Supporting Document

Evaluation Activities for collaborative PP-Module for DBMS in the Cloud

Version 0.4, 2026-06-30

Table of Contents

Chapter 1. Revision History

Table 1. Revision history

Version	Date	Description
0.1	2025-03-12	Initial Evaluation Activities for the DBMS in the Cloud PP-Module.
0.2	2026-01-25	CC:2022 alignment: updated Evaluation Activities for the reformatted SFRs and CC:2022 conformance claims.
0.3	2026-06-26	Aligned with the v0.3 PP-Module: deferred cryptographic SFR evaluation, including FDP_DIT_EXT.1, to the DBMS Cryptographic Functions Module SD; aligned Base PP references with cPP_DBMS Version 2.0; and adopted the shared AsciiDoc rendering assets.
0.4	2026-06-30	Version aligned with the v0.4 module and SD set following the relocation of FDP_DIT_EXT.1 to the DBMS Cryptographic Functions Module. Core cryptographic evaluation of FDP_DIT_EXT.1 is performed under the Crypto Module SD; this Cloud SD retains cloud-specific mapping, configuration, and integration checks.
0.4	2026-07-07	Technology area and TOE characterization broadened to tenant-operated deployments of cloud-native or lift-and-shift DBMS products, matching the PP-Module scope clarification.
0.4	2026-07-07	Renamed the FAU_GEN.1 and FAU_STG.1 sections to FAU_GEN.1/Cloud and FAU_STG.2/Cloud following the module's iteration changes; noted the Base PP SD's continuing coverage of the Base PP's FAU_GEN.1; aligned the audit modification-protection activities with the completed "prevent" selection.
0.4	2026-07-08	Added Evaluation Activities for the new FPT_FLS.1 SFR. The activities are driven by the ST's completions (claimed failure types and TSS-defined secure state) rather than a prescribed failure list, with simulation or provider-supported demonstration permitted where a failure type cannot practically be induced.
0.4	2026-07-08	Removed the FMT_SMF.1/Cloud guidance item for data-at-rest encryption configuration: that management function is not in the module's FMT_SMF.1/Cloud list and is specified and evaluated under the DBMS Crypto Module.

Version	Date	Description
0.4	2026-07-08	Added TSS activities for the new normative channel-binding elements: FIA_UID_EXT.1.4 (identity-provider channel, exercised by the existing Test 12) and FMT_MTD_EXT.1.3 (configuration and secret management channels); TLS protocol behavior remains evaluated under the DBMS Crypto Module SD and the TLS Functional Package.
0.4	2026-07-08	Evaluation-activity corrections: FIA_UID_EXT.1 Test 1 recast as a negative test (no TSF-mediated actions before identification and authentication, consistent with the Base PP's FIA_UID.2/FIA_UAU.2 — the previous test assumed permitted pre-identification actions and was unexecutable). Test 12's certificate-rejection step replaced with confirmation that certificate validation is covered by the DBMS Crypto Module and TLS/X.509 Functional Package evidence, removing duplicated TLS testing. FMT_SMR.1/Cloud activities keyed to the roles assigned in the ST rather than levying role minimums beyond the SFR. Operational-environment mechanisms marked as supplementary, non-TSF evidence in the FPT_ITT.1 mechanisms list and Test 5, FPT_TUD_EXT.1 Test 5 (registry/orchestrator enforcement), and FPT_SBT_EXT.1 Test 4 (admission controllers), consistent with the PP-Module's Security Function Allocation.
0.4	2026-07-08	FMT_MTD_EXT.1 section retitled to cover FMT_MTD.1/Cloud and FMT_MTD_EXT.1 together following the module's component split; element reference updated to FMT_MTD_EXT.1.2 for the channel binding.
0.4	2026-07-08	Editorial sweep: hardcoded section numbers replaced with section names in the Structure of the Document; RFC-2119 capitals normalized in the Evaluation Cloud Environment Requirements; element reference updated to FMT_SMF.1.1/Cloud; CEM cross-reference appendix scope clarified (narrative FAU/FIA/FMT/FPT activities refine the generic ASE/AGD/ATE_IND work units).

Chapter 2. Introduction

2.1. Technology Area and Scope of Supporting Document

This Supporting Document (SD) defines Evaluation Activities (EAs) for the **collaborative PP-Module for DBMS in the Cloud** (DBMS_Cloud_MOD), version 0.4. The technology area addressed is Database Management Systems (DBMS) deployed in tenant-operated cloud Infrastructure-as-a-Service (IaaS) or Platform-as-a-Service (PaaS) environments. This covers both cloud-native DBMS products designed for cloud deployment and traditional DBMS products deployed using a "lift-and-shift" model.

In this deployment model, the DBMS product (the Target of Evaluation, or TOE) is:

- A cloud-native DBMS, or a traditional DBMS functionally equivalent to its on-premises version
- Deployed by the customer or tenant, not by the cloud service provider
- Hosted on cloud infrastructure that provides compute, storage, network, and supporting services
- Integrated with cloud-native identity, audit, and configuration management services

This SD provides Evaluation Activities that evaluators shall perform to determine whether a TOE satisfies the Security Functional Requirements (SFRs) specified in the DBMS Cloud PP-Module. These activities complement the Evaluation Activities defined in the Supporting Document for the collaborative Protection Profile for Database Management Systems (cPP_DBMS SD), which remains applicable for all SFRs inherited from the Base PP.

The Evaluation Activities in this SD are derived from the Common Evaluation Methodology (CEM:2022) work units and are aligned with the framework defined in CC:2022 Part 4 for specifying objective, repeatable, and reproducible evaluation methods.

2.2. Structure of the Document

This Supporting Document is organized to mirror the structure of the PP-Module and follows the SFR class hierarchy defined in CC:2022 Part 2.

The **General Guidance for Evaluators** section provides overarching guidance applicable across multiple SFRs, including:

- Determining TOE boundaries in cloud deployments
- Handling selections and assignments in the ST
- Cloud-specific evaluation considerations
- Trusted Platform assumptions and their evaluation implications
- Multi-module evaluation coordination

The **Assurance Activities Overview** section describes:

- Mapping to Base PP SARs
- Cloud-specific assurance activities
- Documentation requirements for cloud deployments

Subsequent sections define Evaluation Activities organized by SFR class:

- FAU: Security Audit
- FIA: Identification and Authentication
- FMT: Security Management
- FPT: Protection of the TSF
- FDP: User Data Protection and Crypto Module coordination

Within each class section, Evaluation Activities are specified for each SFR, organized into:

- **TSS Activities**: Verification of the TOE Summary Specification
- **Guidance Activities**: Verification of operational and preparative guidance
- **Test Activities**: Independent functional testing procedures

2.3. Terminology

The following terms are used throughout this Supporting Document:

Evaluation Activity (EA)

An activity derived from one or more CEM work units that specifies the actions evaluators shall perform to determine whether the TOE meets a specific SFR or SAR. Evaluation Activities are objective, repeatable, and produce determinate results.

TOE Summary Specification (TSS)

The section of the Security Target that describes how the TOE Security Functionality (TSF) meets each Security Functional Requirement. Evaluators verify that the TSS provides sufficient detail to understand the security mechanisms implemented.

Guidance Documentation

The set of documents provided by the developer that describe how to securely install, configure, and operate the TOE. For cloud deployments, this includes cloud-specific deployment guides, configuration references, and integration documentation.

Test

A procedure performed by the evaluator to verify that the TSF behaves as specified. Tests include test objectives, test setup, test procedures, and expected results.

Selection

An operation performed by the ST author to choose one or more items from a list provided in an SFR component. The evaluator verifies that selections are valid and that the TSS describes how the selected functionality is implemented.

Assignment

An operation performed by the ST author to specify a value or set of values for a parameter in an SFR component. The evaluator verifies that assignments are appropriate and that the TSS describes how the assigned values are implemented.

Trusted Platform

The cloud infrastructure and services relied upon by the TOE to enforce its security policies. Per the CCiTC architectural model, the Trusted Platform includes compute, storage, network resources, orchestration systems, and cloud-native services. The Trusted Platform is part of the operational environment and is not within the evaluation scope.

Cloud IAM

Cloud-native Identity and Access Management services provided by cloud platforms (e.g., AWS IAM, Azure Active Directory, Google Cloud IAM) that the TOE may integrate with for user authentication and authorization.

SIEM

Security Information and Event Management systems that aggregate, correlate, and analyze security events from multiple sources. The TOE may export audit data to SIEM systems.

2.4. Relationship to Other Documents

This Supporting Document must be used in conjunction with the following documents:

2.4.1. Primary PP-Module

- **collaborative PP-Module for DBMS in the Cloud (DBMS_Cloud_MOD)**, version 0.4

  This SD provides Evaluation Activities for the SFRs defined in the PP-Module. Evaluators shall verify conformance to all mandatory SFRs and any selection-based SFRs included in the Security Target.

2.4.2. Base PP and Supporting Document

- **collaborative Protection Profile for Database Management Systems (cPP_DBMS)**

  The Base PP, Version 2.0 dated 27 April 2026, must be claimed in conjunction with this PP-Module. All SFRs and SARs from the cPP_DBMS apply to TOEs claiming conformance to the DBMS Cloud PP-Module.

- **Supporting Document for cPP_DBMS (cPP_DBMS SD)**

  The Base PP SD provides Evaluation Activities for SFRs inherited from the cPP_DBMS. When evaluating a TOE claiming conformance to the DBMS Cloud PP-Module, evaluators shall apply both this SD and the cPP_DBMS SD. Where SFRs are refined or iterated by the PP-Module, the Evaluation Activities in this SD take precedence or supplement those in the Base PP SD.

2.4.3. Required Module and Supporting Document

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

  The DBMS Crypto Module is a mandatory component of any PP-Configuration claiming this PP-Module. Evaluators shall verify that the ST includes the DBMS Crypto Module for every evaluation claiming this PP-Module. The Crypto Module provides the data-at-rest and data-in-transit cryptographic requirements used by the Cloud PP-Configuration.

- **Supporting Document for DBMS Cryptographic Module (DBMS_MOD_CRYPTO SD)**

  Evaluators shall apply the DBMS_MOD_CRYPTO SD for DBMS-specific cryptographic integration activities in every evaluation claiming this PP-Module, and shall apply the applicable Catalogue and Functional Package Evaluation Activities for algorithm and protocol behavior. This SD adds Cloud-specific mapping, configuration, and integration checks where cloud deployment introduces additional evidence needs.

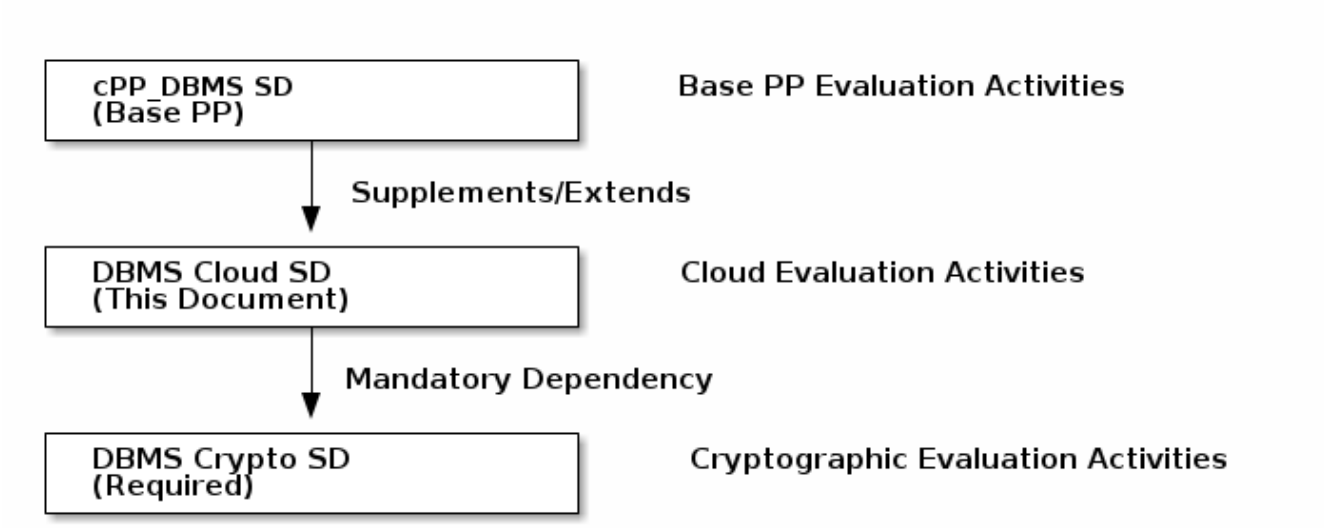
Selection of the Cloud Module does not automatically select the Crypto Module's Enterprise Enhanced use case. When the ST claims Enterprise Enhanced, the evaluator performs the use-case selection-conformance check defined in the Crypto Module SD; this Cloud SD adds no alternative algorithm selections or algorithm Evaluation Activities.

2.4.4. CC Standards

- **Common Criteria for Information Technology Security Evaluation, CC:2022** (Parts 1-5)
- **Common Methodology for Information Technology Security Evaluation, CEM:2022**

2.4.5. Layering of Supporting Documents

Supporting Documents layer in the same manner as PP-Modules:



Evaluators shall apply all three SDs for every evaluation of the DBMS Cloud Module.

- Data-in-Transit: The DBMS Crypto SD is applied for TLS testing required for cloud management

interfaces and other external service channels, including HTTPS interfaces implemented over TLS.

- Data-at-Rest: The DBMS Crypto SD is applied for the selected Crypto Module `FDP_DAR_EXT.1` strategy. This Cloud SD verifies cloud-deployment integration and documentation consistency only.

Chapter 3. General Guidance for Evaluators

This section provides guidance applicable across multiple Evaluation Activities in this Supporting Document. Evaluators shall consider this guidance when performing any evaluation of a TOE claiming conformance to the DBMS Cloud PP-Module.

3.1. TOE Boundary in Cloud Environments

3.1.1. Determining the TOE Boundary

In cloud deployment contexts, establishing the correct TOE boundary is critical for a valid evaluation. The PP-Module does not prescribe one allocation for every database architecture. The evaluator shall verify that the Security Target clearly delineates the allocation used by the evaluated configuration.

Components that may be included in the TOE include:

- The DBMS application software and any tightly integrated subsystems
- Interfaces used to configure and manage security-relevant behavior
- Internal communications between distributed DBMS components
- Any embedded runtime used to bootstrap or orchestrate the DBMS (e.g., sidecar containers, initialization scripts)
- Management interfaces exposed to administrators and cloud services

Components that are typically outside the TOE, but may be included when the ST defines and evaluates them as part of the TOE, include:

- The hypervisor or container runtime environment
- The cloud control plane and management APIs
- Cloud-native IAM services (though the TOE integrates with them)
- Cloud-native logging, monitoring, and key management services
- The underlying hardware, network infrastructure, and storage systems
- Orchestration systems (e.g., Kubernetes, Terraform), except for TOE-specific components included in the TOE

The evaluator shall classify components according to the ST boundary and their security behavior in the evaluated configuration, rather than according to provider ownership or the general service category alone.

3.1.2. Distinction Between TOE and Trusted Platform

The evaluator shall understand the CCiTC Trusted Platform model:

- The **Trusted Platform** is the set of cloud infrastructure and services that the TOE relies upon but that are outside the TOE boundary

- The TOE **assumes** the Trusted Platform operates correctly per the assumptions in the PP-Module (A.TRUSTED_PLATFORM, A.CLOUD_SERVICE_INTEGRITY)
- The evaluator does **not** evaluate Trusted Platform properties as TOE functionality
- The evaluator **does** evaluate the TOE behavior at the boundary, including its integration with and stated reliance upon the Trusted Platform, as required by the applicable SFRs and Evaluation Activities
- The evaluation authority determines whether the evidence offered for Trusted Platform assumptions and Operational Environment objectives is acceptable under scheme policy

This distinction has direct implications for how certain SFR test activities are scoped. In particular, identity assertion validation is evaluated only at the TOE boundary; the evaluator does not re-test the correctness of IAM assertion generation performed by the Trusted Platform. See the FIA_UID_EXT.1-related activities in this SD for specific guidance on identity assertion validation scoping.

3.1.3. Evaluator Actions for TOE Boundary

The evaluator shall:

1. Verify that the ST clearly describes the TOE boundary for cloud deployments
2. Verify that the ST correctly identifies components within vs. outside the TOE
3. Verify that the TOE description addresses all deployment configurations claimed (VMs, containers, clusters)
4. Verify that interfaces between the TOE and Trusted Platform are clearly identified
5. Verify that the TSS identifies, for each claimed SFR, the security behavior performed by the TOE and any supporting property relied upon from the TOE Platform, Trusted Platform, or another operational environment component
6. Confirm that Trusted Platform evidence is not used to satisfy a claimed TOE SFR unless the applicable requirement expressly permits use of a platform-provided mechanism
7. Confirm that each external reliance is linked to an assumption or Operational Environment objective and to evidence submitted for acceptance under the applicable scheme policy

3.2. Handling Selections and Assignments

3.2.1. Evaluating SFRs with Selections

When an SFR includes a selection operation, the evaluator shall:

1. Verify that the ST author selected one or more valid options from the selection list
2. Verify that selected options are consistent with the TOE's actual capabilities
3. Verify that the TSS describes how the selected functionality is implemented
4. Verify that guidance documentation describes how to configure and use the selected functionality

5. Perform tests that exercise the selected functionality

When the ST author selects options that invoke additional requirements:

- Verify that the DBMS Crypto Module is included in the PP-Configuration. This is required for all evaluations claiming this PP-Module and is not contingent on any specific selection.
- Verify that the ST identifies which Crypto Module `FDP_DAR_EXT.1` strategy was selected (Storage-Scope Encryption or Granular Data Encryption) and that the TSS description is consistent with that selection.
- Verify that the ST identifies which protocol was selected in FDP_DIT_EXT.1 and includes the corresponding Functional Package components. HTTPS is treated as HTTP over the selected TLS channel rather than as a separate cryptographic SFR.
- If "integrity failure via self-test" is selected in FPT_ARS_EXT.1, verify that FPT_TST.1 is included in the ST.

3.2.2. Evaluating SFRs with Assignments

When an SFR includes an assignment operation, the evaluator shall:

1. Verify that the ST author provided appropriate values for the assignment
2. Verify that assigned values are consistent with the TOE's capabilities and the security problem definition
3. Verify that the TSS describes how the assigned values are implemented
4. Verify that assigned values are sufficiently specific to enable deterministic testing

For cloud-specific assignments, the evaluator should verify:

- Lists of cloud IAM roles or identity providers are appropriate for the deployment context
- Lists of cloud secret management systems are accurate and complete
- Audit event types include cloud-relevant events (API calls, configuration changes, etc.)
- Management functions include cloud-specific operations

3.2.3. Verifying ST Author Made Valid Selections

The evaluator shall verify that selections are:

- **Valid**: The selected option appears in the SFR selection list
- **Complete**: Required selections are made (no unresolved selections remain)
- **Consistent**: Selections across SFRs are mutually compatible
- **Accurate**: Selected functionality is actually implemented by the TOE

3.3. Cloud-Specific Evaluation Considerations

3.3.1. Evaluation Cloud Environment Requirements

Cloud-native deployments require infrastructure that cannot always be instantiated directly by the evaluator. The vendor shall therefore provide an evaluation-specific cloud environment suitable for executing the activities in this Supporting Document.

When the underlying cloud platform supports safe sub-tenant or compartment isolation (e.g., OCI compartments), the vendor may grant evaluators administrative privileges within that isolated scope to create and manage all resources required for evaluation.

When the cloud platform does not support such isolation or fine-grained delegation, the vendor shall perform administrative operations on behalf of the evaluator, with the evaluator observing the configuration or reviewing audit evidence as appropriate. Evaluators are not required to perform administrative cloud operations that would compromise cloud-wide security boundaries or require tenant-level privileges.

This Supporting Document also permits the use of vendor-supplied emulated cloud services, test harnesses, or preconfigured evaluation artifacts where direct configuration of commercial cloud services is impractical or not permitted.

3.3.2. Testing in Cloud Environments

When performing independent testing of cloud-deployed TOEs, evaluators shall consider:

Test Environment Setup:

- The evaluator may conduct testing in the vendor's cloud environment, the evaluator's cloud environment, or a combination
- The test environment shall be representative of claimed deployment configurations
- The evaluator shall document the cloud provider, region, and resource types used for testing
- Test configurations shall include claimed cloud service integrations (IAM, logging, secret management)

Test Repeatability:

- Test procedures shall be documented with sufficient detail to enable reproduction
- Cloud-specific parameters (instance types, network configurations) shall be recorded
- Tests shall account for eventual consistency behaviors in cloud services
- Tests shall allow for reasonable latency in cloud service responses

Test Coverage:

- Tests shall cover all claimed deployment configurations (single instance, clustered, containerized)
- Tests shall exercise cloud-specific interfaces (IAM authentication, audit export, secret retrieval)
- Tests shall verify behavior under both normal and error conditions

3.3.3. Handling Elastic and Ephemeral Resources

Cloud deployments may involve dynamic resource allocation. The evaluator shall:

- Verify that the TOE maintains security properties during scale-out and scale-in operations
- Verify that security-relevant state is preserved or correctly reconstructed after instance replacement
- Verify that audit records are not lost when instances terminate
- Test the TOE's behavior when cloud services become temporarily unavailable

3.3.4. Evaluating Integration with Cloud Services

When the TOE integrates with cloud-native services, the evaluator shall:

For Cloud IAM Integration (FIA_UID_EXT.1):

- Verify the TSS describes the authentication protocol and assertion validation
- Verify guidance describes how to configure IAM integration
- Test that the TOE correctly validates identity assertions
- Test that invalid or expired assertions are rejected

For Cloud Audit Export (FAU_STG_EXT.1):

- Verify the TSS describes the export mechanism and format
- Verify guidance describes how to configure audit export destinations
- Test that audit records are correctly transmitted to external systems
- Test the TOE's behavior when the audit destination is unavailable

For Cloud Secret Management (FMT_MTD_EXT.1):

- Verify the TSS describes how secrets are retrieved and protected
- Verify guidance describes how to configure secret management integration
- Test that secrets are retrieved securely from cloud services
- Test that the TOE handles secret rotation appropriately

3.3.5. Coordinating Data-at-Rest Evaluation

The Cloud PP-Configuration always includes the DBMS Crypto Module. The evaluator shall verify that data-at-rest protection is claimed through the Crypto Module's `FDP_DAR_EXT.1` requirement and that the selected strategy is either "Storage-Scope Encryption" or "Granular Data Encryption." Platform storage encryption may be described as operational-environment support, but it is not an alternate Cloud Module selection and does not replace the mandatory Crypto Module claim or its evaluation activities.

3.4. Trusted Platform Assumptions

3.4.1. What is NOT Evaluated

The following aspects are assumed to be correctly implemented by the Trusted Platform and are not subject to evaluation:

- **Tenant isolation**: The platform isolates tenants such that one tenant cannot access another's resources
- **Resource protection**: The platform protects compute, memory, and storage from unauthorized access
- **Identity assertion accuracy**: Cloud IAM services provide accurate, unforgeable identity assertions
- **Time synchronization**: The platform provides accurate time services
- **Network isolation**: The platform provides network isolation between tenants

The evaluator shall not attempt to penetration test the cloud platform itself.

3.4.2. What IS Evaluated

The evaluator shall verify:

- The TOE **correctly relies upon** Trusted Platform assumptions
- The TOE **fails securely** when Trusted Platform services are unavailable
- The TOE **validates** data received from Trusted Platform services (e.g., verifies IAM assertions)
- The TOE **documentation** correctly describes Trusted Platform dependencies
- The ST **assumptions** accurately reflect Trusted Platform requirements

3.4.3. Evaluator Actions for Assumptions

For each assumption in the PP-Module, the evaluator shall:

A.TRUSTED_PLATFORM:

- Verify the ST includes this assumption or an equivalent statement
- Verify guidance documentation describes the cloud platform requirements
- Verify the TOE does not claim to provide functionality that is the platform's responsibility

A.SECURE_DEPLOYMENT:

- Verify the ST includes this assumption or an equivalent statement
- Verify preparative guidance describes secure deployment procedures
- Verify the TOE provides mechanisms to verify trusted updates (FPT_TUD_EXT.1), and verify TOE-side startup or deployment artifact integrity only when FPT_SBT_EXT.1 is claimed

A.CLOUD_SERVICE_INTEGRITY:

- Verify the ST includes this assumption or an equivalent statement
- Verify the TSS describes how the TOE handles cloud service failures
- Test that the TOE fails securely when cloud services are unavailable

A.TIME_SYNCHRONIZATION:

- Verify the ST includes this assumption or an equivalent statement
- Verify guidance documentation describes time synchronization requirements
- Verify audit timestamps are derived from the platform time service

3.5. Multi-Module Evaluation

3.5.1. Mandatory Coordination with DBMS Crypto Module

The DBMS Cloud Module requires the inclusion of the DBMS Crypto Module. The evaluator shall coordinate the evaluation as follows:

Coordinate Evaluation Activities:

- Apply this SD (Cloud SD) for cloud-specific SFRs (FAU, FIA, FMT, FPT classes) and for Cloud-specific mapping, configuration, and integration checks associated with Crypto Module requirements.
- Apply the DBMS Crypto Module SD for DBMS-specific cryptographic integration behavior, the Catalogue evaluation methods for consumed FCS components, and the TLS/X.509 Functional Package Evaluation Activities for protocol and certificate behavior.
- Apply the cPP_DBMS SD for SFRs inherited from the Base PP.

Verify Mandatory TLS Usage: Because the TOE is deployed in the cloud, the evaluator shall verify that `FDP_DIT_EXT.1` identifies the protocol used for each external service channel and that the corresponding Functional Package components are included. TLS components are expected for cloud management interfaces exposed to untrusted networks, including web interfaces that provide HTTPS over TLS. The Cloud SD verifies that these components are mapped to deployed cloud interfaces and integration paths; the Crypto SD verifies the DBMS-specific cryptographic integration behavior, and the Functional Package SD verifies the protocol behavior.

Handling Data-at-Rest Selections: The evaluator shall apply the DBMS Crypto Module SD for `FDP_DAR_EXT.1` testing and use this Cloud SD only for cloud-deployment integration checks, such as storage coverage, key-management integration, and guidance consistency.

3.5.2. Evaluation Activity Precedence

When multiple SDs provide Evaluation Activities for related functionality:

1. This SD takes precedence for cloud-specific SFRs defined in the PP-Module.
2. The DBMS Crypto Module SD takes precedence for cryptographic SFRs.

3. The cPP_DBMS SD applies for SFRs inherited without modification.

Chapter 4. Assurance Activities Overview

4.1. Mapping to Base PP SARs

The DBMS Cloud PP-Module inherits all Security Assurance Requirements (SARs) from the collaborative Protection Profile for Database Management Systems (cPP_DBMS). No additional or modified SARs are introduced by this PP-Module.

4.1.1. Inherited SAR Families

The following SAR families from the cPP_DBMS apply unchanged:

SAR Family	Components	Primary SD Coverage
ADV (Development)	ADV_ARC.1, ADV_FSP.2, ADV_TDS.1	cPP_DBMS SD
AGD (Guidance Documents)	AGD_OPE.1, AGD_PRE.1	cPP_DBMS SD + Cloud-specific activities in this SD
ALC (Life-cycle Support)	ALC_CMC.2, ALC_CMS.2, ALC_DEL.1, ALC_FLR.3	cPP_DBMS SD
ASE (Security Target Evaluation)	ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1, ASE_TSS.1	cPP_DBMS SD + PP-Module conformance verification in this SD
ATE (Tests)	ATE_COV.1, ATE_FUN.1, ATE_IND.2	cPP_DBMS SD + Cloud-specific test activities in this SD
AVA (Vulnerability Assessment)	AVA_VAN.2	cPP_DBMS SD + Cloud-specific considerations in this SD

4.1.2. Applying Base PP SAR Activities

For each SAR inherited from the cPP_DBMS, the evaluator shall:

1. Perform all Evaluation Activities specified in the cPP_DBMS SD
2. Apply cloud-specific considerations from this SD where applicable
3. Document findings in the Evaluation Technical Report (ETR)

4.2. Cloud-Specific Assurance Activities

While the PP-Module does not define new SARs, certain assurance activities require cloud-specific focus.

4.2.1. ASE: Security Target Evaluation

In addition to Base PP ST evaluation activities, the evaluator shall verify:

ASE_INT (ST Introduction):

- The TOE description accurately describes cloud deployment configurations
- The TOE boundary correctly distinguishes TOE from Trusted Platform
- Cloud-specific interfaces are identified

ASE_CCL (Conformance Claims):

- The PP-Configuration correctly identifies the Base PP, this PP-Module, and any conditional modules
- Conformance to this PP-Module is claimed as Exact Conformance
- The DBMS Crypto Module is included in the PP-Configuration

ASE_SPD (Security Problem Definition):

- All threats from the PP-Module are addressed or appropriately tailored
- All assumptions are included and accurately reflect the cloud deployment context
- Any additional threats specific to the TOE's deployment are identified

ASE_OBJ (Security Objectives):

- TOE objectives trace to the security problem definition
- OE objectives correctly describe Trusted Platform requirements
- Conditional OE objectives are included when triggered by selections

ASE_TSS (TOE Summary Specification):

- The TSS describes cloud-specific security mechanisms
- Cloud service integrations are documented with sufficient detail
- Fail-secure behaviors for cloud service failures are described

4.2.2. ATE: Tests

Independent testing activities shall include:

Cloud Integration Testing:

- Test IAM authentication using claimed identity providers
- Test audit export to claimed logging services
- Test secret retrieval from claimed secret management systems
- Test behavior when cloud services are unavailable

Elasticity Testing:

- Test security properties during scale operations (if claimed)
- Test audit record preservation during instance termination
- Test configuration consistency across clustered deployments

Deployment Integrity Testing:

- Test update verification mechanisms (FPT_TUD_EXT.1)
- Test secure boot or image verification if claimed (FPT_SBT_EXT.1)
- Test self-test functionality if claimed (FPT_TST.1)

4.2.3. AVA: Vulnerability Assessment

Cloud-specific vulnerability analysis shall consider:

- Publicly disclosed vulnerabilities in claimed cloud service integrations
- Attack vectors specific to cloud deployment models (container escapes, metadata service access)
- Configuration weaknesses in cloud-specific settings
- Risks from cloud service dependencies

Penetration testing activities shall:

- Focus on the TOE, not the underlying cloud platform
- Test cloud-specific attack surfaces (API endpoints, IAM integration)
- Verify that Trusted Platform assumptions cannot be undermined through the TOE

4.3. Documentation Requirements

4.3.1. AGD_OPE: Operational User Guidance - Cloud-Specific Requirements

The operational user guidance shall include cloud-specific sections addressing:

Cloud Deployment Guide:

- Supported cloud providers and deployment configurations
- Required cloud services and their configuration
- Network architecture requirements (VPCs, security groups, etc.)
- IAM policy requirements for TOE operation
- Encryption key management in cloud contexts

Cloud IAM Integration:

- Configuring external identity providers

- Mapping cloud identities to TOE roles
- Managing service principals and API credentials
- Handling token expiration and refresh

Cloud Audit Integration:

- Configuring audit export destinations
- Required IAM permissions for audit export
- Log format and schema documentation
- Troubleshooting audit export failures

Cloud Secret Management:

- Configuring cloud secret management integration
- Supported secret management services
- Secret rotation procedures
- Handling secret retrieval failures

Operational Monitoring:

- Interpreting resilience alerts (FPT_ARS_EXT.1)
- Responding to detected conditions
- Health check and status monitoring

4.3.2. AGD_PRE: Preparative Procedures - Cloud Deployment

The preparative procedures shall include:

Cloud Environment Preparation:

- Prerequisites for the cloud environment (VPC configuration, IAM roles, etc.)
- Required cloud services and their initial configuration
- Network topology and firewall rules

TOE Deployment:

- Retrieving authentic TOE images or packages
- Verifying image integrity before deployment
- Deployment procedures for each supported method (VM, container, etc.)
- Initial security configuration

Post-Deployment Verification:

- Verifying successful deployment

- Testing cloud service integrations
- Baseline security validation checks

The evaluator shall verify that these cloud-specific guidance elements are present and accurate by applying the documented procedures during evaluation.

Chapter 5. FAU Class: Security Audit

5.1. FAU_GEN.1/Cloud Audit Data Generation (Cloud Events)

This SFR is an iteration of the Base PP's FAU_GEN.1. The Base PP SD's FAU_GEN.1 Evaluation Activities remain applicable to the Base PP's FAU_GEN.1; the activities below address the cloud-specific events and record content added by the iteration.

5.1.1. FAU_GEN.1/Cloud Evaluation Activities

5.1.1.1. TSS Activities

The evaluator shall verify the TSS describes:

- The mechanism by which the TSF generates audit records, including whether audit generation is performed synchronously with the audited event or via asynchronous buffering.
- The complete list of auditable events, including:
  - Start-up and shutdown of the audit functions
  - The cloud-specific auditable events specified in FAU_GEN.1.1/Cloud
  - Any additional cloud-specific auditable events assigned by the ST author
- For each auditable event, the specific conditions under which the event is recorded and any event-specific parameters captured.
- The format and structure of audit records, demonstrating compliance with FAU_GEN.1.2/Cloud content requirements (date/time, event type, subject identity, outcome, and the cloud-specific values where applicable).
- How cloud-specific audit information is captured, including:
  - Tenant identifier capture mechanism
  - Cloud region/zone identification
  - Source IP address attribution for API and administrative operations
  - External identity provider authentication event recording
  - Cloud secret management access auditing
- How the TSF obtains reliable timestamps for audit records, referencing the operational environment's time synchronization services per A.TIME_SYNCHRONIZATION.

The evaluator shall verify the TSS identifies all interfaces through which audit records are generated, including internal TSF components and any cloud-native logging APIs.

5.1.1.2. Guidance Activities

The evaluator shall verify the guidance describes:

- How to configure the audit level (minimum, basic, detailed) if the TOE supports multiple levels.
- How to enable and disable audit functions, including any restrictions on when audit functions can be disabled.
- How to configure cloud-specific auditable events, including:
  - Administrative actions via cloud interfaces
  - API interactions with the TOE
  - Configuration or deployment changes
  - Detected failures or unavailability events
  - External identity provider authentication events
  - Changes to cloud secret management integrations
- The complete list of auditable events at each supported audit level, formatted as a table mapping event types to triggering conditions.
- How audit record content is formatted and which fields are mandatory versus optional.
- How to verify audit functions are operating correctly, including any health check or status query mechanisms.
- Any operational constraints on audit functionality (e.g., storage limitations, performance impacts).

5.1.1.3. Test Activities

Test 1: Audit Function Startup/Shutdown Recording

The evaluator shall perform the following steps:

1. Start the TOE from a powered-off or non-operational state.
2. Verify the audit log contains a record indicating start-up of the audit functions.
3. Shut down the TOE using normal administrative procedures.
4. Restart the TOE and verify the audit log contains a record indicating shutdown of the audit functions from the previous session.

Expected result: Audit records for start-up and shutdown events are present with correct timestamps, event types, and outcomes.

Test 2: Auditable Event Generation - Administrative Actions

The evaluator shall perform administrative actions through each available interface (CLI, API, web console if applicable) and verify:

1. Each administrative action generates an appropriate audit record.
2. The audit record contains: date/time, event type, subject identity (the administrator), and outcome (success).
3. For cloud-specific deployments, the tenant identifier and source IP address are recorded.

Expected result: All administrative actions result in correctly formatted audit records with cloud-specific context.

Test 3: Auditable Event Generation - Authentication Events

The evaluator shall:

1. Attempt successful authentication using each supported authentication mechanism (local, cloud IAM, federated directory).
2. Attempt failed authentication using invalid credentials.
3. Verify audit records are generated for both successful and failed authentication attempts.
4. Verify external identity provider authentication events are recorded when federated authentication is used.

Expected result: Authentication events (success and failure) are audited with user identity, authentication method, and outcome.

Test 4: Audit Record Content Verification

For a sample of at least five different event types, the evaluator shall:

1. Trigger the auditable event.
2. Examine the resulting audit record.
3. Verify the record contains all mandatory fields per FAU_GEN.1.2/Cloud:
    - Date and time of the event
    - Type of event
    - Subject identity (if applicable)
    - Outcome (success or failure)
4. Verify any additional cloud-specific information (tenant ID, region, source IP) is present when applicable.

Expected result: All sampled audit records contain the required content and cloud-specific context.

Test 5: Cloud-Specific Event Auditing

The evaluator shall trigger each cloud-specific auditable event type and verify recording:

1. Administrative action via cloud interface (e.g., API call to modify configuration)
2. Configuration or deployment change
3. External identity provider authentication event
4. Access to cloud secret management integration (if applicable)

Expected result: Cloud-specific events are recorded with appropriate context.

Test 6: Negative Test - Audit Tampering Attempt

The evaluator shall attempt to:

1. Generate an auditable event while audit functions are disabled (if disabling is permitted).
2. Verify the event is either not recorded (if audit is disabled) or is recorded (if audit cannot be disabled for this event type).

Expected result: Audit behavior matches the documented configuration. Events that must always be audited are recorded regardless of configuration.

5.2. FAU_SEL.1/Cloud Selective Audit (Cloud)

5.2.1. FAU_SEL.1/Cloud Evaluation Activities

5.2.1.1. TSS Activities

The evaluator shall verify the TSS describes:

- The mechanism by which the TSF selects events for auditing based on the specified attributes.
- How the TSF evaluates selection criteria against each potential auditable event.
- The complete list of supported selection attributes, including:
  - Standard attributes: object identity, user identity, subject identity, host identity, event type
  - Cloud-specific attributes assigned by the ST author (e.g., tenant identifier, IAM role, API endpoint, cloud region, source network range)
- The granularity of selection for each attribute (e.g., exact match, wildcard, range).
- How inclusion and exclusion rules interact when both are configured.
- How selection criteria are stored and protected from unauthorized modification.
- The default selection state (all events audited, no events audited, or specific baseline).

5.2.1.2. Guidance Activities

The evaluator shall verify the guidance describes:

- How to configure audit selection criteria for each supported attribute.
- How to specify inclusion rules (events matching criteria ARE audited).
- How to specify exclusion rules (events matching criteria are NOT audited).
- How to configure tenant-based audit selection, including:
  - Selecting auditing for specific tenant identifiers
  - Auditing all tenants versus specific tenants
- How to configure IAM role-based selection, including:
  - Selecting auditing for specific cloud IAM roles
  - Auditing administrative roles differently from user roles

- How to configure API endpoint selection, including:
  - Selecting auditing for specific API endpoints or operation types
  - Auditing write operations more comprehensively than read operations
- How to configure cloud region or availability zone selection.
- How to configure source network range selection.
- The precedence rules when multiple selection criteria apply to a single event.
- How to verify the current audit selection configuration.
- How to reset selection criteria to defaults.

5.2.1.3. Test Activities

Test 1: Object Identity Based Selection

The evaluator shall:

1. Configure audit selection to include events related to a specific database object (e.g., a particular table or schema).
2. Perform operations on the selected object and on other objects.
3. Verify only events related to the selected object are audited.
4. Configure audit selection to exclude events for the specific object.
5. Repeat operations and verify events for the excluded object are not audited.

Expected result: Audit records are generated only for events matching the selection criteria.

Test 2: User Identity Based Selection

The evaluator shall:

1. Configure audit selection to include events for a specific user identity.
2. Perform operations as the selected user and as other users.
3. Verify only events from the selected user are audited.
4. Configure exclusion for the specific user.
5. Verify events from the excluded user are not audited.

Expected result: User-based audit selection correctly filters audit records.

Test 3: Tenant Identifier Based Selection (Cloud-Specific)

The evaluator shall (in a multi-tenant deployment or simulation):

1. Configure audit selection to include events for a specific tenant identifier.
2. Perform operations in the context of multiple tenants.
3. Verify only events for the selected tenant are audited.

Expected result: Tenant-based selection correctly isolates audit records by tenant.

Test 4: IAM Role Based Selection (Cloud-Specific)

The evaluator shall:

1. Configure audit selection to include events for a specific IAM role (e.g., "cloud audit authority" or "tenant administrator").
2. Perform operations using accounts with different IAM roles.
3. Verify only events from the selected IAM role are audited.

Expected result: IAM role-based selection correctly filters audit records.

Test 5: API Endpoint Based Selection (Cloud-Specific)

The evaluator shall:

1. Configure audit selection to include events for specific API endpoints or operation types (e.g., only audit administrative APIs).
2. Invoke various API endpoints including selected and non-selected endpoints.
3. Verify only events for selected API endpoints are audited.

Expected result: API endpoint selection correctly filters audit records.

Test 6: Combined Selection Criteria

The evaluator shall:

1. Configure multiple selection criteria (e.g., specific user AND specific object).
2. Perform operations that match all criteria, some criteria, and no criteria.
3. Verify only events matching ALL specified inclusion criteria are audited.

Expected result: Combined selection criteria are evaluated correctly using logical AND.

Test 7: Inclusion/Exclusion Precedence

The evaluator shall:

1. Configure conflicting inclusion and exclusion rules for the same event type.
2. Trigger an event that matches both rules.
3. Verify the behavior matches the documented precedence rules.

Expected result: The TSF handles conflicting rules according to documented precedence.

5.3. FAU_STG.2/Cloud Protected Audit Trail Storage

5.3.1. FAU_STG.2/Cloud Evaluation Activities

5.3.1.1. TSS Activities

The evaluator shall verify the TSS describes:

- Where audit records are stored (on the TOE, transmitted to external entity, or other location).
- If audit records are stored on the TOE:
  - The storage mechanism (file system, database, dedicated audit partition)
  - The storage location and access controls
  - The maximum storage capacity and behavior when capacity is reached
- If audit records are transmitted to an external entity:
  - The data-in-transit protection mechanism used, referencing `FDP_DIT_EXT.1` and the applicable TLS Functional Package components
  - The reliability mechanisms (buffering, retry, acknowledgment)
  - Behavior when the external entity is unavailable
- The mechanisms that protect stored audit records from unauthorized deletion.
- The mechanisms that prevent unauthorized modifications to stored audit records (the module completes the FAU_STG.2.2/Cloud selection as "prevent"), including:
  - Access control mechanisms
  - Integrity protection mechanisms (checksums, signatures, append-only storage)
- How the TSF handles audit storage failures in cloud deployments where instances may be ephemeral.

5.3.1.2. Guidance Activities

The evaluator shall verify the guidance describes:

- How to configure the audit storage location.
- How to configure the trusted channel for external audit transmission (if applicable).
- How to monitor audit storage capacity and configure alerts for storage thresholds.
- How to verify the integrity of stored audit records.
- The procedures for authorized deletion of audit records (if permitted).
- The procedures for backing up and restoring audit records.
- How to configure behavior when audit storage is full (if configurable).
- Security considerations for audit storage in ephemeral cloud instances.

5.3.1.3. Test Activities

Test 1: Audit Record Storage Verification

The evaluator shall:

1. Generate multiple auditable events.
2. Verify audit records are stored in the configured location.
3. Retrieve and examine stored audit records to verify content integrity.

Expected result: Audit records are stored correctly and maintain their content integrity.

Test 2: Unauthorized Deletion Prevention

The evaluator shall:

1. As an unprivileged user (or a user without audit management privileges), attempt to delete audit records.
2. Verify the deletion attempt is denied.
3. Verify the deletion attempt itself is audited (if deletion attempts are auditable events).

Expected result: Unauthorized deletion attempts are prevented.

Test 3: Unauthorized Modification Prevention

The evaluator shall:

1. As an unprivileged user, attempt to modify stored audit records through each TSF interface that exposes audit data.
2. Verify each modification attempt is denied.

Expected result: Unauthorized modifications are prevented (the module completes the FAU_STG.2.2/Cloud selection as "prevent").

Test 4: Authorized Deletion Verification (Positive Test)

The evaluator shall:

1. As an authorized administrator with audit management privileges, delete audit records following documented procedures.
2. Verify the deletion succeeds.
3. Verify the deletion action is audited.

Expected result: Authorized deletion procedures function correctly and are audited.

Test 5: Audit Transmission to External Entity (if applicable)

If the TSF transmits audit records to an external entity:

1. Configure the external audit receiver.

2. Generate auditable events.
3. Verify audit records arrive at the external receiver.
4. Verify the transmission uses the specified trusted channel mechanism.

Expected result: Audit records are transmitted reliably via the trusted channel.

Test 6: External Entity Unavailability Handling (if applicable)

If the TSF transmits audit records to an external entity:

1. Make the external audit receiver unavailable.
2. Generate auditable events.
3. Verify the TSF's handling (buffering, alerting, etc.) matches documentation.
4. Restore the external receiver.
5. Verify buffered records are transmitted (if buffering is supported).

Expected result: The TSF handles external entity unavailability according to documented behavior.

5.4. FAU_STG_EXT.1 Audit Export

5.4.1. FAU_STG_EXT.1 Evaluation Activities

5.4.1.1. TSS Activities

The evaluator shall verify the TSS describes:

- The cloud-native logging or SIEM services to which the TSF can export audit data (as assigned by the ST author).
- The export mechanism for each supported service, including:
  - Protocol used for export (e.g., HTTPS over TLS, syslog over TLS, proprietary API over TLS)
  - Authentication mechanism for connecting to the external service
  - Data format of exported records (e.g., JSON, CEF, syslog format)
- The secure export mechanism used, referencing `FDP_DIT_EXT.1` and the applicable TLS Functional Package components.
- The frequency and triggering conditions for audit export (real-time streaming, batch, threshold-based).
- Buffering and retry mechanisms for handling export failures.
- How the TSF maintains export state across ephemeral instance restarts.

5.4.1.2. Guidance Activities

The evaluator shall verify the guidance describes:

- How to configure audit export destinations for each supported cloud-native logging or SIEM service, including:
  - AWS CloudWatch configuration (log group, stream, IAM permissions)
  - Azure Monitor configuration (workspace ID, shared key or managed identity)
  - Splunk configuration (HEC endpoint, token authentication)
  - Tenant-owned SIEM configuration (endpoints, credentials)
- How to configure the secure export mechanism (TLS settings, certificate validation).
- How to configure export format preferences.
- How to configure export frequency and batch sizes.
- How to verify audit export is functioning correctly.
- How to troubleshoot export failures.
- How to handle export credential rotation.

5.4.1.3. Test Activities

Test 1: Audit Export to Cloud Logging Service

For each cloud-native logging service specified in the ST:

1. Configure audit export to the cloud logging service.
2. Generate auditable events on the TOE.
3. Query the cloud logging service to retrieve exported audit records.
4. Verify the exported records match the source audit records in content.

Expected result: Audit records are successfully exported to the cloud logging service with correct content.

Test 2: Export Format Verification

The evaluator shall:

1. Configure audit export to a destination.
2. Generate a sample of different auditable event types.
3. Capture the exported records at the destination.
4. Verify the format matches the documented export format.
5. Verify all required audit record fields are present in the exported format.

Expected result: Exported audit records conform to the documented format with all required fields.

Test 3: Secure Export Mechanism Verification

If a trusted channel is specified for export:

1. Configure audit export using the trusted channel mechanism.

2. Use network analysis tools to capture export traffic.
3. Verify the traffic is protected (e.g., TLS encryption verified).
4. Verify certificate validation is performed (attempt export to a service with an invalid certificate and confirm failure).

Expected result: Audit export uses the specified secure transport mechanism.

Test 4: Export Reliability Testing

The evaluator shall:

1. Configure audit export to a destination.
2. Generate auditable events.
3. Temporarily make the export destination unavailable.
4. Continue generating events during unavailability.
5. Restore the export destination.
6. Verify events generated during unavailability are eventually exported (if buffering is supported) or that the unavailability was detected and handled per documentation.

Expected result: The TSF handles export destination unavailability according to documented behavior.

Test 5: Export with Multiple Destinations (if supported)

If the TSF supports exporting to multiple destinations:

1. Configure export to multiple cloud logging services simultaneously.
2. Generate auditable events.
3. Verify records appear in all configured destinations.

Expected result: Audit records are exported to all configured destinations.

Test 6: Export Credential Authentication

The evaluator shall:

1. Configure audit export with valid credentials.
2. Verify export succeeds.
3. Configure audit export with invalid credentials.
4. Verify export fails with appropriate error handling.
5. Verify the authentication failure is audited or logged.

Expected result: Export authentication is validated and failures are handled appropriately.

Chapter 6. FIA Class: Identification and Authentication

6.1. Base PP Identification and Authentication Coordination

The Base PP supplies FIA_UID.2 and FIA_UAU.2, and the Base PP SD provides the corresponding Evaluation Activities for identification and authentication before any TSF-mediated action. This Cloud SD does not duplicate those activities. The activities below supplement the Base PP by verifying that external identity assertions used in cloud deployments are validated and mapped before the TOE relies on them for access-control decisions.

6.2. FIA_UID_EXT.1 External Identity Integration

6.2.1. FIA_UID_EXT.1 Evaluation Activities

6.2.1.1. TSS Activities

The evaluator shall verify the TSS describes:

- That no TSF-mediated actions are permitted before identification and authentication, consistent with the Base PP's FIA_UID.2 and FIA_UAU.2 and this module's application note.
- How the TSF identifies users through external identity providers, for each selected provider type:
  - Cloud IAM roles: How IAM role ARN/ID is extracted and validated
  - Federated directory users (LDAP/AD): How directory assertions are processed and validated
  - Service principals: How service principal identity is established and validated
  - Other identity sources (as assigned): How identity is established and validated
- The identity assertion formats accepted from each external provider (e.g., SAML, OAuth tokens, OIDC, signed assertions).
- How identity assertions are validated, including:
  - Signature verification of identity assertions
  - Expiration checking
  - Issuer validation
  - Audience verification
- How external identities are mapped to internal user representations or roles within the TOE.
- That communication with each external identity provider uses a channel protected by the inherited FDP_DIT_EXT.1, per FIA_UID_EXT.1.4, identifying the corresponding TLS components claimed in the ST. The channel binding is exercised by Test 12; TLS protocol behavior itself is evaluated under the DBMS Crypto Module SD and the TLS Functional Package.

- How the TSF handles identity provider unavailability or failure.
- How the TSF detects and handles forged or tampered identity assertions.

6.2.1.2. Guidance Activities

The evaluator shall verify the guidance describes:

- How to configure integration with cloud IAM services, including:
  - AWS IAM configuration (trust policies, role assumption)
  - Azure AD configuration (app registration, service principals)
  - GCP IAM configuration (service accounts, workload identity)
- How to configure integration with federated directory services, including:
  - LDAP/AD configuration (server addresses, base DN, bind credentials)
  - SAML configuration (IdP metadata, certificate trust)
  - OIDC configuration (discovery endpoint, client credentials)
- How to configure service principal authentication, including:
  - Certificate-based authentication
  - Client secret authentication
  - Managed identity integration
- How to configure identity-to-role mapping, including:
  - Attribute-based role assignment
  - Group membership mapping
  - Default role assignment
- How to troubleshoot identity provider integration issues.
- How to rotate identity provider credentials.
- Security considerations for external identity integration.

6.2.1.3. Test Activities

Test 1: No Pre-Identification Actions

The evaluator shall, without providing identity:

1. Attempt a representative set of TSF-mediated actions through each available interface (for example, query execution, configuration query, and management operations).
2. Verify each attempt is refused before identification and authentication complete.

Expected result: No TSF-mediated action is permitted before identification and authentication. This test complements, and does not duplicate, the Base PP SD's FIA_UID.2/FIA_UAU.2 activities; it exercises the cloud-facing interfaces this module adds.

Test 2: Cloud IAM Role Integration

If cloud IAM roles are selected:

1. Configure the TOE to accept identity from cloud IAM.
2. Authenticate using a valid cloud IAM role (e.g., via assumed role credentials, instance metadata).
3. Verify the user is identified by their IAM role.
4. Verify the identified IAM role is correctly mapped to TOE permissions.

Expected result: Cloud IAM role identification functions correctly.

Test 3: Cloud IAM - Invalid Role Rejection

The evaluator shall:

1. Attempt identification using credentials from an IAM role not authorized for the TOE.
2. Verify the identification/authentication attempt is rejected.
3. Verify the rejection is audited.

Expected result: Unauthorized IAM roles are rejected.

Test 4: Federated Directory Integration (LDAP/AD)

If federated directory users are selected:

1. Configure the TOE to integrate with an LDAP or AD directory.
2. Authenticate using valid directory credentials.
3. Verify the user is identified by their directory identity.
4. Verify directory group memberships are correctly mapped to TOE roles (if applicable).

Expected result: Federated directory identification functions correctly.

Test 5: Federated Directory - Invalid Credentials Rejection

The evaluator shall:

1. Attempt identification using invalid directory credentials.
2. Verify the attempt is rejected.
3. Verify the rejection is audited.

Expected result: Invalid directory credentials are rejected.

Test 6: Service Principal Authentication

If service principals are selected:

1. Configure a service principal for TOE access.
2. Authenticate using service principal credentials (certificate or secret).

3. Verify the service principal is identified.
4. Verify appropriate access is granted based on service principal permissions.

Expected result: Service principal identification functions correctly.

Test 7: Service Principal - Invalid Credentials Rejection

The evaluator shall:

1. Attempt identification using invalid service principal credentials.
2. Verify the attempt is rejected.
3. Verify the rejection is audited.

Expected result: Invalid service principal credentials are rejected.

Test 8: Identity Assertion Validation

The evaluator shall verify identity assertion validation:

1. Present an identity assertion with an expired timestamp.
2. Verify the assertion is rejected.
3. Present an identity assertion with an invalid signature (if signatures are used).
4. Verify the assertion is rejected.
5. Present an identity assertion from an untrusted issuer.
6. Verify the assertion is rejected.

Expected result: Invalid identity assertions are rejected.

Test 9: Identity Mapping Verification

The evaluator shall:

1. Identify users with different external attributes (e.g., different group memberships, different roles).
2. Verify each user is mapped to the correct internal role based on configured mapping rules.
3. Modify mapping configuration and verify changes take effect.

Expected result: Identity-to-role mapping functions correctly.

Test 10: Identity Provider Unavailability Handling

The evaluator shall:

1. Make the external identity provider unavailable (simulate network failure or service outage).
2. Attempt identification through the unavailable provider.
3. Verify the TOE handles the unavailability according to documented behavior (e.g., fail closed, use cached credentials if permitted, provide appropriate error).

4. Restore the identity provider.
5. Verify normal identification resumes.

Expected result: Identity provider unavailability is handled securely.

Test 11: Multiple Identity Source Interaction (if applicable)

If multiple identity sources are configured:

1. Configure the TOE to accept identity from multiple sources (e.g., both cloud IAM and federated directory).
2. Authenticate using each identity source.
3. Verify each source correctly identifies the user.
4. Verify identity source precedence if the same user exists in multiple sources.

Expected result: Multiple identity sources function correctly together.

Test 12: External Identity Provider Channel Verification (Mandatory)

The evaluator shall:

1. Configure the TOE to use an external identity provider (e.g., Azure AD, AWS IAM).
2. Initiate an authentication attempt.
3. Capture network traffic between the TOE and the identity provider endpoint.
4. Verify that the traffic is protected (e.g., encrypted using TLS, including HTTPS over TLS).
5. Confirm, by reference to the Cryptographic Validation Coverage Matrix and the TLS Functional Package evaluation evidence recorded for the DBMS Crypto Module, that certificate validation for the TLS client role used by this interface is covered there.

Expected result: The connection to the identity provider is protected against disclosure and modification, and the certificate-validation coverage for this channel is confirmed in the Crypto Module evaluation evidence.

Application Note: Because the Crypto Module is mandatory, the TOE must use TLS for external identity provider connections, including HTTPS over TLS where applicable. This test verifies the channel mapping required by FIA_UID_EXT.1.4; certificate-validation and TLS protocol testing are performed under the DBMS Crypto Module SD and the TLS and X.509 Functional Packages and are not duplicated here.

Chapter 7. FMT Class: Security Management

7.1. FMT_MOF.1 Management of Security Functions Behavior

7.1.1. FMT_MOF.1 Evaluation Activities

7.1.1.1. TSS Activities

The evaluator shall verify that the TSS describes:

1. The complete list of security functions whose behavior can be determined, disabled, enabled, or modified, and for each function:
    a. The specific behaviors that can be controlled
    b. The authorized roles permitted to perform each management operation
    c. Any restrictions or conditions on management operations
2. How the TSF enforces role-based restrictions on management operations, including:
    a. The mechanism used to verify role membership before permitting operations
    b. The binding between authenticated identities and their assigned roles
    c. How role checks are performed for cloud-native identity providers when external identity integration (FIA_UID_EXT.1) is used
3. For cloud deployments specifically:
    a. How management functions are exposed via cloud interfaces (API endpoints, management consoles, CLI tools)
    b. Any differences in management capabilities between local and remote administrative interfaces
    c. How the TSF prevents privilege escalation through management interfaces
4. The relationship between FMT_MOF.1 functions and those specified in FMT_SMF.1/Cloud, demonstrating that all cloud management functions are subject to appropriate access restrictions.

7.1.1.2. Guidance Activities

The evaluator shall verify that the operational guidance (AGD_OPE/AGD_PRE):

1. Identifies all security functions subject to management restrictions and documents:
    a. The authorized roles for each management operation
    b. Procedures for assigning roles to users
    c. Any default or initial role configurations
2. Provides clear instructions for administrators on:

a. How to configure role-based restrictions for management functions
b. How to verify current role assignments and permissions
c. How to audit management function access

3. Documents cloud-specific management considerations:
   a. Configuration of management functions via cloud-native interfaces (e.g., Kubernetes ConfigMaps, Terraform, cloud provider consoles)
   b. Secure practices for remote management over untrusted networks
   c. Integration with cloud IAM for management authorization
4. Warns administrators about security implications of:
   a. Modifying default role restrictions
   b. Granting administrative privileges broadly
   c. Configuring management access from public networks without encryption

7.1.1.3. Test Activities

The evaluator shall perform the following tests:

Test 1: Role-Based Access Enforcement for Management Functions

For each security function identified in the TSS:

1. Step: Authenticate as a user assigned to an authorized role for managing the function.
2. Step: Attempt to perform each permitted management operation (determine behavior, disable, enable, modify).
3. Expected Result: All operations succeed for authorized roles.
4. Step: Authenticate as a user assigned to a role NOT authorized to manage the function.
5. Step: Attempt each management operation.
6. Expected Result: All operations are denied with appropriate error messages.

Test 2: Cloud IAM Integration for Management Authorization

If the TOE integrates with external identity providers:

1. Step: Configure a cloud IAM role mapping to a TOE role with management privileges.
2. Step: Authenticate using the cloud IAM identity.
3. Step: Verify that management operations permitted for the mapped role succeed.
4. Step: Modify the cloud IAM role mapping to remove management privileges.
5. Step: Re-authenticate using the same cloud IAM identity.
6. Step: Verify that management operations are now denied.

Test 3: Management Function Restriction in Distributed Deployments

For clustered or distributed DBMS deployments:

1. Step: Verify that management restrictions are consistently enforced across all cluster nodes.
2. Step: Attempt management operations via different nodes in the cluster.
3. Expected Result: Role-based restrictions are identical regardless of which node handles the request.
4. Step: If the cluster includes separate management and data plane components, verify restrictions apply to management plane access.

Test 4: API and CLI Management Interface Restrictions

1. Step: Enumerate all management APIs and CLI commands exposed by the TOE.
2. Step: For each interface, attempt operations requiring elevated privileges using both authorized and unauthorized credentials.
3. Expected Result: Access controls are consistently enforced across all interfaces.

7.2. FMT_MTD.1/Cloud and FMT_MTD_EXT.1 Cloud TSF Data Management and Protection

The activities below address FMT_MTD.1/Cloud (role-based restriction of operations on cloud-specific TSF data) and FMT_MTD_EXT.1 (protection of TSF data exchanged with cloud-native configuration and secret management systems) together, as they are exercised through the same interfaces.

7.2.1. FMT_MTD.1/Cloud and FMT_MTD_EXT.1 Evaluation Activities

7.2.1.1. TSS Activities

The evaluator shall verify that the TSS describes:

1. The complete list of TSF data managed by this requirement, including:
    a. Database credentials and service account keys
    b. Encryption keys and key material references
    c. Configuration parameters affecting security functions
    d. Authentication tokens and session data
2. For each operation (query, modify, delete, clear, and any other specified operations):
    a. The authorized roles permitted to perform the operation
    b. Any constraints or conditions on the operation
    c. Audit records generated for the operation
3. The cloud-native configuration and secret management systems supported by the TOE, such as:
    a. AWS Secrets Manager

b. Azure Key Vault
c. Google Cloud Secret Manager
d. HashiCorp Vault
e. Kubernetes Secrets
f. Environment variables

4. That retrieval of TSF data from, and writes of TSF data to, each supported networked system use a channel protected by the inherited `FDP_DIT_EXT.1`, per FMT_MTD_EXT.1.2, identifying the corresponding TLS components claimed in the ST. TLS protocol behavior itself is evaluated under the DBMS Crypto Module SD and the TLS Functional Package.
5. For each supported cloud secret management system:
   a. The authentication mechanism used by the TOE to access the service (e.g., IAM roles, service principals, API keys)
   b. How secrets are retrieved and protected in memory after retrieval
   c. Support for secret rotation and the TOE's behavior during rotation
   d. Protection of credentials used to access the secret management service itself
6. Protection of environment variables containing sensitive data:
   a. How environment variables are isolated from unauthorized access
   b. Protection against environment variable disclosure through error messages or logs
   c. Handling of sensitive environment variables in container orchestration environments

7.2.1.2. Guidance Activities

The evaluator shall verify that the operational guidance (AGD_OPE/AGD_PRE):

1. Provides instructions for configuring integration with each supported cloud secret management system, including:
   a. Required IAM permissions or service principal configurations
   b. Network connectivity requirements
   c. TLS/mTLS configuration for secret retrieval
2. Documents secure practices for credential rotation:
   a. Procedures for rotating credentials without service interruption
   b. How to configure automatic rotation intervals
   c. Verification steps after credential rotation
3. Describes secure handling of environment variables:
   a. Recommendations for passing secrets via secret management services rather than environment variables
   b. Warnings about environment variable exposure risks in container environments
   c. Secure configuration of orchestration platforms (Kubernetes, Docker, etc.)

4. Documents the protection of credentials in memory:
    a. Any memory protection mechanisms employed
    b. Guidance on minimizing credential lifetime in memory
    c. Configuration options for credential caching
5. Warns administrators about common misconfigurations:
    a. Storing credentials in plaintext configuration files
    b. Exposing credentials in logs or error messages
    c. Overly permissive IAM policies for secret access

7.2.1.3. Test Activities

Test 1: Role-Based Access to TSF Data

For each type of TSF data and each operation (query, modify, delete, clear):

1. Step: Authenticate as a user with an authorized role for the operation.
2. Step: Perform the operation.
3. Expected Result: Operation succeeds.
4. Step: Authenticate as a user without authorization for the operation.
5. Step: Attempt the same operation.
6. Expected Result: Operation is denied.

Test 2: AWS Secrets Manager Integration

If AWS Secrets Manager is supported:

1. Step: Configure the TOE to retrieve database credentials from AWS Secrets Manager.
2. Step: Verify the TOE authenticates to Secrets Manager using IAM role assumption.
3. Step: Verify the TOE successfully retrieves and uses the secret.
4. Step: Rotate the secret in AWS Secrets Manager.
5. Step: Verify the TOE retrieves and uses the new secret value (either automatically or after configured refresh).
6. Step: Revoke the TOE's IAM permissions to access the secret.
7. Step: Verify the TOE handles the access denial securely (fails closed, generates appropriate audit record).

Test 3: Azure Key Vault Integration

If Azure Key Vault is supported:

1. Step: Configure the TOE to retrieve secrets from Azure Key Vault.
2. Step: Verify the TOE authenticates using managed identity or service principal.

3. Step: Verify successful secret retrieval and usage.
4. Step: Rotate the secret in Azure Key Vault.
5. Step: Verify the TOE retrieves the rotated secret.
6. Step: Remove the TOE's access policy from Key Vault.
7. Step: Verify secure failure behavior.

Test 4: HashiCorp Vault Integration

If HashiCorp Vault is supported:

1. Step: Configure the TOE to retrieve secrets from Vault using the appropriate auth method (e.g., Kubernetes auth, AppRole).
2. Step: Verify successful authentication and secret retrieval.
3. Step: Test secret renewal and rotation scenarios.
4. Step: Revoke the TOE's Vault token.
5. Step: Verify secure failure behavior.

Test 5: Environment Variable Protection

1. Step: Configure sensitive data to be passed via environment variables.
2. Step: Verify the TOE does not log or expose environment variable values in error messages.
3. Step: Attempt to retrieve environment variable values through the TOE's interfaces (APIs, logs, debug endpoints).
4. Expected Result: Sensitive environment variable values are not exposed.
5. Step: For containerized deployments, verify environment variables are not exposed via container inspection commands to unauthorized users.

Test 6: Credential Memory Protection

1. Step: Configure the TOE to retrieve credentials from a cloud secret service.
2. Step: If memory inspection capabilities are available (e.g., core dump analysis), verify credentials are not retained in memory longer than necessary.
3. Step: Verify credentials are cleared from memory when the connection is terminated or credentials are rotated.

Test 7: Secret Retrieval Security

For each supported cloud secret management system:

1. Configure the TOE to retrieve a secret (e.g., database connection string or master key) from the cloud service.
2. Verify the retrieval request is made over a secure channel (for example, HTTPS over TLS).

3. Verify the secret is not logged in plaintext by the TOE upon retrieval.
4. If the retrieved secret is a cryptographic key (and the ST claims FCS_CKM_EXT.1 in the Crypto Module), verify that the TOE handles the key material according to the Crypto Module's FCS_CKM.6 key destruction claims and does not persist it to non-volatile storage in plaintext.

Expected result: Secrets are retrieved securely and handled appropriately in memory.

Application Note: General retrieval of configuration values, credentials, or non-key secrets from a cloud secret management service is evaluated as Cloud Module FMT_MTD_EXT.1 behavior with the retrieval channel protected by FDP_DIT_EXT.1. If the retrieved value is a Master Key imported from an external entity under the Crypto Module BYOK path, FCS_CKM_EXT.1.1 selects "Imported from External Entity", which triggers FDP_ITC_EXT.1 and mandatory mutual TLS. HTTPS/TLS secret retrieval under FDP_DIT_EXT.1 does not by itself satisfy the Crypto Module Master Key import requirement.

7.3. FMT_SMF.1/Cloud Specification of Management Functions (Cloud)

7.3.1. FMT_SMF.1/Cloud Evaluation Activities

7.3.1.1. TSS Activities

The evaluator shall verify that the TSS describes each management function listed in FMT_SMF.1.1/Cloud, specifically:

1. **Configuration of audit selection criteria (FAU_SEL.1/Cloud):**
   a. The interface(s) used to configure audit selection
   b. The criteria available for selection (object identity, user identity, tenant identifier, etc.)
   c. How selections are persisted across TOE restart
2. **Configuration of audit export destinations (FAU_STG_EXT.1):**
   a. Supported audit export destinations (CloudWatch, Azure Monitor, Splunk, etc.)
   b. Configuration parameters for each destination
   c. How export credentials are protected
3. **Configuration of secure external communications (FDP_DIT_EXT.1):**
   a. TLS configuration parameters, including HTTPS over TLS where applicable
   b. Certificate management interfaces
   c. Supported cipher suites and protocol versions
4. **Management of external identity provider mappings (FIA_UID_EXT.1):**
   a. How identity providers are registered with the TOE
   b. How identity mappings to internal roles are configured
   c. Testing and validation of identity provider configurations

5. **Monitoring and querying trusted update status and claimed integrity status:**
    a. Interfaces for querying trusted update status and any claimed runtime, startup, or deployment artifact integrity status
    b. Information provided in status reports
    c. Actions available when integrity issues are detected
6. **Rotation of cloud-managed credentials or secrets:**
    a. Interfaces for initiating credential rotation
    b. Automated rotation support
    c. Behavior during credential rotation
7. **Other cloud-specific management functions:**
    a. Any additional functions specified by the ST author

7.3.1.2. Guidance Activities

The evaluator shall verify that the operational guidance (AGD_OPE/AGD_PRE):

1. Documents the interface(s) through which each management function is accessed, including:
    a. Administrative console or dashboard
    b. API endpoints (REST, gRPC, etc.)
    c. CLI commands
    d. Configuration files
2. Provides step-by-step instructions for performing each management function.
3. Documents any prerequisites or dependencies for management functions (e.g., TLS must be configured before enabling HTTPS for management APIs).
4. Describes the impact of each management function on TOE security and operation.
5. Documents cloud-specific management considerations:
    a. Configuration via infrastructure-as-code tools (Terraform, CloudFormation, ARM templates)
    b. Kubernetes ConfigMap and Secret management
    c. Cloud provider-specific management interfaces

7.3.1.3. Test Activities

Test 1: Audit Selection Configuration

1. Step: Access the audit selection configuration interface.
2. Step: Configure audit selection based on each available criterion (user identity, tenant identifier, event type, etc.).
3. Step: Generate events matching and not matching the selection criteria.
4. Expected Result: Only events matching the criteria are audited.
5. Step: Restart the TOE.

6. Step: Verify audit selection configuration persists.

Test 2: Audit Export Configuration

1. Step: Configure audit export to each supported destination.
2. Step: Generate auditable events.
3. Step: Verify events are exported to the configured destination.
4. Step: Misconfigure the export destination (invalid credentials, unreachable endpoint).
5. Step: Verify the TOE handles export failures appropriately (generates local alerts, retains events locally).

Test 3: External Identity Provider Management

1. Step: Register an external identity provider (cloud IAM, LDAP, OIDC).
2. Step: Configure identity-to-role mappings.
3. Step: Test authentication using the external provider.
4. Step: Modify the mappings.
5. Step: Verify the modified mappings take effect.
6. Step: Remove the identity provider configuration.
7. Step: Verify authentication via that provider is no longer possible.

Test 4: Trusted Update and Integrity Status Querying

1. Step: Query trusted update status using available interfaces.
2. Step: Verify the status report includes relevant update information.
3. Step: If FPT_TST.1 or FPT_SBT_EXT.1 is implemented, trigger an integrity check and verify the status is updated.

Test 5: Credential Rotation

1. Step: Initiate credential rotation through the management interface.
2. Step: Verify old credentials are invalidated.
3. Step: Verify new credentials are functional.
4. Step: If automated rotation is supported, configure automatic rotation and verify it executes correctly.

Test 6: Management Function Access via Cloud-Native Interfaces

For containerized deployments:

1. Step: Verify management functions can be configured via Kubernetes ConfigMaps or Helm values.
2. Step: Apply configuration changes using kubectl apply or helm upgrade.
3. Step: Verify the TOE applies the new configuration.

For cloud-deployed TOEs:

1. Step: Verify management functions can be configured via cloud provider interfaces (parameter groups, configuration services).
2. Step: Apply changes via the cloud provider console or CLI.
3. Step: Verify the TOE applies the new configuration.

7.4. FMT_SMR.1/Cloud Security Roles (Cloud)

7.4.1. FMT_SMR.1/Cloud Evaluation Activities

7.4.1.1. TSS Activities

The evaluator shall verify that the TSS describes:

1. The complete list of roles maintained by the TSF, as assigned in FMT_SMR.1.1/Cloud by the ST author. The SFR's application note gives tenant administrator, tenant user, and cloud audit authority (a read-only role for audit data and security status) as examples; this SD does not levy roles beyond the ST's assignment.
2. For each role:
   a. The privileges and capabilities associated with the role
   b. How the role is differentiated from other roles
   c. Any hierarchical relationships between roles
3. The mechanism for associating users with roles:
   a. Direct role assignment within the TOE
   b. Role mapping from external identity providers
   c. Default role assignments for new users
4. How role membership is verified during access control decisions.
5. For cloud deployments specifically:
   a. How roles are mapped from cloud IAM roles or groups
   b. Multi-tenant role isolation (how roles in one tenant cannot affect another tenant)
   c. Service account and machine identity role assignments

7.4.1.2. Guidance Activities

The evaluator shall verify that the operational guidance (AGD_OPE/AGD_PRE):

1. Documents all pre-defined roles and their associated privileges.
2. Provides instructions for:
   a. Creating custom roles (if supported)

   b. Assigning users to roles
   c. Removing users from roles
   d. Configuring role mappings from external identity providers
3. Documents the minimum privileges required for each administrative task.
4. Provides guidance on implementing least-privilege principles using the TOE's role model.
5. Documents cloud-specific role management:
   a. Mapping cloud IAM roles to TOE roles
   b. Managing roles in multi-tenant deployments
   c. Role inheritance and hierarchy (if applicable)

7.4.1.3. Test Activities

Test 1: Role Maintenance

1. Step: Verify the TSF maintains each role specified in the TSS.
2. Step: Query the list of roles using available administrative interfaces.
3. Expected Result: All specified roles are present.

Note: Tests 2 through 4 exercise the roles assigned in the ST, using the example role names for readability. Where the ST does not assign a role corresponding to the one named, the evaluator shall perform the equivalent privilege-separation verification using the roles the ST does assign, and shall omit a test only when no assigned role provides the corresponding capability.

Test 2: User-Role Association

1. Step: Create a new user (or use an existing user not assigned to any role).
2. Step: Associate the user with the Tenant Administrator role.
3. Step: Verify the user can perform administrative functions.
4. Step: Remove the user from the Tenant Administrator role.
5. Step: Verify the user can no longer perform administrative functions.

Test 3: Tenant User Role Verification

1. Step: Associate a user with the Tenant User role.
2. Step: Verify the user can perform standard database operations (queries, data modification as permitted).
3. Step: Verify the user cannot perform administrative operations.

Test 4: Cloud Audit Authority Role Verification

1. Step: Associate a user with the Cloud Audit Authority role.
2. Step: Verify the user can access audit data and security status information.
3. Step: Verify the user cannot modify security configurations or data.

4. Step: Verify the user cannot modify audit records.

Test 5: Cloud IAM Role Mapping

If external identity provider integration is used:

1. Step: Configure a cloud IAM role (e.g., AWS IAM role, Azure AD group) to map to the Tenant Administrator role.
2. Step: Authenticate using an identity assigned the cloud IAM role.
3. Step: Verify the user has Tenant Administrator privileges.
4. Step: Change the IAM role mapping to Tenant User.
5. Step: Re-authenticate using the same identity.
6. Step: Verify the user now has only Tenant User privileges.

Test 6: Multi-Tenant Role Isolation

For multi-tenant deployments:

1. Step: Create roles with the same name in two different tenants.
2. Step: Assign different users to each role.
3. Step: Verify that users in Tenant A cannot access resources in Tenant B, even with the same role name.
4. Step: Verify administrative actions in one tenant do not affect another tenant.

Test 7: Role Assignment/Removal Audit

1. Step: Assign a user to a role.
2. Step: Verify an audit record is generated for the assignment.
3. Step: Remove the user from the role.
4. Step: Verify an audit record is generated for the removal.
5. Step: Verify audit records include user identity, role, action, and timestamp.

Chapter 8. FPT Class: Protection of the TSF

8.1. FPT_ARS_EXT.1 Availability and Resilience Signaling

8.1.1. FPT_ARS_EXT.1 Evaluation Activities

8.1.1.1. TSS Activities

The evaluator shall verify that the TSS describes:

1. The runtime environment conditions monitored by the TSF, from the selection:
    a. **Configuration drift**: Changes to security-relevant configuration from expected baseline
    b. **Resource unavailability**: Failure of required resources (storage, network, services)
    c. **Integrity failure via self-test**: Detection of integrity violations (requires FPT_TST.1)
    d. **Orchestration failure**: Failures in container orchestration or deployment systems
    e. **Other monitored conditions**: Any additional conditions specified by the ST author
2. For each monitored condition:
    a. The specific indicators or metrics used to detect the condition
    b. The monitoring frequency or trigger events
    c. The threshold or criteria for determining a condition exists
    d. The response actions taken upon detection
3. The notification mechanisms and recipients:
    a. Supported notification methods (alerts, logs, API callbacks, cloud-native monitoring)
    b. How notification recipients are configured
    c. The information included in notifications
4. For cloud deployments specifically:
    a. Integration with cloud-native monitoring services (CloudWatch, Azure Monitor, etc.)
    b. Kubernetes health checks and liveness/readiness probes
    c. Container orchestration failure detection

8.1.1.2. Guidance Activities

The evaluator shall verify that the operational guidance (AGD_OPE/AGD_PRE):

1. Documents the configuration of each monitored condition:
    a. How to enable/disable monitoring for specific conditions
    b. How to configure detection thresholds
    c. How to define expected baseline configurations for drift detection

2. Provides instructions for configuring notifications:
    a. Supported notification destinations
    b. Configuration of cloud-native monitoring integration
    c. Alerting rules and escalation procedures
3. Documents recommended responses to each type of detected condition.
4. Provides guidance for cloud-specific monitoring:
    a. Integration with container orchestration health checks
    b. Configuration of cloud provider monitoring services
    c. Best practices for alerting in ephemeral/elastic environments

8.1.1.3. Test Activities

Test 1: Configuration Drift Detection

If configuration drift monitoring is selected:

1. Step: Establish a known security configuration baseline.
2. Step: Modify a security-relevant configuration parameter outside of authorized management interfaces (e.g., directly edit configuration file, modify database system table).
3. Expected Result: TSF detects the drift and generates a notification.
4. Step: Verify the notification includes information about what changed.

Test 2: Resource Unavailability Detection

If resource unavailability monitoring is selected:

1. Step: Identify a resource the TOE depends on (storage volume, network service, cloud service).
2. Step: Make the resource unavailable (disconnect network, unmount storage, stop service).
3. Expected Result: TSF detects the unavailability and generates a notification.
4. Step: Restore the resource.
5. Step: Verify the TSF detects recovery (if recovery notification is supported).

Test 3: Integrity Failure Detection via Self-Test

If integrity failure via self-test is selected (requires FPT_TST.1):

1. Step: Trigger a self-test that will fail (if testing capability exists, e.g., corrupt a test file).
2. Expected Result: TSF detects the integrity failure and generates a notification.
3. Step: Verify the notification identifies the integrity failure.

Test 4: Orchestration Failure Detection

If orchestration failure monitoring is selected:

For Kubernetes deployments:

1. Step: Deploy the TOE as a Kubernetes pod with liveness and readiness probes.
2. Step: Verify probes respond correctly under normal operation.
3. Step: Simulate a condition that should cause probe failure.
4. Expected Result: TSF indicates failure via probe response.
5. Step: Verify Kubernetes takes configured action (restart pod, mark unhealthy).

For other orchestration platforms:

1. Step: Simulate an orchestration failure (deployment timeout, resource allocation failure).
2. Expected Result: TSF detects and signals the failure.

Test 5: Notification Mechanism Verification

For each configured notification recipient:

1. Step: Trigger a monitored condition.
2. Step: Verify the notification is received by the configured recipient.
3. Step: Verify the notification contains required information:
    a. Condition type
    b. Timestamp
    c. Affected component or resource
    d. Severity (if applicable)

Test 6: Cloud-Native Monitoring Integration

If cloud-native monitoring integration is supported:

1. Step: Configure the TOE to send alerts to CloudWatch, Azure Monitor, or equivalent.
2. Step: Trigger a monitored condition.
3. Step: Verify the alert appears in the cloud monitoring service.
4. Step: Verify alert metadata is correct.

8.2. FPT_FLS.1 Failure with Preservation of Secure State

The PP-Module deliberately leaves the FPT_FLS.1.1 failure-type assignment to the ST author, because failure modes and secure-state semantics differ across DBMS implementations and cloud architectures. The Evaluation Activities below are therefore driven by the ST's completions: the evaluator assesses the failure types the ST claims, not a fixed list.

8.2.1. FPT_FLS.1 Evaluation Activities

8.2.1.1. TSS Activities

The evaluator shall verify the TSS:

- identifies each failure type claimed in the FPT_FLS.1.1 assignment;
- defines what constitutes a secure state for the TOE (for example, refusing new connections, denying access to protected data, or controlled shutdown), including whether the secure state differs by failure type;
- describes, for each claimed failure type, how the TOE detects or is informed of the failure and how it transitions to the secure state; and
- where a claimed failure type overlaps a condition monitored under FPT_ARS_EXT.1, describes the relationship between the notification behavior and the secure-state transition.

8.2.1.2. Guidance Activities

The evaluator shall verify the operational guidance describes any configuration that affects failure-handling behavior, and the procedures for recovering the TOE to normal operation from the secure state.

8.2.1.3. Test Activities

Test 1: Secure State Preservation

For each failure type claimed in the ST (or, where a failure type cannot practically be induced in the test environment, for a representative subset with the remainder verified through simulation or provider-supported demonstration recorded in the ETR):

1. Induce or simulate the failure according to the TSS description (for example, revoking connectivity to a required cloud service, detaching storage, or terminating an instance through the orchestrator).
2. Verify the TOE enters the secure state defined in the TSS.
3. While the TOE is in the secure state, attempt to access protected data or perform a security-relevant operation, and verify the attempt is refused consistent with the TSS definition of the secure state.
4. Recover the TOE per the operational guidance and verify normal operation resumes.

Expected result: For each claimed failure type, the TOE preserves the TSS-defined secure state and protected data is not exposed during the failure condition.

8.3. FPT_ITT.1 Internal TSF Data Transfer Protection

8.3.1. FPT_ITT.1 Evaluation Activities

8.3.1.1. TSS Activities

The evaluator shall verify that the TSS describes:

1. The protection type selected (disclosure, modification, or both):
    a. If disclosure protection is selected, the confidentiality mechanisms used
    b. If modification protection is selected, the integrity mechanisms used
2. The separate parts of the TOE between which TSF data is transferred:
    a. Database nodes in a cluster
    b. Control plane and data plane components
    c. Replication endpoints
    d. Management services and database engines
3. The specific TSF data protected during transfer:
    a. Authentication credentials and session tokens
    b. Configuration data
    c. Replication data
    d. Health check and status information
    e. Cryptographic keys or key material
4. The mechanisms used to protect transfers:
    a. TSF-implemented cryptographic protocols (TLS, mTLS)
    b. Authentication between components
    c. Any supplementary operational-environment measures (network isolation, private networks, VPCs, or OS/kernel-implemented protocols such as IPsec) — the TSS shall distinguish these from TSF-provided protection, because they are defense in depth and cannot alone satisfy FPT_ITT.1 (see the PP-Module's Security Function Allocation)
5. For cloud deployments specifically:
    a. Protection of cluster communication in cloud networks
    b. Use of cloud-native encryption for inter-component traffic
    c. Network security groups or policies for component isolation

8.3.1.2. Guidance Activities

The evaluator shall verify that the operational guidance (AGD_OPE/AGD_PRE):

1. Documents the deployment architecture for distributed configurations.
2. Provides instructions for:
    a. Configuring encryption for inter-node communication
    b. Setting up mutual authentication between components
    c. Configuring network isolation for cluster traffic

3. Documents the cryptographic algorithms used for protection (reference to DBMS Crypto Module if applicable).
4. Provides cloud-specific deployment guidance:
    a. Kubernetes network policies for pod-to-pod encryption
    b. Cloud VPC configuration for cluster isolation
    c. Load balancer and service mesh configuration

8.3.1.3. Test Activities

Test 1: Disclosure Protection Verification

If disclosure protection is selected:

1. Step: Deploy the TOE in a distributed configuration (multi-node cluster).
2. Step: Capture network traffic between TOE components.
3. Step: Generate traffic that includes TSF data (authentication, configuration synchronization).
4. Expected Result: Captured traffic is encrypted; TSF data is not visible in plaintext.

Test 2: Modification Protection Verification

If modification protection is selected:

1. Step: Deploy the TOE in a distributed configuration.
2. Step: If possible, intercept and modify traffic between components (man-in-the-middle).
3. Expected Result: Receiving component detects modification and rejects the data.
4. Step: Verify an appropriate error or audit record is generated.

Test 3: Cluster Communication Security

For clustered deployments:

1. Step: Verify all nodes in the cluster use protected communication channels.
2. Step: Attempt to add a rogue node to the cluster without proper credentials.
3. Expected Result: The rogue node is rejected.
4. Step: Verify legitimate cluster operations succeed with protection enabled.

Test 4: Management/Data Plane Separation

If the TOE has separate management and data planes:

1. Step: Verify management plane traffic is protected independently of data plane traffic.
2. Step: Capture traffic on both planes.
3. Expected Result: Both planes use appropriate protection mechanisms.

Test 5: Cloud Network Isolation (Supplementary — Operational Environment)

For cloud deployments. This test examines defense-in-depth configuration of the operational environment and does not contribute TSF evidence for FPT_ITT.1; the TSF evidence is provided by Tests 1 through 4.

1. Step: Verify cluster nodes communicate only over private networks/VPCs.
2. Step: Verify external access to inter-node communication is blocked.
3. Step: For Kubernetes deployments, verify network policies restrict inter-pod communication appropriately.

Test 6: Replication Traffic Protection

For replicated deployments:

1. Step: Configure replication between primary and replica instances.
2. Step: Capture replication traffic.
3. Expected Result: Replication data is protected according to selected protection type.
4. Step: Verify replication functions correctly with protection enabled.

8.4. FPT_TUD_EXT.1 Trusted Update

8.4.1. FPT_TUD_EXT.1 Evaluation Activities

8.4.1.1. TSS Activities

The evaluator shall verify that the TSS describes:

1. The mechanism for querying the current TOE version:
   a. Interface(s) used (CLI, API, console)
   b. Information provided (version number, build date, component versions)
2. The update mechanisms supported:
   a. Cloud-native deployment services (AWS Systems Manager, Azure Update Management)
   b. Trusted image registries (container registries with signing)
   c. Secure boot or image verification mechanisms (if FPT_SBT_EXT.1 is selected)
   d. Package management systems
   e. Manual update procedures
3. The authenticity and integrity verification mechanisms:
   a. Digital signature verification (signing authority, algorithms)
   b. Cryptographic hash verification (algorithms, source of known-good values)
   c. Certificate chain validation
4. For cloud deployments specifically:

a. Container image signature verification (Docker Content Trust, Sigstore, etc.)
b. Verification of images from cloud provider registries
c. Integration with cloud-native update services

8.4.1.2. Guidance Activities

The evaluator shall verify that the operational guidance (AGD_OPE/AGD_PRE):

1. Documents the procedure for querying current TOE version.
2. Provides step-by-step update procedures for each supported mechanism.
3. Documents the verification process:
   a. How to verify update authenticity before installation
   b. Expected signatures or hashes
   c. Actions if verification fails
4. Provides guidance for cloud-native updates:
   a. Container image update procedures
   b. Rolling update strategies for minimal downtime
   c. Rollback procedures if updates fail
5. Documents the trusted sources for updates:
   a. Official repositories or registries
   b. Signing keys or certificates
   c. Verification endpoints

8.4.1.3. Test Activities

Test 1: Version Query

1. Step: Use each available interface to query the current TOE version.
2. Expected Result: Version information is returned accurately.
3. Step: Verify the version information matches the installed TOE version.

Test 2: Authentic Update Installation

1. Step: Obtain a genuine update package from a trusted source.
2. Step: Apply the update using the documented procedure.
3. Step: Verify the update is verified for authenticity and integrity.
4. Step: Verify the update installs successfully.
5. Step: Query the version to confirm the update was applied.

Test 3: Tampered Update Rejection

1. Step: Obtain a genuine update package.

2. Step: Modify the package (change a byte, alter contents).
3. Step: Attempt to apply the tampered update.
4. Expected Result: The TSF rejects the update due to integrity verification failure.
5. Step: Verify an appropriate error message or audit record is generated.

Test 4: Invalid Signature Rejection

1. Step: Create or obtain an update package signed with an untrusted key.
2. Step: Attempt to apply the package.
3. Expected Result: The TSF rejects the update due to authenticity verification failure.
4. Step: Verify an appropriate error message or audit record is generated.

Test 5: Cloud-Native Update Verification

For container deployments. This test contributes TSF evidence for FPT_TUD_EXT.1.3 only where the ST includes the image-verification mechanism in the TOE boundary (for example, via FPT_SBT_EXT.1 or TOE-implemented deployment verification). Where signature enforcement is performed by the registry or orchestrator in the operational environment, this test is a supplementary environment-integration check, and the TSF evidence for FPT_TUD_EXT.1.3 is provided by Tests 2 through 4.

1. Step: Push a signed container image to the registry.
2. Step: Deploy the TOE using the signed image.
3. Expected Result: Deployment succeeds.
4. Step: Push an unsigned or invalidly signed image.
5. Step: Attempt to deploy using the unsigned image.
6. Expected Result: Deployment fails or generates a security alert.

For cloud-managed update services:

1. Step: Configure the TOE to receive updates from the cloud update service.
2. Step: Apply an update through the service.
3. Step: Verify the update was validated before installation.

Test 6: Update Audit

1. Step: Apply a successful update.
2. Step: Verify an audit record is generated indicating:
    a. Previous version
    b. New version
    c. Timestamp
    d. User or system that initiated the update

8.5. FPT_SBT_EXT.1 Secure Boot and Image Verification (Selection-Based)

8.5.1. FPT_SBT_EXT.1 Evaluation Activities

This SFR is selection-based and applies when "secure boot or image verification mechanisms as defined in FPT_SBT_EXT.1" is selected in `FPT_TUD_EXT.1.2`.

8.5.1.1. TSS Activities

The evaluator shall verify that the TSS describes:

1. The boot-time or deployment-time components subject to verification:
    a. Executable binaries
    b. Configuration files
    c. Container images
    d. Dependent libraries or modules
2. The integrity verification mechanisms:
    a. Cryptographic hash algorithms used
    b. Hash storage and comparison methods
    c. Verification timing (before execution, at deployment, etc.)
3. The authenticity verification mechanisms:
    a. Digital signature verification
    b. Signing authorities trusted
    c. Certificate or key management
4. The action taken if verification fails:
    a. Prevent boot/startup
    b. Alert administrators
    c. Other specified actions
5. For containerized deployments:
    a. Container image signature verification (Docker Content Trust, Sigstore, Cosign)
    b. Registry trust configuration
    c. Kubernetes admission controller integration

8.5.1.2. Guidance Activities

The evaluator shall verify that the operational guidance (AGD_OPE/AGD_PRE):

1. Documents the components verified at boot/deployment time.

2. Provides instructions for:
    a. Configuring trusted signing keys or certificates
    b. Setting up image registry trust
    c. Configuring verification policies
3. Documents the expected behavior when verification fails.
4. Provides cloud-specific guidance:
    a. Container image signing procedures
    b. Kubernetes admission controller configuration
    c. Cloud provider image verification services

8.5.1.3. Test Activities

Test 1: Boot Chain Verification

1. Step: Boot the TOE normally.
2. Step: Verify all boot-time integrity checks pass.
3. Step: Verify the TOE starts successfully.

Test 2: Tampered Boot Component Rejection

1. Step: Modify a boot-time component (if possible in the test environment).
2. Step: Attempt to boot the TOE.
3. Expected Result: TOE detects integrity failure and takes configured action (prevent boot or alert).
4. Step: Verify the action matches the configuration.

Test 3: Container Image Signature Verification

For containerized deployments:

1. Step: Deploy the TOE using a properly signed container image.
2. Expected Result: Deployment succeeds.
3. Step: Attempt to deploy using an unsigned image.
4. Expected Result: Deployment fails or generates security alert.
5. Step: Attempt to deploy using an image with invalid signature.
6. Expected Result: Deployment fails or generates security alert.

Test 4: Kubernetes Admission Control Integration

If Kubernetes admission controllers are used. This test contributes TSF evidence for FPT_SBT_EXT.1 only where the ST includes the admission-control verification in the TOE boundary; where the admission controller is operational-environment machinery, this test is a supplementary environment-integration check and the TSF evidence is provided by the other FPT_SBT_EXT.1 tests.

1. Step: Configure an admission controller to validate image signatures.
2. Step: Attempt to deploy a pod with a signed image.
3. Expected Result: Pod is admitted.
4. Step: Attempt to deploy a pod with an unsigned image.
5. Expected Result: Pod is rejected by the admission controller.

Test 5: Administrator Alert on Verification Failure

If alert is selected as the failure action:

1. Step: Trigger a verification failure (deploy unsigned image, modify component).
2. Step: Verify an alert is generated to administrators.
3. Step: Verify the alert includes information about the failure.

8.6. FPT_TST.1 TSF Self-Test (Selection-Based)

8.6.1. FPT_TST.1 Evaluation Activities

This SFR is selection-based and applies when "integrity failure via self-test" is selected in FPT_ARS_EXT.1.

8.6.1.1. TSS Activities

The evaluator shall verify that the TSS describes:

1. The conditions under which self-tests are run:
    a. During initial start-up
    b. Periodically during normal operation (specify interval)
    c. At the request of authorized user
    d. Other specified conditions
2. The self-tests performed:
    a. Cryptographic module integrity checks (if crypto is implemented)
    b. File or image integrity validation
    c. Runtime environment verification
    d. Configuration integrity checks
    e. Other tests as specified
3. For each self-test:
    a. What is tested
    b. Expected results

    c. Actions on failure
4. The mechanism for users to verify TSF integrity:
    a. Interfaces available
    b. Information provided

8.6.1.2. Guidance Activities

The evaluator shall verify that the operational guidance (AGD_OPE/AGD_PRE):

1. Documents all self-tests performed and their purpose.
2. Provides instructions for:
    a. Configuring self-test schedules (if periodic testing is supported)
    b. Initiating on-demand self-tests
    c. Interpreting self-test results
3. Documents the expected behavior when self-tests fail.
4. Provides troubleshooting guidance for self-test failures.

8.6.1.3. Test Activities

Test 1: Startup Self-Test

If startup self-test is selected:

1. Step: Start the TOE.
2. Step: Verify self-tests are executed during startup (check logs, audit records).
3. Step: Verify self-tests complete successfully.
4. Step: Verify the TOE becomes operational after successful tests.

Test 2: Periodic Self-Test

If periodic self-test is selected:

1. Step: Configure the self-test interval.
2. Step: Wait for the interval to elapse.
3. Step: Verify self-tests are executed (check logs, audit records).

Test 3: On-Demand Self-Test

If on-demand self-test is selected:

1. Step: As an authorized user, initiate a self-test.
2. Step: Verify the self-test executes.
3. Step: Verify results are reported to the user.

Test 4: Self-Test Failure Detection

1. Step: If possible, cause a self-test to fail (corrupt a verified file, alter configuration).
2. Step: Trigger the self-test.
3. Expected Result: TSF detects the failure.
4. Step: Verify the configured failure action is taken (alert, shutdown, degraded mode).
5. Step: Verify an audit record is generated for the failure.

Test 5: TSF Data Integrity Verification

1. Step: Request TSF data integrity verification (as authorized user).
2. Step: Verify the result indicates current integrity status.
3. Step: Modify TSF data (if possible in test environment).
4. Step: Request integrity verification again.
5. Expected Result: Verification detects the modification.

Test 6: Cryptographic Self-Test

If cryptographic self-tests are implemented:

1. Step: Verify known-answer tests or algorithm validation tests are performed.
2. Step: Verify cryptographic operations are blocked until self-tests pass.

Chapter 9. FDP Class: User Data Protection Coordination

This Supporting Document (SD) provides Cloud-specific coordination activities for FDP requirements inherited from the mandatory DBMS Crypto Module, as well as cloud-specific Security Assurance Requirement (SAR) activities that supplement the base PP's assurance requirements.

9.1. Scope

This document covers:

- **Part 1**: Cloud-specific coordination activities for Crypto Module `FDP_DAR_EXT.1` (Data-at-Rest Protection) and `FDP_DIT_EXT.1` (Data-in-Transit Protection)
- **Part 2**: Cloud-specific Assurance Activities for ADV, AGD, ALC, ATE, and AVA classes

9.2. Relationship to Other Documents

- **PP-Module**: collaborative PP-Module for DBMS in the Cloud [DBMS_Cloud_MOD]
- **Base PP SD**: Supporting Document - Evaluation Activities for cPP_DBMS
- **Crypto Module SD**: Supporting Document - Evaluation Activities for DBMS Cryptographic Module

The cryptographic testing activities for encryption algorithms, TLS protocol implementation, X.509 validation, and key management are defined in the DBMS Crypto Module SD. This document addresses selection verification, cloud interface mapping, deployment integration, and module coordination.

The FDP activities in this SD coordinate Cloud Module evaluation with the mandatory DBMS Crypto Module. Data-at-rest cryptographic behavior and core data-in-transit cryptographic protocol behavior are evaluated under the Crypto Module SD; this Cloud SD verifies cloud-deployment mapping and integration.

The evaluator shall:

1. Verify the ST includes the mandatory DBMS Crypto Module.
2. Confirm the TSS maps cloud storage and external interfaces to the applicable Crypto Module SFRs.
3. Validate that guidance documentation addresses cloud deployment considerations.
4. Coordinate cloud-specific integration testing with Crypto Module cryptographic testing.

9.3. Data-at-Rest Coordination with DBMS Crypto Module

9.3.1. Crypto Module Requirement Reference

The Cloud PP-Module does not define a Cloud-local `FDP_DAR_EXT.1` requirement. Data-at-rest encryption is evaluated through `FDP_DAR_EXT.1` in the mandatory DBMS Crypto Module. The ST author selects the applicable strategy ("Storage-Scope Encryption" or "Granular Data Encryption") and includes the corresponding Catalogue-derived components consumed in the Crypto Module.

9.3.2. EA-FDP_DAR_EXT.1: Cloud Coordination Evaluation Activities

9.3.2.1. EA-FDP_DAR_EXT.1.1: TSS Evaluation

Work Unit	Activity
EA-FDP_DAR_EXT.1.1-1	The evaluator shall verify the ST includes the DBMS Crypto Module in the PP-Configuration claim and identifies the selected Crypto Module `FDP_DAR_EXT.1` strategy.
EA-FDP_DAR_EXT.1.1-2	The evaluator shall examine the TSS to verify it maps cloud-deployed persistent storage objects to the data-at-rest protection described for the selected Crypto Module strategy, including database files, transaction or redo logs, temporary files, backup or archive data, configuration data containing security parameters, and credential or key material where applicable.
EA-FDP_DAR_EXT.1.1-3	The evaluator shall verify the TSS describes any cloud-specific integration used to support data-at-rest protection, such as cloud HSMs, key vault services, storage classes, volume types, object storage, deployment automation, or secret retrieval. Detailed cryptographic key management and algorithm testing remains governed by the DBMS Crypto Module SD.

9.3.2.2. EA-FDP_DAR_EXT.1.2: AGD Evaluation

Work Unit	Activity
EA-FDP_DAR_EXT.1.2-1	The evaluator shall examine the operational guidance to verify it describes how to configure data-at-rest protection in cloud deployment environments, including prerequisites, key-management setup, storage configuration, recovery procedures, and any cloud-native service integration used by the TOE.
EA-FDP_DAR_EXT.1.2-2	The evaluator shall verify the guidance does not present platform storage encryption or an unencrypted storage mode as an alternate way to satisfy the mandatory DBMS Crypto Module `FDP_DAR_EXT.1` requirement.

9.3.2.3. EA-FDP_DAR_EXT.1.3: ATE Evaluation

Work Unit	Activity
EA-FDP_DAR_EXT.1.3-1	The evaluator shall verify that cryptographic testing for data-at-rest encryption is performed under the DBMS Crypto Module evaluation and that the Cloud Module ETR references the applicable Crypto Module test results.
EA-FDP_DAR_EXT.1.3-2	The evaluator shall independently verify cloud-deployment integration for data-at-rest protection, including that encrypted storage coverage remains consistent across deployment automation, scaling, restart, migration, backup, and restore scenarios claimed by the TOE.

9.3.2.4. EA-FDP_DAR_EXT.1.4: Cloud-Specific Testing Considerations

Work Unit	Activity
EA-FDP_DAR_EXT.1.4-1	When testing in cloud environments, the evaluator shall: a) Verify the encryption configuration persists across instance stop/start cycles b) Verify encryption is maintained when storage volumes are detached and reattached c) Verify encryption configuration is preserved during cloud orchestration operations (scaling, migration) d) Verify audit records are generated for encryption configuration changes
EA-FDP_DAR_EXT.1.4-2	The evaluator shall verify that cloud-specific storage types used by the TOE are covered by the encryption mechanism, including: a) Root volumes (if TOE binaries/config are stored there) b) Data volumes (where database files reside) c) Temporary storage / instance storage (if used for sensitive data) d) Cloud object storage (if used for backups or data export)

9.4. FDP_DIT_EXT.1 Data-in-Transit Protection Cloud Coordination

9.4.1. Crypto Module Requirement Reference

The Cloud PP-Module does not define a Cloud-local `FDP_DIT_EXT.1` requirement. Data-in-transit protection is defined and evaluated through mandatory `FDP_DIT_EXT.1` in the DBMS Crypto Module. The Cloud Module identifies the cloud deployment channels to which that requirement applies and verifies that those channels are configured and exercised in representative cloud deployments.

9.4.2. EA-FDP_DIT_EXT.1: Cloud Coordination Evaluation Activities

9.4.2.1. EA-FDP_DIT_EXT.1.1: TSS Evaluation

9.4.2.1.1. General TSS Requirements

Work Unit	Activity
EA-FDP_DIT_EXT.1.1-1	The evaluator shall verify the TSS identifies all external interfaces that transmit data requiring protection, including: * Client-to-DBMS connections (queries, results) * Administrative interfaces (management consoles, APIs) * Replication/backup interfaces * Integration interfaces (cloud IAM, audit export, secret retrieval) * Inter-node communication (for distributed deployments, addressed separately by FPT_ITT.1)
EA-FDP_DIT_EXT.1.1-2	The evaluator shall verify the TSS clearly identifies which selection was made in the Crypto Module `FDP_DIT_EXT.1.1` and specifies which cloud-facing interfaces use which protection mechanism. For HTTPS interfaces, the TSS shall describe the interface as HTTP over the selected TLS channel.
EA-FDP_DIT_EXT.1.1-3	The evaluator shall verify the TSS describes the TOE's cloud-deployment behavior when a protected connection cannot be established, such as external identity provider, audit export, secret retrieval, or management API connection failure. The detailed certificate validation and protocol mismatch behavior is evaluated under the Crypto Module SD; this activity verifies that the cloud integration fails securely and does not fall back to an unprotected path.

9.4.2.1.2. Selection-Specific TSS Activities

When TLS, including HTTPS over TLS where applicable, is selected:

Work Unit	Activity
EA-FDP_DIT_EXT.1.1-4	The evaluator shall verify the ST includes the applicable requirements from the TLS Functional Package for each TLS-protected cloud-facing interface, including `FCS_TLSC_EXT.1`, `FCS_TLSS_EXT.1`, or both as applicable to the TOE role. The evaluator shall verify the TSS maps each interface to its TLS client or server behavior without duplicating TLS protocol evaluation.
EA-FDP_DIT_EXT.1.1-5	The evaluator shall verify the TSS describes the cloud deployment parameters that select or constrain the Crypto Module protected channel behavior, including: a) TLS versions and cipher suites as references to the applicable TLS Functional Package components and the Catalogue-derived primitives consumed in the Crypto Module b) Which deployment interfaces are TLS clients, TLS servers, or both c) Whether mutual TLS (mTLS) is supported or required for any cloud integration d) Integration with cloud certificate management or secrets management services e) Behavior when cloud routing, load balancer, proxy, or service mesh configuration affects channel termination or re-encryption

Work Unit	Activity
EA-FDP_DIT_EXT.1.1-6	The evaluator shall verify the TSS identifies which TOE interfaces act as: a) TLS clients (covered by FCS_TLSC_EXT.1) b) TLS servers (covered by FCS_TLSS_EXT.1) c) Both client and server (requiring both SFRs)
EA-FDP_DIT_EXT.1.1-7	The evaluator shall verify the TSS describes how the TOE obtains and manages TLS certificates in cloud environments, including: a) Certificate sources (cloud-native certificate services, third-party CA, self-signed) b) Certificate storage and protection c) Certificate rotation procedures d) Integration with cloud secrets management for private keys

For interfaces that provide HTTPS over the selected TLS channel:

Work Unit	Activity
EA-FDP_DIT_EXT.1.1-8	The evaluator shall verify HTTPS use is mapped to the corresponding TLS client or server requirements. No separate HTTPS cryptographic component claim is required.
EA-FDP_DIT_EXT.1.1-9	The evaluator shall verify the TSS describes: a) Which interfaces use HTTPS (typically REST APIs, web-based management consoles) b) The underlying TLS configuration for HTTPS c) HTTP Strict Transport Security (HSTS) support (if applicable) d) Behavior when HTTP (non-secure) connections are attempted
EA-FDP_DIT_EXT.1.1-10	The evaluator shall verify the TSS describes how the TOE enforces HTTPS-only access to protected interfaces and whether HTTP-to-HTTPS redirection is supported or if HTTP is completely disabled.

When "other cryptographic protocols" is assigned:

Work Unit	Activity
EA-FDP_DIT_EXT.1.1-11	The evaluator shall verify the TSS identifies any non-TLS protocol assigned in the Crypto Module FDP_DIT_EXT.1.1 and maps it to specific cloud-facing interfaces, including: a) Protocol identification and version b) The Functional Package components that specify and evaluate the protocol c) Authentication mechanism d) Reference to applicable standards or specifications e) The cloud interfaces and deployment paths where the protocol is used
EA-FDP_DIT_EXT.1.1-12	The evaluator shall verify that the alternative protocol is covered by scheme-acceptable evaluation activities through the Crypto Module claim. The Cloud SD does not create a new cryptographic protocol evaluation method for the alternative protocol.

Work Unit	Activity
EA-FDP_DIT_EXT.1.1-13	The evaluator shall verify the cloud deployment does not use the alternative protocol on any interface not mapped to the corresponding Crypto Module claim.

9.4.2.2. EA-FDP_DIT_EXT.1.2: AGD Evaluation

Work Unit	Activity
EA-FDP_DIT_EXT.1.2-1	The evaluator shall examine the operational guidance to verify it describes how to configure data-in-transit protection in cloud environments, including: a) Enabling TLS on all applicable interfaces, including HTTPS over TLS where applicable b) Certificate installation and configuration procedures c) Cipher suite configuration (if configurable) d) Client certificate requirements (for mTLS deployments)
EA-FDP_DIT_EXT.1.2-2	The evaluator shall verify the guidance describes integration with cloud-native certificate and secrets management services, including: a) AWS Certificate Manager / Secrets Manager integration b) Azure Key Vault integration c) Google Cloud Certificate Manager integration d) HashiCorp Vault integration e) Kubernetes secrets integration (for containerized deployments)
EA-FDP_DIT_EXT.1.2-3	The evaluator shall verify the guidance describes: a) How to verify TLS, including HTTPS over TLS, is correctly configured b) How to test connectivity using protected channels c) How to diagnose connection failures related to TLS/certificate issues d) Certificate renewal and rotation procedures
EA-FDP_DIT_EXT.1.2-4	The evaluator shall verify the guidance identifies all TOE interfaces requiring protection and provides interface-specific configuration instructions for cloud deployment scenarios.

9.4.2.3. EA-FDP_DIT_EXT.1.3: ATE Evaluation

Work Unit	Activity
EA-FDP_DIT_EXT.1.3-1	**For TLS selections, including HTTPS over TLS:** The evaluator shall verify that protocol testing is performed under the applicable TLS Functional Package evaluation and coordinated with the DBMS Crypto Module integration evaluation. The evaluator shall confirm: a) `FCS_TLSC_EXT.1` testing covers TLS client behavior for all client interfaces b) `FCS_TLSS_EXT.1` testing covers TLS server behavior for all server interfaces c) HTTPS interfaces are mapped to the underlying TLS client or server testing, with HTTP-specific enforcement checked by this Cloud SD d) Test results are documented in the Crypto Module ETR NOTE: The evaluator is not required to duplicate TLS protocol testing. Coordination with the Crypto Module evaluation team is sufficient.
EA-FDP_DIT_EXT.1.3-2	The evaluator shall independently verify cloud deployment enforcement for representative protected interfaces: a) Unprotected access paths, such as plaintext HTTP for an HTTPS management interface, are disabled, rejected, or redirected exactly as described in the ST and guidance b) The deployed cloud route, load balancer, proxy, or service mesh preserves the protected channel properties claimed for the interface, including re-encryption where TLS is terminated before the TOE c) Certificate or trust-store misconfiguration for a cloud integration prevents the integration from being used rather than causing fallback to an unprotected channel d) Evidence from the Crypto Module evaluation covers detailed TLS, X.509, and cipher-suite behavior for the same TOE roles used by the cloud-facing interfaces
EA-FDP_DIT_EXT.1.3-3	**For alternative protocols:** The evaluator shall coordinate with the Crypto Module evaluation and execute only Cloud-specific integration tests needed to verify: a) The protocol is used only on the cloud-facing interfaces identified in the ST b) The deployment does not expose an unprotected fallback path for those interfaces c) The protocol operates as described in the cloud deployment guidance d) The Crypto Module evaluation covers the cryptographic behavior of the protocol

9.4.2.4. EA-FDP_DIT_EXT.1.4: Cloud-Specific Testing Considerations

Work Unit	Activity
EA-FDP_DIT_EXT.1.4-1	When testing in cloud environments, the evaluator shall verify data-in-transit protection for: a) Connections from external networks (internet-facing) b) Connections within the cloud VPC/VNet (private network) c) Connections across availability zones d) Connections across cloud regions (if applicable)

Work Unit	Activity
EA-FDP_DIT_EXT.1.4-2	The evaluator shall verify the TOE correctly handles cloud load balancer scenarios: a) TLS termination at load balancer (with re-encryption to TOE) b) TLS passthrough to TOE c) End-to-end encryption through load balancers
EA-FDP_DIT_EXT.1.4-3	The evaluator shall verify: a) Certificate rotation does not cause connection failures for active sessions b) The TOE handles certificate refresh from cloud services appropriately c) Audit records capture TLS connection establishment/failure events
EA-FDP_DIT_EXT.1.4-4	The evaluator shall verify that data-in-transit protection is maintained when: a) The TOE is scaled horizontally (new instances) b) The TOE is migrated between hosts c) The TOE is restarted or recovered

Chapter 10. Cloud-Specific SAR Assurance Activities

10.1. Introduction

This section provides cloud-specific assurance activities that supplement the base PP's SAR requirements. These activities address unique considerations for evaluating DBMS products deployed in cloud environments and should be performed in conjunction with (not in place of) the base PP's assurance activities.

10.2. ADV: Development

10.2.1. ADV_FSP.2: Functional Specification - Cloud Considerations

The following activities supplement ADV_FSP.2 requirements from the base PP to address cloud integration points.

Work Unit	Activity
EA-ADV_FSP.Cloud-1	The evaluator shall verify the functional specification identifies and describes all TSFIs for cloud integration points, including: a) Cloud IAM integration interfaces (authentication tokens, role assertions) b) Cloud secrets management interfaces (credential retrieval, rotation) c) Cloud audit/logging integration interfaces (log export, SIEM integration) d) Cloud configuration management interfaces (environment variables, config maps) e) Cloud orchestration interfaces (health checks, readiness probes, lifecycle hooks)
EA-ADV_FSP.Cloud-2	The evaluator shall verify the functional specification describes the API interfaces exposed by the TOE for cloud deployment, including: a) REST/HTTP APIs for management b) gRPC or protocol-specific APIs (if applicable) c) Cloud provider SDK integrations d) Kubernetes or container orchestration APIs (if applicable)
EA-ADV_FSP.Cloud-3	The evaluator shall verify the functional specification describes the TOE's behavior when cloud services are unavailable, including: a) Timeout handling for cloud service calls b) Retry logic and backoff strategies c) Fallback behavior (fail-secure vs. cached credentials) d) Error reporting and logging

Work Unit	Activity
EA-ADV_FSP.Cloud-4	The evaluator shall verify the functional specification describes the TOE's authentication and authorization model for cloud-originated requests, including: a) How cloud IAM tokens/assertions are validated b) How cloud identities are mapped to TOE roles c) How authorization decisions are made for cloud API calls

10.3. AGD: Guidance Documents

10.3.1. AGD_OPE.1: Cloud Operational Guidance

The following activities supplement AGD_OPE.1 requirements from the base PP to address cloud-specific operational guidance.

Work Unit	Activity
EA-AGD_OPE.Cloud-1	The evaluator shall verify the operational guidance covers cloud platform prerequisites, including: a) Minimum cloud provider requirements (service versions, feature availability) b) Required cloud services (IAM, KMS, logging, networking) c) Network configuration requirements (VPC, subnets, security groups, firewall rules) d) Instance/container resource requirements (CPU, memory, storage) e) Required cloud provider permissions/roles for the TOE service account
EA-AGD_OPE.Cloud-2	The evaluator shall verify the operational guidance covers cloud IAM integration procedures, including: a) Configuring the TOE to trust specific identity providers b) Mapping cloud IAM roles/groups to TOE roles c) Configuring service accounts/principals for TOE operation d) Setting up federated identity (if applicable) e) Revoking access for cloud identities
EA-AGD_OPE.Cloud-3	The evaluator shall verify the operational guidance covers audit export configuration, including: a) Configuring audit export destinations (CloudWatch, Azure Monitor, etc.) b) Setting up log formats compatible with cloud logging services c) Configuring log retention and rotation policies d) Integrating with SIEM solutions e) Verifying audit log delivery and completeness
EA-AGD_OPE.Cloud-4	The evaluator shall verify the operational guidance covers cloud secrets management, including: a) Configuring the TOE to retrieve secrets from cloud key vaults b) Setting up secret rotation procedures c) Protecting secrets in transit from key vaults to TOE d) Handling secret retrieval failures e) Auditing secret access

Work Unit	Activity
EA-AGD_OPE.Cloud-5	The evaluator shall verify the operational guidance covers environmental deployment artifact controls, and TOE-side deployment artifact verification when FPT_SBT_EXT.1 is claimed, including: a) Verifying image signatures before deployment b) Checking image digests/hashes c) Validating deployment manifests (Helm charts, Terraform configs) d) Ensuring trusted image sources (registries) e) Detecting and responding to tampered artifacts
EA-AGD_OPE.Cloud-6	The evaluator shall verify the operational guidance covers cloud-specific security hardening, including: a) Network isolation (private subnets, service endpoints) b) Instance metadata service protection (IMDSv2 enforcement) c) Storage encryption configuration d) Backup encryption configuration e) Logging and monitoring best practices

10.3.2. AGD_PRE.1: Cloud Preparative Procedures

The following activities supplement AGD_PRE.1 requirements from the base PP to address cloud deployment preparation.

Work Unit	Activity
EA-AGD_PRE.Cloud-1	The evaluator shall verify the preparative procedures cover cloud deployment preparation, including: a) Provisioning required cloud resources (compute, storage, networking) b) Configuring cloud security groups and network ACLs c) Setting up cloud IAM roles and policies d) Creating and configuring secrets in cloud key vaults e) Preparing deployment artifacts (images, manifests)

Work Unit	Activity
EA-AGD_PRE.Cloud-2	The evaluator shall verify the preparative procedures identify the Trusted Platform reliance for the evaluated configuration, including: a) Identifying the cloud provider, Cloud Service Offering, region or zone, and relied-upon services b) Identifying the assumptions and Operational Environment objectives supported by each relied-upon service c) Identifying the cloud authorization, certification, scheme policy, or other evidence submitted for the Trusted Platform d) Confirming that the stated scope of the evidence covers the identified offering, region, services, and evaluated configuration e) Providing the configuration steps needed to use the relied-upon services as described in the ST Acceptance criteria for the submitted evidence, including recognized authorization programs, assurance levels, currency, and exceptions, are determined by the evaluation authority under the applicable scheme policy. This Evaluation Activity does not require the evaluator to assess the Trusted Platform as part of the TOE or independently establish the sufficiency of its controls.
EA-AGD_PRE.Cloud-3	The evaluator shall verify the preparative procedures cover secure image/container deployment, including: a) Downloading the TOE image from authorized sources b) Verifying image signatures or hashes c) Scanning images for vulnerabilities (if required by organization) d) Storing images in trusted private registries e) Configuring container runtime security settings
EA-AGD_PRE.Cloud-4	The evaluator shall verify the preparative procedures cover Infrastructure as Code (IaC) deployment, including: a) Reviewing deployment templates for security compliance b) Validating parameters against security baseline c) Testing deployment in non-production environment d) Enabling deployment logging and audit trails e) Storing IaC templates securely with version control
EA-AGD_PRE.Cloud-5	The evaluator shall apply the preparative procedures to deploy the TOE in a test cloud environment to confirm the procedures are complete, accurate, and result in a secure configuration.

10.4. ALC: Life-cycle Support

10.4.1. ALC_DEL.1: Cloud Delivery Considerations

The following activities supplement ALC_DEL.1 requirements from the base PP to address cloud-specific delivery mechanisms.

Work Unit	Activity
EA-ALC_DEL.Cloud-1	The evaluator shall verify the delivery documentation describes secure delivery via cloud marketplaces and registries, including: a) Official cloud marketplace listings (AWS Marketplace, Azure Marketplace, GCP Marketplace) b) Official container registries (Docker Hub, cloud provider registries, private registries) c) Identification information for authentic listings (vendor identity, product identifiers) d) Version identification for marketplace/registry listings
EA-ALC_DEL.Cloud-2	The evaluator shall verify the delivery documentation describes image integrity verification procedures, including: a) Digital signatures for VM images and containers b) Cryptographic hashes (SHA-256 or stronger) for all artifacts c) Signed metadata files listing artifact hashes d) Procedures to verify signatures against vendor public keys e) Procedures to compare downloaded hashes against published values
EA-ALC_DEL.Cloud-3	The evaluator shall verify the delivery documentation describes protection of delivery channels, including: a) HTTPS-only access to download locations b) Authenticated access to private registries c) Supply chain security measures (SBOM, provenance attestation) d) Detection of unauthorized modifications to marketplace listings
EA-ALC_DEL.Cloud-4	The evaluator shall verify the delivery documentation describes procedures for consumers to report suspected counterfeit or tampered artifacts.
EA-ALC_DEL.Cloud-5	The evaluator shall independently verify: a) The TOE is available from the documented delivery channels b) Published signatures/hashes can be verified c) The verification process described in guidance can be followed successfully

10.5. ATE: Tests

10.5.1. ATE_IND.2: Cloud Independent Testing Guidance

The following activities provide guidance for evaluator independent testing in cloud environments.

Work Unit	Activity
EA-ATE_IND.Cloud-1	**Test Environment Setup:** The evaluator shall establish a test environment that reflects realistic cloud deployment, including: a) Deployment in a supported cloud provider environment (or functional equivalent) b) Configuration of required cloud services (IAM, KMS, logging) c) Network configuration representative of production deployments d) Multiple instances/nodes for distributed testing (if applicable)

Work Unit	Activity
EA-ATE_IND.Cloud-2	**Test Environment Documentation:** The evaluator shall document the test environment including: a) Cloud provider and region b) Instance/container types and specifications c) Cloud service versions used d) Network topology e) TOE configuration (referencing guidance procedures used)
EA-ATE_IND.Cloud-3	**Handling Ephemeral Resources:** The evaluator shall develop testing strategies that account for ephemeral cloud resources: a) Test procedures shall be repeatable across instance replacements b) Test data shall be preserved across instance terminations (if needed) c) Tests shall not depend on specific instance identifiers d) Tests shall verify security properties persist through orchestration events
EA-ATE_IND.Cloud-4	**Handling Elastic/Scaling Events:** The evaluator shall test TOE behavior during scaling operations: a) Security properties maintained when scaling out (adding instances) b) Security properties maintained when scaling in (removing instances) c) Session handling during scale events d) Audit continuity during scale events
EA-ATE_IND.Cloud-5	**Handling Cloud Service Failures:** The evaluator shall test TOE behavior when cloud services are unavailable: a) Simulate IAM service unavailability (e.g., network block) b) Simulate KMS service unavailability c) Simulate logging service unavailability d) Verify TOE fails securely and does not bypass security checks
EA-ATE_IND.Cloud-6	**Multi-Zone/Multi-Region Testing:** If the TOE supports deployment across availability zones or regions, the evaluator shall test: a) Security properties maintained for cross-zone communication b) Consistency of security configuration across zones c) Audit aggregation from multiple zones d) Failover behavior maintains security properties
EA-ATE_IND.Cloud-7	**Container-Specific Testing (if applicable):** For containerized deployments, the evaluator shall test: a) Security properties with different container runtimes (if supported) b) Security properties under different orchestration platforms (Kubernetes, ECS, etc.) c) Resource limit enforcement d) Container isolation properties

10.6. AVA: Vulnerability Assessment

10.6.1. AVA_VAN.2: Cloud Vulnerability Considerations

The following activities supplement AVA_VAN requirements from the base PP to address cloud-

specific vulnerabilities.

Work Unit	Activity
EA-AVA_VAN.Cloud-1	**Cloud-Specific Attack Surface Analysis:** The evaluator shall analyze the cloud-specific attack surface, including: a) Cloud API exposure (management interfaces accessible from cloud networks) b) Instance metadata service access (IMDS vulnerabilities) c) Cloud IAM token handling (token theft, replay, scope escalation) d) Secrets exposure through environment variables or config maps e) Container escape risks (if containerized) f) Shared tenancy risks (side-channel, resource exhaustion)
EA-AVA_VAN.Cloud-2	**Cloud Infrastructure Vulnerability Considerations:** The evaluator shall consider how cloud infrastructure vulnerabilities could affect the TOE: a) Hypervisor vulnerabilities (cross-tenant attacks) b) Container runtime vulnerabilities c) Cloud provider service vulnerabilities d) Network infrastructure vulnerabilities (VPC misconfigurations) NOTE: The evaluator is not expected to discover zero-day vulnerabilities in cloud infrastructure, but shall consider the TOE's resilience against known cloud infrastructure attack patterns.
EA-AVA_VAN.Cloud-3	**Multi-Tenancy Vulnerability Analysis:** The evaluator shall analyze vulnerabilities related to cloud multi-tenancy: a) Data leakage to other tenants (memory, storage, network) b) Resource exhaustion by other tenants affecting TOE availability c) Cross-tenant attack vectors through shared services d) Insufficient isolation in container orchestration environments
EA-AVA_VAN.Cloud-4	**Supply Chain Vulnerability Analysis:** The evaluator shall analyze supply chain vulnerabilities in cloud deployments: a) Compromised base images b) Vulnerable dependencies in container images c) Tampered deployment artifacts d) Malicious operators in CI/CD pipelines
EA-AVA_VAN.Cloud-5	**Cloud-Specific Penetration Testing:** The evaluator shall include the following in penetration testing: a) Attempt to access instance metadata from TOE interfaces b) Attempt to escalate privileges using cloud IAM misconfigurations c) Attempt to access secrets through environment/config exposure d) Attempt to intercept or modify cloud service communications e) Attempt to exfiltrate data through cloud egress paths

Work Unit	Activity
EA-AVA_VAN.Cloud-6	**Vulnerability Public Domain Search (Cloud-Specific):** The evaluator shall search public vulnerability databases and sources for: a) CVEs affecting the TOE in cloud deployments b) CVEs affecting cloud provider services used by the TOE c) CVEs affecting container base images used by the TOE d) Security advisories from cloud providers relevant to the TOE's deployment model e) Published research on DBMS-in-cloud attack patterns
EA-AVA_VAN.Cloud-7	**Residual Vulnerability Documentation:** The evaluator shall document any cloud-specific residual vulnerabilities that cannot be exploited in the intended operational environment but could be exploited under different conditions, including: a) Vulnerabilities mitigated by Trusted Platform assumptions b) Vulnerabilities mitigated by OE security controls c) Vulnerabilities requiring elevated cloud administrator access d) Vulnerabilities dependent on specific cloud misconfigurations

Appendix A: Cross-Reference to CEM Work Units

This appendix maps the identifier-based evaluation activities in this document (the FDP coordination activities and the SAR activities) to CEM:2022 work units. The narrative TSS, Guidance, and Test activities defined for the module's FAU, FIA, FMT, and FPT SFRs refine the generic ASE_TSS.1, AGD_OPE.1/AGD_PRE.1, and ATE_IND.2 work units respectively and are not individually enumerated here.

A.1. FDP Evaluation Activities to CEM Mapping

EA Identifier	CEM Work Unit(s)	Notes
EA-FDP_DAR_EXT.1.1-1 to 1.1-3	ASE_TSS.1-1	TSS examination and Crypto Module coordination activities
EA-FDP_DAR_EXT.1.2-1 to 1.2-2	AGD_OPE.1-1, AGD_OPE.1-4	Guidance examination activities
EA-FDP_DAR_EXT.1.3-1 to 1.3-2	ATE_IND.2-3, ATE_IND.2-4	Independent testing and Crypto Module result coordination activities
EA-FDP_DAR_EXT.1.4-1 to 1.4-2	ATE_IND.2-3, ATE_IND.2-4	Cloud-specific integration testing activities
EA-FDP_DIT_EXT.1.1-1 to 1.1-13	ASE_TSS.1-1	Cloud interface mapping and TSS coordination activities
EA-FDP_DIT_EXT.1.2-1 to 1.2-4	AGD_OPE.1-1, AGD_OPE.1-4	Cloud deployment guidance examination activities
EA-FDP_DIT_EXT.1.3-1 to 1.3-3	ATE_IND.2-3, ATE_IND.2-4	Cloud-specific integration testing activities coordinated with Crypto Module results

A.2. SAR Evaluation Activities to CEM Mapping

EA Identifier	CEM Work Unit(s)	Notes
EA-ADV_FSP.Cloud-1 to Cloud-4	ADV_FSP.2	Supplements base PP ADV_FSP activities
EA-AGD_OPE.Cloud-1 to Cloud-6	AGD_OPE.1-1, AGD_OPE.1-2, AGD_OPE.1-4, AGD_OPE.1-5	Supplements base PP AGD_OPE activities
EA-AGD_PRE.Cloud-1 to Cloud-5	AGD_PRE.1-1, AGD_PRE.1-2	Supplements base PP AGD_PRE activities
EA-ALC_DEL.Cloud-1 to Cloud-5	ALC_DEL.1-1, ALC_DEL.1-2	Supplements base PP ALC_DEL activities

EA Identifier	CEM Work Unit(s)	Notes
EA-ATE_IND.Cloud-1 to Cloud-7	ATE_IND.2	Cloud-specific independent testing guidance
EA-AVA_VAN.Cloud-1 to Cloud-7	AVA_VAN.2	Cloud-specific vulnerability analysis activities

Appendix B: Relationship to DBMS Crypto Module SD

B.1. Cryptographic Testing Coordination

The FDP_DAR_EXT.1 and FDP_DIT_EXT.1 evaluation activities reference cryptographic requirements defined in the DBMS Crypto Module. The following table clarifies the division of evaluation responsibilities:

Aspect	DBMS Cloud Module SD (This Document)	DBMS Crypto Module SD
Selection Verification	Verify the PP-Configuration includes the mandatory Crypto Module and identifies the selected Crypto Module strategy or protocol for cloud interfaces	Verify selected cryptographic options are valid and tested
TSS Description	Verify TSS describes integration with crypto functions	Verify TSS describes crypto algorithm details
Algorithm Testing	Confirm Crypto Module tests cover algorithms used	Execute CAVP/algorithm testing
Protocol Testing (TLS, including HTTPS over TLS)	Confirm applicable TLS package or Crypto Module tests cover protocol behavior and verify HTTPS interfaces are mapped to the underlying TLS role	Coordinate TLS package evaluation activities for included TLS components and execute DBMS-specific cryptographic integration testing
Key Management Testing	Verify cloud integration for key storage/retrieval	Execute key generation, storage, destruction testing
Integration Testing	Test encryption/TLS enable/disable, cloud-specific scenarios	Test cryptographic operations in isolation

B.2. Information Sharing Between Evaluation Teams

When a TOE claims both the DBMS Cloud Module and the DBMS Crypto Module:

1. The Cloud Module evaluation team shall request test results from the Crypto Module evaluation team for:
    - FCS_COP.1 testing (encryption algorithms)
    - FCS_CKM.1 testing (key generation)
    - FCS_TLSC_EXT.1 testing (TLS client)
    - FCS_TLSS_EXT.1 testing (TLS server)
    - Mapping of HTTPS interfaces to the applicable TLS client or server tests

2. The Crypto Module evaluation team shall confirm:
    - Testing covers the algorithms/protocols used by the TOE for data-at-rest and data-in-transit protection
    - Test results are documented in the Crypto Module ETR
3. The Cloud Module ETR shall reference the Crypto Module ETR and confirm that cryptographic testing obligations have been met through module coordination.

Appendix C: Test Environment Guidance for Cloud Evaluators

C.1. Recommended Cloud Test Configurations

The following configurations are recommended for independent testing:

C.1.1. IaaS Deployment (VM-based)

- **Compute**: Cloud VM instances matching TOE minimum requirements
- **Storage**: Encrypted block storage volumes (for testing external encryption scenarios)
- **Network**: Private VPC/VNet with controlled egress
- **IAM**: Dedicated test IAM roles with minimal permissions
- **Logging**: Cloud-native logging service configured
- **Secrets**: Cloud key vault with test credentials

C.1.2. Container Deployment (Kubernetes)

- **Orchestrator**: Managed Kubernetes service or equivalent
- **Container Runtime**: Container runtime supported by TOE
- **Storage**: Persistent volumes with encryption
- **Network**: Network policies restricting pod communication
- **IAM**: Workload identity/IRSA configured
- **Secrets**: Kubernetes secrets or external secrets operator

C.2. Test Data Handling

- Use synthetic test data that does not contain actual sensitive information
- Ensure test data is deleted after evaluation completes
- Document data handling procedures in ETR

C.3. Cloud Account Security

- Use dedicated cloud accounts for evaluation
- Enable cloud audit logging for evaluation activities
- Restrict access to evaluation resources
- Delete evaluation resources after completion

Appendix D: Acronyms and Abbreviations

Acronym	Full Term
AD	Active Directory
API	Application Programming Interface
CAP	Composed Assurance Package
CC	Common Criteria
CCiTC	Common Criteria in the Cloud Technical Community
CEM	Common Methodology for Information Technology Security Evaluation
DBMS	Database Management System
EA	Evaluation Activity
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IAM	Identity and Access Management
IaaS	Infrastructure as a Service
LDAP	Lightweight Directory Access Protocol
mTLS	Mutual Transport Layer Security
NTP	Network Time Protocol
OCI	Oracle Cloud Infrastructure
OE	Operational Environment
OIDC	OpenID Connect
OSP	Organizational Security Policy
PaaS	Platform as a Service
PP	Protection Profile
SAR	Security Assurance Requirement
SD	Supporting Document
SFR	Security Functional Requirement
SIEM	Security Information and Event Management
SPD	Security Problem Definition
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSS	TOE Summary Specification

Acronym	Full Term
VPC	Virtual Private Cloud

Appendix E: Document References

- [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.
- [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.
- [CEM] Common Methodology for Information Technology Security Evaluation, Evaluation methodology, CCMB-2022-11-006, CEM:2022 Revision 1, November 2022.
- [DBMS_Cloud_MOD] collaborative PP-Module for DBMS in the Cloud (DBMS_Cloud_MOD), Version 0.4, 2026-06-30.
- [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 0.4, 2026-06-30.
- [DBMS_MOD_CRYPTO_SD] Supporting Document - Evaluation Activities for DBMS Cryptographic Functions Module, Version 0.4, 2026-06-30.