

Common Criteria Quick Reference Card

- PDF version has direct links to standards & guides -

For Common Criteria (CC) edition 3.1 R5 (2017-04).

Designed and edited by [Axel Rennoch](#) and [Jan de Meer](#).



Contents

1. Security Functional Requirements (SFRs)	2
FAU, FCO, FCS, FDP, FIA	2
FMT, FPR, FPT, FRU, FTA, FTP	3
2. Security Assurance Requirements (SARs)	4
ASE, ALC	4
ADV, AGD	5
ATE, AVA, ACO	6
APE, ACE	7
3. Evaluation Assurance Levels (EALs)	7
4. Further Information	8

References

- [1] Common Criteria for Information Technology Security Evaluation, part 1: Introduction and general model (2017-04)
- [2] Common Criteria for Information Technology Security Evaluation, part 2: Security functional components (2017-04)
- [3] Common Criteria for Information Technology Security Evaluation, part 3: Security assurance components (2017-04)
- [4] Common Criteria for Information Technology Security Evaluation, Evaluation methodology (CEM) (2017-04)
- [5] Guidelines for Evaluation Reports according to Common Criteria Version 3.1 *Revision 3 (!)*, BSI (AIS 14) (2010-07)

1. Security Functional Requirements (SFRs)

CLASS	FAMILY	COMPONENT [2]	ELEMENTS/OPERATIONS/NOTES [2]	
FAU Security audit [DT]	ARP	Security audit automatic response	1 Security alarms 1 act	
	GEN	Security audit data generation	1 Audit data generation 2 User identity association 1 level, evt, 2 inf	
		SAA	Security audit analysis	1 Potential violation analysis 2 Profile based anomaly detection 3 Simple attack heuristics 4 Complex attack heuristics 1, 2 evt, rules 1 profile, 2, 3 con 1 violation-evt, 2 activity-inf, 3 1 penetration-evt, indicator-evt, 2 inf, 3
	SAR	Security audit review	1 Audit review 2 Restricted audit review 3 Selectable audit review 1 usr, inf, 2	
		SEL	Security audit event selection	1 Selective audit 1 att, att
	STG	Security audit event storage	1 Protected audit trail storage 2 Guarantees of audit data availability 3 Action in case of possible audit data loss 4 Prevention of audit data loss 1, 2 ability 1, 2 ability, 3 metric, con 1 act, lim 1 act, act	
		FCO Communi- cation [DT]	NRO	Non-repudiation of origin
NRR	Non-repudiation of receipt		1 Selective proof of receipt 2 Enforced proof of receipt 1 inf-type, role(3rdParty), 2 att, inf-fields, 3 role(3rdParty), lim 1 inf-type, 2 att, inf-fields, 3 role(3rdParty), lim	
FCS Crypto- graphic support [DT]	CKM	Cryptographic key generation	1 algor., keysize, standard	
		Cryptographic key distribution	1 keysize, standard	
FDP User Data Protection [DT]	COP	Cryptographic key access	1 type, method, standard	
		Cryptographic key destruction	1 method, standard	
FCS Crypto- graphic support [DT]	ACC	Access control policy	1 Subset access control 2 Complete access control 1 pol, sub/obj/opr 1 pol, sub/obj/opr, 2	
		ACF	Access control functions	1 Security attribute based access control 1 pol, sub/obj/att, 2 gov.-rules, 3 auth.-rules, 4 deny-rules
	DAU	Data authentication	1 Basic Data Authentication 2 Data Authentication with Identity of Guarantor 1 obj/inf-types, 2 sub 1 obj/inf-types, 2 sub	
	ETC	Export from the TOE	1 Export of user data without security att 2 Export of user data with security attributes 1 pol, 2 1 pol, 2, 3, 4 rules	
		IFC	Information flow control policy	1 Subset information flow control 2 Complete information flow control 1 sub/inf, 2
	IFF	Information flow control functions	1 Simple security attributes 2 Hierarchical security attributes 1 sub/inf/att, 2 flow-rule, 3 add.-rule, 4 auth-rules, 5 deny-rules 1 sub/inf/att, 2 opr-relations, 3 rules, 4 auth-rules, 5 deny-rules, 6 1 flow-types, capacity 1 pol, flow-types, capacity, 2 flow-types	
			Limited illicit information flows	1 pol, flow-types, capacity, 2 flow-types
		Partial elimination of illicit information flows	1 pol -name	
		No illicit information flows	1 pol, flow-types, capacity	
	ITC	Import from outside of the TOE	1 Import of user data without security att. 2 Import of user data with security attributes 1 pol, 2, 3 rules 1 pol, 2, 3, 4, 5 rules	
		ITT	Internal TOE transfer	1 Basic internal transfer protection 2 Transmission separation by attribute 3 Integrity monitoring 4 Attribute-based integrity monitoring 1 pol, evt 1 access-pol, evt, 2 att 1 pol, err, 2 act 1 pol, err, att, 2 act
	RIP		Residual information protection	1 Subset residual information protection 2 Full residual information protection 1 act, obj 2 act
	ROL	Rollback	1 Basic rollback 2 Advanced rollback 1 pol, opr, 2 lim 1 pol, opr, 2 lim	
		SDI	Stored data integrity	1 Stored data integrity monitoring 2 Stored data integrity monitoring and action 1 err, att 1 err, att, 2 act
	UCT	Inter-TSF user data confidentiality transfer protection	1 Basic data exchange confidentiality 1 pol, act	
	UIT	Inter-TSF user data integrity transfer protection	1 Data exchange integrity 2 Source data exchange recovery 3 Destination data exchange recovery 1 pol, act, act 2 act 1 pol, err 1 pol, err	
		FIA Identificati- on and authentic- ation [DT]	AFL	Authentication failures
ATD	User att. definition		1 User attribute definition 1 att	
SOS	Specification of secrets		1 Verification of secrets 2 TSF Generation of secrets 1 metric 1 metric, 2 fct	
	UAU		User authentication	1 Timing of authentication 2 User authentication before any action 3 Unforgeable authentication 4 Single-use authentication mechanisms 5 Multiple authentication mechanisms 6 Re-authenticating 7 Protected authentication feedback 1 act, 2 1 1 act, 2 act 1 mechanism 1 mechanism, 2 rules 1 con 1 feedback
UID			User identification	1 Timing of identification 2 User identification before any action 1 act, 2 1
USB			User-subject binding	1 User-subject binding 1 att, 2 association-rules, 3 change-rules

Conventions: **[DT]** Dependency table; "-" hierarchical component; SFR element operation colours (selection, assignment).

Abbreviations: act (action), att (attribute), con (condition), err (error), evt (event), inf (information), lim (limitation), num (number), obj (object), opr (operation), pol (policy), sub (subject), u/s (user/subject).

CLASS	FAMILY	COMPONENT [2]	ELEMENTS/OPERATIONS/NOTES [2]
FMT Security management [DT]	MOF	Management of functions in TSF 1	Management of security functions behaviour 1 act, fct, roles
	MSA	Management of security attributes 1	Management of security attributes 1 pol, act(opr), att, role
		Secure security attributes 2	1 att
		Static attribute initialisation 3	1 pol, act(opr), 2 role
		Security attribute value inheritance 4	1 value-setting-rules
	MTD	Management of TSF data 1	Management of TSF data 1 act(opr), data, roles
		Management of limits on TSF data 2	1 data, roles, 2 act
	REV	Revocation 1	Secure TSF data 1 data
SAE	Revocation 1	Revocation 1 att, groups(resources), roles, 2 rules	
SMF	Security attribute expiration 1	Time-limited authorisation 1 att, roles, 2 act	
SMR	Specification of Management fct. 1	Specification of Management Functions 1 fct	
	Security management roles 1 -2 3	Security roles Restrictions on security roles Assuming roles 1 roles, 2 1 roles, 2, 3 con 1 roles	
FPR Privacy [DT]	ANO	Anonymity 1	Anonymity 1 u/s, sub/opr/obj
		Anonymity without soliciting information -2	1 u/s, sub/opr/obj, 2 service, sub
	PSE	Pseudonymity 1	Pseudonymity 1 u/s, sub/opr/obj, 2 num, sub, 3 opr, metric
		Reversible pseudonymity -2	1 u/s, sub/opr/obj, 2 num, sub, 3 opr, metric, 4 usr(resources), con
	UNL	Unlinkability 1	Alias pseudonymity 1 u/s, sub/opr/obj, 2 num, sub, 3 opr, metric, 4 con
UNO	Unlinkability 1	Unlinkability 1 u/s, opr, cause(relations)	
	Unobservability 1 -2 3 4	Unobservability Allocation of information impacting unobservability Unobservability without soliciting information Authorised user observability 1 u/s, opr, obj, usr/sub 1 inf, 2 con 1 service, sub, inf 1 usr, resource/service	
FPT Protection of the TOE [DT]	FLS	Fail secure 1	Failure with preservation of secure state 1 failure types
	ITA	Availability of exported TSF data 1	Inter-TSF availability within a defined availability metric 1 data-types, metric, con
	ITC	Confidentiality of exported TSF data 1	Inter-TSF confidentiality during transmission 1
	ITI	Integrity of exported TSF data 1	Inter-TSF detection of modification Inter-TSF detection and correction of modification 1 metric, 2 act 1 metric, 2 act, 3 mod-type
		-2	
	ITT	Internal TOE TSF data transfer 1	Basic internal TSF data transfer protection 1 opr
		-2 3	TSF data transfer separation TSF data integrity monitoring 1 opr, 2 1 evt(err), 2 act
	PHP	TSF physical protection 1	Passive detection of physical attack 1, 2
		-2 3	Notification of physical attack Resistance to physical attack 1, 2, 3 device/element, usr/role 1 scenarios, device/element
	RCV	Trusted recovery 1	Manual recovery 1 failures
		-2 -3 4	Automated recovery Automated recovery without undue loss Function recovery 1 failures, 2 failures 1 failures, 2 failures, 3 quantification, 4 1 fct/scenarios
	RPL	Replay detection 1	Replay detection 1 entities, 2 act
	SSP	State synchrony protocol 1	Simple trusted acknowledgement 1
		-2	Mutual trusted acknowledgement 1, 2
	STM	Time stamps 1	Reliable time stamps 1
TDC	Inter-TSF TSF data consistency 1	Inter-TSF basic TSF data consistency 1 data-types, 2 rules	
TEE	Testing of external entities 1	Testing of external entities 1 evt(con), properties 2 act	
TRC	Internal TOE TSF data replication consistency 1	Internal TSF consistency 1, 2 fct	
TST	TSF self test 1	TSF testing 1 evt(con), TSF(parts), 2 TSF-data(parts), 3 TSF(parts)	
FRU Resource Utilisation [DT]	FLT	Fault tolerance 1	Degraded fault tolerance 1 TOE-capabilities, failure-types
		Limited fault tolerance -2	1 failure-types
	PRS	Priority of service 1	Limited priority of service 1, 2 resources
RSA	Full priority of service -2	1, 2	
	Resource allocation 1	Maximum quotas 1 resources, u/s, time	
-2	Minimum and maximum quotas 1 resources, u/s, time, 2 resources, u/s, time		
FTA TOE access [DT]	LSA	Limitation on scope of selectable attributes 1	Limitation on scope of selectable attributes 1 session-att, att
	MCS	Limitation on multiple concurrent sessions 1	Basic limitation on multiple concurrent sessions 1, 2 default-lim
		Per user attribute limitation on multiple concurrent sessions -2	1 rules, 2 default-lim
	SSL	Session locking 1	TSF-initiated session locking 1 time-interval, 2 evt
		2	User-initiated locking 1, 2 evt
		3 4	TSF-initiated termination User-initiated termination 1 time-interval 1
TAB	TOE access banners 1	Default TOE access banners 1	
TAH	TOE access history 1	TOE access history 1 succ-display, 2 unsucc-display, 3	
TSE	TOE session establish. 1	TOE session establishment 1 att	
FTP Trusted path/channel	ITC	Inter-TSF trusted channel 1	Inter-TSF trusted channel 1, 2 TSF/product, 3 fct
	TRP	Trusted path 1	Trusted path 1 rem/local, evt(violation), 2 rem/local-usr, 3 auth(service)

Conventions: **[DT]** Dependency table; “-” hierarchical component; SFR element operation colours (selection, assignment).

Abbreviations: act (action), att (attribute), con (condition), err (error), evt (event), inf (information), lim (limitation), num (number), obj (object), opr (operation), pol (policy), sub (subject), u/s (user/subject).

2. Security Assurance Requirements (SARs)

CLASS	FAMILY	COMPONENT [3]	WU/CEM [4]	NOTES/BSI [5]	EAL			
ASE ST evaluati on <u>[DT]</u>	INT	ST introduction	<u>1</u> (ST content), <u>2</u> (ST reference), <u>3</u> (TOE ref id), <u>4</u> (TOE ref not misleading), <u>5</u> (sec features), <u>6</u> (TOE type), <u>7</u> (type not misleading), <u>8</u> (non-TOE), <u>9</u> (physical scope), <u>10</u> (logical scope), <u>11</u> (consistency)	<u>1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11</u>	1-7			
	CCL	Conformance claims	<u>1</u> (CC version), <u>2</u> ([2] extension), <u>3</u> ([3] extension), <u>4</u> (extended SFR), <u>5</u> (extended SAR), <u>6</u> (PP claim), <u>7</u> (package claim), <u>8</u> (package names), <u>9</u> (PP TOE type), <u>10</u> (PP SPD), <u>11</u> (PP sec objectives), <u>12</u> (PP SFRs)	<u>1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12</u>	1-7			
	SPD	Security problem definition	<u>1</u> (threats), <u>2</u> (threat description), <u>3</u> (OSPs), <u>4</u> (OE assumptions)	<u>1, 2, 3, 4</u>	2-7			
	OBJ	Security objectives	<u>1</u> (OE sec objectives) <u>2</u> (Security objectives)	<u>1</u> (OE sec objectives) <u>1, 2, 3, 4, 5, 6</u> (TOE+OE sec objectives), <u>2</u> (TOE obj. to threats/OSPs), <u>3</u> (OE obj. to OSPs+assumptions), <u>4</u> (counter threats), <u>5</u> (enforce OSPs), <u>6</u> (OE assumptions)	<u>1</u> <u>1, 2, 3, 4, 5, 6</u>	1 2-7		
	ECD	Extended components definition	<u>1</u> (non-ext. req in [2]/[3]), <u>2</u> (ext. req. covered), <u>3</u> (CC taxonomy), <u>4</u> (dependencies), <u>5</u> ([2] comp model), <u>6</u> ([2] family model), <u>7</u> ([2] class model), <u>8</u> ([3] comp model), <u>9</u> (SAR method), <u>10</u> ([3] family model), <u>11</u> ([3] class model), <u>12</u> (measurable elements), <u>13</u> (no existing comp)	<u>1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13</u>	1-7			
	REQ	Security requirements	<u>1</u> (SFRs), <u>2</u> (SARs), <u>3</u> (terms defined), <u>4</u> (operations), <u>5</u> (assignments), <u>6</u> (iterations), <u>7</u> (selections), <u>8</u> (refinements), <u>9</u> (dependencies), <u>10</u> (consistency) <u>2</u> (Derived security requirements)	<u>1, 2, 3, 4, 5, 6, 7, 8, 9, 10</u> (trace to objective), <u>11</u> (meet objectives), <u>12</u> (SAR justification), <u>13</u>	<u>1, 2, 3, 4, 5, 6, 7, 8, 9, 10</u> 1 (1-1), 2 (1-2), 3 (1-3), 4 (1-4), 5 (1-5), 6 (1-6), 7 (1-7), 8 (1-8), 9 (1-9), <u>10, 11, 12, 13</u> (1-10)	1 2-7		
	TSS	TOE summary specification	<u>1</u> (TOE summary specification (TSS)) <u>2</u> (TSS with architect. design summary)	<u>1</u> (TOE meets SFRs), <u>2</u> (consistency with overview/description) <u>1, 2, 3, 4</u>	<u>1, 2</u> n/a	1-7		
ALC Life- cycle <u>[DT]</u>	CMC	CM capabilities	<u>1</u> (Labelling of the TOE) <u>2</u> (Use of a CM system) <u>3</u> (Authorisation controls) <u>4</u> (Production support, acceptance procedures and automation) <u>5</u> (Advanced support)	<u>1</u> (unique label), <u>2</u> (consistent references) <u>1, 2, 3</u> (unique config ids), <u>4</u> (consistent ids) <u>1, 2, 3, 4, 5</u> (CM access), <u>6</u> (CM plan), <u>7</u> (CM use), <u>8</u> (config maintenance), <u>9</u> (CM records), <u>10</u> (CM operation) <u>1, 2, 3, 4, 5</u> (CM access control), <u>6</u> (automated production), <u>7</u> (effective production), <u>8, 9, 10</u> (config modification), <u>11, 12, 13</u> <u>1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20</u>	<u>1, 2</u> 1 (1-1), 2 (1-2), <u>3, 4</u> 1 (1-1), 2 (1-2), 3 (2-3), 4 (2-4), <u>5, 6, 7, 8, 9, 10</u> 1 (1-1), 2 (1-2), 3 (2-3), 4 (2-4), <u>5, 6, 7, 8</u> (3-6), 9 (3-7), <u>10, 11</u> (3-8), 12 (3-9), 13 (3-10) n/a	1 2 3 4+5 6+7		
		CMS	CM scope	<u>1</u> (TOE CM coverage) <u>2</u> (Parts of the TOE CM coverage) <u>3</u> (Implementation representation CM coverage) <u>4</u> (Problem tracking CM coverage) <u>5</u> (Development tools CM coverage)	<u>1</u> (config list TOE, evidence by SAR), <u>2</u> (unique config items) <u>1</u> (config list TOE, parts, evidence by SAR), <u>2, 3</u> (item developer) <u>1</u> (config list TOE, parts, impl., evidence by SAR), <u>2, 3</u> <u>1</u> (config list TOE, parts, impl., evidence by SAR, docu), <u>2, 3</u> <u>1, 2</u> (1-2), 3 (2-3)	<u>1, 2</u> <u>1, 2</u> (1-2), <u>3</u> <u>1, 2</u> (1-2), 3 (2-3) <u>1, 2</u> (1-2), 3 (2-3)	1 2 3 4	
			DEL	Delivery	<u>1</u> (Delivery procedures)	<u>1</u> (versions distribution), <u>2</u> (procedure use)	<u>1, 2</u>	2-7
			DVS	Development security	<u>1</u> (Identification of security measures) <u>2</u> (Sufficiency of security measures)	<u>1</u> (environment), <u>2</u> (policy sufficiency), <u>3</u> (measure application) <u>1, 2, 3, 4</u>	<u>1, 2, 3</u> n/a	3-5 6+7
		FLR	Flaw remediation	<u>1</u> (Basic flaw remediation) <u>2</u> (Flaw reporting procedures) <u>3</u> (Systematic flaw remediation)	<u>1</u> (track reported flaws), <u>2</u> (flaw description), <u>3</u> (flaw status identification), <u>4</u> (flaw correction identification), <u>5</u> (user information) <u>1, 2, 3, 4, 5, 6</u> (correction requests), <u>7</u> (correction help), <u>8</u> (remediation support), <u>9</u> (no adverse), <u>10</u> (flaw correction) <u>1, 2, 3, 4, 5, 6</u> (developer receive reports), <u>7</u> (reg. user receives report timely), <u>8</u> (autom. distribution), <u>9</u> (ensure flaw correction), <u>10, 11, 12, 13</u> (guidance to register), <u>14</u> (guidance for reports)	<u>1, 2, 3, 4, 5</u> 1 (1-1), 2 (1-2), 3 (1-3), 4 (1-4), 5 (1-5), <u>6, 7, 8, 9, 10</u> 1 (1-1), 2 (1-2), 3 (1-3), 4 (1-4), 5 (1-5), <u>6, 7, 8, 9, 10</u> (2-8), 11 (2-9), 12 (2-10), <u>13, 14</u>		
	LCD		Life-cycle definition	<u>1</u> (Developer defined life-cycle model) <u>2</u> (Measurable life-cycle model)	<u>1</u> (cover maintenance), <u>2</u> (positive contribution) <u>1, 2, 3</u>	<u>1, 2</u> n/a	3-6 7	
	TAT	Tools and techniques	<u>1</u> (Well-defined development tools) <u>2</u> (Compliance with implementation standards) <u>3</u> (Compliance with implementation standards - all parts)	<u>1</u> (well-defined tools), <u>2</u> (impl. statements/conventions), <u>3</u> (impl. options) <u>1, 2, 3, 4</u> (application around aspects) <u>1, 2, 3, 4</u>	<u>1, 2, 3</u> 1 (1-1), 2 (1-2), 3 (1-3), <u>4</u> n/a	4 5 6+7		

Conventions: [DT] Dependency table; WU task colours (*check, examine, other*), EAL4 highlighted in case of multiple components in family.

Abbreviations: beh. (behaviour), enf. (enforcing), ext. (extended), IF (interface), impl (implementation), interf. (interfering), mod. (module), pen (penetration), pot. (potential), req (requirement), s/e (supporting/enforcing), subs. (subsystem), sup. (supporting), vul. (vulnerabilities), doc. (documentation), dep. (dependent), comp. (component).

CLASS	FAMILY	COMPONENT [3]	WU/CEM [4]	NOTES/BSI [5]	EAL	
ADV Development <u>IDI</u>	ARC Security Architecture	<u>1</u>	Security architecture description	<u>1</u> (SFR-enf. abstractions), <u>2</u> (sec. domains), <u>3</u> (init process), <u>4</u> (TSF self-protection), <u>5</u> (SFRs not bypassed)	<u>1, 2, 3, 4, 5</u>	2-7
	FSP Functional specification	<u>1</u>	Basic functional specification	<u>1</u> (purpose s/e TSFI), <u>2</u> (method of use s/e TSFI), <u>3</u> (parameter s/e TSFI), <u>4</u> (non-interf. IF), <u>5</u> (SFR link to TSFI), <u>6</u> (complete SFR instantiation), <u>7</u> (accurate SFR instantiation)	<u>1, 2, 3, 4, 5, 6, 7</u>	1
		<u>2</u>	Security-enforcing functional specification	<u>1</u> (TSF fully repr.), <u>2</u> (TSFI purpose), <u>3</u> (method of use), <u>4</u> (parameter ident.), <u>5</u> (parameter desc.), <u>6</u> (SFR enf. TSFI), <u>7</u> (error msg.), <u>8, 9, 10</u>	<u>1, 2, 3, 4, 5, 6, 7, 8</u> (1-5), 9 (1-6), 10 (1-7)	2
		<u>3</u>	Functional specification with complete summary	<u>1, 2, 3, 4, 5, 6, 7</u> (invocation error msg.), <u>8</u> (s/e actions), <u>9, 10, 11</u>	1 (2-1), 2 (2-2), 3 (2-3), 4 (2-4), 5 (2-5), 6 (2-6), <u>7, 8, 9</u> (1-5), 10 (1-6), 11 (1-7)	3
		<u>4</u>	Complete functional specification	<u>1, 2, 3, 4</u> (TSFI complete), <u>5, 6, 7</u> (all actions), <u>8</u> (invocation error msg), <u>9</u> (error msg. meaning), <u>10, 11, 12</u>	1 (2-1), 2 (2-2), 3 (2-3), <u>4, 5</u> (2-4), 6 (2-5), <u>7, 8, 9, 10</u> (1-5), 11 (1-6), 12 (1-7)	4
		<u>5</u>	Complete semi-formal functional specification with additional error information	<u>1, 2</u> (semiformal style), <u>3, 4, 5, 6, 7, 8, 9, 10, 11</u> (non-invocation error msg), <u>12</u> (non-invocation error msg rational), <u>13, 14, 15</u>	1 (2-1), <u>2, 3</u> (2-2), 4 (2-3), 5 (4-4), 6 (2-4), 7 (2-5), 8 (4-7), 9 (4-8), 10 (4-9), <u>11, 12, 13</u> (1-5), 14 (1-6), 15 (1-7)	5+6
	<u>6</u>	Complete semi-formal functional specification with additional formal specification	n/a	n/a	7	
	IMP Implementation representation	<u>1</u>	Implementation representation of the TSF	<u>1</u> (TSF generation), <u>2</u> (form used by developers), <u>3</u> (mapping design/impl sample)	<u>1, 2, 3</u>	4+5
		<u>2</u>	Complete mapping of the impl. representation of the TSF	n/a	n/a	6+7
	INT TSF internals	<u>1</u>	Well-structured subset of TSF internals	<u>1, 2, 3, 4, 5</u>	n/a	
		<u>2</u>	Well-structured internals	<u>1, 2, 3, 4</u>	<u>1, 2, 3, 4</u>	5
		<u>3</u>	Minimally complex internals	n/a	n/a	6+7
	SPM Security policy modelling	<u>1</u>	Formal TOE security policy model	n/a	n/a	6+7
	TDS TOE design	<u>1</u>	Basic design	<u>1</u> (subs. structure), <u>2</u> (all subs. id.), <u>3</u> (sup./non-interf. subs.), <u>4</u> (compl. SFR enf. subs.), <u>5</u> (subs. interactions), <u>6</u> (TSFI mapping to subs.), <u>7</u> (SFR covered by design), <u>8</u> (SFR instantiation)	<u>1, 2, 3, 4, 5, 6, 7, 8</u>	2
		<u>2</u>	Architectural design	<u>1, 2, 3</u> (non-interf. subs.), <u>4</u> (SFR enf. beh.), <u>5</u> (SFR sup./non-interf. beh.), <u>6</u> (SFR sup. subs.), <u>7</u> (subs. interactions), <u>8, 9, 10</u>	1 (1-1), 2 (1-2), <u>3, 4, 5, 6, 7, 8</u> (1-6), 9 (1-7), 10 (1-8)	3
<u>3</u>		Basic modular design	<u>1</u> (subs. structure), <u>2</u> (TSF mod.), <u>3, 4</u> (TSF subs. roles in SFR enforce.), <u>5</u> (SFR non-interf. subs.), <u>6</u> (subs. interactions), <u>7</u> (complete mod./subs. map), <u>8</u> (accurate mod./subs. map), <u>9</u> (SFR enf. mod. purpose+relationships), <u>10</u> (SFR related params), <u>11</u> (SFR sup./non-interf. mod. categorized), <u>12</u> (sup./non-interf. mod. purposes), <u>13</u> (sup./non-interf. mod. interact), <u>14</u> (TSFI map to mod.), <u>15, 16</u>	<u>1, 2, 3</u> (1-2), <u>4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15</u> (1-7), 16 (1-8)	4	
<u>4</u>		Semiformal modular design	<u>1, 2, 3</u> (TSF mod. id.), <u>4, 5</u> (semif. notation def/ref), <u>6, 7, 8, 9, 10, 11</u> (s/e mod. purpose+relationships), <u>12</u> (s/e mod. params), <u>13</u> (non-interf. mod. categorized), <u>14</u> (non-interf. mod. purposes), <u>15</u> (non-interf. mod. interactions), <u>16, 17, 18</u>	1 (3-1), 2 (3-2), <u>3, 4</u> (1-2), <u>5, 6</u> (3-4), 7 (3-5), 8 (3-6), 9 (3-7), 10 (3-8), <u>11, 12, 13, 14, 15, 16</u> (3-14), 17 (1-7), 18 (1-8)	5	
<u>5</u>		Complete semiformal modular design	n/a	n/a	6	
<u>6</u>	Complete semiformal modular design with formal high-level design present.	n/a	n/a	7		
AGD Guidance <u>IDI</u>	OPE Operational user guidance	<u>1</u>	Operational user guidance	<u>1</u> (functions and privileges), <u>2</u> (IF use), <u>3</u> (parameter), <u>4</u> (events), <u>5</u> (operation modes), <u>6</u> (measures/role), <u>7</u> (clear), <u>8</u> (reasonable)	<u>1, 2, 3, 4, 5, 6, 7, 8</u>	1-7
	PRE Preparative procedures	<u>1</u>	Preparative procedures	<u>1</u> (delivery procedure), <u>2</u> (installation steps), <u>3</u> (preparation)	<u>1, 2, 3</u>	1-7

Conventions: IDI Dependency table; WU task colours (*check, examine, other*), EAL4 highlighted in case of multiple components in family.

Abbreviations: beh. (behaviour), enf. (enforcing), ext. (extended), IF (interface), impl (implementation), interf. (interfering), mod. (module), pen (penetration), pot. (potential), req (requirement), s/e (supporting/enforcing), subs. (subsystem), sup. (supporting), vul. (vulnerabilities), doc. (documentation), dep. (dependent), comp. (component).

CLASS	FAMILY	COMPONENT [3]	WU/CEM [4]	NOTES/BSI [5]	EAL
ATE Tests [DT]	COV Coverage	1 Evidence of coverage	1 (test docu/TSFI correspondence)	1	2
		2 Analysis of coverage	1 (test docu/TSFI correspondence), 2 (test plan IF approach demonstrative), 3 (test adequate), 4 (func. spec interface and test docu complete)	1, 2, 3, 4	3-5
		3 Rigorous analysis of coverage	n/a	n/a	6+7
	DPT Depth	1 Testing: basic design	1 (test docu incl. TSF subs. beh.+interactions), 2 (beh. tests for all subs. beh.), 3 (beh. test for subs. interactions), 4 (all subs. beh.+interactions tested)	1, 2, 3, 4	3+4
		2 Testing: security enforcing modules	1, 2, 3, 4 (SFR-enf. mod. IF in test docu), 5 (test approach demo. SFR-enf. mod. IF beh), 6, 7 (all SFR-enf. mod. IF tested)	1 (1-1), 2 (1-2), 3 (1-3), 4, 5, 6 (1-4), 7	
		3 Testing: modular design	1, 2, 3, 4 (TSF mod. IF in test docu), 5 (test approach demo. TSF mod. IF beh), 6, 7 (all TSF mod. IF tested)	1 (1-1), 2 (1-2), 3 (1-3), 4, 5, 6 (1-4), 7	5+6
		4 Testing: implementation representation	n/a	n/a	7
	FUN Functional tests	1 Functional testing	1 (testplan+results incl.), 2 (test run scenario), 3 (ST/test-config consistent), 4 (order dependencies), 5 (expected test results), 6 (actual/expected test results consistent), 7 (developer test effort)	1, 2, 3, 4, 5, 6, 7	2-5
		2 Ordered functional testing	n/a	n/a	6+7
	IND Independent testing	1 Independent testing - conformance	1 (config consistent with ST), 2 (proper installation), 3 (create test subset), 4 (produce test subset docu), 5 (run test subset), 6 (record test info), 7 (actual/expected test results), 8 (report test effort)	1, 2, 3, 4, 5, 6, 7, 8	1
2 Independent testing - sample		1, 2, 3 (use of resources), 4 (run developer test samples), 5 (act/exp test results), 6, 7, 8, 9, 10, 11 (evaluator test effort)	1 (1-1), 2 (1-2), 3, 4, 5, 6 (1-3), 7 (1-4), 8 (1-5), 9 (1-6), 10 (1-7), 11	2-6	
3 Independent testing - complete		n/a	n/a	7	

AVA Vulnerability [DT]	VAN Vulnerability analysis	1 Vulnerability survey	1 (config consistent with ST), 2 (proper installation), 3 (public pot. vul.), 4 (pot.vul. test candidates), 5 (create pen. tests), 6 (produce pen. test docu), 7 (run pen. tests), 8 (record test results), 9 (evaluator pen. test effort), 10 (results wrt. "basic" attack), 11 (report vul.)	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11	1
		2 Vulnerability analysis	1, 2, 3 (public pot. vul.), 4 (search pot. vul.), 5, 6 (create search-based pen tests), 7, 8, 9, 10, 11, 12	1 (1-1), 2 (1-2), 3, 4, 5 (1-4), 6, 7 (1-6), 8 (1-7), 9 (1-8), 10 (1-9), 11 (1-10), 12 (1-11)	2+3
		3 Focused vulnerability analysis	1, 2, 3 (public pot. vul.), 4 (search pot. vul.), 5, 6 (create search-based pen tests), 7, 8, 9, 10, 11 (results wrt. "enhanced" attack), 12	1 (1-1), 2 (1-2), 3, 4, 5 (1-4), 6, 7 (1-6), 8 (1-7), 9 (1-8), 10 (1-9), 11, 12 (1-11)	4
		4 Methodical vulnerability analysis	1, 2, 3, 4 (analyse pot. vul.), 5, 6 (create search-based pen tests), 7, 8, 9, 10, 11 (results wrt. "moderate" attack), 12	1 (1-1), 2 (1-2), 3 (3-3), 4, 5 (1-4), 6, 7 (1-6), 8 (1-7), 9 (1-8), 10 (1-9), 11, 12 (1-11)	5
		5 Advanced methodical vulnerability analysis	n/a	n/a	6+7

ACO Composition [DT]	COR Composition rationale	1 Composition rationale	1 (identify IF), 2 (TSF IF considered), 3 (assurance measures)		
	DEV Development evidence	1 Functional Description	1 (IF purposes), 2 (IF correspondence), 3 (IF description)		
		2 Basic evidence of design	1 (1-1), 2 (IF usage), 3 (comp. beh.), 4 (1-2), 5 (1-3)		
		3 Detailed evidence of design	1 (1-1), 2 (2-1), 3 (identify subs. IF), 4 (subs. comp. beh.), 5 (IF/subs. correspondence), 6 (1-2), 7 (1-3)		
	REL Reliance of dependent comp.	1 Basic reliance information	1 (TSF HW/firmware/SW), 2 (OE objectives), 3 (comp. interactions), 4 (TSF protection)		
		2 Reliance information	1 (1-1), 2 (1-2), 3 (1-3), 4 (interaction IF/return value), 5 (1-4)		
CTT Composed TOE testing	1 Interface testing	1 (composed test doc.), 2 (base IF test doc.), 3 (demo TSF beh.), 4 (demo base comp. IF), 5 (proper install), 6 (equiv. resources), 7 (verify SFR subset test), 8 (confirm TSF SFR subset test)		n/a	n/a
	2 Rigorous interface testing	1 (1-1), 2 (1-2), 3 (test doc. wrt. composed ST), 4 (1-3), 5 (test rely dep. comp. spec), 6 (test rely dep. comp. beh.), 7 (1-5), 8 (1-6), 9 (test selection), 10 (1-8), 11 (confirm IF subset test)			
VUL Composition vulnerability analysis	1 Composition vulnerability review	1 (proper install), 2 (config. fulfil STs), 3 (vul. from base), 4 (vul. from dep. comp.), 5 (public info about base), 6 (public info about dep. comp.), 7 (record pot. vul.), 8 (conduct pen test)			
	2 Composition vulnerability analysis	1 (1-1), 2 (1-2), 3 (1-3), 4 (1-4), 5 (1-5), 6 (1-6), 7 (1-7), 8 (conduct ST/doc./info/rationale on pot. vul.), 9 (1-8)			
	3 Enhanced-Basic Composition vulnerability analysis	1 (1-1), 2 (1-2), 3 (1-3), 4 (1-4), 5 (1-5), 6 (1-6), 7 (1-7), 8 (2-8), 9 (2-9)			

Conventions: [\[DT\]](#) Dependency table; WU task colours (*check, examine, other*), EAL4 highlighted in case of multiple components in family.

Abbreviations: beh. (behaviour), enf. (enforcing), ext. (extended), IF (interface), impl (implementation), interf. (interfering), mod. (module), pen (penetration), pot. (potential), req (requirement), s/e (supporting/enforcing), subs. (subsystem), sup. (supporting), vul. (vulnerabilities), doc. (documentation), dep. (dependent), comp. (component).

CLASS	FAMILY	COMPONENT [3]	WU/CEM [4]	NOTES/BSI [5]	CR	
APE PP evaluation [DT]	INT	PP introduction	1 PP introduction	1 (PP reference/TOE overview), 2 (PP reference), 3 (TOE usage/sec features), 4 (TOE type), 5 (non-TOE)	1, 2, 3, 4, 5	1
	CCL	Conformance claims	1 Conformance claims	1 (CC version), 2 ([2] extension), 3 ([3] extension), 4 (extended SFR), 5 (extended SAR), 6 (PP claim), 7 (package claim), 8 (package names), 9 (PP TOE type), 10 (PP SPD), 11 (PP sec objectives), 12 (PP SFRs), 13 (PP conf. statement)	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	1
	SPD	Security problem definition	1 Security problem definition	1 (threats), 2 (threat description), 3 (OSPs), 4 (OE assumptions)	1, 2, 3, 4	1
	OBJ	Security objectives	1 Security objectives for the OE 2 Security objectives	1 (OE sec objectives) 1 (TOE+OE sec objectives), 2 (TOE obj. to threats/OSPs), 3 (OE obj. to OSPs+assumptions), 4 (counter threats), 5 (enforce OSPs), 6 (OE assumptions)	1 1, 2, 3, 4, 5, 6	1 2
	ECD	Extended components definition	1 Extended components definition	1 (non-ext. req in [2]/[3]), 2 (ext. req. covered), 3 (CC taxonomy), 4 (dependencies), 5 ([2] comp model), 6 ([2] family model), 7 ([2] class model), 8 ([3] comp model), 9 (SAR method), 10 ([3] family model), 11 ([3] class model), 12 (measurable elements), 13 (no existing comp)	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	1
	REQ	Security requirements	1 Stated security requirements 2 Derived security requirements	1 (SFRs), 2 (SARs), 3 (terms defined), 4 (operations), 5 (assignments), 6 (iterations), 7 (selections), 8 (refinements), 9 (dependencies), 10 (consistency) 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 (trace to objective), 11 (meet objectives), 12 (SAR justification), 13	1, 2, 3, 4, 5, 6, 7, 8, 9, 10 1 (1-1), 2 (1-2), 3 (1-3), 4 (1-4), 5 (1-5), 6 (1-6), 7 (1-7), 8 (1-8), 9 (1-9), 10, 11, 12, 13 (1-10)	1 2

ACE PP configuration [DT]	INT	Introduction	1 PP-Module introduction	APE_INT(1-1...1-5), 1 (identify Base-PP), 2 (TOE overview diffs),	n/a	n/a
	CCL	Conformance claim	1 PP-Module conformance claims	1 (CC version), 2 ([2] extension), 3 (SFR packages), 4 (extended SFR)		
	SPD	Security problem definition	1 PP-Module security problem definition (= APE_SPD.1)	APE_SPD(1-1...1-4)		
	OBJ	Security objectives	1 PP-Module security objectives (= APE_OBJ.2)	APE_OBJ(2-1...2-6)		
	ECD	Extended components def.	1 PP-Module extended components definition	APE_ECD(1-1...1-12)		
	REQ	Security requirements	1 PP-Module security requirements	APE_REQ(2-1...2-13; w/o SAR part)		
	MCO	Consistency	1 PP-Module consistency	1 (rationale TOE type), 2 (rationale SDP), 3 (rationale security objectives), 4 (rationale SFRs)		
CCO	Conf. consistency	1 PP-Configuration consistency	1 (PP-Configuration ref), 2 (unique PPs and PP-Modules), 3 (kind of conformity), 4 (SAR statement), 5 (Base-PP included), 6 (components consistent)			

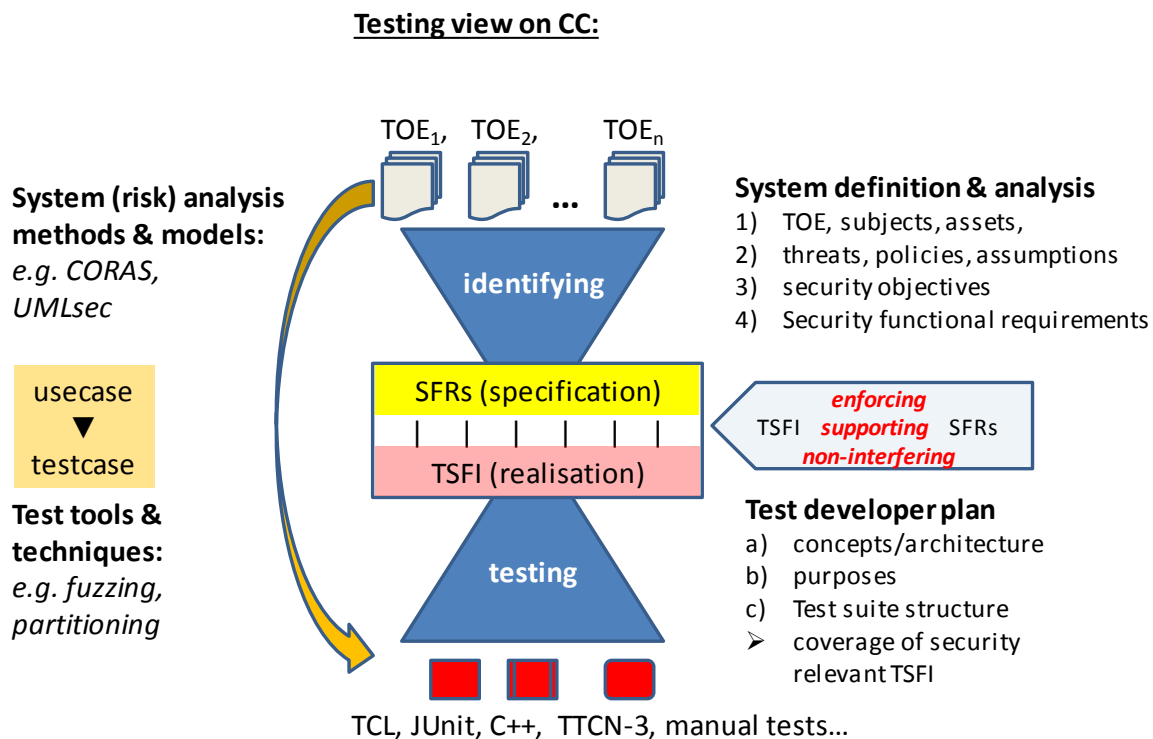
3. Evaluation Assurance Levels (EALs)

EAL7	INT1	CCL1	SPD1	OBJ2	ECD1	REQ2	TSS1	CMC5	CMS5	DEL1	DVS2	(FLR)	LCD2	TAT3	ARC1	FSP6	IMP2	INT3	SPM1	TDS6	OPE1	PRE1	COV3	DPT4	FUN2	IND3	VAN5	EAL7
EAL6	INT1	CCL1	SPD1	OBJ2	ECD1	REQ2	TSS1	CMC5	CMS5	DEL1	DVS2		LCD1	TAT3	ARC1	FSP5	IMP2	INT3	SPM1	TDS5	OPE1	PRE1	COV3	DPT3	FUN2	IND2	VAN5	EAL6
EAL5	INT1	CCL1	SPD1	OBJ2	ECD1	REQ2	TSS1	CMC4	CMS5	DEL1	DVS1		LCD1	TAT2	ARC1	FSP5	IMP1	INT2		TDS4	OPE1	PRE1	COV2	DPT3	FUN1	IND2	VAN4	EAL5
EAL4	INT1	CCL1	SPD1	OBJ2	ECD1	REQ2	TSS1	CMC4	CMS4	DEL1	DVS1		LCD1	TAT1	ARC1	FSP4	IMP1			TDS3	OPE1	PRE1	COV2	DPT1	FUN1	IND2	VAN3	EAL4
EAL3	INT1	CCL1	SPD1	OBJ2	ECD1	REQ2	TSS1	CMC3	CMS3	DEL1	DVS1		LCD1		ARC1	FSP3				TDS2	OPE1	PRE1	COV2	DPT1	FUN1	IND2	VAN2	EAL3
EAL2	INT1	CCL1	SPD1	OBJ2	ECD1	REQ2	TSS1	CMC2	CMS2	DEL1					ARC1	FSP2				TDS1	OPE1	PRE1	COV1		FUN1	IND2	VAN2	EAL2
EAL1	INT1	CCL1		OBJ1	ECD1	REQ1	TSS1	CMC1	CMS1							FSP1					OPE1	PRE1				IND1	VAN1	EAL1
	ASE				ALC				ADV				AGD		ATE			AVA										

Conventions: **[DT]** Dependency table; WU task colours (*check, examine, other*), EAL4 highlighted in case of multiple components in family.

Abbreviations: beh. (behaviour), enf. (enforcing), ext. (extended), IF (interface), impl (implementation), interf. (interfering), mod. (module), pen (penetration), pot. (potential), req (requirement), s/e (supporting/enforcing), subs. (subsystem), sup. (supporting), vul. (vulnerabilities), doc. (documentation), dep. (dependent), comp. (component).

4. Further Information



NOTES:

This Quick Reference Card summarizes Common Criteria components to support users. The document is not part of a standard, not warranted to be error-free, and a 'work in progress'. For comments or suggestions, please contact the editors via ccQRC@school-of-technology.de.