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

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	1 *level*, **evt**, 2 **inf**
			2	User identity association	1
	SAA	Security audit analysis	1	Potential violation analysis	1, 2 **evt**, **rules**
			2	Profile based anomaly detection	1 **profile**, 2, 3 **con**
			3	Simple attack heuristics	1 **violation-evt**, 2 **activity-inf**, 3
			- 4	Complex attack heuristics	1 **penetration-evt**, **indicator-evt**, 2 **inf**, 3
	SAR	Security audit review	1	Audit review	1 **usr**, **inf**, 2
			2	Restricted audit review	1
			3	Selectable audit review	1 **methods**, **criteria**
	SEL	Security audit event selection	1	Selective audit	1 *att*, **att**
	STG	Security audit event storage	1	Protected audit trail storage	1, 2 *ability*
			- 2	Guarantees of audit data availability	1, 2 *ability*, 3 **metric**, *con*
			3	Action in case of possible audit data loss	1 **act**, **lim**
			- 4	Prevention of audit data loss	1 *act*, **act**
FCO Communication [DT]	NRO	Non-repudiation of origin	1	Selective proof of origin	1 **inf-type**, *role*(3rdParty), 2 **att**, **inf-fields**, 3 *role*(3rdParty), **lim**
			- 2	Enforced proof of origin	1 **inf-type**, 2 **att, inf-fields**, 3 *role*(3rdParty), **lim**
	NRR	Non-repudiation of receipt	1	Selective proof of receipt	1 **inf-type**, *role*(3rdParty), 2 **att**, **inf-fields**, 3 *role*(3rdParty), **lim**
			- 2	Enforced proof of receipt	1 **inf-type**, 2 **att**, **inf-fields**, 3 *role*(3rdParty), **lim**
FCS Cryptographic support [DT]	CKM	Cryptographic key management	1	Cryptographic key generation	1 **algor.**, **keysize**, **standard**
			2	Cryptographic key distribution	1 **keysize**, **standard**
			3	Cryptographic key access	1 **type**, **method**, **standard**
			4	Cryptographic key destruction	1 **method**, **standard**
	COP	Cryptographic opr.	1	Cryptographic operation	1 **opr**, **algor.**, **keysize**, **standard**
FDP User Data Protection [DT]	ACC	Access control policy	1	Subset access control	1 **pol**, **sub/obj/opr**
			- 2	Complete access control	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	1 **obj/inf-types**, 2 **sub**
			2	Data Authentication with Identity of Guarantor	1 **obj/inf-types**, 2 **sub**
	ETC	Export from the TOE	1	Export of user data without security att	1 **pol**, 2
			2	Export of user data with security attributes	1 **pol**, 2, 3, 4 **rules**
	IFC	Information flow control policy	1	Subset information flow control	1 **pol**, **sub/inf/opr**
			- 2	Complete information flow control	1 **sub/inf**, 2
	IFF	Information flow control functions	1	Simple security attributes	1 **sub/inf/att**, 2 **flow-rule**, 3 **add.-rule**, 4 **auth-rules**, 5 **deny-rules**
			- 2	Hierarchical security attributes	1 **sub/inf/att**, 2 **opr-relations**, 3 **rules**, 4 **auth-rules**, 5 **deny-rules**, 6
			3	Limited illicit information flows	1 **flow-types**, **capacity**
			- 4	Partial elimination of illicit information flows	1 **pol**, **flow-types**, **capacity**, 2 **flow-types**
			5	No illicit information flows	1 **pol -name**
			6	Illicit information flow monitoring	1 **pol**, **flow-types**, **capacity**
	ITC	Import from outside of the TOE	1	Import of user data without security att.	1 **pol**, 2, 3 **rules**
			2	Import of user data with security attributes	1 **pol**, 2, 3, 4, 5 **rules**
	ITT	Internal TOE transfer	1	Basic internal transfer protection	1 **pol**, *evt*
			- 2	Transmission separation by attribute	1 **access- pol**, *evt*, 2 **att**
			3	Integrity monitoring	1 **pol**, **err**, 2 **act**
			- 4	Attribute-based integrity monitoring	1 **pol**, **err**, **att**, 2 **act**
	RIP	Residual information protection	1	Subset residual information protection	1 *act*, **obj**
			- 2	Full residual information protection	2 *act*
	ROL	Rollback	1	Basic rollback	1 **pol**, **opr**, 2 **lim**
			- 2	Advanced rollback	1 **pol**, **opr**, 2 **lim**
	SDI	Stored data integrity	1	Stored data integrity monitoring	1 **err**, **att**
			- 2	Stored data integrity monitoring and action	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	1 **pol**, *act*, *act* 2 *act*
			2	Source data exchange recovery	1 **pol**, **err**
			- 3	Destination data exchange recovery	1 **pol**, **err**
FIA Identification and authentification [DT]	AFL	Authentication failures	1	Authentication failure handling	1 **num/range**, **evt**, 2 *evt*, **act**
	ATD	User att. definition	1	User attribute definition	1 **att**
	SOS	Specification of secrets	1	Verification of secrets	1 **metric**
			2	TSF Generation of secrets	1 **metric**, 2 **fct**
	UAU	User authentication	1	Timing of authentication	1 **act**, 2
			- 2	User authentication before any action	1
			3	Unforgeable authentication	1 *act*, 2 *act*
			4	Single-use authentication mechanisms	1 **mechanism**
			5	Multiple authentication mechanisms	1 **mechanism**, 2 **rules**
			6	Re-authenticating	1 **con**
			7	Protected authentication feedback	1 **feedback**
	UID	User identification	1	Timing of identification	1 **act**, 2
			- 2	User identification before any action	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**
			2	Secure security attributes	1 **att**
			3	Static attribute initialisation	1 **pol**, *act*(opr), 2 **role**
			4	Security attribute value inheritance	1 **value-setting-rules**
	MTD	Management of TSF data	1	Management of TSF data	1 *act*(opr), **data**, **roles**
			2	Management of limits on TSF data	1 **data**, **roles**, 2 **act**
			3	Secure TSF data	1 **data**
	REV	Revocation	1	Revocation	1 **att**, *groups*(resources), **roles**, 2 **rules**
	SAE	Security attribute expiration	1	Time-limited authorisation	1 **att**, **roles**, 2 **act**
	SMF	Specification of Management fct.	1	Specification of Management Functions	1 **fct**
	SMR	Security management roles	1	Security roles	1 **roles**, 2
			- 2	Restrictions on security roles	1 **roles**, 2, 3 **con**
			3	Assuming roles	1 **roles**
FPR Privacy [DT]	**ANO**	Anonymity	1	Anonymity	1 **u/s**, **sub/opr/obj**
			- 2	Anonymity without soliciting information	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**
			- 2	Reversible pseudonymity	1 **u/s**, **sub/opr/obj**, 2 **num**, **sub**, 3 *opr*, **metric**, 4 *usr*(resources), **con**
			- 3	Alias pseudonymity	1 **u/s**, **sub/opr/obj**, 2 **num**, **sub**, 3 *opr*, **metric**, 4 **con**
	UNL	Unlinkability	1	Unlinkability	1 **u/s**, **opr**, *cause*(relations)
	UNO	Unobservability	1	Unobservability	1 **u/s**, **opr**, **obj**, **usr/sub**
			- 2	Allocation of information impacting unobservability	1 **inf**, 2 **con**
			3	Unobservability without soliciting information	1 **service**, **sub**, **inf**
			4	Authorised user observability	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	1 **metric**, 2 **act**
			- 2	Inter-TSF detection and correction of modification	1 **metric**, 2 **act**, 3 **mod-type**
	ITT	Internal TOE TSF data transfer	1	Basic internal TSF data transfer protection	1 *opr*
			- 2	TSF data transfer separation	1 *opr*, 2
			3	TSF data integrity monitoring	1 *evt*(err), 2 **act**
	PHP	TSF physical protection	1	Passive detection of physical attack	1, 2
			- 2	Notification of physical attack	1, 2, 3 **device/element**, **usr/role**
			3	Resistance to physical attack	1 **scenarios**, **device/element**
	RCV	Trusted recovery	1	Manual recovery	1 **failures**
			- 2	Automated recovery	1 **failures**, 2 **failures**
			-- 3	Automated recovery without undue loss	1 **failures**, 2 **failures**, 3 **quantification**, 4
			4	Function recovery	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**
			- 2	Limited fault tolerance	1 **failure-types**
	PRS	Priority of service	1	Limited priority of service	1, 2 **resourses**
			- 2	Full priority of service	1, 2
	RSA	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**
			- 2	Per user attribute limitation on multiple concurrent sessions	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	TSF-initiated termination	1 **time-interval**
			4	User-initiated termination	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 evaluation [DT]	**INT**	ST introduction	1	ST introduction	1 (*ST content*), 2 (**ST reference**), 3 (**TOE ref id**), 4 (**TOE ref not misleading**), 5 (**sec features**), 6 (**TOE type**), 7 (**type not misleading**), 8 (**non-TOE**), 9 (**physical scope**), 10 (**logical scope**), 11 (**consistency**)	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11	1-7
	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**)	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12	1-7
	SPD	Security problem definition	1	Security problem definition	1 (*threats*), 2 (**threat description**), 3 (**OSPs**), 4 (**OE assumptions**)	1, 2, 3, 4	2-7
	OBJ	Security objectives	1	Security objectives for the OE	1 (*OE sec objectives*)	1	1
			2	Security 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, 2, 3, 4, 5, 6	2-7
	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	1-7
	REQ	Security requirements	1	Stated 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	1
			2	Derived security requirements	1, 2, 3, 4, 5, 6, 7, 8, 9, 10 (*trace to objective*), 11 (**meet objectives**), 12 (*SAR justification*), 13	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*)	2-7
	TSS	TOE summary specification	1	TOE summary specification (TSS)	1 (**TOE meets SFRs**), 2 (**consistency with overview/description**)	1, 2	1-7
			2	TSS with architect. design summary	1, 2, 3, 4	n/a	
ALC Life-cycle [DT]	**CMC**	CM capabilities	1	Labelling of the TOE	1 (*unique label*), 2 (*consistent references*)	1, 2	1
			2	Use of a CM system	1, 2, 3 (**unique config ids**), 4 (**consistent ids**)	1 (*1-1*), 2 (*1-2*), 3, 4	2
			3	Authorisation controls	1, 2, 3, 4, 5 (**CM access**), 6 (*CM plan*), 7 (**CM use**), 8 (*config maintenance*), 9 (*CM records*), 10 (**CM operation**)	1 (*1-1*), 2 (*1-2*), 3 (*2-3*), 4 (*2-4*), 5, 6, 7, 8, 9, 10	3
			4	Production support, acceptance procedures and automation	1, 2, 3, 4, 5 (**CM access control**), 6 (*automated production*), 7 (**effective production**), 8, 9, 10 (**config modification**), 11, 12, 13	1 (*1-1*), 2 (*1-2*), 3 (*2-3*), 4 (*2-4*), 5, 6, 7, 8 (*3-6*), 9 (*3-7*), 10, 11 (*3-8*), 12 (*3-9*), 13 (*3-10*)	4+5
			5	Advanced support	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20	n/a	6+7
	CMS	CM scope	1	TOE CM coverage	1 (*config list TOE, evidence by SAR*), 2 (**unique config items**)	1, 2	1
			2	Parts of the TOE CM coverage	1 (*config list TOE, parts, evidence by SAR*), 2, 3 (*item developer*)	1, 2 (*1-2*), 3	2
			3	Implementation representation CM coverage	1 (*config list TOE, parts, impl., evidence by SAR*), 2, 3	1, 2 (*1-2*), 3 (*2-3*)	3
			4	Problem tracking CM coverage	1 (*config list TOE, parts, impl., evidence by SAR, docu*), 2, 3	1, 2 (*1-2*), 3 (*2-3*)	4
			5	Development tools CM coverage	1 (*config list TOE, parts, impl., evidence by SAR, docu, tools*), 2, 3	1, 2 (*1-2*), 3 (*2-3*)	5-7
	DEL	Delivery	1	Delivery procedures	1 (**versions distribution**), 2 (**procedure use**)	1, 2	2-7
	DVS	Development security	1	Identification of security measures	1 (**environment**), 2 (**policy sufficiency**), 3 (**measure application**)	1, 2, 3	3-5
			2	Sufficiency of security measures	1, 2, 3, 4	n/a	6+7
	FLR	Flaw remediation	1	Basic flaw remediation	1 (**track reported flaws**), 2 (**flaw description**), 3 (**flaw status identification**), 4 (*flaw correction identification*), 5 (**user information**)	1, 2, 3, 4, 5	
			2	Flaw reporting procedures	1, 2, 3, 4, 5, 6 (**correction requests**), 7 (**correction help**), 8 (**remediation support**), 9 (**no adverse**), 10 (**flaw correction**)	1 (*1-1*), 2 (*1-2*), 3 (*1-3*), 4 (*1-4*), 5 (*1-5*), 6, 7, 8, 9, 10	
			3	Systematic flaw remediation	1, 2, 3, 4, 5, 6 (**developer receive reports**), 7 (**reg. user receives report timely**), 8 (**autom. distribution**), 9 (**ensure flaw correction**), 10, 11, 12, 13 (**guidance to register**), 14 (**guidance for reports**)	1 (*1-1*), 2 (*1-2*), 3 (*1-3*), 4 (*1-4*), 5 (*1-5*), 6, 7, 8, 9, 10 (*2-8*), 11 (*2-9*), 12 (*2-10*), 13, 14	
	LCD	Life-cycle definition	1	Developer defined life-cycle model	1 (**cover maintenance**), 2 (**positive contribution**)	1, 2	3-6
			2	Measurable life-cycle model	1, 2, 3	n/a	7
	TAT	Tools and techniques	1	Well-defined development tools	1 (**well-defined tools**), 2 (**impl. statements/conventions**), 3 (**impl. options**)	1, 2, 3	4
			2	Compliance with implementation standards	1, 2, 3, 4 (**application around aspects**)	1 (*1-1*), 2 (*1-2*), 3 (*1-3*), 4	5
			3	Compliance with implementation standards - all parts	1, 2, 3, 4	n/a	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 [DT]	**ARC** Security Architecture	1 Security architecture description	1 (**SFR-enf. abstractions**), 2 (**sec. domains**), 3 (**init process**), 4 (**TSF self-protection**), 5 (**SFRs not bypassed**)	1, 2, 3, 4, 5	2-7
	FSP Functional specification	1 Basic functional specification	1 (**purpose s/e TSFI**), 2 (**method of use s/e TSFI**), 3 (**parameter s/e TSFI**), 4 (**non-interf. IF**), 5 (*SFR link to TSFI*), 6 (**complete SFR instantiation**), 7 (**accurate SFR instantiation**)	1, 2, 3, 4, 5, 6, 7	1
		2 Security-enforcing functional specification	1 (**TSF fully repr.**), 2 (**TSFI purpose**), 3 (**method of use**), 4 (**parameter ident.**), 5 (**parameter desc.**), 6 (**SFR enf. TSFI**), 7 (**error msg.**), 8, 9, 10	1, 2, 3, 4, 5, 6, 7, 8 (*1-5*), 9 (*1-6*), 10 (*1-7*)	2
		3 Functional specification with complete summary	1, 2, 3, 4, 5, 6, 7 (**invocation error msg.**), 8 (**s/e actions**), 9, 10, 11	1 (*2-1*), 2 (*2-2*), 3 (*2-3*), 4 (*2-4*), 5 (*2-5*), 6 (*2-6*), 7, 8, 9 (*1-5*), 10 (*1-6*), 11 (*1-7*)	3
		4 Complete functional specification	1, 2, 3, 4 (**TSFI complete**), 5, 6, 7 (**all actions**), 8 (**invocation error msg**), 9 (**error msg. meaning**), 10, 11, 12	1 (*2-1*), 2 (*2-2*), 3 (*2-3*), 4, 5 (*2-4*), 6 (*2-5*), 7, 8, 9, 10 (*1-5*), 11 (*1-6*), 12 (*1-7*)	4
		5 Complete semi-formal functional specification with additional error information	1, 2 (**semiformal style**), 3, 4, 5, 6, 7, 8, 9, 10, 11 (**non-invocation error msg**), 12 (**non-invocation error msg rational**), 13, 14, 15	1 (*2-1*), 2, 3 (*2-2*), 4 (*2-3*), 5 (*4-4*), 6 (*2-4*), 7 (*2-5*), 8 (*4-7*), 9 (*4-8*), 10 (*4-9*), 11, 12, 13 (*1-5*), 14 (*1-6*), 15 (*1-7*)	5+6
		6 Complete semi-formal functional specification with additional formal specification	n/a	n/a	7
	IMP Implementation representation	1 Implementation representation of the TSF	1 (*TSF generation*), 2 (*form used by developers*), 3 (**mapping design/impl sample**)	1, 2, 3	4+5
		2 Complete mapping of the impl. representation of the TSF	n/a	n/a	6+7
	INT TSF internals	1 Well-structured subset of TSF internals	1, 2, 3, 4, 5	n/a	
		2 Well-structured internals	1, 2, 3, 4	1, 2, 3, 4	5
		3 Minimally complex internals	n/a	n/a	6+7
	SPM Security policy modelling	1 Formal TOE security policy model	n/a	n/a	6+7
	TDS TOE design	1 Basic design	1 (**subs. structure**), 2 (**all subs. id.**), 3 (**sup./non-interf. subs.**), 4 (**compl. SFR enf. subs.**), 5 (**subs. interactions**), 6 (**TSFI mapping to subs.**), 7 (**SFR covered by design**), 8 (**SFR instantiation**)	1, 2, 3, 4, 5, 6, 7, 8	2
		2 Architectural design	1, 2, 3 (**non-interf. subs.**), 4 (**SFR enf. beh.**), 5 (**SFR sup./non-interf. beh.**), 6 (**SFR sup. subs.**), 7 (**subs. interactions**), 8, 9, 10	1 (*1-1*), 2 (*1-2*), 3, 4, 5, 6, 7, 8 (*1-6*), 9 (*1-7*), 10 (*1-8*)	3
		3 Basic modular design	1 (**subs. structure**), 2 (**TSF mod.**), 3, 4 (**TSF subs. roles in SFR enforce.**), 5 (**SFR non-interf. subs.**), 6 (**subs. interactions**), 7 (**complete mod./subs. map**), 8 (**accurate mod./subs. map**), 9 (**SFR enf. mod. purpose+relationships**), 10 (**SFR related params**), 11 (**SFR sup./non-interf. mod. categorized**), 12 (**sup./non-interf. mod. purposes**), 13 (**sup./non-interf. mod. interact**), 14 (**TSFI map to mod.**), 15, 16	1, 2, 3 (*1-2*), 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15 (*1-7*), 16 (*1-8*)	4
		4 Semiformal modular design	1, 2, 3 (*TSF mod. id.*), 4, 5 (**semif. notation def/ref**), 6, 7, 8, 9, 10, 11 (**s/e mod. purpose+relationships**), 12 (**s/e mod. params**), 13 (**non-interf. mod. categorized**), 14 (**non-interf. mod. purposes**), 15 (**non-interf. mod. interactions**), 16, 17, 18	1 (*3-1*), 2 (*3-2*), 3, 4 (*1-2*), 5, 6 (*3-4*), 7 (*3-5*), 8 (*3-6*), 9 (*3-7*), 10 (*3-8*), 11, 12, 13, 14, 15, 16 (*3-14*), 17 (*1-7*), 18 (*1-8*)	5
		5 Complete semiformal modular design	n/a	n/a	6
		6 Complete semiformal modular design with formal high-level design present.	n/a	n/a	7

CLASS	FAMILY	COMPONENT [3]	WU/CEM [4]	NOTES/BSI [5]	EAL
AGD Guidance [DT]	**OPE** Operational user guidance	1 Operational user guidance	1 (**functions and privileges**), 2 (**IF use**), 3 (**parameter**), 4 (**events**), 5 (**operation modes**), 6 (**measures/role**), 7 (**clear**), 8 (**reasonable**)	1, 2, 3, 4, 5, 6, 7, 8	1-7
	PRE Preparative procedures	1 Preparative procedures	1 (**delivery procedure**), 2 (**installation steps**), 3 (***preparation***)	1, 2, 3	1-7

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
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**)	n/a	n/a
	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***)		
			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	1 (*OE sec objectives*)	1	1
			2	Security 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, 2, 3, 4, 5, 6	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	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	1
			2	Derived security requirements	1, 2, 3, 4, 5, 6, 7, 8, 9, 10 (*trace to objective*), 11 (**meet objectives**), 12 (*SAR justification*), 13	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*)	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)

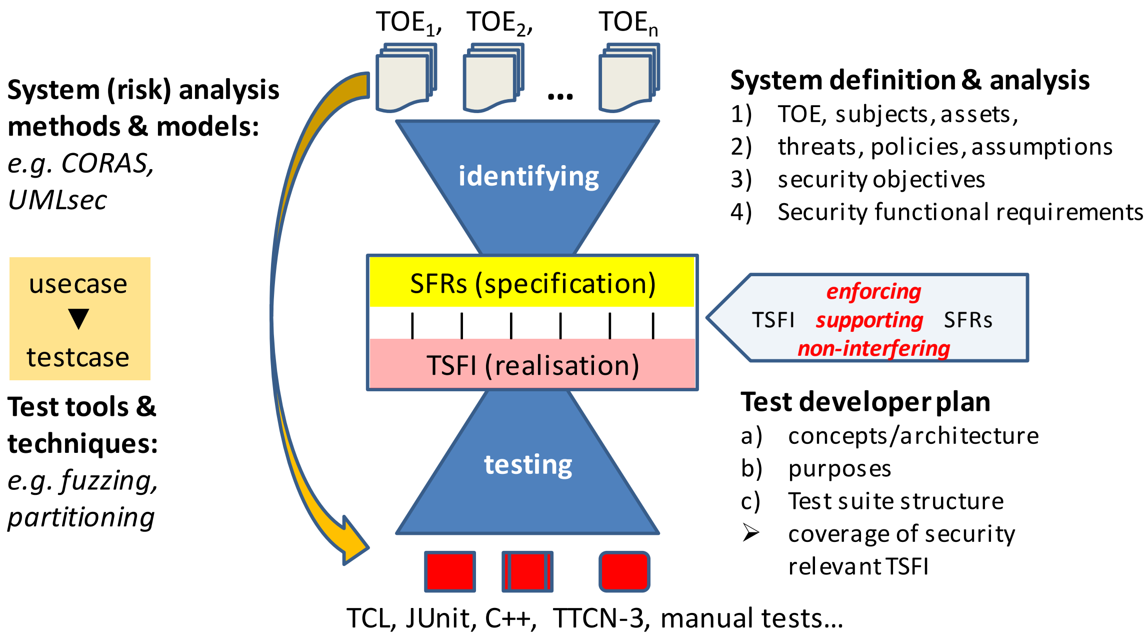
EAL7	INT1	CCL1	SPD1	OBJ2	ECD1	REQ2	TSS1	CMC5	CMS5	DEL1	DVS2	(FLR)	LCD2	TAT3	ARC1	FSP6	IMP2	INT3	SPM1	TDS6	OPE1	PRE1	COV3	DPT4	FUN2	IND3	VAN5	EAL7
EAL6	INT1	CCL1	SPD1	OBJ2	ECD1	REQ2	TSS1	CMC5	CMS5	DEL1	DVS2		LCD1	TAT3	ARC1	FSP5	IMP2	INT3	SPM1	TDS5	OPE1	PRE1	COV3	DPT3	FUN2	IND2	VAN5	EAL6
EAL5	INT1	CCL1	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

Testing view on CC:



TOE_1, TOE_2, … TOE_n

System (risk) analysis methods & models:
e.g. CORAS, UMLsec

usecase
▼
testcase

Test tools & techniques:
e.g. fuzzing, partitioning

identifying

SFRs (specification)

TSFI (realisation)

testing

System definition & analysis

1) TOE, subjects, assets,
2) threats, policies, assumptions
3) security objectives
4) Security functional requirements

TSFI *enforcing* *supporting* *non-interfering* SFRs

Test developer plan

a) concepts/architecture
b) purposes
c) Test suite structure
➢ coverage of security relevant TSFI

TCL, JUnit, C++, TTCN-3, manual tests…

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.