

# ISO/IEC 21827:2008-10 (E)

## Information technology - Security techniques - Systems Security Engineering - Capability Maturity Model® (SSE-CMM®)

---

<b>Contents</b>		<b>Page</b>
Foreword .....		v
0	Introduction .....	vi
1	Scope .....	1
2	Normative references .....	1
3	Terms and definitions .....	2
4	Background .....	6
4.1	Reason for Development .....	7
4.2	The Importance of Security Engineering .....	7
4.3	Consensus .....	7
5	Structure of the Document .....	8
6	Model Architecture .....	8
6.1	Security Engineering .....	8
6.2	Security Engineering Process Overview .....	11
6.3	SSE-CMM® Architecture Description .....	14
6.4	Summary Chart .....	22
7	Security Base Practices .....	23
7.1	PA01 Administer Security Controls .....	24
7.2	PA02 - Assess Impact .....	28
7.3	PA03 - Assess Security Risk .....	32
7.4	PA04 - Assess Threat .....	36
7.5	PA05 - Assess Vulnerability .....	39
7.6	PA06 - Build Assurance Argument .....	43
7.7	PA07 - Coordinate Security .....	46
7.8	PA08 - Monitor Security Posture .....	49
7.9	PA09 - Provide Security Input .....	54
7.10	PA10 - Specify Security Needs .....	59
7.11	PA11 - Verify and Validate Security .....	63
Annex A (normative) Generic Practices .....		67
Annex B (normative) Project and Organizational Base Practices .....		68
B.1	General .....	68
B.2	General Security Considerations .....	68
B.3	PA12 - Ensure Quality .....	69
B.4	PA13 - Manage Configurations .....	74
B.5	PA14 - Manage Project Risks .....	78
B.6	PA15 - Monitor and Control Technical Effort .....	82
B.7	PA16 - Plan Technical Effort .....	86
B.8	PA17 - Define Organization's Systems Engineering Process .....	92
B.9	PA18 - Improve Organization's Systems Engineering Processes .....	96
B.10	PA19 - Manage Product Line Evolution .....	99
B.11	PA20 - Manage Systems Engineering Support Environment .....	102

<b>B.12</b>	<b>PA21 - Provide Ongoing Skills and Knowledge</b> .....	<b>106</b>
<b>B.13</b>	<b>PA22 - Coordinate with Suppliers</b> .....	<b>112</b>
<b>Annex C (informative) Capability Maturity Model Concepts</b> .....		<b>117</b>
<b>C.1</b>	<b>General</b> .....	<b>117</b>
<b>C.2</b>	<b>Process Improvement</b> .....	<b>117</b>
<b>C.3</b>	<b>Expected Results</b> .....	<b>118</b>
<b>C.4</b>	<b>Common Misunderstandings</b> .....	<b>118</b>
<b>C.5</b>	<b>Key Concepts</b> .....	<b>120</b>
<b>Annex D (informative) Generic Practices</b> .....		<b>124</b>
<b>D.1</b>	<b>General</b> .....	<b>124</b>
<b>D.2</b>	<b>Capability Level 1 - Performed Informally</b> .....	<b>125</b>
<b>D.3</b>	<b>Capability Level 2 - Planned and Tracked</b> .....	<b>126</b>
<b>D.4</b>	<b>Capability Level 3 - Well Defined</b> .....	<b>132</b>
<b>D.5</b>	<b>Capability Level 4 - Quantitatively Controlled</b> .....	<b>137</b>
<b>D.6</b>	<b>Capability Level 5 - Continuously Improving</b> .....	<b>139</b>
<b>Bibliography</b> .....		<b>142</b>