collaborative PP-Module for

Database-as-a-Service (DBaaS)

20 July 2026

Version 0.5

Table of Contents

Acknowledgements

This collaborative Protection Profile Module (PP-Module) was developed by the Database Management Systems international Technical Community (iTC) also known as DBMS-iTC with representatives from industry, Government agencies, Common Criteria Test Laboratories, and members of academia. The organizations that contributed to the development of this PP-Module include:

INDUSTRY

IBM

Microsoft

Oracle Corp.

COMMON CRITERIA TEST LABORATORIES

atsec information security

Intertek EWA-Canada and Intertek Acumen

TÜViT

Teron Labs

Combitech

GOVERNMENT AGENCIES

FMV/CSEC - Swedish Certification Body for IT Security

BSI - Bundesamt für Sicherheit in der Informationstechnik

JISEC - Japan IT Security Evaluation and Certification Scheme

Revision History

Table 1. Revision history

Version	Date	Description
0.1	2026-01-25	Initial draft for DBaaS deployments.
0.2	2026-05-14	Incorporated DBaaS improvement notes: aligned module with the CCiTC SaaS evaluation model, clarified TOE and platform boundaries, narrowed provider-administrator threats to customer-controlled key disclosure, added trusted-platform assumptions and objectives, refined customer-controlled key SFRs, and split tenant isolation into FDP_ACC and FDP_ACF.

Version	Date	Description
0.3	2026-06-30	Structural completeness update to align with the published Cloud and Crypto Modules: added Conformance Claims, Allowed PP-Configurations, SARs, full SFR dependency rationale, and a consistency rationale with the Base PP. Iterated reused Base PP components as `/DBaaS`, added the DBaaS role model (`FMT_SMR.1/DBaaS`, `FMT_SMF.1/DBaaS`) and a protected backup/restore requirement (`FDP_BKP_EXT.1`), recorded the inheritance of mandatory data-in-transit protection from the DBMS Cryptographic Functions Module, aligned Base PP references with cPP_DBMS Version 2.0, and adopted the shared AsciiDoc PDF/HTML rendering assets. This module remains in draft and is expected to mature on a later schedule than the Cloud and Crypto Modules.
0.4	2026-06-30	Focused FDP_BKP_EXT.1 to its provider-plaintext-restore-prevention and tenant-binding elements, with data-at-rest protection of backups inherited from the Crypto Module's FDP_DAR_EXT.1 rather than restated. Confirmed inheritance of the now-mandatory FDP_DIT_EXT.1 from the DBMS Cryptographic Functions Module. Version aligned with the v0.4 Cloud and Crypto Module set. This module remains in draft and is expected to mature on a later schedule than the Cloud and Crypto Modules.
0.4	2026-07-07	Replaced extended components that duplicated CC:2022 Part 2 components with iterated Part 2 claims: FAU_STG_EXT.2 is now FAU_STG.2/DBaaS (tenant-interface prohibition retained as a refinement), and FDP_RSG_EXT.1 is now FRU_RSA.1/DBaaS plus the narrow FRU_RSG_EXT.1 enforcement-action extension, removing the FAU_STG_EXT and FDP_RSG_EXT family definitions (and the FAU_STG_EXT family collision with the Cloud Module). Corrected FIA_USB.2/DBaaS to FIA_USB.1/DBaaS (CC Part 2 defines no FIA_USB.2). Split FMT_MOF.1/DBaaS into the single-element iterations FMT_MOF.1/DBaaS-Disable and FMT_MOF.1/DBaaS-Modify. Deleted the invented FAU_SEL.1.2/DBaaS element (audit query restriction is enforced by FDP_ACF.1.2/DBaaS). Restored the CC Part 2 text of FDP_ACC.2.1/2.2/DBaaS.

Version	Date	Description
0.4	2026-07-08	Renamed the FPT_TUD_EXT family to FPT_TUD_DBAAS_EXT (component FPT_TUD_DBAAS_EXT.1, formerly FPT_TUD_EXT.2), resolving the extended-family name collision with the DBMS Cloud Module's FPT_TUD_EXT; family behaviour now states the distinction explicitly.
0.4	2026-07-08	Corrected APE to ACE for PP-Module evaluation under CC:2022 (introduction, conformance methodology, and SAR statements). Stated the Cloud/DBaaS module boundary criterion explicitly in the Preface and the Relationship section: administrative authority over the DBMS software lifecycle (installation, patching, version selection, instance configuration) determines the applicable module. Reworded the A.CONNECT consistency analysis: FDP_DIT_EXT.1 supplements, and does not replace, A.CONNECT; inter-TSF transfer for distributed TOEs remains covered by A.CONNECT, provided in DBaaS deployments by the Trusted Platform under OE.TRUSTED_PLATFORM.
0.4	2026-07-08	Stated the cross-module selection coupling for FCS_CKM_DBAAS_EXT.1.1: import mechanisms correspond to the Crypto Module's "Imported from External Entity" Key Origin, and external-KMS or key-reference mechanisms to its new "Externally Managed" Key Origin, each including FDP_ITC_EXT.1; dependency table updated to reflect the conditional inclusion.
0.4	2026-07-08	Exact Conformance now cites its definition in CC:2022 Part 1 directly, replacing the legacy "subset of Strict Conformance" gloss (set-wide alignment).

Version	Date	Description
0.4	2026-07-18	Closed three follow-on gaps from the audit-channel and vantage analysis. Autonomous subjects: automated autonomous management logic is stated to be a subject class, its in-tenant-context actions carry tenant attribution under FIA_USB.1/DBaaS and tenant-visible service event stream records, and the FMT audit data contents now identify the acting subject rather than presupposing a human user. Retention: P.AUDIT_RETENTION now applies per audit channel, with the ST identifying retention treatment and tenant exportability for the DBMS audit trail and the service event stream separately. Recovery/restore coupling: FCS_CKM_DBAAS_EXT.1 and FDP_BKP_EXT.1 application notes state that a recovery mechanism implemented as a restore from backup is a single mechanism satisfying both components' constraints. Tenant lifecycle termination (offboarding, backup disposition, key destruction on deprovisioning) is deferred and tracked in OPEN-ITEMS.md.
0.4	2026-07-18	Introduced the service event stream as a second audit channel alongside the DBMS audit trail, resolving the observability inversion in the auditable-events refinement: the module’s lifecycle and key-state events (key-unavailable enforcement transition, recovery-mechanism use, update deployment) are generated while or because the database is not serving connections and cannot be required of an audit trail that becomes unreachable at that moment. The auditable-events table gains an Audit Channel column assigning every event; the ST identifies the stream’s implementing mechanism, boundary allocation, and tenant retrieval interface, with Trusted-Platform-delivered streams relying on OE.TRUSTED_PLATFORM and OE.EXTERNAL_SERVICES. Service event stream records concerning a tenant’s instance, keys, or backups are tenant-visible regardless of acting subject, including provider-initiated actions; audit data contents for FCS_CKM_DBAAS_EXT.1 and FDP_BKP_EXT.1 now identify the acting subject rather than presupposing a tenant context. Glossary entry added.

Version	Date	Description
0.4	2026-07-18	Stated that Tenant User, Tenant Administrator, and Service Provider Administrator are module-level role labels, not required TOE role names: the FMT_SMR.1/DBaaS application note now requires the ST to map each label to the TOE's own role terminology, permits one-to-many and many-to-one mappings, and constrains the mapping to preserve the provider/tenant authority boundaries; glossary entries marked as labels and a Tenant User entry added.
0.4	2026-07-18	Added a key-state enforcement interval assignment to FCS_CKM_DBAAS_EXT.1.3, replacing the implicit immediate-enforcement reading. The interval bounds the latency between a key-state change at the external key provider and TSF denial of access to protected data, accommodating the polling-based key-state detection and bounded unreachability grace periods documented by production DBaaS offerings; the completed interval must be a fixed documented bound covering worst-case detection latency, any unreachability grace period, and cached-key lifetime, and must not be indefinite or extensible by provider action. FCS_CKM_DBAAS_EXT.1.2 is unaffected and admits no such interval. Auditable events extended with the transition to the key-unavailable enforcement state; extended component definition and SFR rationale aligned.

Version	Date	Description
0.4	2026-07-14	Maturity pass toward the Cloud/Crypto structural baseline. FPT_TUD_DBAAS_EXT.1 redesigned as Trusted Service Update: the deployment model (rolling, tenant-deferral, or maintenance-window) is declared by selection, signature verification of service software before it is placed into service is the mandatory floor (envelope format unconstrained; algorithms per FCS_COP.1/SigVer), and a tenant-visible version or revision identifier is required; the conditional out-of-boundary escape was removed. Security Problem Definition extended with T.MALICIOUS_TENANT_ADMIN, T.SECRETS_EXPOSURE, T.UNAUTHORIZED_UPDATE, organizational security policies P.AUDIT_RETENTION and P.ACCESS_CONTROL_POLICY, O.TRUSTED_UPDATE, and OE.PROVIDER_ROLE_SEPARATION (DBaaS service and Trusted Platform administration through logically distinct roles, accounts, and control planes). Added TOE boundary diagram, TOE use cases, an auditable-events refinement of the Base PP's Table 4 for all module SFRs, and complete objective tracing for FMT_SMR.1/DBaaS and FMT_SMF.1/DBaaS. Editorial: operation-completion typesetting normalized, X.509 Functional Package bibliography entry added, JISEC acknowledged, A.CONNECT consistency analysis split into external-entity and inter-TSF legs.
0.4	2026-07-14	Two design corrections from self-review. FCS_CKM_DBAAS_EXT.1.3's recovery-mechanism exception now requires that recovery be authorized by the tenant or an agent under the tenant's control (provider-held escrow or any unilaterally exercisable provider recovery path cannot complete the exception), with recovery-mechanism use added to the auditable events. FDP_ACC.2/DBaaS replaced by FDP_ACC.1/DBaaS (Subset access control): the Tenant Isolation SFP governs tenant-scoped subjects, objects, and operations, and the complete-access-control claim is not made because completeness across all TSF-controlled subjects and objects is a property of the composed ST rather than of this module.

Version	Date	Description
0.4	2026-07-20	Aligned customer-controlled key models with the Crypto Module’s role-specific ML-KEM design. Added an optional customer-authorized KEM-establishment mechanism and mapped it to the "Established through Key Encapsulation" Key Origin. Clarified that the TOE claims only ML-KEM operations inside its boundary, that the KEM shared secret is passed through `FCS_CKM.5` to derive the Master Key, and that customer revocation or denial remains subject to the bounded key-state enforcement requirement.
0.5	2026-07-20	Rolled the completed managed-service security architecture, normative audit model, provider-role separation, trusted service update, and customer-authorized ML-KEM integration into the coordinated Version 0.5 review set.

Preface

This PP-Module, the **Database-as-a-Service (DBaaS) Module**, extends the collaborative Protection Profile for Database Management Systems (cPP_DBMS). It applies to database services where a DBMS TOE is offered as a managed cloud service and is accessed by customers through tenant-facing database, administrative, and programmatic interfaces.

This PP-Module applies the CC in the Cloud Technical Community (CCiTC) Software as a Service (SaaS) evaluation model to Database-as-a-Service deployments of a DBMS TOE. The module does not evaluate the complete cloud service provider infrastructure or the provider's complete cloud authorization scheme. Instead, it identifies the DBMS TOE, the TOE Platform, the Trusted Platform, and the operational environment dependencies that support the evaluated configuration.

Security functionality implemented by the TOE is evaluated through this module and the cPP_DBMS. Security properties provided by the Trusted Platform are addressed through assumptions, operational environment objectives, and scheme-accepted evidence for the Trusted Platform.

This module adopts a zero-trust key-management posture for customer-controlled database encryption keys. This posture does not imply that the TOE resists arbitrary compromise by the Trusted Platform, cloud control plane, or cloud service provider infrastructure. Rather, it means that the TOE shall not provide service provider administrators with access to customer-controlled master key material through DBMS or service interfaces, and shall support cryptographic separation such that protected tenant data cannot be decrypted except through authorized use of the customer-controlled key.

In contrast to the DBMS in the Cloud Module, which addresses tenant-operated databases deployed on cloud infrastructure-as-a-service or platform-as-a-service offerings, this module addresses provider-operated databases in which the cloud service provider operates and manages the DBMS on behalf of tenants. The two modules are mutually exclusive: a TOE is evaluated against the Cloud Module or the DBaaS Module according to who holds administrative authority over the DBMS software lifecycle — installation, patching, version selection, and instance configuration. Where the tenant holds that authority, the Cloud Module applies; where the cloud service provider holds it, this module applies.

Objectives of Document

This document expresses the security functional requirements for DBaaS deployments, focusing on logical tenant isolation, resource governance, tenant-scoped audit behavior, protected backup and restore, and customer-controlled cryptographic controls for database data.

Scope of Document

This document presents the Common Criteria (CC) collaborative Protection Profile Module (PP-Module) to express the security functional requirements (SFRs) for Database Management Systems offered as a managed Database-as-a-Service. The Evaluation Activities that specify the actions the evaluator performs to determine if a product satisfies the SFRs captured within this PP-Module are

described in [DBMS_MOD_DBAAS_SD].

Intended Readership

The target audiences of this PP-Module are DBMS service developers and providers, Common Criteria Testing Laboratories (CCTLs), evaluators, government agencies, schemes, and consumers concerned with the security of Database-as-a-Service deployments.

Related Documents

- [CC1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, CCMB-2022-11-001, CC:2022 Revision 1, November 2022.
- [CC2] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements, CCMB-2022-11-002, CC:2022 Revision 1, November 2022.
- [CC3] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements, CCMB-2022-11-003, CC:2022 Revision 1, November 2022.
- [CC4] Common Criteria for Information Technology Security Evaluation, Part 4: Framework for the specification of evaluation methods and activities, CCMB-2022-11-004, CC:2022 Revision 1, November 2022.
- [CC5] Common Criteria for Information Technology Security Evaluation, Part 5: Pre-defined packages of security requirements, CCMB-2022-11-005, CC:2022 Revision 1, November 2022.
- [CEM] Common Methodology for Information Technology Security Evaluation, Evaluation methodology, CCMB-2022-11-006, CEM:2022 Revision 1, November 2022.
- [CCE] Common Criteria for Information Technology Security Evaluation, Errata and interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), CCMB-002, Version 1.1, July 22, 2024.
- [cPP_DBMS] collaborative Protection Profile for Database Management Systems, Version 2.0, 27 April 2026.
- [cPP_DBMS_SD] Supporting Document Mandatory Technical Document Evaluation Activities for the collaborative Protection Profile for Database Management Systems, Version 2.0, 27 April 2026.
- [DBMS_MOD_CRYPTO] collaborative PP-Module for DBMS Cryptographic Functions, Version 0.5.
- [DBMS_MOD_CRYPTO_SD] Supporting Document - Evaluation Activities for DBMS Cryptographic Functions Module, Version 0.5.
- [DBMS_MOD_DBAAS_SD] Supporting Document - Evaluation Activities for DBaaS Module, Version 0.5.
- [Crypto_Catalog] Specification of Functional Requirements for Cryptography (CCDB-018), Version 1.0, January 2025.
- [TLS_FP] Functional Package for Transport Layer Security (TLS), Version 2.1, 2025-08-25.
- [X509_FP] Functional Package for X.509 Certificates, Version 1.0. Available at commoncriteria.github.io/X509.

- [CCiTC_SaaS] Common Criteria in the Cloud Technical Community, Guidance for Cloud Evaluations, Version 1.1.

For more information, see the Common Criteria Portal.

Chapter 1. PP-Module Introduction

This document is in accordance with the requirements for a PP-Module as defined in [CC1], and the corresponding ACE assurance class defined in [CC3], under which a PP-Module is evaluated as part of a PP-Configuration.

1.1. PP-Module Reference Identification

Table 2. PP-Module Identification

Attribute	Value
PP-Module Title	collaborative PP-Module for Database-as-a-Service (DBaaS)
PP-Module Short Name	DBMS_MOD_DBAAS
PP-Module Version	0.5
PP-Module Publication Date	2026-07-20
PP-Module Sponsor	Database Management Systems international Technical Community (DBMS-iTC)
CC Version	CC:2022
PP-Module Keywords	Database, DBaaS, Cloud, SaaS, Managed Service, Multi-Tenant, Isolation, Customer-Controlled Keys

Chapter 2. PP-Module Base

This section specifies the Base PP that must be used in conjunction with this PP-Module and defines the allowed PP-Configurations, per CC:2022 requirements for PP-Module conformance claims.

This PP-Module requires the **collaborative Protection Profile for Database Management Systems** (cPP_DBMS) [[cPP_DBMS]], Version 2.0, as its Base PP.

2.1. Required Modules

This PP-Module requires the following PP-Module to be claimed in conjunction with the Base PP:

- **PP-Module for DBMS Cryptographic Functions (DBMS_MOD_CRYPTO)** [[DBMS_MOD_CRYPTO]]

Rationale: In a DBaaS model the customer does not control the physical infrastructure, and protected tenant data is stored and transmitted within provider-operated infrastructure. Customer-controlled database key management and the cryptographic protection of tenant data at rest and in transit are therefore mandatory for the module's DBMS-specific security value. The DBMS Cryptographic Functions Module defines the DBMS-specific requirements and consumes the applicable Crypto Catalogue components for algorithms, key generation, key lifecycle, key destruction, and data-at-rest encryption. TLS and certificate behavior are specified by the applicable Functional Packages.

Application Note: Selection of this DBaaS Module does not automatically select the Crypto Module's optional `[USE CASE 2] Enterprise Enhanced`. An ST may claim Enterprise Enhanced when the DBaaS deployment requires its FIPS 140-3, NIAP, and CNSA 2.0-aligned cryptographic selections; the ST then follows the selection template defined entirely by the Crypto Module.

Note: The Crypto Module is mandatory. Data-at-rest protection for DBaaS PP-Configurations is satisfied through the Crypto Module's `FDP_DAR_EXT.1` requirement, and data-in-transit protection for tenant-facing database, administrative, and programmatic interfaces is satisfied through the Crypto Module's mandatory `FDP_DIT_EXT.1` requirement. This module does not redefine those requirements; it inherits them from the mandatory Crypto Module and adds DBaaS-specific controls on top of them.

2.2. Allowed PP-Configurations

The only allowed PP-Configuration for this module is:

1. **cPP_DBMS + DBMS DBaaS Module + DBMS Cryptographic Module**

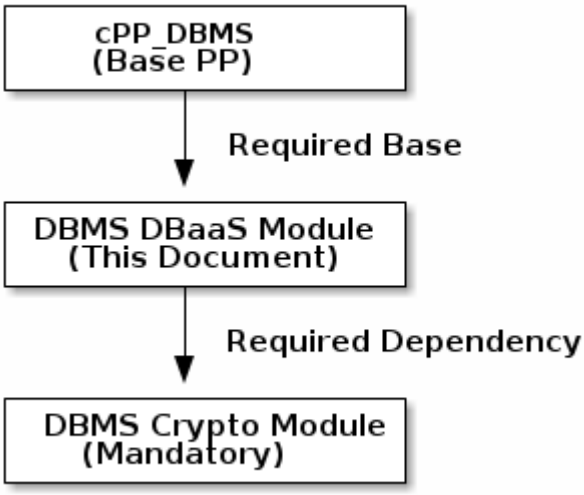
   This configuration is required for all evaluations claiming this PP-Module. It ensures that the TOE provides:

   - **Customer-Controlled Cryptographic Protection**: Data-at-rest encryption under customer-controlled keys and protected data-in-transit, provided by the mandatory Crypto Module.
   - **DBaaS-Specific Controls**: Logical tenant isolation, residual information protection, resource

governance, tenant-scoped and immutable audit, protected backup and restore, and trusted service update, provided by this module.

Any PP-Configuration claiming this PP-Module that does not include the DBMS Cryptographic Module is not valid.

2.3. PP-Module Relationship Diagram



2.4. Relationship to the DBMS in the Cloud Module

This module and the DBMS in the Cloud Module both extend the cPP_DBMS for cloud deployments, but they address different operational models and are claimed in separate, mutually exclusive PP-Configurations:

- The **DBMS in the Cloud Module** addresses a **tenant-operated** DBMS deployed by the customer on cloud infrastructure-as-a-service or platform-as-a-service offerings (for example, a customer-managed database service running on provider-supplied infrastructure).
- This **DBaaS Module** addresses a **provider-operated** DBMS offered and managed by the cloud service provider on behalf of tenants (for example, a fully managed or autonomous database service).

A single TOE is evaluated against one of these modules according to who holds administrative authority over the DBMS software lifecycle (installation, patching, version selection, and instance configuration): the tenant for the Cloud Module, the cloud service provider for this module. Both configurations share the mandatory Crypto Module, which provides their common cryptographic foundation.

Chapter 3. TOE Overview

This PP-Module applies to Database Management Systems offered as a managed Database-as-a-Service. The Target of Evaluation (TOE) is the DBMS service instance and the DBMS service components that enforce the SFRs claimed in the Security Target.

3.1. TOE Type

The TOE type addressed by this PP-Module is: a Database Management System offered as a managed Database-as-a-Service.

3.2. TOE

For this module, the TOE is the DBMS service instance and the DBMS service components that enforce the SFRs claimed in the Security Target. The TOE may include the database engine, tenant-facing database interfaces, DBMS security management logic, DBMS audit logic, DBMS tenant-isolation mechanisms, DBMS key-management integration logic, and autonomous DBMS management logic when those components enforce claimed SFRs.

The TOE does not include the complete cloud service provider infrastructure merely because the TOE is delivered as a managed service. Unless explicitly included in the TOE boundary, the cloud control plane, hypervisor, physical infrastructure, cloud networking, cloud storage substrate, provider operational tooling, provider personnel processes, and general cloud authorization controls are part of the operational environment or Trusted Platform.

3.3. TOE Platform

The TOE Platform is the immediate software, firmware, or hardware environment on which the DBMS TOE executes and from which the TOE obtains services that support TOE operation. Depending on the evaluated architecture, this may include an operating system, container runtime, database runtime environment, or other execution environment. The ST shall identify each TOE Platform service relied upon by the TOE to satisfy or support claimed SFRs.

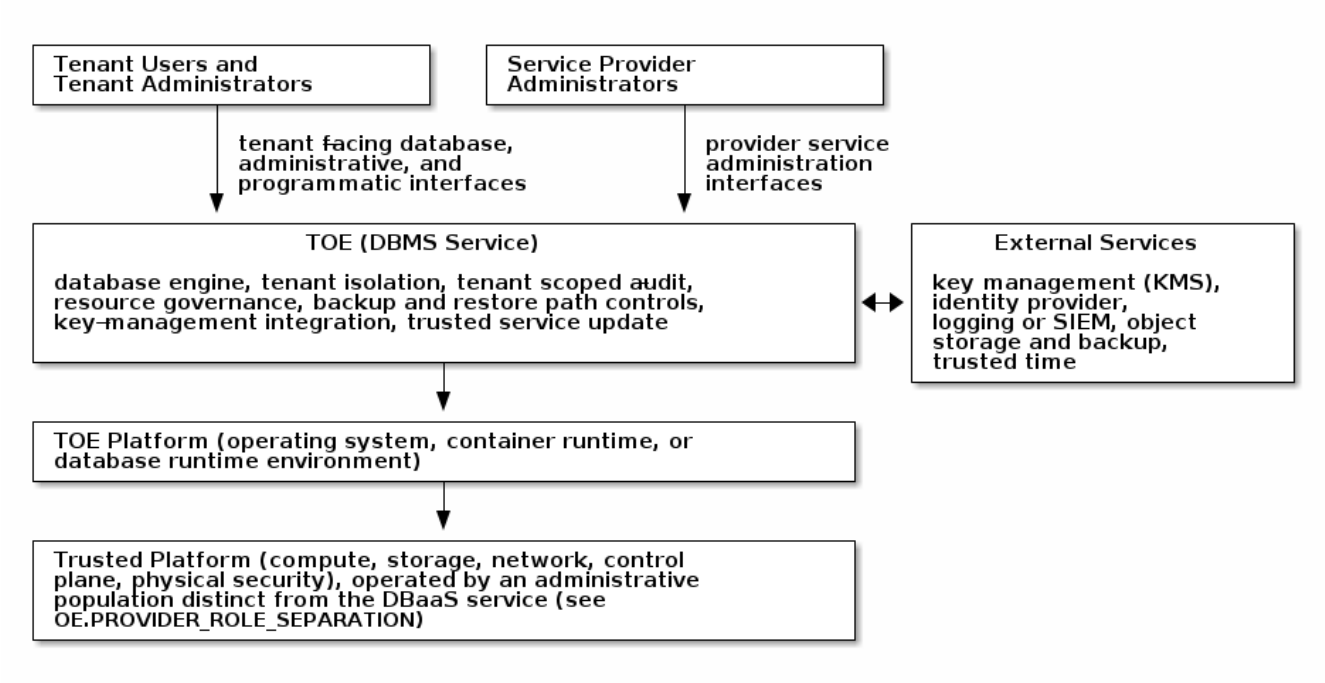
3.4. Trusted Platform

The Trusted Platform is the cloud hosting environment outside the TOE boundary that provides infrastructure services relied upon by the TOE and TOE Platform. Depending on the evaluated architecture, these services may include physical security, virtualization or hardware isolation, cloud networking, storage infrastructure, and provider-operated infrastructure services. The Trusted Platform is relied upon to satisfy operational environment assumptions and security objectives identified by this module, subject to acceptance by the applicable evaluation scheme.

3.5. TOE Boundary

The following diagram shows the generic boundary for a provider-operated DBaaS TOE and the interfaces this module constrains. The exact allocation of components to the TOE, TOE Platform,

and Trusted Platform is declared by the ST under Security Function Allocation.



Tenant-facing interfaces and the provider's service administration interfaces terminate at the TOE and are subject to the Tenant Isolation SFP, the role model, and the management restrictions of this module; channels between the TOE and external entities are protected as required by the mandatory DBMS Cryptographic Functions Module (FDP_DIT_EXT.1). The Trusted Platform's own control plane is not a TOE interface: administrative authority over it is held by a population distinct from the Service Provider Administrators of the DBaaS service, as required by OE.PROVIDER_ROLE_SEPARATION.

3.6. Operational Environment Dependencies

The ST shall identify operational environment services relied upon by the TOE, including external key management services, identity providers, logging or SIEM services, object storage services, backup services, management consoles, cloud authorization evidence, and trusted time services when those services support the evaluated configuration.

The ST shall identify whether each dependency is part of the TOE, TOE Platform, Trusted Platform, or another operational environment component. Security functionality implemented by the TOE shall be evaluated as TOE functionality. Security properties provided by trusted external services shall be addressed through assumptions, operational environment objectives, and evidence accepted by the applicable evaluation scheme. An ST cannot allocate a claimed SFR wholly to the operational environment unless the applicable requirement expressly permits use of a platform-provided mechanism.

3.7. Security Function Allocation

This PP-Module does not prescribe a single implementation boundary for every DBaaS architecture. A component or service may be allocated differently in different evaluated products when the resulting TOE boundary, SFR claims, assumptions, and Operational Environment objectives remain

internally consistent. Provider ownership or operation of a component does not by itself determine its allocation.

For each component or service that implements or supports security behavior relevant to a claimed SFR, the ST shall identify:

- its allocation to the TOE, TOE Platform, Trusted Platform, or another operational environment component;
- the security behavior performed by the TOE and any security property relied upon from an external component;
- the interface through which the TOE uses the component or service; and
- the applicable SFR, assumption, or Operational Environment objective.

Where an applicable requirement permits the TOE to use a platform-provided mechanism, the TSS shall distinguish the TSF behavior being evaluated from the external property on which that behavior relies. Trusted Platform evidence shall not otherwise be used as a substitute for satisfying or evaluating a claimed SFR.

This PP-Module defines the Trusted Platform properties needed by the evaluated configuration but does not prescribe which cloud authorization, certification, or other evidence is acceptable. The evaluation authority determines the acceptance criteria for Trusted Platform evidence under the applicable scheme policy.

Chapter 4. TOE Use Case

This section describes representative deployment scenarios for provider-operated DBaaS TOEs. Both scenarios share the module's discriminator — the cloud service provider holds administrative authority over the DBMS software lifecycle — and differ in tenancy architecture, key-management model, and update cadence. They illustrate how the module's requirements, including the mandatory cryptographic protections inherited from the DBMS Cryptographic Functions Module, apply across the range of real managed database services.

4.1. Multi-Tenant Managed Database Service

A cloud service provider operates a fleet of DBMS instances as a managed service. Multiple tenants share DBMS service infrastructure, with tenant boundaries implemented by DBMS constructs such as databases, pluggable databases, schemas, or tenant identifiers. The deployment consists of:

- Provider-operated DBMS instances on shared, provider-managed infrastructure;
- Tenant access through tenant-facing database, administrative, and programmatic interfaces over untrusted networks;
- Customer-controlled master keys held in an external key management service under tenant control (BYOK or external KMS integration);
- Versioned service updates deployed by the provider on a published schedule, with tenant-configurable deferral or maintenance windows.

In this scenario the module's tenant-isolation, resource-governance, and tenant-scoped audit requirements carry the security value of the shared-infrastructure model, and the customer-controlled key requirements ensure the provider cannot reach tenant plaintext through TOE interfaces. Data-in-transit protection for the tenant-facing interfaces and data-at-rest encryption under the customer-controlled key hierarchy are inherited as mandatory requirements from the DBMS Cryptographic Functions Module (`FDP_DIT_EXT.1`, `FDP_DAR_EXT.1`). The update model is declared in `FPT_TUD_DBAAS_EXT.1.1` through the tenant-deferral or maintenance-window selection.

4.2. Autonomous, Continuously Deployed Database Service

A cloud service provider operates an autonomous database service in which provider-managed automation performs operational database management, and service software is deployed continuously: a single live service target receives rolling updates from the provider's deployment pipeline, with no discrete versions offered to tenants and no tenant deferral. The deployment consists of:

- Provider-operated, automation-managed DBMS service instances;
- Rolling deployment of service software from pipeline artifacts that are digitally signed and verified before being placed into service;
- A service revision identifier that tenants can query for change-management and support purposes;

- Customer-controlled keys accessed by reference through an external key management service, without plaintext key export to the TOE.

In this scenario the update path is the distinctive security surface: `FPT_TUD_DBAAS_EXT.1` is completed with the uniform-rolling-deployment selection, signature verification applies to the deployment artifacts, and the revision identifier satisfies the tenant-visibility requirement without semantic versioning. The automated management logic is declared as a role in `FMT_SMR.1/DBaaS`, and its management authority is bounded by the `FMT_MOF.1/DBaaS` iterations. The customer-controlled key model couples to the "Externally Managed" Key Origin of the DBMS Cryptographic Functions Module.

Application Note: These DBaaS deployment use cases do not automatically select the Crypto Module's optional `[USE CASE 2] Enterprise Enhanced`. An ST may claim Enterprise Enhanced for a DBaaS PP-Configuration when the deployment requires its FIPS 140-3, NIAP, and CNSA 2.0-aligned cryptographic selections; the ST then follows the selection template defined entirely by the Crypto Module.

Chapter 5. CC Conformance Claims

As defined by the references [CC1], [CC2], and [CC3], this PP-Module:

- conforms to the requirements of Common Criteria CC:2022, Revision 1.
- is CC Part 2 extended.
- is CC Part 3 conformant.

The methodology applied for the PP-Module evaluation is defined in [CEM]. This PP-Module is evaluated against the ACE assurance families of CC:2022 Part 3 (ACE_INT.1, ACE_CCL.1, ACE_SPD.1, ACE_OBJ.1, ACE_ECD.1, ACE_REQ.1, and ACE_MCO.1) within the evaluation of a PP-Configuration that includes it.

5.1. Package Conformance

This PP-Module does not introduce additional functional package claims or additional assurance package claims beyond those inherited from the Base PP. A PP-Configuration including this PP-Module inherits the cPP_DBMS claim of conformance to the EAL2 assurance package defined in CC:2022 Part 5 [[CC5]], augmented by ALC_FLR.3 Systematic flaw remediation.

A TOE claiming this PP-Module includes, through the mandatory DBMS Cryptographic Functions Module, the applicable Catalogue-derived components consumed there and, for trusted channels, the applicable components of the Functional Package for TLS [[TLS_FP]] and the Functional Package for X.509 Certificates [[X509_FP]].

5.2. PP-Module Conformance Type

This PP-Module requires **Exact Conformance** of the Security Target to this PP-Module, as defined for PP-Modules in conjunction with the Base PP. Exact Conformance is defined in CC:2022 Part 1 [CC1].

The following rules apply to a PP-Configuration that includes this PP-Module:

1. **Mandatory SFRs**: The ST shall include all SFRs that are listed as mandatory in this PP-Module and in the Base PP.
2. **Selection-Based SFRs**: The ST shall include the selection-based SFRs of this PP-Module that are triggered by selections made in other SFRs. This PP-Module defines no selection-based SFRs; selections within its mandatory SFRs do not make those SFRs selection-based.
3. **Optional SFRs**: The ST may include the optional SFRs of this PP-Module. This PP-Module defines no optional SFRs.
4. **No Additional Requirements**: While iteration is allowed, the ST shall not include additional requirements from CC Part 2 [[CC2]], CC Part 3 [[CC3]], or definitions of extended components not already included in this PP-Module, the Base PP (cPP_DBMS), or another module in the claimed PP-Configuration.
5. **Operations**: All assignments, selections, and refinements shall be completed in accordance with

the SFR specifications in this PP-Module and the Base PP.

5.3. Conformance Claim Rationale

A Security Target claiming conformance to a PP-Configuration that includes this PP-Module shall include:

1. A statement that the claimed PP-Configuration includes the required Base PP (cPP_DBMS).
2. A statement that the claimed PP-Configuration includes the mandatory DBMS Cryptographic Module.
3. A statement of Exact Conformance to this PP-Module.
4. The mandatory SFRs of this PP-Module, completed in accordance with their specifications. (This PP-Module defines no selection-based or optional SFRs.)

Chapter 6. Security Problem Definition

The security problem is described in terms of the threats that the TOE, or the TOE and its operational environment, addresses, and the assumptions made about the operational environment. The threats, assumptions, and objectives defined in this PP-Module supplement those defined in the Base PP and do not contradict them. The consistency of this PP-Module's Security Problem Definition with that of the Base PP is demonstrated in Consistency Rationale.

6.1. Threats

T.KEY_DISCLOSURE_TO_PROVIDER_ADMIN

A service provider administrator, service account, or provider-operated management function may attempt to access customer-controlled master key material or cause the TOE to disclose plaintext key material through DBMS interfaces, provider administration interfaces, local DBMS storage, DBMS logs, backups, diagnostic outputs, or key-management integration functions.

T.TENANT_ISOLATION_FAILURE

A malicious tenant may attempt to access the data, metadata, memory resources, temporary storage, or audit records of another tenant sharing the same DBMS service infrastructure.

T.NOISY_NEIGHBOR

A tenant may consume excessive shared resources such as CPU, I/O, memory, sessions, query slots, storage throughput, or other DBMS-managed resources, causing denial of service or performance degradation for other tenants on the shared platform.

T.AUDIT_TAMPERING

A malicious tenant, tenant administrator, or compromised service account may attempt to delete, modify, suppress, or disable audit records to conceal unauthorized activities.

T.MALICIOUS_TENANT_ADMIN

A malicious or negligent tenant administrator may attempt to weaken the security configuration of the tenant's service — including disabling audit generation or data-at-rest encryption — or abuse tenant administrative interfaces to act outside the tenant's scope.

T.SECRETS_EXPOSURE

Secrets handled by the TOE — tenant credentials, service account credentials, external key-management service credentials, and customer-controlled key references — may be exposed to other tenants or to unauthorized roles through DBMS logs, diagnostic outputs, backups, error messages, or TOE interfaces.

T.UNAUTHORIZED_UPDATE

An attacker who compromises the update distribution path or deployment pipeline, or an unauthorized actor within the service provider, may cause unverified or malicious DBMS service software to be placed into service, compromising the TSF for all tenants of the service.

6.2. Assumptions

A.TRUSTED_PLATFORM_ADMIN

Trusted Platform administrators are trusted to follow the controls, procedures, and restrictions associated with the Trusted Platform and any scheme-recognized cloud authorization evidence. The TOE is not expected to defend against a Trusted Platform administrator who actively modifies the TOE, TOE Platform, cloud infrastructure, memory, storage substrate, or control plane to bypass TOE security functions.

A.TRUSTED_PLATFORM_CONTROLS

The Trusted Platform provides and is configured to provide sufficient physical, logical, operational, and administrative controls to protect the TOE and TOE Platform from infrastructure-level compromise, cross-tenant infrastructure access, unauthorized physical access, and unauthorized administrative access outside the TOE boundary.

A.SERVICE_AVAILABILITY

The Service Provider ensures the availability of the infrastructure hosting the TOE in accordance with the evaluated configuration and any service-level commitments relied upon by the ST.

A.EXTERNAL_SERVICES

External key management, identity provider, logging, object storage, backup, and management services relied upon by the TOE are correctly configured, protected, and operated in accordance with the assumptions and operational guidance for the evaluated configuration.

6.3. Organizational Security Policies

This section defines the organizational security policies that the TOE must support or enforce. These policies represent security rules that organizations deploying or consuming the TOE are expected to implement.

P.AUDIT_RETENTION

The organization shall define and enforce audit record retention policies that specify:

- The minimum retention period for audit records based on regulatory requirements (e.g., GDPR, HIPAA, PCI-DSS, SOX) and organizational security policies;
- The storage location and protection requirements for retained audit records;
- Procedures for secure disposal of audit records after the retention period expires;
- Requirements for audit record availability during incident investigations or compliance audits.

  The TOE must support the export of tenant-scoped audit records so that tenants can implement their retention policies using external audit storage solutions, and must protect retained audit records from unauthorized modification and deletion while under TOE control. In a provider-operated service, retention obligations apply to both the provider (service-level audit) and the tenant (tenant-scoped audit), and to both audit channels defined by this module's auditable-events refinement: the ST identifies, for the DBMS audit trail and

the service event stream separately, the retention treatment applicable to each and which records are exportable to tenants.

P.ACCESS_CONTROL_POLICY

The organization shall implement role-based access control with least-privilege principles for all TOE access. Specifically:

- Each user and service account shall be assigned to defined roles with explicitly documented privileges;
- Privileges shall be limited to the minimum necessary for users to perform their authorized functions;
- Administrative privileges shall be separated from regular user privileges, and service provider administrative privileges shall be separated from tenant administrative privileges;
- Access control decisions shall be logged for accountability;
- Role assignments shall be reviewed periodically and adjusted as organizational needs change.

  The TOE must provide mechanisms to define roles, assign users to roles, and enforce access control decisions based on role membership and tenant context.

Chapter 7. Security Objectives

7.1. Security Objectives for the TOE

O.CUSTOMER_CONTROLLED_KEYS

The TOE shall support customer-controlled key management such that customer-controlled master key material is not disclosed to service provider administrators through TOE interfaces, and protected database data cannot be decrypted except through authorized use of the customer-controlled key or an approved key-management integration.

O.LOGICAL_ISOLATION

The TOE shall enforce logical isolation between tenants, ensuring that one tenant cannot access another tenant's data, metadata, audit records, or tenant-scoped DBMS resources unless explicitly authorized by an evaluated cross-tenant sharing mechanism.

O.RESOURCE_GOVERNANCE

The TOE shall enforce resource governance on a per-tenant basis to prevent any single tenant from consuming DBMS-managed resources in a manner that denies service to other tenants.

O.IMMUTABLE_AUDIT

The TOE shall ensure that audit records, once generated, are protected from unauthorized modification and deletion by tenant administrators, ordinary tenant users, and other roles not authorized by the evaluated configuration.

O.PROTECTED_BACKUP

The TOE shall ensure that backup and restore of protected tenant data preserves data-at-rest encryption and customer-controlled key binding, such that backup data cannot be decrypted or restored in plaintext without authorized use of the applicable customer-controlled master key.

O.TRUSTED_UPDATE

The TOE shall apply updates to the DBMS service software only through the service provider's authorized update process, shall verify the authenticity and integrity of updates by digital signature before the updated software is placed into service, and shall make the version or revision identifier of the deployed service software visible to tenants.

7.2. Security Objectives for the Operational Environment

OE.TRUSTED_PLATFORM

The operational environment shall provide a Trusted Platform that satisfies the physical, logical, administrative, and operational controls needed to host the TOE and TOE Platform in accordance with the evaluated configuration: it shall enforce infrastructure-level tenant isolation, protect the compute, storage, and network resources supporting the TOE, provide correct operation of the infrastructure services relied upon by the TOE, and be responsible for the availability of underlying resources.

Application Note: This objective states, for the provider-operated DBaaS context, the same platform responsibilities that the DBMS Cloud Module's OE.TRUSTED_PLATFORM states for tenant-operated deployments (infrastructure isolation, resource protection, and infrastructure-service correctness). The two modules are never claimed together; the shared name denotes the shared platform role.

OE.TRUSTED_PLATFORM_ADMIN

Trusted Platform administrators shall manage the Trusted Platform in accordance with accepted cloud authorization controls, provider procedures, and scheme-accepted operational evidence, and shall not act to bypass or compromise the TOE.

OE.PROVIDER_ROLE_SEPARATION

The service provider shall exercise administrative authority over the DBaaS service and administrative authority over the Trusted Platform through logically distinct roles, accounts, and control planes, assigned according to least privilege, such that no single administrative identity holds both DBaaS service administration and Trusted Platform administration.

Application Note: This objective constrains the provider's operating model, not the provider's corporate structure: a provider may operate both the DBaaS service and the underlying platform (vertical integration is expressly permitted), provided the two administrative populations, their credentials, and their control planes are distinct and least-privilege-assigned. This separation is what keeps A.TRUSTED_PLATFORM_ADMIN scoped to the platform population only: without it, the Service Provider Administrator — the threat agent of T.KEY_DISCLOSURE_TO_PROVIDER_ADMIN — could fall inside the assumption's exempted population, collapsing the module's customer-controlled key claims into an assumption. The provider demonstrates the separation through its role and account model documentation, evaluated as described in the Supporting Document.

OE.SERVICE_AVAILABILITY

The operational environment shall provide the infrastructure availability, recovery, and continuity services needed to support the DBaaS TOE in accordance with the evaluated configuration.

OE.EXTERNAL_SERVICES

External services relied upon by the TOE, including key management services, identity providers, logging services, object storage services, backup services, management interfaces, and trusted time services, shall provide the security properties and operational behavior described in the ST and operational guidance.

Chapter 8. Security Rationale

8.1. Threats to Objectives Mapping

Threat	Security Objectives Addressing the Threat	Rationale
T.KEY_DISCLOSURE_TO_PROVIDER_ADMIN	O.CUSTOMER_CONTROLLED_KEYS, O.PROTECTED_BACKUP, OE.TRUSTED_PLATFORM_ADMIN, OE.PROVIDER_ROLE_SEPARATION	O.CUSTOMER_CONTROLLED_KEYS requires TOE behavior that prevents service provider administrators from using TOE interfaces to view, export, or recover plaintext customer-controlled master key material. O.PROTECTED_BACKUP extends that protection to backup and restore paths, which are a common provider-administrator disclosure vector. OE.TRUSTED_PLATFORM_ADMIN states the operational trust placed in administrators of infrastructure outside the TOE boundary. OE.PROVIDER_ROLE_SEPARATION keeps the Service Provider Administrator population distinct from the Trusted Platform administrative population, so that the threat agent of this threat is not exempted by A.TRUSTED_PLATFORM_ADMIN.
T.TENANT_ISOLATION_FAILURE	O.LOGICAL_ISOLATION, OE.TRUSTED_PLATFORM	O.LOGICAL_ISOLATION requires the TOE to enforce tenant separation within DBMS-controlled data, metadata, audit, and tenant-scoped resources. OE.TRUSTED_PLATFORM addresses infrastructure-level isolation relied upon outside the TOE boundary.
T.NOISY_NEIGHBOR	O.RESOURCE_GOVERNANCE, OE.SERVICE_AVAILABILITY	O.RESOURCE_GOVERNANCE requires TOE controls over DBMS-managed tenant resource consumption. OE.SERVICE_AVAILABILITY addresses provider-operated availability and infrastructure continuity outside the TOE boundary.
T.AUDIT_TAMPERING	O.IMMUTABLE_AUDIT, OE.EXTERNAL_SERVICES	O.IMMUTABLE_AUDIT requires the TOE to protect TOE-generated audit records from unauthorized modification or deletion. OE.EXTERNAL_SERVICES addresses external audit export, logging, or storage services when such services are relied upon by the evaluated configuration.

Threat	Security Objectives Addressing the Threat	Rationale
T.MALICIOUS_TENANT_ADMIN	O.LOGICAL_ISOLATION, O.IMMUTABLE_AUDIT, O.CUSTOMER_CONTROLLED_KEYS	O.LOGICAL_ISOLATION confines tenant administrative authority to the tenant's own scope. O.IMMUTABLE_AUDIT denies tenant administrators the ability to modify or delete audit records, and the management restrictions supporting it and O.CUSTOMER_CONTROLLED_KEYS prevent any role — including a tenant administrator — from disabling audit generation or data-at-rest encryption in the evaluated configuration.
T.SECRETS_EXPOSURE	O.CUSTOMER_CONTROLLED_KEYS, O.LOGICAL_ISOLATION, OE.EXTERNAL_SERVICES	O.CUSTOMER_CONTROLLED_KEYS prevents disclosure of customer-controlled key material through TOE interfaces, including logs, diagnostics, and backups. O.LOGICAL_ISOLATION prevents one tenant's secrets from being reachable by another tenant through DBMS-controlled resources. OE.EXTERNAL_SERVICES addresses the protection of secrets while held by external key-management, identity, or secret-management services outside the TOE boundary. The lifecycle protection of master key material itself is addressed by the mandatory DBMS Cryptographic Functions Module's key-management objectives.
T.UNAUTHORIZED_UPDATE	O.TRUSTED_UPDATE, OE.TRUSTED_PLATFORM	O.TRUSTED_UPDATE requires that DBMS service software is placed into service only through the provider's authorized update process and only after signature verification, and that the deployed version is visible to tenants, so an unverified or malicious update is not silently applied. OE.TRUSTED_PLATFORM addresses the integrity of the infrastructure hosting the deployment pipeline outside the TOE boundary.

8.2. Assumptions to Objectives Mapping

Assumption	Security Objectives Addressing the Assumption	Rationale
A.TRUSTED_PLATFORM_ADMIN	OE.TRUSTED_PLATFORM_ADMIN, OE.PROVIDER_ROLE_SEPARATION	OE.TRUSTED_PLATFORM_ADMIN directly requires Trusted Platform administrators to operate the platform according to accepted controls and not act to bypass or compromise the TOE. OE.PROVIDER_ROLE_SEPARATION bounds the population to which this assumption applies: it keeps Trusted Platform administration distinct from DBaaS service administration, so the assumption's exemption cannot extend to Service Provider Administrators of the DBaaS service.
A.TRUSTED_PLATFORM_CONTROLS	OE.TRUSTED_PLATFORM	OE.TRUSTED_PLATFORM directly requires the operational environment to provide the physical, logical, administrative, and operational controls needed for the TOE and TOE Platform.
A.SERVICE_AVAILABILITY	OE.SERVICE_AVAILABILITY	OE.SERVICE_AVAILABILITY directly states the operational environment availability and continuity support relied upon by the DBaaS TOE.
A.EXTERNAL_SERVICES	OE.EXTERNAL_SERVICES	OE.EXTERNAL_SERVICES directly states the expected security properties and operational behavior for external services relied upon by the TOE.

8.3. Organizational Security Policies to Objectives Mapping

Organizational Security Policy	Security Objectives Addressing the Policy	Rationale
P.AUDIT_RETENTION	O.IMMUTABLE_AUDIT, OE.EXTERNAL_SERVICES	O.IMMUTABLE_AUDIT protects retained audit records from unauthorized modification and deletion while under TOE control, and the audit export configuration functions restricted to authorized roles enable tenants and the provider to move records into retention storage. OE.EXTERNAL_SERVICES addresses the external logging and storage services in which exported records are retained.

Organizational Security Policy	Security Objectives Addressing the Policy	Rationale
P.ACCESS_CONTROL_POLICY	O.LOGICAL_ISOLATION, OE.PROVIDER_ROLE_SEPARATION	O.LOGICAL_ISOLATION enforces role- and tenant-scoped access control over DBMS-controlled data and resources, supported by the module's role model and management restrictions. OE.PROVIDER_ROLE_SEPARATION applies the policy's least-privilege and separation requirements to the provider's own administrative populations.

8.4. Objectives to SFRs Mapping

Objective	SFRs	Rationale
O.CUSTOMER_CONTROLLED_KEYS	FCS_CKM_DBAAS_EXT.1, and DBMS Cryptographic Functions Module requirements	FCS_CKM_DBAAS_EXT.1 requires the TOE to support customer-controlled master keys, prevents service provider administrator access to plaintext key material, and requires denial of access to protected data within a bounded key-state enforcement interval when authorization to use a customer-controlled key is revoked, unavailable, or denied. The cryptographic mechanisms, key destruction, and trusted channel for key import are provided by the mandatory DBMS Cryptographic Functions Module.
O.LOGICAL_ISOLATION	FDP_ACC.1/DBaaS, FDP_ACF.1/DBaaS, FDP_RIP.1/DBaaS, FIA_USB.1/DBaaS, FAU_SEL.1/DBaaS	The tenant isolation access control policy, residual information protection, user-subject binding, and tenant-aware audit selection together prevent unauthorized cross-tenant access to data, metadata, audit records, and tenant-scoped resources.
O.RESOURCE_GOVERNANCE	FRU_RSA.1/DBaaS, FRU_RSG_EXT.1, FMT_SMF.1/DBaaS	FRU_RSA.1/DBaaS requires the TOE to enforce tenant resource quotas, and FRU_RSG_EXT.1 requires a defined enforcement action (terminate, throttle, queue, or reject) on operations that exceed configured limits. FMT_SMF.1/DBaaS provides the quota and enforcement-behavior configuration functions on which both depend.

Objective	SFRs	Rationale
O.IMMUTABLE_AUDIT	FAU_STG.2/DBaaS, FMT_MOF.1/DBaaS-Disable, FMT_MOF.1/DBaaS-Modify, FMT_SMR.1/DBaaS, FMT_SMF.1/DBaaS	FAU_STG.2/DBaaS protects stored audit records from unauthorised modification and deletion, including by tenant administrators. FMT_MOF.1/DBaaS-Disable prevents any role from disabling audit generation, and FMT_MOF.1/DBaaS-Modify restricts audit export configuration to provider roles. FMT_SMR.1/DBaaS defines the role model, and FMT_SMF.1/DBaaS the audit management functions, on which those restrictions operate.
O.PROTECTED_BACKUP	FDP_BKP_EXT.1, and DBMS Cryptographic Functions Module requirements	Data-at-rest protection of backup data is provided by FDP_DAR_EXT.1 of the mandatory DBMS Cryptographic Functions Module, under which protected data, and therefore its backups, are encrypted under the customer-controlled key hierarchy. FDP_BKP_EXT.1 adds the backup/restore-path requirements: it prevents plaintext restore or export by service provider administrators without authorized use of the customer-controlled key, and binds restored data to the originating tenant so that restore does not bypass the Tenant Isolation SFP.
O.TRUSTED_UPDATE	FPT_TUD_DBAAS_EXT.1, FMT_MOF.1/DBaaS-Modify	FPT_TUD_DBAAS_EXT.1 requires updates to be applied through the provider's authorized update process under a declared deployment model, verified by digital signature before being placed into service, with the deployed version or revision identifier visible to tenants. FMT_MOF.1/DBaaS-Modify restricts modification of patching and update behavior to provider roles, so tenants and unauthorized roles cannot alter the update process.

The security management SFRs FMT_SMR.1/DBaaS and FMT_SMF.1/DBaaS additionally support O.CUSTOMER_CONTROLLED_KEYS and O.LOGICAL_ISOLATION by defining the roles and management functions on which FCS_CKM_DBAAS_EXT.1 and FDP_ACF.1/DBaaS depend.

Chapter 9. Security Functional Requirements

9.1. Conventions

The individual security functional requirements are specified in the sections below. The following conventions are used:

- [text within square brackets] indicates the completion of a selection or assignment; where a completed assignment or selection is presented as a list, the list items are set in italics.
- Selections and assignments left to the ST author retain the [selection: …] and [assignment: …] operation form.
- **Bold text** indicates a refinement of a Base PP or CC Part 2 requirement.
- `/DBaaS` following a component identifier indicates an iteration of a Base PP or CC Part 2 component, refined for the DBaaS context.

The mandatory SFRs in this PP-Module extend or refine SFRs defined in the cPP_DBMS Base PP, aligned with the provider-operated DBaaS deployment context and the CCiTC SaaS evaluation model. Cryptographic algorithm, key lifecycle, and data-at-rest mechanisms are provided by the mandatory DBMS Cryptographic Functions Module using Catalogue-derived components consumed there. Data-in-transit protocol and certificate mechanisms are supplied by the applicable Functional Packages.

Chapter 10. Security Functional Requirements (Mandatory)

10.1. FCS: Cryptographic Support

10.1.1. FCS_CKM_DBAAS_EXT.1 Customer-Controlled Keys

FCS_CKM_DBAAS_EXT.1.1 The TSF shall support customer-controlled master encryption keys using one or more of the following mechanisms: [selection: customer-generated master keys imported into the TOE through a trusted channel specified by the DBMS Cryptographic Functions Module; externally managed master keys accessed through a key management service interface where plaintext master key material is not exported to the TOE; customer-controlled key references or key handles that permit the TOE to perform authorized cryptographic operations without exposing plaintext master key material to service provider administrators; customer-authorized Master Key establishment through ML-KEM with an authenticated external entity, using the role-specific key-encapsulation and key-derivation requirements of the DBMS Cryptographic Functions Module].

FCS_CKM_DBAAS_EXT.1.2 The TSF shall not provide an interface by which a service provider administrator can view, export, or recover plaintext customer-controlled master key material.

FCS_CKM_DBAAS_EXT.1.3 The TSF shall prevent access to protected database data no later than [assignment: key-state enforcement interval] after authorized use of the applicable customer-controlled master key is revoked, unavailable, or denied, except for data that remains available through an explicitly documented and evaluated recovery mechanism whose use requires authorization by the tenant or an agent under the tenant's control.

Application Note: This requirement is intended to address DBaaS customer-controlled key models such as BYOK, HYOK, external KMS integration, or equivalent key-reference mechanisms. The recovery-mechanism exception in FCS_CKM_DBAAS_EXT.1.3 cannot be completed by provider-held escrow or any mechanism the service provider can exercise unilaterally: a recovery path usable without tenant authorization would reintroduce exactly the disclosure this component excludes (T.KEY_DISCLOSURE_TO_PROVIDER_ADMIN). Use of a recovery mechanism is an auditable event (see the auditable-events table). Where the documented recovery mechanism is implemented as a restore from backup — the common case, using a retained older key version — it is the same operation addressed by FDP_BKP_EXT.1: a single use of the mechanism shall satisfy both the tenant-authorization constraint of this component and the restore authorization and tenant binding of FDP_BKP_EXT.1. This requirement does not require the TOE to protect against arbitrary modification of the Trusted Platform or cloud control plane. If the TOE stores, caches, wraps, transforms, or re-exports key material after receipt, the ST shall identify that behavior and the applicable DBMS-specific and Catalogue-derived key protection components in the DBMS Cryptographic Functions Module.

+ The key-state enforcement interval assignment in FCS_CKM_DBAAS_EXT.1.3 accommodates the key-state detection and availability behavior of production managed database services: external key-provider state is typically detected by periodic polling rather than synchronous notification, and services commonly document a bounded grace period during which cached key material

remains in use when the external key provider is unreachable, so that a transient key-service or network fault does not immediately take down the database. Production DBaaS offerings document detection intervals on the order of minutes and unreachability grace periods on the order of hours. The ST author shall complete the assignment with the maximum interval between a key-state change at the external key provider and TSF denial of access to protected database data, covering both worst-case detection latency and any documented unreachability grace period, and covering the lifetime of any cached key material identified under the caching disclosure above. The completed interval shall be a fixed, documented bound: an interval that is indefinite, that is extensible by service provider action, or that resets on continued data access does not satisfy the requirement. Expiration of the interval and the resulting transition to the key-unavailable enforcement state are auditable events (see the auditable-events table). The interval bounds enforcement latency only; it does not weaken FCS_CKM_DBAAS_EXT.1.2, which admits no interval during which plaintext customer-controlled master key material may be exposed to a service provider administrator.

+ The mechanisms selected in FCS_CKM_DBAAS_EXT.1.1 couple to the Key Origin selection in the Crypto Module's FCS_CKM_EXT.1.1: customer-generated master keys imported into the TOE correspond to "Imported from External Entity"; externally managed master keys and customer-controlled key references correspond to "Externally Managed"; and customer-authorized ML-KEM establishment corresponds to "Established through Key Encapsulation". The ST shall complete FCS_CKM_EXT.1.1 with the corresponding selection, and every external origin includes FDP_ITC_EXT.1 (Trusted Channel for Key Import, External Key Management, and Key Establishment).

+ For the KEM-established model, the ST shall identify whether the TOE performs encapsulation, decapsulation, or both; shall include FCS_CKM.1/KEM only for TOE-performed ML-KEM.KeyGen; and shall identify any operation performed by an external KMS or customer-controlled service as outside the TOE boundary. The ML-KEM shared secret is not itself the customer-controlled Master Key: the Crypto Module's FCS_CKM.5 derives the Master Key with a context that binds the customer, service instance, key purpose, and applicable establishment transaction. Selection of this mechanism is permitted only where the customer or its authorized external entity retains a control whose revocation, unavailability, or denial causes the TSF to enforce FCS_CKM_DBAAS_EXT.1.3 within the assigned interval. A one-time KEM exchange after which the provider can use the derived Master Key indefinitely without customer authorization does not satisfy this customer-controlled model.

Table 3. FCS_CKM_DBAAS_EXT.1 Dependencies

Dependency	Resolution
Key management trusted channel, key destruction, data-at-rest encryption	Satisfied by the mandatory DBMS Cryptographic Functions Module: FDP_ITC_EXT.1 is included through the coupled "Imported from External Entity", "Externally Managed", or "Established through Key Encapsulation" selection in that module's FCS_CKM_EXT.1.1 (see the Application Note), together with FCS_CKM.6, FDP_DAR_EXT.1, and the applicable Catalogue-derived or anticipated role-specific ML-KEM components consumed there.
FMT_SMF.1	Satisfied by FMT_SMF.1/DBaaS (configuration of customer-controlled key references and key-management integration).

10.2. FDP: User Data Protection

10.2.1. FDP_RIP.1/DBaaS Residual Information Protection (Memory and Temporary Resources)

FDP_RIP.1.1/DBaaS The TSF shall ensure that any previous information content of a resource is made unavailable upon the allocation of the resource to a different tenant for the following resources: [selection: memory, buffer cache, temporary storage, query work areas, diagnostic structures, [assignment: other shared DBMS resources]].

Application Note: In shared DBaaS architectures, this requirement addresses residual tenant data in DBMS-managed resources that may be reallocated across tenant contexts. The ST should describe whether tenant data can be present in shared memory, buffer cache, temporary storage, query work areas, diagnostic structures, or other shared DBMS resources, and how such resources are cleared, reinitialized, or access-controlled before reuse. This iteration refines the Base PP `FDP_RIP.1` for cross-tenant resource reuse in a multi-tenant managed service.

Table 4. FDP_RIP.1/DBaaS Dependencies

Dependency	Resolution
No dependencies	FDP_RIP.1 has no dependencies in CC Part 2.

10.2.2. FDP_ACC.1/DBaaS Tenant Isolation Policy

FDP_ACC.1.1/DBaaS The TSF shall enforce the Tenant Isolation SFP on [*tenant subjects, tenant data objects, tenant metadata objects, tenant audit records, and all operations among tenant subjects and those objects*].

Application Note: This SFR is CC:2022 Part 2 FDP_ACC.1 (Subset access control), iterated for the Tenant Isolation SFP. Subset access control is claimed deliberately: the Tenant Isolation SFP governs tenant-scoped subjects, objects, and operations, while subjects and objects outside its scope — including the Base PP's users and objects and provider-side automation — are governed by the access control SFPs of the Base PP as claimed in the composed ST. A complete-access-control claim (FDP_ACC.2) is not made, because completeness across all TSF-controlled subjects and objects is a property of the composed ST rather than of this module in isolation.

Table 5. FDP_ACC.1/DBaaS Dependencies

Dependency	Resolution
FDP_ACF.1	Satisfied by `FDP_ACF.1/DBaaS`.

10.2.3. FDP_ACF.1/DBaaS Tenant Isolation Policy Rules

FDP_ACF.1.1/DBaaS The TSF shall enforce the Tenant Isolation SFP based on the following security attributes: [*tenant identifier, user identifier, service role, object owner, object tenant identifier, object type, and operation*].

FDP_ACF.1.2/DBaaS The TSF shall enforce the following rules:

- *a tenant subject shall access only tenant data objects associated with the same tenant identifier unless explicitly authorized by an evaluated cross-tenant sharing mechanism;*
- *a tenant subject shall access only metadata associated with the same tenant identifier or metadata explicitly defined as global system metadata;*
- *a tenant subject shall access only audit records associated with the same tenant identifier unless explicitly authorized by an evaluated provider or compliance function;*
- *service provider administrative subjects shall be restricted from tenant data access except through interfaces and roles explicitly identified in the ST.*

FDP_ACF.1.3/DBaaS The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes, that explicitly authorize access of subjects to objects].

FDP_ACF.1.4/DBaaS The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects].

Application Note: The ST should identify the tenant boundary used by the TOE, such as databases, pluggable databases, schemas, namespaces, tablespaces, tenant identifiers, accounts, or other DBMS constructs. If an evaluated cross-tenant sharing mechanism is claimed, the ST shall describe the authorization model, audit behavior, and limits of that mechanism.

Table 6. FDP_ACF.1/DBaaS Dependencies

Dependency	Resolution
FDP_ACC.1	Satisfied by `FDP_ACC.1/DBaaS`.
FMT_MSA.3	Satisfied by the Base PP `FMT_MSA.3` for the security attributes used by the Tenant Isolation SFP, refined by the ST for tenant-scoped attributes.

10.2.4. FRU_RSA.1/DBaaS Maximum Quotas (Tenant Resources)

FRU_RSA.1.1/DBaaS The TSF shall enforce maximum quotas of the following resources: [selection: CPU, memory, I/O bandwidth, storage, sessions, query concurrency, workload queues, [assignment: other DBMS-managed resources]] that [*individual tenants, as defined groups of users*] can use [selection: simultaneously, over a specified period of time].

Application Note: This SFR is CC:2022 Part 2 FRU_RSA.1, iterated for tenant resource governance. The Part 2 assignment of controlled resources is narrowed to the selection shown; the subject selection is completed by treating each tenant as a defined group of users. It does not require the TOE to enforce infrastructure-level resource controls provided solely by the Trusted Platform unless those controls are included in the TOE boundary and claimed in the ST.

Table 7. FRU_RSA.1/DBaaS Dependencies

Dependency	Resolution
No dependencies	FRU_RSA.1 has no dependencies in CC Part 2.

Dependency	Resolution
FMT_SMF.1 (management)	Quota configuration is provided by FMT_SMF.1/DBaaS.

10.2.5. FRU_RSG_EXT.1 Resource Governance Enforcement Action

FRU_RSG_EXT.1.1 The TSF shall [selection: terminate, throttle, queue, reject, [assignment: other enforcement action]] operations that exceed the resource quotas enforced by FRU_RSA.1/DBaaS.

Application Note: CC Part 2 FRU_RSA.1 requires quota enforcement but does not specify the action taken when a quota is exceeded; this extended component specifies that action so it can be evaluated.

Table 8. FRU_RSG_EXT.1 Dependencies

Dependency	Resolution
FRU_RSA.1	Satisfied by FRU_RSA.1/DBaaS.
FMT_SMF.1	Satisfied by FMT_SMF.1/DBaaS (configuration of enforcement behavior).

10.2.6. FDP_BKP_EXT.1 Protected Backup and Restore

FDP_BKP_EXT.1.1 The TSF shall not provide an interface by which a service provider administrator can restore or export protected tenant data from a backup in plaintext without authorized use of the applicable customer-controlled master key.

FDP_BKP_EXT.1.2 The TSF shall bind restored tenant data to the originating tenant identifier such that a restore operation does not place tenant data outside the Tenant Isolation SFP.

Application Note: This requirement addresses backup and restore as a disclosure vector specific to provider-operated DBaaS, where backups are commonly created, stored, and restored by provider tooling. Backups of protected tenant data inherit data-at-rest protection from FDP_DAR_EXT.1 of the mandatory DBMS Cryptographic Functions Module: because protected data is encrypted at rest under the customer-controlled key hierarchy, its backup is encrypted under the same hierarchy, and this SFR does not restate that protection. This SFR instead specifies the requirements particular to the backup and restore path: that the TOE provides no interface for a service provider administrator to obtain plaintext tenant data through restore or export without authorized key use, and that restore preserves tenant isolation. If the TOE delegates backup storage to an external object storage or backup service, the ST shall identify whether the restore authorization and tenant binding are provided by the TOE or by an external service addressed through OE.EXTERNAL_SERVICES; the data-at-rest protection of externally stored backups is addressed by FDP_DAR_EXT.1. A restore that serves as the documented recovery mechanism of FCS_CKM_DBAAS_EXT.1.3 is additionally subject to that component's tenant-authorization constraint; where the two coincide, the ST shall describe them as a single mechanism.

Table 9. FDP_BKP_EXT.1 Dependencies

Dependency	Resolution
Data-at-rest protection of backup data	Inherited from the mandatory DBMS Cryptographic Functions Module (FDP_DAR_EXT.1) and the applicable Catalogue-derived components consumed there; see the application note.
FCS_CKM_DBAAS_EXT.1 (authorized key use)	Satisfied within this module.
FDP_ACC.1 (tenant binding on restore)	Satisfied by FDP_ACC.1/DBaaS.

10.3. FIA: Identification and Authentication

10.3.1. FIA_USB.1/DBaaS User-Subject Binding (Tenant Context)

FIA_USB.1.1/DBaaS The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [*tenant identifier, user identifier, and service role*].

FIA_USB.1.2/DBaaS The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [*a subject shall bind to the tenant identifier of the authenticating user or service account before the subject performs tenant-scoped operations*].

FIA_USB.1.3/DBaaS The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [*a tenant identifier associated with a subject shall not be changed by tenant-controlled session parameters, connection attributes, or request inputs except through an evaluated mechanism identified in the ST*].

Application Note: This SFR is an iteration of CC:2022 Part 2 FIA_USB.1, completed for tenant-context binding in a multi-tenant managed service. This binding is critical for the database engine to enforce the logical isolation policies defined in FDP_ACC.1/DBaaS and FDP_ACF.1/DBaaS. It is independent of the Base PP's optional extended component FIA_USB_EXT.2; if the ST also claims FIA_USB_EXT.2, the tenant attributes defined here apply to that component's binding rules as well.

+ Subjects need not act on behalf of a human user. Where the automated autonomous management logic role is selected in FMT_SMR.1/DBaaS, a subject acting on its behalf within a tenant context binds the tenant identifier of the affected tenant under the same rules, so that autonomous actions remain inside the Tenant Isolation SFP and their audit records remain tenant-attributable.

Table 10. FIA_USB.1/DBaaS Dependencies

Dependency	Resolution
FIA_ATD.1	Satisfied by the Base PP user attribute definition, refined by the ST to include tenant identifier and service role.

10.4. FMT: Security Management

10.4.1. FMT_SMR.1/DBaaS Security Roles (DBaaS)

FMT_SMR.1.1/DBaaS The TSF shall maintain the roles: Tenant User, Tenant Administrator, Service Provider Administrator, and [selection: automated autonomous management logic, [assignment: other roles]].

FMT_SMR.1.2/DBaaS The TSF shall be able to associate users with roles.

Application Note: This iteration defines the DBaaS-specific role model on which the management restrictions in the FMT_MOF.1/DBaaS iterations and the access-control rules in FDP_ACF.1/DBaaS depend. The Tenant Administrator manages tenant data and tenant-level configuration only to the extent permitted by the evaluated configuration; the Service Provider Administrator operates the managed service but is excluded from the customer-controlled key and tenant-data access paths constrained by this module.

+ Automated autonomous management logic, where selected, is a subject class rather than a human role: its actions within a tenant context carry tenant attribution under FIA_USB.1/DBaaS, its audit records identify it as the acting subject (see the auditable-events table), and where it acts on a tenant's service instance those records are visible to the affected tenant in the service event stream.

+ The role names Tenant User, Tenant Administrator, and Service Provider Administrator are module-level labels for scopes of authority, not required TOE role names. The TSF is not required to maintain roles under these names. The ST shall map each label to the TOE role, privilege set, group, or account class that realizes it in the TOE's own terminology; one label may be realized by several TOE roles, and several TOE roles may share a label. The mapping shall preserve the authority boundaries the labels denote: no mapping may assign a single TOE role both Service Provider Administrator authority and tenant-scoped authority in a way that vacates the separation enforced by the FMT_MOF.1/DBaaS iterations, FDP_ACF.1/DBaaS, or FCS_CKM_DBAAS_EXT.1. Throughout this module and its Supporting Document, a reference to one of these role names means the TOE role or roles the ST maps to that label.

Table 11. FMT_SMR.1/DBaaS Dependencies

Dependency	Resolution
FIA_UID.1	Satisfied by the Base PP FIA_UID.2, which is hierarchical to FIA_UID.1.

10.4.2. FMT_SMF.1/DBaaS Specification of Management Functions (DBaaS)

FMT_SMF.1.1/DBaaS The TSF shall be capable of performing the following management functions:

- *configuration of customer-controlled key references, key import, and external key-management integration;*
- *configuration of tenant resource quotas and enforcement behavior;*
- *configuration of audit export, audit retention, and authorized audit query roles;*
- *configuration of update deployment, including tenant deferral policy or maintenance windows where selected in FPT_TUD_DBAAS_EXT.1.1;*
- *configuration of evaluated cross-tenant sharing mechanisms, where claimed;*

- [assignment: other DBaaS security management functions].

Application Note: The management functions defined here are the functions on which FCS_CKM_DBAAS_EXT.1, FRU_RSA.1/DBaaS, FRU_RSG_EXT.1, FAU_SEL.1/DBaaS, and the FMT_MOF.1/DBaaS iterations depend. The roles authorized to perform each function are defined by FMT_SMR.1/DBaaS and constrained by the FMT_MOF.1/DBaaS iterations.

Table 12. FMT_SMF.1/DBaaS Dependencies

Dependency	Resolution
No dependencies	FMT_SMF.1 has no dependencies in CC Part 2.

10.4.3. FMT_MOF.1/DBaaS-Disable Management of Security Functions Behaviour (Disable Restriction)

FMT_MOF.1.1/DBaaS-Disable The TSF shall restrict the ability to [*disable*] the functions [*audit generation and data-at-rest encryption for protected tenant data*] to [*no role in the evaluated configuration*].

Application Note: No role, including the Service Provider Administrator, may disable the identified functions in the evaluated configuration. CC Part 2 FMT_MOF.1 has a single element; the disable restriction and the provider-role restriction are therefore expressed as two iterations rather than as two elements of one component.

Table 13. FMT_MOF.1/DBaaS-Disable Dependencies

Dependency	Resolution
FMT_SMF.1	Satisfied by FMT_SMF.1/DBaaS.
FMT_SMR.1	Satisfied by FMT_SMR.1/DBaaS.

10.4.4. FMT_MOF.1/DBaaS-Modify Management of Security Functions Behaviour (Provider Functions)

FMT_MOF.1.1/DBaaS-Modify The TSF shall restrict the ability to [*modify the behaviour of*] the functions [*resource governance policies, patching and updates, audit export configuration, and* [assignment: other DBaaS security functions]] to [selection: Service Provider Administrator, automated autonomous management logic, [assignment: other authorized role]].

Application Note: The Tenant Administrator is excluded from the provider-operated functions identified in this requirement. Tenant administrators may manage tenant data and tenant-level configuration only to the extent permitted by the evaluated configuration and the ST.

Table 14. FMT_MOF.1/DBaaS-Modify Dependencies

Dependency	Resolution
FMT_SMF.1	Satisfied by FMT_SMF.1/DBaaS.
FMT_SMR.1	Satisfied by FMT_SMR.1/DBaaS.

10.5. FAU: Security Audit

10.5.1. FAU_SEL.1/DBaaS Selective Audit (Tenant Separation)

FAU_SEL.1.1/DBaaS The TSF shall be able to select the set of events to be audited from the set of all auditable events based on the following attributes: [*tenant identifier, user identifier, service role, object identifier, and event type*].

Application Note: This iteration of the Base PP's FAU_SEL.1 adds tenant-scoped audit selection in a multi-tenant managed service. Restriction of audit record queries to the owning tenant is not audit pre-selection; it is enforced as an access-control rule by FDP_ACF.1.2/DBaaS (tenant subjects access only audit records associated with the same tenant identifier).

Table 15. FAU_SEL.1/DBaaS Dependencies

Dependency	Resolution
FAU_GEN.1	Satisfied by the Base PP FAU_GEN.1.
FMT_MTD.1	Satisfied by the Base PP security management of audit data, refined by FMT_SMF.1/DBaaS for tenant-scoped audit query roles.

10.5.2. FAU_STG.2/DBaaS Protected Audit Trail Storage (Immutable Audit Stream)

FAU_STG.2.1/DBaaS The TSF shall protect the stored audit records in the audit trail from unauthorised deletion, **including deletion attempted by a tenant administrator through TOE interfaces**.

FAU_STG.2.2/DBaaS The TSF shall be able to [**prevent**] unauthorised modifications to the stored audit records in the audit trail, **including modifications attempted by a tenant administrator through TOE interfaces**.

Application Note: This SFR is CC:2022 Part 2 FAU_STG.2 (Protected audit trail storage), iterated with the modification selection completed as "prevent" and refined to state explicitly that tenant administrators are not authorized subjects for modification or deletion of TOE-generated audit records: the TOE provides no tenant-facing interface for those operations. If audit records are exported to an external logging or storage service, the ST shall identify whether the export mechanism, external service, or both are included in the TOE. External services relied upon for storage immutability are addressed by OE.EXTERNAL_SERVICES unless claimed as TOE functionality.

Table 16. FAU_STG.2/DBaaS Dependencies

Dependency	Resolution
FAU_GEN.1	Satisfied by the Base PP FAU_GEN.1.

10.6. FPT: Protection of the TSF

10.6.1. FPT_TUD_DBAAS_EXT.1 Trusted Service Update

FPT_TUD_DBAAS_EXT.1.1 The TSF shall apply updates to the DBMS service software through the service provider's authorized update process using [selection: uniform rolling deployment to all service instances, deployment with tenant-configurable deferral within [assignment: maximum deferral period], deployment within tenant-selectable maintenance windows].

FPT_TUD_DBAAS_EXT.1.2 The TSF shall verify the authenticity and integrity of DBMS service software updates by digital signature before the updated software is placed into service, without requiring tenant administrator intervention.

FPT_TUD_DBAAS_EXT.1.3 The TSF shall provide tenants the ability to determine the version or revision identifier of the DBMS service software currently serving the tenant.

Application Note: Conformance to this component means the service provider stands behind a defined update mechanism; the deployment model of that mechanism is declared through the selection in FPT_TUD_DBAAS_EXT.1.1 rather than prescribed. A continuously deployed service that maintains a single live service target conforms by selecting uniform rolling deployment and identifying the deployment artifacts to which signature verification applies. The signature envelope format is not constrained: X.509 certificate-based signatures, OpenPGP signatures, and detached signatures over deployment artifacts are all acceptable, provided the signature algorithm and its hash are completions allowed by `FCS_COP.1/SigVer` in the mandatory DBMS Cryptographic Functions Module and the verification key is integrity protected. Hash algorithms outside the allowed completions (for example, SHA-1) cannot be claimed. Certificate path validation is in scope of the Functional Package for X.509 Certificates [[X509_FP]] only when certificates are used.

+ Update pipeline mechanics may reside partly in the operational environment, but the update verification and tenant-facing version visibility required by this component are TSF behavior: the TSS shall describe the end-to-end update process, identify where signature verification occurs, and identify the TOE-side enforcement points. An ST in which update handling lies wholly outside the TOE boundary cannot complete this component and therefore cannot claim conformance to this PP-Module. The version or revision identifier of FPT_TUD_DBAAS_EXT.1.3 need not be a semantic version: a build identifier or rollout identifier satisfies the requirement, provided it unambiguously identifies the deployed service software for tenant change-management and support purposes.

Table 17. FPT_TUD_DBAAS_EXT.1 Dependencies

Dependency	Resolution
Signature verification	Satisfied by `FCS_COP.1/SigVer` and its supporting Hash or XOF component as consumed in the mandatory DBMS Cryptographic Functions Module.
FMT_SMF.1 (update management)	Update deployment configuration and deferral policy are managed through `FMT_SMF.1/DBaaS` and restricted to provider roles by `FMT_MOF.1/DBaaS-Modify`.

10.7. Auditable Events for the SFRs of this PP-Module

When this PP-Module is claimed, Table 4: Auditable Events of the Base PP is refined to add the

following entries; this refinement makes the audit records on which this module's Evaluation Activities rely normatively required.

A provider-operated managed service records security-relevant events in two channels, and the table assigns each event to its channel:

- The **DBMS audit trail** is the audit trail of the Base PP. Events assigned to it are generated under the Base PP's FAU_GEN.1, which is claimed unchanged, and are protected by FAU_STG.2/DBaaS.
- The **service event stream** is the tenant-visible service-level audit channel in which lifecycle and control-plane events concerning a tenant's service instance are recorded. It is distinct from the DBMS audit trail and remains available when the database is not serving connections — which is precisely when several of this module's events are generated: the transition to the key-unavailable enforcement state, use of a recovery mechanism, and update deployment all occur while or because the database is not serving tenants. Generation of these events is TSF behavior; the stream itself may be implemented by the TSF or delivered through an audit or event service of the Trusted Platform. The ST shall identify the mechanism that implements the service event stream, its allocation to the TOE, TOE Platform, or Trusted Platform, and the tenant interface through which its records are retrieved. Where the stream is delivered by the Trusted Platform, its integrity and availability are operational environment properties under OE.TRUSTED_PLATFORM and OE.EXTERNAL_SERVICES.

Service event stream records concerning a tenant's service instance, customer-controlled keys, or backups shall be visible to that tenant regardless of the acting subject, including provider-initiated and service-initiated actions. Not every event in the table has a tenant subject: an attempted export of customer-controlled key material or an attempted plaintext restore is most security-relevant when the acting subject is a service provider administrator, and the audit data for such events identifies the acting subject rather than presupposing a tenant context. Attempts made directly against an external key management service under tenant control are recorded by that service and are outside the TOE's audit generation; the module's events cover attempts made through TOE interfaces.

Table 18. Auditable Events for DBaaS Module SFRs

Column 1: Security Functional Requirement	Column 2: Auditable Event(s)	Column 3: Additional Audit Data Contents	Column 4: Audit Channel
FCS_CKM_DBAAS_EXT.1	Key import; key-reference configuration; key-management service authorization failure; key revocation detection; transition to the key-unavailable enforcement state upon expiration of the key-state enforcement interval; denial of access to protected data due to revoked, unavailable, or denied key authorization; use of a documented recovery mechanism; attempted export or recovery of customer-controlled key material	Key reference or key identifier; the identity and role of the acting subject, with the tenant identifier where the subject acts in a tenant context; for enforcement-state transitions, the key-state change that triggered the transition; for recovery-mechanism use, the identity of the authorizing tenant agent. Plaintext key material shall not be included in audit records.	Service event stream. Key import and key-reference configuration performed through database interfaces may instead appear in the DBMS audit trail, as identified in the ST.
FDP_RIP.1/DBaaS	None	None	—
FDP_ACC.1/DBaaS	None	None	—
FDP_ACF.1/DBaaS	All denied accesses under the Tenant Isolation SFP; use of an evaluated cross-tenant sharing mechanism, where claimed	Subject tenant identifier, object tenant identifier, and operation	DBMS audit trail
FRU_RSA.1/DBaaS	Tenant resource quota violation	Tenant identifier and affected resource	DBMS audit trail
FRU_RSG_EXT.1	Enforcement action taken on quota exhaustion (termination, throttling, queueing, or rejection)	Tenant identifier, affected resource, and enforcement action	DBMS audit trail
FDP_BKP_EXT.1	Backup creation; restore initiation and completion; restore authorization failure; attempted plaintext restore or export of protected tenant data	Tenant identifier of the affected data and backup identifier; for restore, restore-failure, and attempted-restore events, the identity and role of the acting subject	Service event stream
FIA_USB.1/DBaaS	Unsuccessful binding of tenant security attributes to a subject	Attempted tenant identifier, user identifier, and service role	DBMS audit trail

Column 1: Security Functional Requirement	Column 2: Auditable Event(s)	Column 3: Additional Audit Data Contents	Column 4: Audit Channel
FMT_SMR.1/DBaaS	Modifications to the users associated with a role	Role and user identity	DBMS audit trail or service event stream, as identified in the ST
FMT_SMF.1/DBaaS	Use of the management functions defined by this module	Function invoked; identity and role of the invoking subject, including automated autonomous management logic where selected; and the tenant identifier where the function acts on a tenant context	DBMS audit trail or service event stream, as identified in the ST
FMT_MOF.1/DBaaS-Disable	Attempted disabling of audit generation or of data-at-rest encryption for protected tenant data	Role and identity of the attempting subject	DBMS audit trail or service event stream, as identified in the ST
FMT_MOF.1/DBaaS-Modify	Modifications to the behaviour of provider-managed functions (resource governance policies, patching and updates, audit export configuration)	Function modified; identity and role of the invoking subject, including automated autonomous management logic where selected	Service event stream
FAU_SEL.1/DBaaS	All modifications to the audit configuration that occur while the audit collection functions are operating, including tenant-scoped selection changes	The identity of the authorized administrator that made the change, and the tenant identifier where the change is tenant-scoped	DBMS audit trail or service event stream, as identified in the ST
FAU_STG.2/DBaaS	Attempted unauthorized deletion or modification of stored audit records	Role and identity of the attempting user, and tenant identifier of the affected records	DBMS audit trail
FPT_TUD_DBAAS_EXT.1	Update deployment initiation and completion; signature verification failure; update failure; tenant deferral or maintenance-window events, where selected	The service software version or revision identifiers before and after the update	Service event stream

Chapter 11. Security Assurance Requirements (SARs)

This PP-Module does not define additional Security Assurance Requirements beyond those already specified by the collaborative Protection Profile for Database Management Systems (cPP_DBMS) Version 2.0.

All SARs defined in the cPP_DBMS apply directly and fully to TOEs claiming conformance with this DBaaS Module. The applicable SAR set is inherited from cPP_DBMS Version 2.0: EAL2 as defined in CC:2022 Part 5 [[CC5]], augmented by ALC_FLR.3 Systematic flaw remediation.

The ACE assurance requirements of CC:2022 Part 3 [[CC3]] apply to the evaluation of this PP-Module itself, within the evaluation of a PP-Configuration that includes it.

Appendix A: Extended Component Definitions

This appendix defines the extended components introduced by this PP-Module. The cryptographic, key-management, and trusted-channel extended components relied upon by this module are defined in the DBMS Cryptographic Functions Module and are not redefined here.

A.1. FCS: Cryptographic Support

A.1.1. FCS_CKM_DBAAS_EXT: Customer-Controlled Keys

A.1.1.1. Family Behaviour

This family defines DBaaS-specific requirements for customer-controlled database master keys. It complements the DBMS Cryptographic Functions Module by addressing the managed-service separation requirement that service provider administrators cannot access customer-controlled master key material through TOE interfaces.

A.1.1.2. Component levelling

FCS_CKM_DBAAS_EXT.1 requires the TOE to support customer-controlled master keys, prevent service provider administrator access to plaintext key material, and prevent access to protected data, within a defined key-state enforcement interval, when authorized key use is revoked, unavailable, or denied.

A.1.1.3. Management: FCS_CKM_DBAAS_EXT.1

The following actions could be considered for the management functions in FMT: configuration of customer-controlled key references, key import, external KMS integration, key revocation behavior, recovery mechanisms, and key-use auditing.

A.1.1.4. Audit: FCS_CKM_DBAAS_EXT.1

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST: key import, key reference configuration, KMS authorization failure, key revocation detection, transition to the key-unavailable enforcement state, protected-data access denial due to unavailable key authorization, use of a documented recovery mechanism, and attempted key export or recovery.

A.1.1.5. FCS_CKM_DBAAS_EXT.1 Customer-Controlled Keys

Hierarchical to: No other components.

Dependencies: FDP_ITC_EXT.1, FCS_CKM.6, and FDP_DAR_EXT.1 (DBMS Cryptographic Functions Module); FMT_SMF.1.

FCS_CKM_DBAAS_EXT.1.1 The TSF shall support customer-controlled master encryption keys using one or more defined customer-controlled mechanisms.

FCS_CKM_DBAAS_EXT.1.2 The TSF shall not provide an interface by which a service provider administrator can view, export, or recover plaintext customer-controlled master key material.

FCS_CKM_DBAAS_EXT.1.3 The TSF shall prevent access to protected database data no later than [assignment: key-state enforcement interval] after authorized use of the applicable customer-controlled master key is revoked, unavailable, or denied, except for data that remains available through an explicitly documented and evaluated recovery mechanism whose use requires authorization by the tenant or an agent under the tenant's control.

A.2. FDP: User Data Protection

A.2.1. FDP_BKP_EXT: Protected Backup and Restore

A.2.1.1. Family Behaviour

This family defines requirements specific to the backup and restore path in managed DBaaS environments, ensuring that backup and restore do not become a plaintext disclosure path for service provider administrators and that restore preserves tenant isolation. Data-at-rest protection of backup data is provided by the DBMS Cryptographic Functions Module and is not restated by this family.

A.2.1.2. Component levelling

FDP_BKP_EXT.1 requires the TOE to prevent plaintext restore or export of protected tenant data by service provider administrators without authorized key use, and to bind restored data to the originating tenant.

A.2.1.3. Management: FDP_BKP_EXT.1

The following actions could be considered for the management functions in FMT: configuration of backup schedules, backup destinations, restore authorization roles, and backup encryption and key-binding settings.

A.2.1.4. Audit: FDP_BKP_EXT.1

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST: backup creation, restore initiation and completion, restore authorization failure, and attempted plaintext export of backup data.

A.2.1.5. FDP_BKP_EXT.1 Protected Backup and Restore

Hierarchical to: No other components.

Dependencies: FCS_CKM_DBAAS_EXT.1, FDP_ACC.1. Data-at-rest protection of backup data is inherited from FDP_DAR_EXT.1 of the DBMS Cryptographic Functions Module.

FDP_BKP_EXT.1.1 The TSF shall not provide an interface by which a service provider administrator can restore or export protected tenant data from a backup in plaintext without authorized use of the applicable customer-controlled master key.

FDP_BKP_EXT.1.2 The TSF shall bind restored tenant data to the originating tenant identifier such that a restore operation does not place tenant data outside the Tenant Isolation SFP.

A.3. FRU: Resource Utilisation

A.3.1. FRU_RSG_EXT: Resource Governance Enforcement

A.3.1.1. Family Behaviour

This family defines requirements for the enforcement action the TOE takes when a resource quota is exceeded. CC Part 2 FRU_RSA (Resource allocation) requires the enforcement of maximum quotas but does not specify the action taken on quota exhaustion; this family makes that action an evaluable property. Quota enforcement itself is claimed via CC Part 2 FRU_RSA.1 and is not redefined by this family.

A.3.1.2. Component levelling

FRU_RSG_EXT.1 requires the TOE to take a defined enforcement action on operations that exceed enforced resource quotas.

A.3.1.3. Management: FRU_RSG_EXT.1

The following actions could be considered for the management functions in FMT: configuration of tenant resource quotas, resource pools, workload queues, throttling behavior, enforcement thresholds, and authorized roles for resource governance management.

A.3.1.4. Audit: FRU_RSG_EXT.1

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST: resource quota configuration changes, quota violations, throttling, queueing, rejection, and termination of tenant operations due to resource governance.

A.3.1.5. FRU_RSG_EXT.1 Resource Governance Enforcement Action

Hierarchical to: No other components.

Dependencies: FRU_RSA.1; FMT_SMF.1.

FRU_RSG_EXT.1.1 The TSF shall [selection: terminate, throttle, queue, reject, [assignment: other enforcement action]] operations that exceed the resource quotas enforced by FRU_RSA.1.

A.4. FPT: Protection of the TSF

A.4.1. FPT_TUD_DBAAS_EXT: Trusted Service Update

A.4.1.1. Family Behaviour

This family defines requirements for provider-managed trusted update of the DBMS service software: the deployment model is declared, updates are signature-verified before being placed

into service, and the deployed service software version is visible to tenants. It is specific to provider-operated DBaaS TOEs and is distinct from the FPT_TUD_EXT family defined by the DBMS Cloud Module for tenant-managed trusted update; the two families are never claimed together because the Cloud and DBaaS Modules are mutually exclusive. CC Part 2 FPT (and the Cloud Module's FPT_TUD_EXT) address updates that a TOE administrator obtains, verifies, and installs; no existing family addresses updates that the service provider deploys to a running service without tenant installation, which is the behavior this family makes evaluable.

A.4.1.2. Component levelling

FPT_TUD_DBAAS_EXT.1 requires the TOE to apply updates through the provider's authorized update process under a declared deployment model, to verify update authenticity and integrity by digital signature before the updated software is placed into service, and to make the deployed service software version or revision identifier visible to tenants.

A.4.1.3. Management: FPT_TUD_DBAAS_EXT.1

The following actions could be considered for the management functions in FMT: update deployment configuration, update scheduling, tenant deferral policy and maintenance windows where selected, update source trust anchors, and update audit settings.

A.4.1.4. Audit: FPT_TUD_DBAAS_EXT.1

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST: update deployment initiation and completion, signature verification failure, update failure, tenant deferral or maintenance-window events where selected, and unauthorized attempts to block or delay updates.

A.4.1.5. FPT_TUD_DBAAS_EXT.1 Trusted Service Update

Hierarchical to: No other components.

Dependencies: No dependencies. Signature verification is provided by the mandatory DBMS Cryptographic Functions Module.

FPT_TUD_DBAAS_EXT.1.1 The TSF shall apply updates to the DBMS service software through the service provider's authorized update process using [selection: uniform rolling deployment to all service instances, deployment with tenant-configurable deferral within [assignment: maximum deferral period], deployment within tenant-selectable maintenance windows].

FPT_TUD_DBAAS_EXT.1.2 The TSF shall verify the authenticity and integrity of DBMS service software updates by digital signature before the updated software is placed into service, without requiring tenant administrator intervention.

FPT_TUD_DBAAS_EXT.1.3 The TSF shall provide tenants the ability to determine the version or revision identifier of the DBMS service software currently serving the tenant.

Appendix B: SFR Dependency Rationale

The following table summarizes the resolution of all SFR dependencies for the mandatory SFRs of this PP-Module. Dependencies are resolved within this module, by the Base PP (cPP_DBMS), or by the DBMS-specific and Catalogue-derived components included through the mandatory DBMS Cryptographic Functions Module.

Table 19. SFR Dependency Summary

SFR	Dependencies	Resolution
FCS_CKM_DBAAS_EXT.1	FDP_ITC_EXT.1, FCS_CKM.6, FDP_DAR_EXT.1, FMT_SMF.1	DBMS Crypto Module; FMT_SMF.1/DBaaS
FDP_RIP.1/DBaaS	None	N/A
FDP_ACC.1/DBaaS	FDP_ACF.1	FDP_ACF.1/DBaaS
FDP_ACF.1/DBaaS	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/DBaaS; Base PP FMT_MSA.3
FRU_RSA.1/DBaaS	None (management via FMT_SMF.1)	FMT_SMF.1/DBaaS
FRU_RSG_EXT.1	FRU_RSA.1, FMT_SMF.1	FRU_RSA.1/DBaaS; FMT_SMF.1/DBaaS
FDP_BKP_EXT.1	FCS_CKM_DBAAS_EXT.1, FDP_ACC.1 (DAR inherited)	This module; FDP_ACC.1/DBaaS; data-at-rest inherited from Crypto Module FDP_DAR_EXT.1
FIA_USB.1/DBaaS	FIA_ATD.1	Base PP user attribute definition
FMT_SMR.1/DBaaS	FIA_UID.1	Base PP FIA_UID.2 (hierarchical to FIA_UID.1)
FMT_SMF.1/DBaaS	None	N/A
FMT_MOF.1/DBaaS-Disable	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1/DBaaS; FMT_SMR.1/DBaaS
FMT_MOF.1/DBaaS-Modify	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1/DBaaS; FMT_SMR.1/DBaaS
FAU_SEL.1/DBaaS	FAU_GEN.1, FMT_MTD.1	Base PP FAU_GEN.1; Base PP audit data management refined by FMT_SMF.1/DBaaS
FAU_STG.2/DBaaS	FAU_GEN.1	Base PP FAU_GEN.1
FPT_TUD_DBAAS_EXT.1	Signature verification; FMT_SMF.1 (update management)	DBMS Crypto Module (`FCS_COP.1/SigVer` and supporting Hash or XOF component); FMT_SMF.1/DBaaS with FMT_MOF.1/DBaaS-Modify

Appendix C: Consistency Rationale

This appendix demonstrates that this PP-Module is consistent with, and does not contradict, the Base PP (cPP_DBMS) Version 2.0 and the mandatory DBMS Cryptographic Functions Module, as required for Exact Conformance of a PP-Module.

C.1. Consistency of TOE Type

The Base PP defines a Database Management System TOE. This PP-Module constrains that TOE type to a DBMS offered as a managed Database-as-a-Service. It does not introduce a different TOE type; it scopes the deployment model and adds DBaaS-specific functionality. All Base PP SFRs continue to apply to the DBMS TOE.

C.2. Consistency of Security Problem Definition

The threats and assumptions in this PP-Module supplement those of the Base PP and address the multi-tenant, provider-operated DBaaS deployment context (cross-tenant access, provider-administrator key disclosure, resource contention, audit tampering, tenant-administrator abuse, secrets exposure, and unauthorized service update). The organizational security policies (P.AUDIT_RETENTION, P.ACCESS_CONTROL_POLICY) are additive and have no Base PP counterpart with which to conflict. They do not remove or weaken any Base PP threat or assumption. The Trusted Platform assumptions (A.TRUSTED_PLATFORM_ADMIN, A.TRUSTED_PLATFORM_CONTROLS) scope the infrastructure trust appropriate to a managed service and are consistent with the CCiTC SaaS evaluation model; they do not contradict the Base PP's operational environment assumptions.

C.3. Consistency of Data-in-Transit Protection (Base PP A.CONNECT)

The Base PP does not define cryptographic SFRs. It addresses the protection of transmitted data through the environmental assumption A.CONNECT, which also discharges the FPT_ITT.1 dependency of FPT_TRC.1 for distributed TOEs.

For PP-Configurations that include this PP-Module, the DBMS Cryptographic Functions Module is mandatory and provides TOE-enforced protection for data transmitted between the TOE and external entities through its mandatory FDP_DIT_EXT.1 requirement, using TLS and X.509 components from the applicable Functional Packages [[TLS_FP]][[X509_FP]]. CCDB-018 provides cryptographic primitives and does not provide TLS or certificate-validation components. FDP_DIT_EXT.1 supplements A.CONNECT; it does not replace it. This module inherits, and does not redefine, data-in-transit protection; the inherited requirement strengthens, and does not contradict, the Base PP.

Transfers between separate parts of a distributed TOE are a distinct leg of A.CONNECT, and FDP_DIT_EXT.1 does not address them: it covers channels between the TOE and external entities, not inter-TSF transfer. The assumption is therefore retained in full and remains the basis for the inter-TSF leg, which also discharges the FPT_ITT.1 dependency of FPT_TRC.1. In a DBaaS deployment that inter-TSF protection is provided by the Trusted Platform under OE.TRUSTED_PLATFORM.

C.4. Consistency of Security Objectives

The TOE security objectives introduced by this PP-Module (O.CUSTOMER_CONTROLLED_KEYS, O.LOGICAL_ISOLATION, O.RESOURCE_GOVERNANCE, O.IMMUTABLE_AUDIT, O.PROTECTED_BACKUP, O.TRUSTED_UPDATE) address the DBaaS-specific threats and are additive to the Base PP objectives. The operational environment objectives address the Trusted Platform and external service dependencies and are consistent with the Base PP operational environment objectives.

C.5. Consistency of Security Functional Requirements

All CC Part 2 components reused in this PP-Module are iterated with a /DBaaS label (FDP_RIP.1/DBaaS, FDP_ACC.1/DBaaS, FDP_ACF.1/DBaaS, FRU_RSA.1/DBaaS, FIA_USB.1/DBaaS, FMT_SMR.1/DBaaS, FMT_SMF.1/DBaaS, FMT_MOF.1/DBaaS-Disable, FMT_MOF.1/DBaaS-Modify, FAU_SEL.1/DBaaS, FAU_STG.2/DBaaS) so that components also defined by the Base PP are refined for the multi-tenant managed-service context without altering the Base PP requirements themselves; the Base PP components remain claimed in their original form. The extended components introduced by this PP-Module (FCS_CKM_DBAAS_EXT.1, FDP_BKP_EXT.1, FRU_RSG_EXT.1, FPT_TUD_DBAAS_EXT.1) are DBaaS-specific, are defined only where no CC Part 2 component provides the required behavior, and do not duplicate or contradict any Base PP or Crypto Module component. Cryptographic functionality is delegated entirely to the mandatory DBMS Cryptographic Functions Module.

Appendix D: SFR List

Table 20. Security Functional Requirements

Requirement Class	Requirement Component	Type
Cryptographic Support (FCS)	FCS_CKM_DBAAS_EXT.1 Customer-Controlled Keys	Mandatory
	DBMS Cryptographic Functions Module key-management, key-destruction, and data-at-rest requirements, including consumed Catalogue components; applicable Functional Package trusted-channel requirements	Mandatory dependency
User Data Protection (FDP)	FDP_RIP.1/DBaaS Residual Information Protection	Mandatory
	FDP_ACC.1/DBaaS Tenant Isolation Policy	Mandatory
	FDP_ACF.1/DBaaS Tenant Isolation Policy Rules	Mandatory
	FDP_BKP_EXT.1 Protected Backup and Restore	Mandatory
Resource Utilisation (FRU)	FRU_RSA.1/DBaaS Maximum Quotas (Tenant Resources)	Mandatory
	FRU_RSG_EXT.1 Resource Governance Enforcement Action	Mandatory
Identification and Authentication (FIA)	FIA_USB.1/DBaaS User-Subject Binding	Mandatory
Security Management (FMT)	FMT_SMR.1/DBaaS Security Roles	Mandatory
	FMT_SMF.1/DBaaS Specification of Management Functions	Mandatory
	FMT_MOF.1/DBaaS-Disable Management of Security Functions Behaviour (Disable Restriction)	Mandatory
	FMT_MOF.1/DBaaS-Modify Management of Security Functions Behaviour (Provider Functions)	Mandatory
Security Audit (FAU)	FAU_SEL.1/DBaaS Selective Audit	Mandatory
	FAU_STG.2/DBaaS Protected Audit Trail Storage (Immutable Audit Stream)	Mandatory
Protection of the TSF (FPT)	FPT_TUD_DBAAS_EXT.1 Trusted Service Update	Mandatory

Appendix E: Glossary

Table 21. Terms and Definitions

Term	Definition
Customer-Controlled Key	A master encryption key whose use is controlled by the customer (tenant), such that the service provider cannot obtain plaintext key material through TOE interfaces. Includes BYOK, HYOK, external KMS-managed keys, and key-reference or key-handle models.
Service Event Stream	The tenant-visible service-level audit channel in which lifecycle and control-plane events concerning a tenant's service instance are recorded. Distinct from the DBMS audit trail and available when the database is not serving connections; may be implemented by the TSF or delivered through an audit or event service of the Trusted Platform, as identified in the ST. See the auditable-events refinement.
Service Provider Administrator	Module-level role label for an administrator who operates the managed DBMS service on behalf of the provider. Constrained by this module from accessing customer-controlled key material and tenant data except through interfaces and roles explicitly identified in the ST. The ST maps this label to the TOE's own role terminology (see the FMT_SMR.1/DBaaS application note).
Tenant	A customer of the managed service whose data, metadata, and resources are logically isolated from those of other customers sharing the DBMS service infrastructure.
Tenant Administrator	Module-level role label for a customer role that manages tenant data and tenant-level configuration to the extent permitted by the evaluated configuration. Excluded from disabling security-critical functions identified in this module. The ST maps this label to the TOE's own role terminology (see the FMT_SMR.1/DBaaS application note).
Tenant User	Module-level role label for a customer role that accesses tenant data through the tenant-facing database interfaces without tenant-level administrative authority. The ST maps this label to the TOE's own role terminology (see the FMT_SMR.1/DBaaS application note).
Trusted Platform	The cloud hosting environment that provides infrastructure services to the TOE and TOE Platform, relied upon to satisfy operational environment assumptions and objectives and accepted by the applicable evaluation scheme.
TOE Platform	The immediate software, firmware, or hardware environment on which the DBMS TOE executes and from which the TOE obtains supporting services.

Appendix F: Acronyms

Table 22. Acronyms used in this PP-Module

Acronym	Meaning
BYOK	Bring Your Own Key
CC	Common Criteria
CCiTC	Common Criteria in the Cloud Technical Community
cPP	collaborative Protection Profile
DBaaS	Database-as-a-Service
DBMS	Database Management System
DEK	Data Encryption Key
HYOK	Hold Your Own Key
IaaS	Infrastructure-as-a-Service
KMS	Key Management Service
PaaS	Platform-as-a-Service
PP	Protection Profile
SaaS	Software-as-a-Service
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSS	TOE Summary Specification