budget price of its customer-partner(s). SRIT is, today, looked upon as a Total Solution Provider as opposed to a mere Coder.

Besides the ODC, SRIT specializes in the following areas:

- Banking & Financial Services
- Environmental Health, Science & Safety
- E-Governance
- Total Enterprise and, Enterprise Application Integration
- Telecom OSS & BSS, Intelligent Network and NMS.
- Application Software Development across industries and domains
- Legacy migration and re-engineering

With its demonstrated multi-vertical expertise and an established global delivery model, SRIT has won the trust and delight of its valued customer-partners. Some of the software product rollouts:

- **Banking & Finance:** Renaissance's suite of products for financial institutions.
- **Automotive:** Renaissance's ERP product "ELF" addresses Automotive Companies & their global/local/retail distribution.
- **Healthcare:** Renaissance CARE suite of products offers solutions for integrated hospital management and health delivery system.

- **Telecom:** Solutions in Billing & Mediation Devices and, Interconnect.
- **EHS:** An Integrated Enterprise wide application N'vizion for Environmental, Health & Safety solutions.
- **Enterprise Solutions:** Solutions built on SOA framework that constitutes a highly scalable functional framework and robust technical architecture.

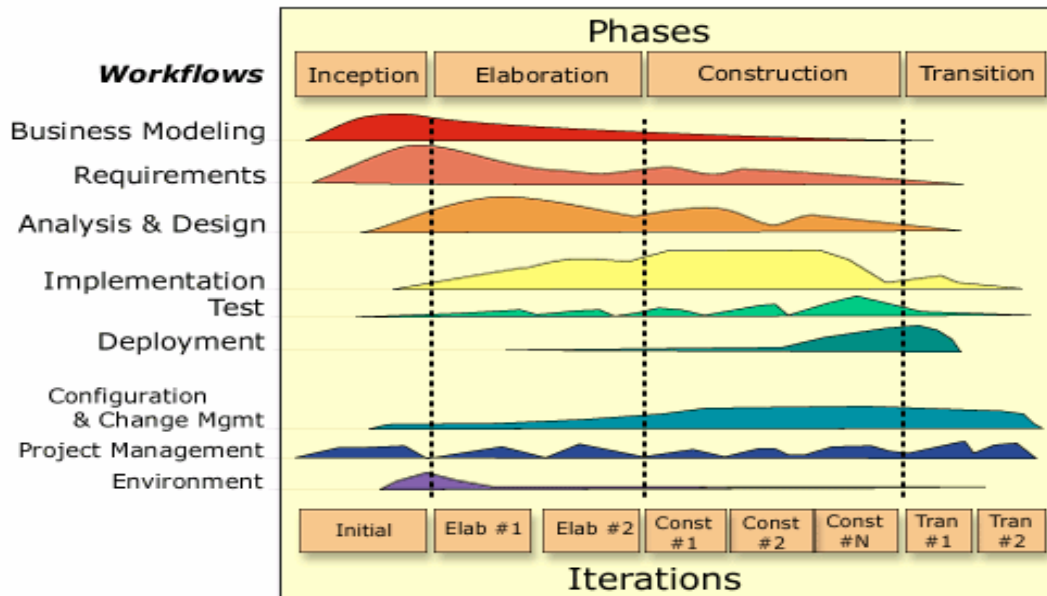
2. Our Development Methodology - Rational Unified Process

The development process follows the Rational Unified Process (RUP).

- RUP is proven best methodology to address the managerial & technical risks of a project
- RUP allows for effective management of requirements
- RUP enables high quality output of all project deliverables
- RUP allows good management of changes

RUP segments the development lifecycle into four phases:

- **Inception:** The major goal of the inception phase is to achieve concurrence among all stakeholders on the lifecycle objectives for the project. The inception phase is of significance primarily for new development efforts, in which there is significant business and requirement risks that must be addressed before the project can proceed.
- **Elaboration:** The goal of the elaboration phase is to baseline the architecture of the system to provide a stable basis for the bulk of the design and implementation effort in the construction phase.
- **Construction:** The goal of the construction phase is to clarify the remaining requirements and complete the development of the system based upon the baselined architecture.
- **Transition:** The focus of the Transition Phase is to ensure that software is available for its end users.



3.1 CMM Specific

- Initiated the SEI-CMM process early part of the year 2002 (consulting by TUV)
- Initiated the P-CMM process early part of the year 2003 (consulting by KPMG)
- Initiated SSE-CMM Pilot process early part of the year 2004 (consulting by BSI)
- Initiated SSE-CMM Appraisal process mid of the year 2004 (consulting by BSI)

3.2 Others

- Initiated the BS7799-2:2002 Audit & Appraisal process in the year 2003 (consulting by BSI)

4. Status of various process models

4.1 CMM Specific

- Assessed & rated at SEI-CMM level 5 early part of the year 2004
- Assessed & rated for P-CMM level 5 early part of the year 2004
- Assessed for SSE-CMM (Pilot assessment) in June/July 2004 by BSI and rated at levels equivalent to level 3 of SEI-CMM
- Ongoing assessments for SSE-CMM maturity levels continued. Rated at highest maturity levels in all the 22 KPAs by BSI. Equivalent to level 5 of SEI-CMM.

4.2 Others

- BS7799-2:2002 BSI, certificate number IS 84145 Valid till 17th June' 2007
- ISO 9001:2000 TUV, certificate number 01 100 011833 valid till May' 2005

4.3 Our CMMi & Six Sigma Integrated Program

This program has been rolled out in Jan 2005. A number of Black Belt and Green Belt members are being trained in order that each trained member undertakes Six Sigma Projects.

Pilot on SSE-CMM

At any given point in time, SRIT has in excess of 50 Software projects addressing the Health Delivery space, Product Testing & Certification space, Telecommunication, Banking and, Enterprise Solutions including CRM and Knowledge Management.

SRIT's process areas of PA 12 to PA 22 were already assessed and rated at the highest maturity levels based on the already established and certified Software Engineering (SEI-CMM L5) and People Practice(P-CMM L5) programs undertaken from the year 2002 through the year 2004.

During the period of selection of the projects for SSE-CMM, all the basic security practices were already in place; such as visitor entry control, restricted time, attendance and, access control at all locations and, background check of all the staff members.

Thereafter, SRIT began setting-up new and additional security processes and practices based on a semi-quantitative method of risk assessment and risk treatment. All such processes and practices were mapped with the base practices of SSE-CMM process areas – i.e. Assessing threat, Assessing Vulnerability, Assessing Risk, Assessing Business Impact Analysis, Building Assurance Framework, Setting-up Business Continuity Planning. But the maturity of these security processes were still in the improvement stages.

At the time of pilot assessment, the documents and processes in place provided just the evidence to support all the base practices that SRIT followed; existing, defined organizational processes. Metrics were also evidenced. However, as these were at very preliminary stage and, no further activities to enhance or improve the process were evidenced, the security process area's were assessed at a level equivalent to Level-3 in the SEI-CMM.

Thereby, SRIT achieved maturity level three (L3) in 16 out of 22 KPA's at the time of SSE-CMM pilot assessment during the period June-July 2004.

For the pilot assessment, SRIT selected four projects and, six assessors independent of these four projects as also, independent of the Supporting IT infrastructure Group. In order to provide awareness of the SSE-CMM model to the project implementation team members; as also, the SSAM assessment methodology to the Assessment Team Members (ATMs), SRIT engaged the services of an SSE-CMM Lead Appraiser from BSI. This Lead Appraiser had a formal authorization from ISSEA to conduct the audits & assessments for SRIT.

4.4 Result of the SSE-CMM Pilot Assessment



4.5 Lessons Learnt from the SSE-CMM Pilot Assessment

- The time-frame was too tight

- All the questions need not have been administered to all the team members
- Relevant PA questions should have been administered only to the relevant personals (Auditees should have been selected according to their area of expertise)
- Associates with relevant experience should have been selected as auditees
- Project security profile should have been improved to ensure capturing the maximum security related information
- Auditor's tone & tenor should not have been threatening
- Time tracking sheets should have been maintained in a disciplined manner
- Deviation from the SSAM method should not have been made i.e. took up 4 projects as compared to 3 projects prescribed in the SSAM model.

5. SSE-CMM Implementation and Assessment

5.1 Type of Assessment

- Assisted Self-Appraisal

5.2 Appraisal Team Members

Lead Appraiser

- Sudarshan M N (from BSI India Pvt Ltd)

Executive spokes person

- Niraj K Srivastava

Onsite coordinator

- Martin P C

Facilitator's

- Sridhar Suswaram
- Jaychandran (Also ATM)

ATM's

- Jaychandran B
- Vasudevan
- Shaini
- Manish P
- Kumar K. S

Observers

- Subhash Gaitonde

Time keeper

- Vignesh Raj Kumar
- Poorna Nagraj

Evidence Custodian

- Binu Sekhar

Auditees

- Surender Nath Indarapu (Project Manager)
- Zafrulla Khan (Project Lead)
- Sri Ranganatha V (Practitioner)
- Arun K Pandey (Practitioner)

- Ravi Kumar LR (Practitioner)

5.3 About the project Assessed

SRIT conceptualized, strategized, architected and, developed a security product named **Machine Monitoring System (MMS)**.

The functionality of the product is defined in the below sections

- Reader
 - The application has a feature to read all the network traffic information from the available Ethernet interfaces. This traffic data is then formatted and pushed into temporary storages for the analyzer to take further actions.
- Analyzer
 - The processed information sent from the reader is analyzed to identify the abnormality of the network traffic considering the details available in the knowledge base. Using this, the system can generate different flags that are supplied to the protector
- Protector
 - Based on the flags that are received from the analyzer, the protector agent will generate alerts and, based on the response for these alerts, actions are taken. The actions could be,
 - Allow the traffic
 - Kill the process
 - Quarantine
 - And these actions are written to the user knowledge base
- Knowledge base
 - The application maintains two type of knowledge base
 - System Knowledge base
 - These are the standard settings (i.e. machine behaviour) required at organization level or at the administrator level
 - User Knowledge base
 - These are the user level configuration settings of the machine.

In rolling out the MMS product, SRIT decided to strictly conform to all the base practices and the generic practices of ISO 21827(SSE-CMM) and ISO 15408 (Common Criteria). During the course of the development of the product, SRIT continually improved the Software engineering processes and security features of the product.

6. Assessment Model

SSAM IDEAL model was followed for the Assessment comprising of the following details in each phase:

6.1 Initiating Phase

- **Stimulus for Change**
 - Preparing Vision Document For SSE-CMM
- **Set Context**
 - Preparing Project plan for SSE CMM
 - Review & Approval from SEPG and MMS Project Execution Team
- **Build Sponsorship**
 - Get approval from the Senior Management

- **Charter Infrastructure**
 - Forming Organization structure for SSE CMM
 - Establishment of resources
 - Project Kick-off meeting

6.2 Diagnosing Phase

- **Characterize Current and Desired State**
 - Conducting Process awareness workshop to SSE team members
 - Conducting Gap Analysis
- **Process mapping**
 - Base practice
 - Generic Practice
- **Develop Recommendations**
 - Submitting Gap analysis results and Process mapping documents
 - Approval From SEPG for Process Changes

6.3 Establishing Phase

- **Set Priorities**
 - Develop action items based on Diagnosis phase Recommendations
 - Prepare prioritized Action list
 - Prepare new process documents
- **Develop Approach**
 - Submit Consolidated DCR and IP to SEPG
 - Place the SSE CMM process Changes in organization PAL (DRAFT)
 - Conduct a Process workshop to Pilot Project(MMS) team members
- **Plan Actions**
 - Set the dates for Implementation action items
 - Prepare the Meeting schedules with Pilot Project team
 - Daily Meeting
 - Weekly Meeting
 - Prepare Audit Schedule
 - Prepare communication matrix (PA 07)

6.4 Acting Phase

- **Create Solution**
 - Collect the details for PA09-PA10
 - Conduct Risk assessment including the requirements of (PA02-PA05)
 - "Identify The Safeguards and controls (PA01,PA08)"
 - Prepare & Submit Process/Security Metrics for 11 Security Process Area
 - Submit the project security profile to the MMS team (PA06)
- **Pilot/Test Solution**
 - Collect the results of SSE CMM Process audits
 - "Conduct Process review meeting (SSE,MMS team)"
- **Refine Solution**
 - Identify Alternative solutions/Process
 - Document the refinements
- **Implement Solution**
 - Implement the Refined Process
 - Collect Evidences for the Process Audit Lifecycle

6.5 Learning Phase

- **Analyze and Validate**
 - SSE CMM Pre-certification Assessments

- Submit the Assessment results to the management
- **Propose Future Actions**
 - Fill the Identified GAPS
 - Refine the Process Documents
 - Finalize the SSAM Audit plan for Final Assessment

7. Certification

- ATM Training by BSI
- Pre assessment By BSI
- Final assessment by BSI Lead Appraiser as per authorization from ISSEA
- Submitting assessment results to Management

8. Flow of activities for SSE-CMM process implementation

8.1 Assessing the Risk

- First, by assessing all the threats, SRIT arrived at comprehensive threat information, i.e. the potential risks that may be encountered in implementing the product.
- Next, by assessing the vulnerabilities by considering the global threat list, that is, the output of the above activity, SRIT arrived at a detailed vulnerability list.
- Next, by assessing tangible and intangible impact of each of the threats, and vulnerabilities, SRIT arrived at detailed impact information covering direct and cascading costs involved because of different risks in developing the product.
- By considering all the above inputs, SRIT arrived at a complete risk information related to product development.

8.2 Evolving security processes

- With the risk information prepared and the client needs made available, SRIT arrived at the security needs of the product and development process
- For the security needs identified, SRIT's internal security solutions group provided best practices to implement these needs following the organizational processes & policies.
- Different security controls were identified, i.e. all security controls needed to be addressed for implementing the best practices as recommended by SRIT's internal security solutions group.
- A regressive health check was planned and effected in order to monitor the security controls that are implemented for the environment and product development. Quantitative analysis was performed based on the data available and, the defined metrics.
- Co-ordination mechanism was defined as part of the process that is followed in the due course of all activities related to product development and security issues. Organizational chart with roles and responsibilities, escalation mechanism & communication protocols were established for achieving effective co-ordination.

8.3 Security Process Compliance checks

- Extensive security and quality audits were planned spanning through initiation till transition phases of the development life cycle.

- Follow-up audits were conducted to ensure the customer & security requirements are met in compliance with the process; total emphasis were on the testing and requirements traceability.
- Review of the audits findings were conducted to plan the corrective and/or improvement proposals.

8.4 Others

- Continuous monitoring was done to ensure sufficient data is gathered through audits to efficiently analyze the performance at different levels.
- Mapping data against metrics defined was done to verify and validate any corrective or improvement plans.
- Project Security profile document was maintained to ensure the status of the product were maintained for development as per the different process stages.

For the security risk analysis, SRIT adopted the “Attack tree methodology”. SRIT ensured that it took inputs from subject matter experts.

With the objective of practicing & demonstrating the highest maturity levels (Level-5) in the security engineering process areas, SRIT adopted the guidelines provided for in the **NIST 800-55**.

During the phase of design and implementation, SRIT engaged the services of its internal SQA team to conduct in excess of six audits right from the design through the product implementation phases.

9. Assessment on SSE-CMM

During the assessments, the documents and process in place provided evidence to support the following

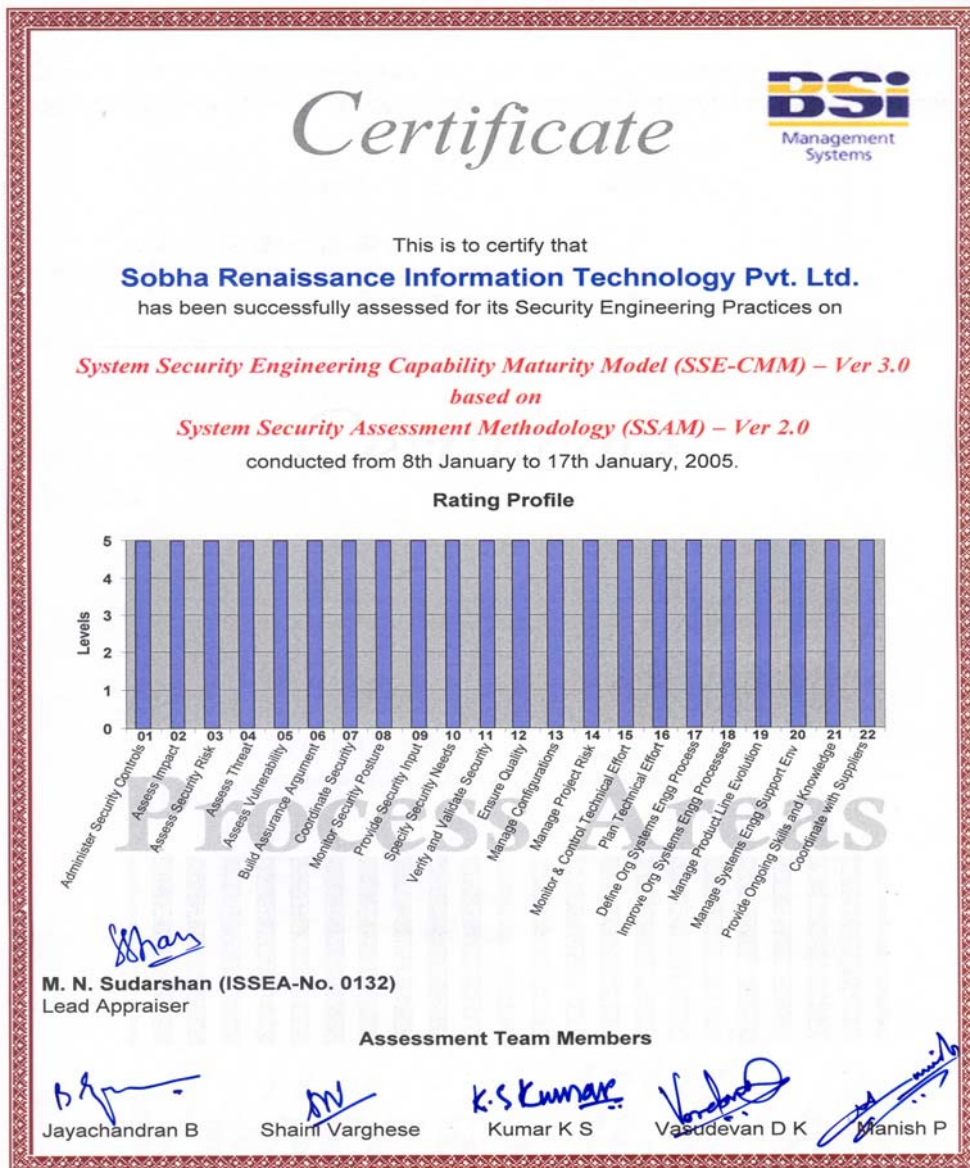
- Base practices being followed
- All practices are well defined
- Existing organizational processes was available as process assets library.
- Metrics were evidenced for different measurable activities as defined by the process.
- Defect analysis, corrective & preventive actions and, improvement proposals were also evidenced.

Consequently, SRIT achieved maturity level Five (5) in 22 out of 22 KPA's at the time of SSE-CMM assessments conducted in the month of January, 2005.

For these assessments, SRIT selected one security product (MMS) and five assessors independent of the MMS Security project and, also independent of SRIT's internal System Support IT infrastructure Group members.

In order to provide awareness on the SSE-CMM model and the SSAM assessment methodology to the Assessment Team Members (ATMs), SRIT engaged the services of an ISSEA-authorized SSE-CMM Lead Appraiser from BSI.

9.1 Result of the Assessment



9.2 Lessons Learnt from the SSE-CMM Assessment

- **Deviations from the SSAM**
 - Data tracking sheet (DTS) was not keyed in for pre-assessment. However, the purpose for revising the questionnaire was achieved.
 - DTS was not keyed in for Project Manager / Project Leader before interviewing the Practitioners.
 - Evidence Request Tracking Summary Sheet and Evidence Use Summary Tracking Sheet were prepared on Day 2 afternoon for both Day 1 and Day 2.
- **Lessons Learnt (ATMs')**

- Lessons learnt from the Pilot Assessment In June-July 2004 proved beneficial. Accordingly, all gaps were plugged.
 - For PA 05 and PA 08, two auditees – Project Manager and Practitioner were interviewed simultaneously.
 - Time in each session for interviewing Project Manager and Project Lead should have been increased to 3 hours with a fifteen-minutes break.
 - Time in each session for interviewing Practitioners should have been increased to 1.15 hours. This is specific to PA's where individual practitioners are questioned for process compliance.
 - Internal Document Review during Pre-Assessment (not a part of SSAM) is recommended. This can be initiated either by the Project Manager or the ATMs requesting specific evidence.
 - Evidence Custodian and Timekeeper roles were separated. This proved very useful.
- **Lessons Learnt (Auditees)**
 - During the interviews, Auditees should be allowed to bring-in evidence and/or should be permitted online access to bring-in evidences.
 - A minimum of 5 working days gap is recommended between Pre-assessment phase and Onsite Phase.
 - ATMs should rephrase the customized questions and/or create follow-up questions based on the roles for interviewing the auditees.
 - Last minute schedule requests for Follow-up Interviews to be indicated in the Plan itself.
 - **Suggestions for the Sponsor**
 - Monthly health-check to be conducted to include SSE CMM (PA 01-PA 11) components within the Quality Management System (QMS).
 - PA 01 to PA 11 from SSE CMM to be integrated with CMMi Level 5.

10. Any queries

- Dr. Madhu Nambiar
 - +91 802 525 0102 (Office)
 - +91 984 506 9510 (Mobile)
 - madhu@renaissance-it.com
- Niraj K Srivastava
 - +91 802 521 3190 (Office)
 - +91 984 518 1893 (Mobile)
 - niraj@renaissance-it.com
- Surender Nath Indarapu
 - +91 802 521 3190 (Office)
 - +91 984 520 3463 (Mobile)
 - surendermath@renaissance-it.com
- Zafrulla Khan
 - +91 802 521 3190 (Office)
 - +91 934 378 0871 (Mobile)
 - zafrullakhan@renaissance-it.com
- Sudarshan M N

- +91 805 113 4654 (Office)
- +91 934 256 5504 (Mobile)
- sudarshan.mn@bsi-india.com

- Jaychandaran B
 - +91 802 521 3190 (Office)
 - +91 984 549 0151 (Mobile)
 - jayachandran@renaissance-it.com

11. References

- www.sse-cmm.org
- csrc.nist.gov/publications/nistpubs/800-55/
- www.bsi.bund.de/english/

The profile & statement going into the site:

SRIT's success is primarily attributed to its absolute commitment to consistently deliver highest quality products and services both to its internal and, external customer-partners. As an integral part of this delivery commitment, SRIT is committed to provide both its internal and, external customer-partner(s) a secure information infrastructure by championing and, continuously improving its security and operational practices through a highly proactive approach. By doing this, SRIT has been consistently minimizing the risk in Information System Infrastructure and, consequently, safeguarding both its internal and, external customer(s) interests. The goal of SRIT's IS policy is to assure absolute protection of SRIT's and, SRIT's customer-partners' systems and operations thus re-affirming its internal and external customer's faith in SRIT's ability to uphold confidentiality, integrity and, availability of information.

SRIT takes pride to demonstrate its leadership position in so far as its Systems Security Engineering Practices(SSE) are concerned. SRIT becomes the first company to have got assessed for the highest maturity levels in SSE practices and, consequently, rated at Level 5 by the BSI Lead Appraiser under authorizations from ISSEA.

Both in terms of Software Engineering Practices and People Practices, SRIT has consistently demonstrated practicing at the highest maturity levels (L5) and, these are evidenced through regular assessments, re-audits & re-certifications.

Quality is a never-ending journey because, it is all about continuous improvement. SRIT has, this year, embarked on its two ambitious program. Once again, aimed at taking the leadership position,

- The integrated Six Sigma-CMMi Level 5 program
- Setting up its Software Testing Lab mapped to CC standards