7.3.2.3 CMM-SEC rating

Ratings are given as None (0), Initial (1), Repeatable (2), Defined (3), Managed (4), or Optimizing (5) for both current state and goal state. Add up values and divide current state by the goal state then multiply by 10 to get the overall rating.

Area of CMM - Security Engineering	*Rate*	*Goal*
- Process areas		
- Base practices		
Administer security controls:		
- Establish responsibilities		
- Manage configuration		
- Manage awareness, training, and educational programs		
- Manage services & control mechanisms		
Assess impact:		
- Prioritize capabilities		
- Identify system assets		
- Select metrics		
- Identify metric relationship		
- Identify and characterize consequences		
- Monitor consequences		
Assess security risk:		
- Select risk analysis method		
- Identify exposures		
- Assess exposure risks		
- Assess total uncertainty		
- Prioritize risks		
- Monitor risks and characteristics		
Assess threat:		
- Identify natural and human threats		
- Identify units of measure for threats		
- Assess threat capabilities and intents		
- Assess likelihood		
- Monitor threats and characteristics		
Assess vulnerability:		
- Select vulnerability analysis method		

Area of CMM - Security Engineering	Rate	Goal
- Identify vulnerabilities		
- Gather vulnerability data		
- Synthesize system vulnerabilities		
- Monitor vulnerabilities and characteristics		
Build assurance argument:		
- Identify assurance objectives		
- Diffuse assurance strategy		
- Control assurance evidence		
- Analyze evidence		
- Provide assurance argument		
Coordinate security:		
- Define coordination objectives		
- Identify coordination mechanisms		
- Facilitate coordination		
- Coordinate decisions and recommendations		
- Facilitate coordination		
- Coordinate decisions and recommendations		
Monitor system security posture:		
- Analyze event records		
- Monitor changes		
- Identify incidents		
- Monitor safeguards		
- Review security posture		
- Manage incident response		
- Protect monitoring artifacts		
Provide security input:		
- Understand security input needs		
- Determine constraints and considerations		
- Identify alternatives		
- Analyze engineering alternatives		
- Provide engineering guidance		
- Provide operational guidance		
Specify security needs:		

Area of CMM - Security Engineering	Rate	Goal
- Gain understanding of protection needs		
- Identify applicable laws and regulations		
- Identify system security context		
- Capture view of system operation		
- Define requirements		
- Obtain agreement on protection		
Verify and validate security:		
- Identify V&V targets		
- Define V&V approach		
- Perform validation		
- Perform verification		
- Provide V&V results		
Organization:		
- Institutionalization of process areas		
- Implementation of process areas		
- Define organizational security engineering process		
- Improve organizational security engineering process		
- Manage product evolution		
- Manage engineering support environment		
- Provide ongoing skills and knowledge		
- Coordinate with suppliers		
Project:		
- Ensure Quality		
- Manage configurations		
- Manage program risk		
- Monitor and control technical effort		
- Plan technical effort		
TOTAL		
Rating (divide current into goal and multiply by 10)		**450**

(Total ratings / maximum goal (450) * 10 is the basis for comparison here)

Startup	Diligence	Typical	Excellent	Best
1	3	5	7	9

7.3.2.3.1 CMM-SEC detailed ratings

CMM-SEC ratings are given by identifying all of the items within the level under consideration that are fulfilled under the risk management (R), Engineering (E), Assurance (A), and Coordination (C) efforts, and giving each of those fulfilled the value indicated by the value column (V). Stop as soon as an item is not fulfilled or a total is not a whole number. The rating column (Rate) gets the sum of those other ratings divided by 4 and the total rows get totals from their section.

Level	*Item within level*	*V*	*Rate*	*R*	*E*	*A*	*C*
0 None		0					
1 Initial	Few processes defined. Success depends on individual talent and heroic effort						
	1.1 base practices performed	1					
TOTAL							
1 Repeatable	Necessary process discipline is in place to repeat earlier successes on similar projects						
	Requirements management is in place	0.1					
	Project planning is done	0.1					
	Project tracking and oversight is done	0.1					
	Subcontract management is done	0.1					
	Quality assurance is done	0.1					
	Configuration management is done	0.1					
	Performance is planned	0.1					
	Performance is disciplined	0.1					
	Performance is verified	0.1					
	Performance is tracked	0.1					
TOTAL							
2 Defined	The process for both management and engineering activities is documented, standardized, and used on all projects organization-wide.	2					
	Process focus is documented	0.1					
	Process definition is documented	0.1					
	Training programs are provided	0.1					
	Integrated management is in place	0.1					
	Product engineering is universally	0.1					
	Intergroup coordination is universal	0.1					
	Peer reviews are universal	0.1					
	Standard processes are defined	0.1					
	Defined processes are perform	0.1					
	Practices are coordinated	0.1					
TOTAL							

Level	*Item within level*	*V*	*Rate*	*R*	*E*	*A*	*C*
4 Managed	Both the process and end-products are quantitatively understood and controlled using detailed measures	4					
	Quality management is universal	0.25					
	Quantitative process management exists	0.25					
	Measurable performance goals are used	0.25					
	Performance is objectively managed	0.25					
TOTAL							
5 Optimizing	Continuous process improvement is enabled by quantitative feedback from the process and from testing innovative ideas and technologies						
	Defect prevention is systematic	0.2					
	Technology change management is systematically applied	0.2					
	Process change management is systematically applied	0.2					
	Organizational capability is systematically measured and improved	0.2					
	Process effectiveness is systematically measured and improved	0.2					
TOTAL							
RATING	Add up TOTAL ratings in each column						

The rating value comes from adding up the totals of each of the previous total rows. This value provides a CMM-SEC rating in each of the 4 areas and an aggregate rating.

7.3.2.3.2 Key process areas

1. Security Risk Management - processes dealing with estimating risk at each of the maturity levels
2. Engineering - processes involved with architecting a system and managing security requirements;
3. Assurance Management - processes dealing with generating, managing, presenting assurance evidence;
4. Coordination - processes that coordinate security engineering activities with other engineering disciplines.

Ratings are based on commitment to perform, ability to perform, actual performance, measurement of performance, and verification of performance.