Basic Robustness: CCv2.3 → CCv3.1

This collection of tables presents a mapping between the requirements of Basic Robustness (as defined in the CIM) and the requirements of CCv3.1. The right column cites the corresponding requirements from CCv3.1.

ACM_CAP.2 (v2.3)	ALC_CMC.2; ALC_CMS.2 (v3.1)
ACM_CAP.2.1C - The reference for the TOE shall be unique to each version of the TOE.	ALC_CMC.2.1C - The TOE shall be labelled with its unique reference.
ACM_CAP.2.2C - The TOE shall be labelled with its reference.	
ACM_CAP.2.3C - The CM documentation shall include a configuration list.	ALC_CMS.2.1C - The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; and the parts that comprise the TOE.
ACM_CAP.2.4C - The configuration list shall uniquely identify all configuration items that comprise the TOE.	ALC_CMC.2.3C - The CM system shall uniquely identify all configuration items.
ACM_CAP.2.5C - The configuration list shall describe the configuration items that comprise the TOE.	ALC_CMS.2.1C - The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; and the parts that comprise the TOE.
ACM_CAP.2.6C - The CM documentation shall describe the method used to uniquely identify the configuration items that comprise the TOE.	ALC_CMC.2.2C - The CM documentation shall describe the method used to uniquely identify the configuration items.
ACM_CAP.2.7C - The CM system shall uniquely identify all configuration items that comprise the TOE.	ALC_CMS.2.2C - The configuration list shall uniquely identify the configuration items.
	ALC_CMS.2.3C - For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

ADO_DEL.1 (v2.3)	ALC_DEL.1; AGD_PRE.1 (v3.1)
ADO_DEL.1.1C - The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.	ALC_DEL.1.1C - The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.
	AGD_PRE.1.1C - The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

ADO_IGS.1 (v2.3)	AGD_PRE.1 (v3.1)

ADO_IGS.1.1C - The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation and start-up of the TOE.	AGD_PRE.1.2C - The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.
ADO_IGS.1.2E - The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.	AGD_PRE.1.2E - The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

FPT_SEP; FPT_RVM [Part 2]	ADV_ARC.1 (v3.1)
FPT_SEP.*.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects. FPT_SEP.*.3 The TSF shall maintain the part of the TSF that enforces the access control and/or information flow control SFPs in a security domain for its own execution that protects them from interference and tampering by the remainder of the TSF and by subjects untrusted with respect to the TSP.	ADV_ARC.1.2D The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities. ADV_ARC.1.4C - The security architecture description shall demonstrate that the TSF protects itself from tampering. ADV_ARC.1.3C - The security architecture description shall describe how the TSF initialisation process is secure. These element prevent all potential sources of tampering, whether elsewhere in the TSF, from outside the TSF, or from the initialization code (which may be considered inside or outside the TSF).
FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.	ADV_ARC.1.1D The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed. ADV_ARC.1.5C - The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.
FPT_SEP.*.2 The TSF shall enforce separation between the security domains of subjects in the TSC.	ADV_ARC.1.2C - The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.
In version 2.3, the security architecture requirements were functional. As such there were no requirements for (or guidance on) its description. As a Part 3 requirement (v3.1), there must be a description provided, and there is opportunity to explain how the description should be made.	ADV_ARC.1.3D The developer shall provide a security architecture description of the TSF. ADV_ARC.1.1C - The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.

ADV_FSP.1 (v2.3)	ADV_FSP.2 (v3.1)
ADV_FSP.1.1C - The functional specification shall describe the TSF and its external interfaces using an informal style.	The requirement for informal presentation has been dropped because it is the lowest level; anything more formal will still meet the requirement.
ADV_FSP.1.2C - The functional specification shall be internally consistent.	There is no longer an explicit check for inconsistency; if it is inconsistent, it doesn't make sense, so it can't fulfill ANY of the requirements.
ADV_FSP.1.3C - The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.	ADV_FSP.2.2C - The functional specification shall describe the purpose and method of use for all TSFI. ADV_FSP.2.3C - The functional specification shall identify and describe all parameters associated with each TSFI. ADV_FSP.2.4C - For SFR-enforcing TSFIs, the functional specification shall describe the SFR-enforcing actions associated with the TSFI. ADV_FSP.2.5C - For SFR-enforcing TSFIs, the functional specification shall describe direct error messages resulting from processing associated with the SFR-enforcing actions. The term "details" has been clarified as actions and parameters (but only SFR-related ones). The term "as appropriate" has been replaced by the specific direct messages and SFR-enforcing TSFI.
ADV_FSP.1.4C - The functional specification shall completely represent the TSF.	ADV_FSP.2.1C - The functional specification shall completely represent the TSF.
ADV_FSP.1.2E - The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.	ADV_FSP.2.2E - The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

ADV_HLD.1 (v2.3)	ADV_TDS.1 (v3.1)
ADV_HLD.1.1C - The presentation of the high-level design shall be informal.	The requirement for informal presentation has been dropped because it is the lowest level; anything more formal will still meet the requirement.

ADV_HLD.1.2C - The high-level design shall be internally consistent.	There is no longer an explicit check for inconsistency; if it is inconsistent, it doesn't make sense, so it can't fulfill ANY of the requirements.
ADV_HLD.1.3C - The high-level design shall describe the structure of the TSF in terms of subsystems.	ADV_TDS.1.1C - The design shall describe the structure of the TOE in terms of subsystems. ADV_TDS.1.2C - The design shall identify all subsystems of the TSF.
ADV_HLD.1.4C - The high-level design shall describe the security functionality provided by each subsystem of the TSF.	ADV_TDS.1.3C - The design shall describe the behaviour of each SFR-supporting or SFR-non-interfering TSF subsystem in sufficient detail to determine that it is not SFR-enforcing. ADV_TDS.1.4C - The design shall summarise the SFR-enforcing behaviour of the SFR-enforcing subsystems. (These three elements result in less work, because the less security-relevance a subsystem has, the less detail that is required.)
ADV_HLD.1.5C - The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.	Reliance upon the environment is the province of ACO; communicating with that environment is FSP.
ADV_HLD.1.6C - The high-level design shall identify all interfaces to the subsystems of the TSF.	ADV_TDS.1.5C - The design shall provide a description of the interactions among SFR-enforcing subsystems of the TSF, and between the SFR-enforcing subsystems of the TSF and other subsystems of the TSF. "Interfaces" was seen as too intense for EAL2; this has been eased to merely a description of the interactions.
ADV_HLD.1.7C - The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.	All externally-visible interfaces are the province of FSP.
ADV_HLD.1.2E - The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.	ADV_TDS.1.2E - The evaluator shall determine that the design is an accurate and complete instantiation of all security functional requirements.

ADV_RCR.1 (v2.3)	CC v3.1
ADV_RCR.1.1C - For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.	The correspondence between adjacent pairs (i.e. the RCR family) was distributed among each of the different levels of abstraction: each examines a correspondence to the previous (see specifics below). This distributed approach reflects the approach in CCv1. ADV_FSP.2.6C - The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification. ADV_TDS.1.6C - The mapping shall demonstrate that all behaviour described in the TOE design is mapped to the TSFIs that invoke it.

AGD_ADM.1 (v2.3)	AGD_OPE.1 (v3.1)
AGD_ADM.1.1C - The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.	AGD_OPE.1.3C - The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.
AGD_ADM.1.2C - The administrator guidance shall describe how to administer the TOE in a secure manner.	AGD_OPE.1.2C - The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner. AGD_OPE.1.5C - The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.
AGD_ADM.1.3C - The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.	AGD_OPE.1.1C - The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.
AGD_ADM.1.4C - The administrator guidance shall describe all assumptions regarding user behaviour that are relevant to secure operation of the TOE.	AGD_OPE.1.5C - The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AGD_ADM.1.5C - The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.	AGD_OPE.1.3C - The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.
AGD_ADM.1.6C - The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.	AGD_OPE.1.4C - The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.
AGD_ADM.1.7C - The administrator guidance shall be consistent with all other documentation supplied for evaluation.	AGD_OPE.1.7C - The operational user guidance shall be clear and reasonable.
AGD_ADM.1.8C - The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.	AGD_OPE.1.6C - The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfill the security objectives for the operational environment as described in the ST.

AGD_USR.1 (v2.3)	AGD_OPE.1 (v3.1)
AGD_USR.1.1C - The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.	AGD_OPE.1.3C The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.
AGD_USR.1.2C - The user guidance shall describe the use of user-accessible security functions provided by the TOE.	AGD_OPE.1.1C - The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.
AGD_USR.1.3C - The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.	AGD_OPE.1.1C - The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.
AGD_USR.1.4C - The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of TOE security environment.	AGD_OPE.1.2C - The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner. AGD_OPE.1.4C - The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

	AGD_OPE.1.5C - The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.
AGD_USR.1.5C - The user guidance shall be consistent with all other documentation supplied for evaluation.	AGD_OPE.1.7C - The operational user guidance shall be clear and reasonable.
AGD_USR.1.6C - The user guidance shall describe all security requirements for the IT environment that are relevant to the user.	AGD_OPE.1.6C - The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfill the security objectives for the operational environment as described in the ST.

ALC_FLR.2 (v2.3) **[*EAL2+*]**	ALC_FLR.2 (v3.1) **[*EAL2+*]** – no change
ALC_FLR.2.1C - The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.	ALC_FLR.2.1C - The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.
ALC_FLR.2.2C - The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.	ALC_FLR.2.2C - The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.
ALC_FLR.2.3C - The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.	ALC_FLR.2.3C - The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.
ALC_FLR.2.4C - The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.	ALC_FLR.2.4C - The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.
ALC_FLR.2.5C - The flaw remediation procedures shall describe a means by which the developer receives from TOE users reports and enquiries of suspected security flaws in the TOE.	ALC_FLR.2.5C - The flaw remediation procedures shall describe a means by which the developer receives from TOE users reports and enquiries of suspected security flaws in the TOE.
ALC_FLR.2.6C - The procedures for processing reported security flaws shall ensure that any reported flaws are corrected and the correction issued to TOE users.	ALC_FLR.2.6C - The procedures for processing reported security flaws shall ensure that any reported flaws are corrected and the correction issued to TOE users.
ALC_FLR.2.7C - The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.	ALC_FLR.2.7C - The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.
ALC_FLR.2.8C - The flaw remediation	ALC_FLR.2.8C - The flaw remediation

guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE.	guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE.

ATE_COV.1 (v2.3)	ATE_COV.1 (v3.1)
ATE_COV.1.1C - The evidence of the test coverage shall show the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.	ATE_COV.1.1C - The evidence of the test coverage shall show the correspondence between the tests in the test documentation and the TSFIs in the functional specification.

ATE_FUN.1 (v2.3)	ATE_FUN.1 (v3.1)
ATE_FUN.1.1C - The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.	ATE_FUN.1.1C - The test documentation shall consist of test plans, expected test results and actual test results. The difference between test plans and test procedures was vague, so the two were combined. It's the content, not the name, that is important.
ATE_FUN.1.2C - The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.	ATE_FUN.1.2C - The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.
ATE_FUN.1.3C - The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.	
ATE_FUN.1.4C - The expected test results shall show the anticipated outputs from a successful execution of the tests.	ATE_FUN.1.3C - The expected test results shall show the anticipated outputs from a successful execution of the tests.
ATE_FUN.1.5C - The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.	ATE_FUN.1.4C - The actual test results shall be consistent with the expected test results.

ATE_IND.2 (v2.3)	ATE_IND.2 (v3.1)
ATE_IND.2.1C - The TOE shall be suitable for testing.	ATE_IND.2.1C - The TOE shall be suitable for testing.
ATE_IND.2.2C - The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.	ATE_IND.2.2C - The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

ATE_IND.2.2E - The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.	ATE_IND.2.3E - The evaluator shall test a subset of the TSF interfaces to confirm that the TSF operates as specified.
ATE_IND.2.3E - The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.	ATE_IND.2.2E - The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

AVA_MSU.1 (v2.3) ***[EAL2+]***	v3.1
AVA_MSU.1.1C - The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.	The entire misuse analysis (i.e. the MSU family) was incorporated into the AGD families that address the documents subjected to such analysis.
AVA_MSU.1.2C - The guidance documentation shall be complete, clear, consistent and reasonable.	
AVA_MSU.1.3C - The guidance documentation shall list all assumptions about the intended environment.	
AVA_MSU.1.4C - The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).	
AVA_MSU.1.2E - The evaluator shall repeat all configuration and installation procedures to confirm that the TOE can be configured and used securely using only the supplied guidance documentation.	
AVA_MSU.1.3E - The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.	

AVA_SOF.1 (v2.3)	v3.1
AVA_SOF.1.1C - For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.	The strength-of-function analysis (i.e. the SOF family) was incorporated into the AVA family as part of the vulnerability analysis. There is no more SOF claim made in the ST.
AVA_SOF.1.2C - For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.	

AVA_SOF.1.2E - The evaluator shall confirm that the strength claims are correct.	

AVA_VLA.1 (v2.3)	AVA_VAN.2 (v2.3)
AVA_VLA.1.1C - The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for obvious ways in which a user can violate the TSP.	AVA_VAN.2.1C - The TOE shall be suitable for testing. AVA_VAN.2.2E -The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE. (The bulk of the penetration testing work is done by the evaluator, not the developer.)
AVA_VLA.1.2C - The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities.	AVA_VAN.2.3E - The evaluator shall perform an independent vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design and security architecture description to identify potential vulnerabilities in the TOE. (The problematic term “obvious” is replaced by specifics)
AVA_VLA.1.3C - The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.	
AVA_VLA.1.2E - The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.	AVA_VAN.2.4E - The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.