U.S. Government Protection Profile for Database Management Systems in Basic Robustness Environments

Version 1.0

Information Assurance Directorate

September 30, 2004

Protection Profile Title:

U.S. Government Protection Profile for Database Management Systems in Basic Robustness Environments.

Criteria Version:

This Protection Profile (PP) was developed using Version 2.1 of the Common Criteria (CC) and by applying the National Information Assurance Partnership (NIAP) interpretations that have been approved by the Common Criteria Evaluation and Validation Scheme (CCEVS) Management as of September 15, 2004.

Table of Contents

List of Figures

List of Tables

1 INTRODUCTION TO THE PROTECTION PROFILE

1.1 PP Identification

Title: U.S. Government Protection Profile for Database Management Systems in Basic Robustness Environments
Sponsor: National Security Agency (NSA)
CC Version: Common Criteria (CC) Version 2.1, and applicable interpretations.
PP Version: 1.0
Keywords: database management system, DBMS, COTS, commercial security, basic robustness, access control, discretionary access control, DAC, CC EAL2 augmented.

1.2 Overview of the Protection Profile

The "U.S. Government Protection Profile for Database Management Systems in Basic Robustness Environments" specifies security requirements for a commercial-off-the-shelf (COTS) database system that includes, but is not limited to, DBMS clients and DBMS servers and will be evaluated as a software only application layered on an underlying system (i.e., operating system, hardware, network services and/or custom software) and is usually embedded as a component of a larger system within an operational environment. This profile establishes the requirements necessary to achieve the security objectives of the Target of Evaluation (TOE) and its environment.
Conformant products provide access control based on user identity (e.g., Discretionary Access Control (DAC)) and generation of audit records for security relevant events. The IT environment must provide the following functionality: identification and authentication, security administration and audit record storage, and audit review. A conformant product, in conjunction with its IT environment that satisfies all the requirements in this protection profile, provides necessary security services, mechanisms, and assurances to process administrative, private, and sensitive/proprietary information. The intended environment for conformant products has a relatively low threat for the sensitivity of the data processed. Authorized users, including authorized administrators, of the TOE generally are trusted not to attempt to circumvent access controls implemented by the TOE to gain access to data for which they are not authorized.

1.3 Conventions

Except for replacing United Kingdom spelling with American spelling, the notation, formatting, and conventions used in this PP are consistent with version 2.1 of the CC. Selected presentation choices are discussed here to aid the PP reader.
The CC allows several operations to be performed on functional requirements; *refinement*, *selection*, *assignment*, and *iteration* are defined in paragraph 2.1.4 of Part 2 of the CC. Each of these operations is used in this PP.
The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**.

The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections that have been made by the PP authors are denoted by *italicized text*, selections to be filled in by the Security Target (ST) author appear in square brackets with an indication that a selection is to be made, [selection:], and are not italicized.
The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments that have been made by the PP authors are denoted by showing the value in square brackets, [Assignment_value], assignments to be filled in by the ST author appear in square brackets with an indication that an assignment is to be made [assignment:].
The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing the iteration number in parenthesis following the component identifier, (iteration_number).
As this PP was sponsored, in part by National Security Agency (NSA), National Information Assurance Partnership (NIAP) interpretations are used and are presented with the NIAP interpretation number as part of the requirement identifier (e.g., **FAU_GEN.1-NIAP-0410** for Audit data generation).
The CC paradigm also allows protection profile and security target authors to create their own requirements. Such requirements are termed 'explicit requirements' and are permitted if the CC does not offer suitable requirements to meet the authors' needs. **Explicit requirements** must be identified and are required to use the CC class/family/component model in articulating the requirements. In this PP, explicit requirements will be indicated with the "(EXP)" following the component name.
This PP also includes security requirements on the IT environment. Explicit Environmental requirements will be indicated with the "(ENV)" following the component name.
Application Notes are provided to help the developer, either to clarify the intent of a requirement, identify implementation choices, or to define "pass-fail" criteria for a requirement. For those components where Application Notes are appropriate, the Application Notes will follow the requirement component.

1.4 Glossary of Terms

See Appendix B for the Glossary.

1.5 Document Organization

Section 1 provides the introductory material for the protection profile.
Section 2 describes the Target of Evaluation in terms of its envisaged usage and connectivity.
Section 3 defines the expected TOE security environment in terms of the threats to its security, the security assumptions made about its use, and the security policies that must be followed.
Section 4 identifies the security objectives derived from these threats and policies.
Section 5 identifies and defines the security functional requirements from the CC that must be met by the TOE and the IT environment in order for the functionality-based objectives to be met. This section also identifies the security assurance requirements for EAL2 augmented.
Section 6 provides a rationale to explicitly demonstrate that the information technology security objectives satisfy the policies and threats. Arguments are provided for the coverage of each policy and threat. The section then explains how the set of requirements are complete relative to

the objectives, and that each security objective is addressed by one or more component requirement. Arguments are provided for the coverage of each objective.
Section 7 Appendices, includes the appendices that accompany the PP and provides clarity and/or explanation for the reader.
Appendix A, References, provides background material for further investigation by users of the PP.
Appendix B, Glossary, provides a listing of definitions of terms.
Appendix C, Acronyms, provides a listing of acronyms used throughout the document.
Appendix D, Robustness Environment Characterization, contains a discussion characterizing the level of robustness TOEs compliant with the PP can achieve. The PPRB created a discussion that provides a definition of factors for TOE environments as well as an explanation of how a given level of robustness is categorized.
Appendix E, Refinements, identifies the refinements that were made to CC requirements where text is deleted from a requirement.

2 TOE DESCRIPTION

2.1 Product Type

The product type of the Target of Evaluation (TOE) described in this Protection Profile (PP) is a database management system (DBMS) with the capability to limit TOE access to authorized users, enforce Discretionary Access Controls on objects under the control of the database management system based on user authorizations, and to provide user accountability via audit of users' actions.
A DBMS is a computerized repository that stores information and allows authorized users to retrieve and update that information. A DBMS may be a single-user system, in which only one user may access the DBMS at a given time, or a multi-user system, in which many users may access the DBMS simultaneously.
A DBMS supports two major types of users:

- Users who interact with the DBMS to observe and/or modify data objects for which they have authorization to access;
- Authorized administrators who implement and manage the various information-related policies of an organization (e.g., access, integrity, consistency, availability) on the databases that they manage and/or own.

A DBMS, in conjunction with the IT environment, stores, and controls access to, two types of data:

- The user data that the DBMS maintains and protects. User data may consist of the following:
  a) The user data stored in or as database objects;
  b) The definitions of user databases and database objects, commonly known as DBMS metadata;
  c) User-developed queries, functions, or procedures that the DBMS maintains for users.
- The DBMS data (e.g., configuration parameters, user security attributes, transaction log, audit instructions and records) that the DBMS maintains and uses to operate the DBMS.

Most commercial DBMSs have the following major components:

- The DBMS server application that performs the following functions:
  a) Controlling users' accesses to user data and DBMS data;

b) Interacting with, and possibly supplementing portions of, the underlying operating system to retrieve and present the data that are under the DBMS's management;

c) Indexing data values to their physical locations for quick retrievals based on a value or range of values;

d) Executing pre-written programs (i.e., utilities) to perform common tasks like database backup, recovery, loading, and copying;

e) Supporting mechanisms that enable concurrent database access (e.g., locks);

f) Assisting recovery of user data and DBMS data (e.g., transaction log); and

g) Tracking operations performed by users.

- The database client application through which DBMS users interact with the DBMS server (e.g., direct queries, stored procedures);

- A data model with which the DBMS data structures and organization can be conceptualized (e.g., hierarchical, object-oriented, relational data models) and DBMS objects defined; and

- High-level language(s) or interfaces that allow authorized users to define database constructs; access and modify user or DBMS data; present user or DBMS data; and perform operations on those data.

A DBMS specification is the proper document in which to identify the detailed requirements for the DBMS manager/server and client functions listed above (and any additional DBMS functions). This PP identifies the requirements for the security functions that the DBMS performs in addition to, or as part of, those DBMS manager/server and client functions. This PP also identifies security requirement for the IT environment in which the DBMS operates.

2.2 TOE Definition

The TOE consists of one or more instance(s) of the DBMS server application with its associated guidance documentation and the interfaces to the external IT entities with which the DBMS interacts. Also part of the TOE is the client that allows users to interface with the DBMS server. There may be one or more clients. They may be co-located with the Server (i.e., on the same physical computer) or on distributed computers. All requirements in the protection profile must be satisfied by the evaluated configuration. If the server satisfies all requirements without relying on the client, then the client may be excluded from the evaluated configuration.
The external IT entities with which the DBMS may interact—and which are outside the TOE—include the following:

- The host operating system (host OS) on which the TOE has been installed;

- The networking, printing, data-storage, and other devices and services with which the host OS may interact on behalf of the DBMS or the DBMS user; and

- The other IT products such as application servers, web servers, authentication servers, audit servers, and transaction processors with which the DBMS may interact to perform a DBMS function or a security function.

The user and DBMS data may reside on a single host or be distributed among several hosts. If the TOE is a distributed architecture, the TOE depends on the IT environment to provide adequate protection, whether through physical or cryptographic means, of transmitted user and DBMS data between the components comprising the TOE.
A particular DBMS must specify the host OS on which it must reside to provide the desired degree of security feature integration. However, the goals of confidentiality, integrity and availability for the TOE must be met by the total package: the DBMS and the external IT entities with which it interacts. In all cases the TOE must be installed and administered in accordance with the TOE installation and administration instructions.

2.3 General TOE Security Functionality

A DBMS evaluated against this PP will provide the following security services either completely or in cooperation with the IT environment.
Security services that must be provided by the TOE:

- Discretionary Access Control (DAC) which controls access to objects based on the identity of the subjects or groups to which the subjects and objects belong, and which allows authorized users to specify how the objects that they control are protected.

- Audit Capture function that creates information on all auditable events.

- Authorized administration role to allow authorized administrators to configure the policies for discretionary access control, identification and authentication, and auditing. The TOE must enforce the authorized administration role.

Security services that must be provided by the IT environment:

- Identification and Authentication (I&A) by which users are uniquely identified and authenticated before they are authorized to access information stored on the DBMS.

- Audit Storage service that stores records for all security-relevant operations that users perform on user and DBMS data.

- Audit Review service that allows the authorized administrator to review stored audit records in order to detect potential and actual security violations.

- Non-bypassibility of the security functions so as to prohibit any access to data or the TOE that is not governed by the TOE security policies.

- Domain separation to ensure that other software operating on the same computer as the TOE cannot interfere with or negate the security functions of the TOE. Domain separation also ensures that multiple instances of the TOE concurrently executing cannot interfere with one another.

However, a compliant DBMS will not be able to provide the following:

- Physical protection mechanisms and the administrative procedures for using them.

- Mechanisms to ensure the complete availability of the data residing on the DBMS. The DBMS can provide simultaneous access to data to make the data available to more than one person at a given time, and it can enforce DBMS resource allocation limits to prevent users from monopolizing a DBMS service/resource. However, it cannot detect or prevent the unavailability that may occur as a result of a physical or environmental disaster, a storage device failure, or a hacker attack on the underlying operating system. For such threats to availability, the environment must provide the required countermeasures.

- Mechanisms to ensure that users properly secure the data that they retrieve from the DBMS. The security procedures of the organization(s) that use and manage the DBMS must define users' data retrieval, storage, and disposition responsibilities.

- Mechanisms to ensure that authorized administrators wisely use DAC. Although the DBMS can support an access control policy by which users are granted access only to the data that they need to perform their jobs, it cannot completely ensure that authorized administrators who are able to set access controls will do so prudently.

2.4 TOE Operational Environment

2.4.1 Basic-Robustness Environment

The TOE described in this PP is intended to operate in environments having a basic level of robustness as defined in the Glossary in Appendix B.
Basic robustness allows processing of data at a single sensitivity level in an environment where users are cooperative and threats are minimum. Authorized users of the TOE are cleared for all information managed by the DBMS, but may not have the need-to-know authorization for all of the data. Hence, the risk that significant damage will be done due to compromise of data is low. Entities in the IT environment on which the TOE depends for security functions must be of at least the same level of robustness as the TOE. It is necessary for such an environment that the underlying operating system on which the DBMS is installed be evaluated against a basic robustness protection profile for operating systems, such as the draft protection profile, *U.S. Government Protection Profile for Single-level Operating Systems in Environments Requiring Basic Robustness*, Version 0.3, dated 29 January 2004.
The TOE in and of itself is not of sufficient robustness to store and protect information of such criticality that the integrity or secrecy is critical to the survival of the enterprise.

2.4.2 Enclave

The term, "enclave", further characterizes the environment in which the TOE is intended to operate. An enclave is under the control of a single authority and has a homogeneous security policy, including personnel and physical security, to protect it from other environments. An enclave can be specific to an organization or a mission and it may contain multiple networks. Enclaves may be logical, such as an operational area network, or be based on physical location and proximity. Any local and external elements that access resources within the enclave must satisfy the policy of the enclave.
The DBMS is expected to interact with other IT products that reside in the host OS, in the IT environment in which the host computer and host OS reside, outside that environment but inside the enclave. The IT and non-IT mechanisms used for secure exchanges of information between the DBMS and such products are expected to be administratively determined and coordinated. Similarly, the IT and non-IT mechanisms for negotiating or translating the DAC policy involved in such exchanges are expected to be resolved by the organizations involved.

2.4.3 TOE Architectures

A TOE may operate in several architectures, for example:

- A stand-alone system workstation running both the DBMS server and a DBMS client and serving one online user at a given time.
- A network of workstations or terminals running DBMS clients and communicating with a DBMS server simultaneously; these devices may be hardwired to the host computer or be connected to it by means of local or wide-area networks.
- A network of workstations communicating with one or more application servers, which in turn interact with the DBMS on behalf of the workstation users or other subjects (e.g., a DBMS server interacting with a transaction processor that manages user requests).
- A network of workstations communicating with several distributed DBMS servers simultaneously; the DBMS servers may all be within a single local area network, or they may be distributed geographically.

This PP allows each of these architectures as well as others to be supported in each configuration, the TOE is the DBMS server application, and possibly DBMS procedures that reside on an application server, as well as the DBMS clients on user workstations. The other configuration components are external IT entities. Figure 1 shows an enclave in which DBMS users access the TOE via a local area network (LAN) and also possibly using a dial-up connection. Users in other enclaves will access the LAN and the host computers and servers on it by way of one or more boundary protection mechanisms (e.g., a firewall) and then through a communications server or router to the LAN. Depending on the particular enclave configuration and the DBMS access policy that it supports, all users (both inside and outside the enclave) may then access an application server, which either connects the TOE user to the enclave computer on which the TOE operates or manages the complete user/DBMS session.

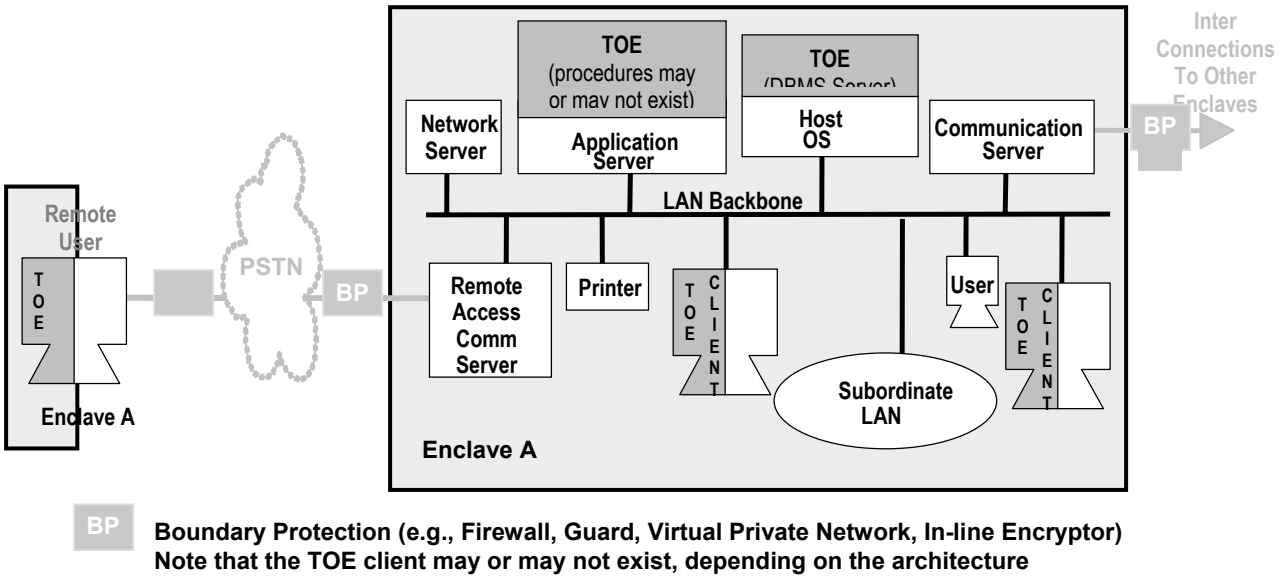


Figure 1 Depiction of TOE Configuration

2.4.4 TOE Administration

Authorized administrators of the TOE will have capabilities that are commensurate with their assigned administrative roles. There may be one or more administrative roles. The TOE developers will establish some roles for their products. If the security target allows it, the administrators of the system may establish other roles. This PP defines one necessary administrator role (authorized administrator) and allows the DBMS developer or ST writer to define more. When the DBMS is established, the ability to segment roles and assign capabilities with significant freedom regarding the number of roles and their responsibilities must also exist. Of course the very ability to establish and assign roles will be a privileged function.

3 SECURITY ENVIRONMENT

The security environment for the functions addressed by this specification includes threats, security policies, and usage assumptions, as discussed below.
Basic robustness TOEs falls in the upper left area of the robustness figures shown in Appendix D. A Basic Robustness TOE is considered sufficient for low threat environments or where compromise of protected information will not have a significant impact on mission objectives. This implies that the motivation of the threat agents will be low in environments that are suitable for TOEs of this robustness. In general, basic robustness results in "good commercial practices" that counter threats based in casual and accidental disclosure or compromise of data protected by the TOE.
Threat agent motivation can be considered in a variety of ways. One possibility is that the value of the data process or protected by the TOE will generally be seen as of little value to the adversary (i.e., compromise will have little or no impact on mission objectives). Another possibility, (where higher value data is processed or protected by the TOE) is that procuring organizations will provide other controls or safeguards (i.e., controls that the TOE itself does not enforce) in the fielded system in order to increase the threat agent motivation level for compromise beyond a level of what is considered reasonable or expected to be applied.

3.1 Threats

3.1.1 Threat Agent Characterization

In addition to helping define the robustness appropriate for a given environment, the threat agent is a key component of the formal threat statements in the PP. Threat agents are typically characterized by a number of factors such as *expertise*, *available resources*, and *motivation*. Because each robustness level is associated with a variety of environments, there are corresponding varieties of specific threat agents (that is, the threat agents will have different combinations of motivation, expertise, and available resources) that are valid for a given level of robustness. The following discussion explores the impact of each of the threat agent factors on the ability of the TOE to protect itself (that is, the robustness required of the TOE).
The *motivation* of the threat agent seems to be the primary factor of the three characteristics of threat agents outlined above. Given the same expertise and set of resources, an attacker with low motivation may not be as likely to attempt to compromise the TOE. For example, an entity with no authorization to low value data none-the-less has low motivation to compromise the data; thus a basic robustness TOE should offer sufficient protection. Likewise, the fully authorized user with access to highly valued data similarly has low motivation to attempt to compromise the data, thus again a basic robustness TOE should be sufficient.
Unlike the motivation factor, however, the same can't be said for *expertise*. A threat agent with low motivation and low expertise is just as unlikely to attempt to compromise a TOE as an attacker with low motivation and high expertise; this is because the attacker with high expertise does not have the motivation to compromise the TOE even though they may have the expertise to do so. The same argument can be made for *resources* as well.

Therefore, when assessing the robustness needed for a TOE, the motivation of threat agents should be considered a "high water mark". That is, the robustness of the TOE should increase as the motivation of the threat agents increases.

Having said that, the relationship between expertise and resources is somewhat more complicated. In general, if resources include factors other than just raw processing power (money, for example), then expertise should be considered to be at the same "level" (low, medium, high, for example) as the resources because money can be used to purchase expertise. Expertise in some ways is different, because expertise in and of itself does not automatically procure resources. However, it may be plausible that someone with high expertise can procure the requisite amount of resources by virtue of that expertise (for example, hacking into a bank to obtain money in order to obtain other resources).

It may not make sense to distinguish between these two factors; in general, it appears that the only effect these may have is to lower the robustness requirements. For instance, suppose an organization determines that, because of the value of the resources processed by the TOE and the trustworthiness of the entities that can access the TOE, the motivation of those entities would be "medium". This normally indicates that a medium robustness TOE would be required because the likelihood that those entities would attempt to compromise the TOE to get at those resources is in the "medium" range. However, now suppose the organization determines that the entities (threat agents) that are the least trustworthy have no resources and are unsophisticated. In this case, even though those threat agents have medium motivation, the likelihood that they would be able to mount a successful attack on the TOE would be low, and so a basic robustness TOE may be sufficient to counter that threat.

It should be clear from this discussion that there is no "cookbook" or mathematical answer to the question of how to specify exactly the level of motivation, the amount of resources, and the degree of expertise for a threat agent so that the robustness level of TOEs facing those threat agents can be rigorously determined. However, an organization can look at combinations of these factors and obtain a good understanding of the likelihood of a successful attack being attempted against the TOE. Each organization wishing to procure a TOE must look at the threat factors applicable to their environment; discuss the issues raised in the previous paragraph; consult with appropriate accreditation authorities for input; and document their decision regarding likely threat agents in their environment.

The important general points we can make are:

- The motivation for the threat agent defines the upper bound with respect to the level of robustness required for the TOE.

- A threat agent's expertise and/or resources that is "lower" than the threat agent's motivation (e.g., a threat agent with high motivation but little expertise and few resources) may lessen the robustness requirements for the TOE (see next point, however).

- The availability of attacks associated with high expertise and/or high availability of resources (for example, via the Internet or "hacker chat rooms") introduce problem when trying to define the expertise of, or resources available to, a threat agent.

The following threats were drawn from the *Consistency Instruction Manual for Development of US Government Protection Profiles for Use in Basic Robustness Environments*, Version 2.0

(CIM) and are addressed by the TOE and should be read in conjunction with the threat rationale, Section 6.1. There are other threats that the TOE does not address (e.g., malicious developer inserting a backdoor into the TOE) and it is up to a site to determine how these types of threats apply to its environment.

Table 1 Basic Robustness Applicable Threats

Threat	Definition
T. ACCIDENTAL_ADMIN_ERROR	An administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.
T.MASQUERADE	A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources
T.POOR_DESIGN	Unintentional errors in requirements specification or design of the TOE may occur, leading to flaws that may be exploited by a casually mischievous user or program.
T.POOR_IMPLEMENTATION	Unintentional errors in implementation of the TOE design may occur, leading to flaws that may be exploited by a casually mischievous user or program.
T.POOR_TEST	Lack of or insufficient tests to demonstrate that all TOE security functions operate correctly (including in a fielded TOE) may result in incorrect TOE behavior being discovered thereby causing potential security vulnerabilities.
T.RESIDUAL_DATA	A user or process may gain unauthorized access to data through reallocation of TOE resources from one user or process to another.
T.TSF_COMPROMISE	A malicious user or process may cause configuration data to be inappropriately accessed (viewed, modified or deleted).
T.UNAUTHORIZED_ACCESS	A user may gain unauthorized access to user data for which they are not authorized according to the TOE security policy.

Threat	Definition
T.UNIDENTIFIED_ACTIONS	Failure of the authorized administrator to identify and act upon unauthorized actions may occur.

The following table includes threats recommended by the CIM that do not apply to a DBMS in a basic robustness environment. This table of threats not applicable to the TOE are included per Instruction 9 Step 9.

Table 2 Basic Robustness Threats Not Applicable to the TOE

Threat Name	Threat Definition	Rationale for NOT Including this Threat
T.ACCIDENTAL_AUDIT_ COMPROMISE	A user or process may view audit records, cause audit records to be lost or modified, or prevent future audit records from being recorded, thus masking a user's action.	This threat is not applicable to the TOE because the IT environment will provide proper storage, viewing, and management mechanisms. This threat was replaced by an assumption on the IT environment that it will handle secure storage of the audit logs, A.AUDIT_STORAGE.
T.ACCIDENTAL_ CRYPTO_ COMPROMISE	A user or process may cause key, data or executable code associated with the cryptographic functionality to be inappropriately accessed (viewed, modified, or deleted), thus compromising the cryptographic mechanisms and the data protected by those mechanisms.	This threat is not applicable to the TOE due to the absence of cryptographic requirements for the TOE.

T.UNATTENDED_SESSION	A user may gain unauthorized access to an unattended session.	This threat is not applicable to the TOE because the IT environment will provide the session locking capabilities. Requirements are levied on the IT environment to address this threat which map to A.I_AND_A.

3.2 Organizational Security Policies

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs

Table 3 Basic Robustness Applicable Policies

Policy	Definition
P.ACCESS_BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.
P.ACCOUNTABILITY	The authorized users of the TOE shall be held accountable for their actions within the TOE.
P.ROLES	The TOE shall provide an authorized administrator role for secure administration of the TOE. This role shall be separate and distinct from other authorized users.

3.3 Assumptions

This section contains assumptions regarding the IT environment which the TOE will reside.

Table 4 Basic Robustness Applicable Assumptions

Assumption	Definition

Assumption	Definition
A.AUDIT_REVIEW	The IT environment will provide the proper mechanisms to handle review of the TOE audit logs.
A.AUDIT_STORAGE	The IT environment will provide a means for secure storage of the TOE audit logs and management of that data.
A.DOMAIN_SEPARATION	The IT environment will provide a separate domain for the TOE's operation.
A.I_AND_A	It is assumed that the IT environment will provide identification and authentication mechanisms for the TOE.
A.NO_BYPASS	The IT environment will ensure the TSF cannot be bypassed in order to gain access to TOE data.
A.NO_EVIL	Administrators are non-hostile, appropriately trained, and follow all administrator guidance.
A.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on DBMS servers, other than those services necessary for the operation, administration and support of the DBMS.
A.PHYSICAL	It is assumed that appropriate physical security is provided within the domain for the value of the IT assets protected by the TOE and the value of the stored, processed, and transmitted information.
A.ROBUST_ENVIRONMENT	It is assumed that the IT environment is at least as robust as the TOE.
A.SECURE_COMMS	It is assumed that the IT environment will provide a secure line of communications between the remote user and the TOE.

Assumption	Definition
A.TIME_STAMPS	It is assumed that the IT environment will provide the TOE with the necessary reliable timestamps.

4 SECURITY OBJECTIVES

This section identifies the security objectives of the TOE and its supporting environment. The security objectives identify the responsibilities of the TOE and its environment in meeting the security needs.

4.1 TOE Security Objectives

Table 5 Basic Robustness Security Objectives

Objective Name	Objective Definition
O.ACCESS_HISTORY	The TOE will display information (to authorized users) related to previous attempts to establish a session.
O.ADMIN_GUIDANCE	The TOE will provide administrators with the necessary information for secure management.
O.ADMIN_ROLE	The TOE will provide authorized administrator roles to isolate administrative actions.
O.AUDIT_GENERATION	The TOE will provide the capability to detect and create records of security relevant events associated with users.
O.CONFIGURATION_IDENTIFICATION	The configuration of the TOE is fully identified in a manner that will allow implementation errors to be identified, corrected with the TOE being redistributed promptly.
O.CORRECT_TSF_OPERATION	The TOE will provide the capability to test the TSF to ensure the correct operation of the TSF at a customer's site.
O.DISPLAY_BANNER	The TOE will display an advisory warning regarding use of the TOE.
O.DOCUMENTED_DESIGN	The design of the TOE is adequately and accurately documented.

Objective Name	Objective Definition
O.MANAGE	The TOE will provide all the functions and facilities necessary to support the authorized administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
O.MEDIATE	The TOE must protect user data in accordance with its security policy.
O.INTERNAL_TOE_DOMAINS	The TSF will maintain internal domains for separation of data and queries belonging to concurrent users.
O.PARTIAL_FUNCTIONAL_TEST	The TOE will undergo some security functional testing that demonstrates the TSF satisfies some of its security functional requirements.
O.PARTIAL_SELF_PROTECTION	The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure through its own interfaces.
O.RESIDUAL_INFORMATION	The TOE will ensure that any information contained in a protected resource within its Scope of Control is not released when the resource is reallocated.
O.TOE_ACCESS	The TOE will provide mechanisms that control a user's logical access to the TOE.
O.VULNERABILITY_ANALYSIS	The TOE will undergo some vulnerability analysis to demonstrate the design and implementation of the TOE does not contain any obvious flaws.

4.2 Environment Security Objectives

Table 6 Basic Robustness Environmental Security Objectives

Environmental Objective Name	Environmental Objective Definition
OE.AUDIT_REVIEW	The IT environment will contain mechanisms to allow the authorized administrator to view and sort the audit logs.
OE.AUDIT_STORAGE	The IT environment will contain mechanisms to provide secure storage and management of the audit log.
OE.DOMAIN_SEPARATION	The IT environment will provide an isolated domain for the execution of the TOE.
OE.I_AND_A	The IT environment will contain identification and authentication mechanisms for users to login to the TOE.
OE.NO_BYPASS	The IT environment shall ensure the TOE security mechanisms cannot be bypassed in order to gain access to the TOE resources.
OE.NO_EVIL	Sites using the TOE shall ensure that authorized administrators are non-hostile, appropriately trained and follow all administrator guidance.
OE.CONFIG	The TOE will be installed, configured, managed and maintained in accordance with its guidance documentation and applicable security policies and procedures.
OE. NO_GENERAL_ PURPOSE	There will be no general-purpose computing capabilities (e.g., compilers or user applications) available on DMBS servers, other than those services necessary for the operation, administration and support of the DBMS.

Environmental Objective Name	Environmental Objective Definition
OE.PHYSICAL	Physical security will be provided within the domain for the value of the IT assets protected by the TOE and the value of the stored, processed, and transmitted information.
OE.ROBUST_ENVIORNMENT	The IT environment that supports the TOE for enforcement of its security objectives will be of at least the same level of robustness as the TOE.
OE.SECURE_COMMS	The IT environment will provide a secure line of communications between the remote user and the TOE.
OE.TIME_STAMPS	The IT environment will provide reliable time stamps.
OE.TRUST_IT	Each IT entity the TOE relies on for security functions will be installed, configured, managed and maintained in a manner appropriate to the IT entity, and consistent with the security policy of the TOE and the relationship between them.

5 IT SECURITY REQUIREMENTS

5.1 TOE Security Functional Requirements

This section defines the functional requirements for the TOE. Functional requirements in this PP were drawn directly from Part 2 of the CC, or were based on Part 2 of the CC, including the use of NIAP and International Interpretations and explicit components. These requirements are relevant to supporting the secure operation of the TOE.

Table 7 Security Functional Requirements

Functional Components	
FAU_GEN.1-NIAP-0410	Audit data generation
FAU_GEN.2-NIAP-0410	User identity association
FAU_SEL.1-NIAP-0407	Selective audit
FDP_ACC.1	Subset access control
FDP_ACF.1-NIAP-0407	Security attribute based access control
FDP_RIP.2	Full residual information protection
FIA_ATD.1	User attribute definition
FMT_MOF.1	Management of security functions behavior
FMT_MSA.1(1)	Management of security attributes
FMT_MSA.3(1)	Static attribute initialization
FMT_MTD.1(1)	Management of TSF data
FMT_REV.1(1)	Revocation (user attributes)
FMT_REV.1(2)	Revocation (subject, object attributes)
FMT_SMF.1(1)	Specification of management functions
FMT_SMR.1	Security roles
FPT_ITD_(EXP).1	Internal TOE domains

Functional Components	
FPT_SEP_(EXP).1	TSF domain separation
FPT_TRC_(EXP).1	Internal TSF consistency
FPT_TST_(EXP).1	TSF Testing
FTA_MCS.1	Basic limitation on multiple concurrent sessions
FTA_TAB.1	Default TOE access banners
FTA_TAH.1	TOE access history
FTA_TSE.1	TOE session establishment

5.1.1 Security Audit (FAU)

5.1.1.1 Audit data generation (FAU_GEN.1-NIAP-0410)

FAU_GEN.1.1-NIAP-0410 **Refinement**: The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the *minimal* level of audit **listed in Table 8**;

c) **[Start-up and shutdown of the DBMS;**

d) **Use of special permissions (e.g., those often used by authorized** administrators **to circumvent access control policies); and**

e) [selection: [assignment: events at a minimal level of audit introduced by the inclusion of additional SFRs determined by the ST author], [assignment: events commensurate with a minimal level of audit introduced by the inclusion of explicit requirements determined by the ST author], "no additional events"]].

1 *Application Note: For the selection, the ST author should choose one or both of the assignments (as detailed in the following paragraphs), or select "no additional events".*

2 *Application Note: For the first assignment, the ST author augments the table (or lists explicitly) the audit events associated with the minimal level of audit for any SFRs that the ST author includes that are not included in this PP.*

3 *Application Note: Likewise, for the second assignment the ST author includes audit events that may arise due to the inclusion of any explicit requirements not already in the*

PP. Because "minimal" audit is not defined for such requirements, the ST author will need to determine a set of events that are commensurate with the type of information that is captured at the minimal level for similar requirements.

4 *Application Note: If no additional (CC or explicit) SFRs are included, or if additional SFRs are included that do not have "minimal" audit associated with them, then it is acceptable to assign "no additional events" in this item.*

FAU_GEN.1.2-NIAP-0410 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [information specified in column three of Table 8 below].

5 *Application Note: In column 3 of the table below, "Audit Record Contents" is used to designate data that should be included in the audit record if it "makes sense" in the context of the event that generates the record. If no other information is required (other than that listed in item a) above) for a particular auditable event type, then an assignment of "none" is acceptable.*

Table 8 Auditable Events

Security Functional Requirement	Auditable Event(s)	Additional Audit Record Contents
FAU_GEN.1-NIAP-0410	None	
FAU_GEN.2-NIAP-0410	None	
FAU_SEL.1-NIAP-0407	All modifications to the audit configuration that occur while the audit collection functions are operating.	The identity of the authorized administrator that made the change to the audit configuration.
FDP_ACC.1	None	

Security Functional Requirement	Auditable Event(s)	Additional Audit Record Contents
FDP_ACF.1-NIAP-0407	Successful requests to perform an operation on an object covered by the SFP.	The identity of the subject performing the operation.
FDP_RIP.2	None	
FIA_ATD.1	None	
FMT_MOF.1	None	
FMT_MSA.1(1)	None	
FMT_MSA.3(1)	None	
FMT_MTD.1(1)	None	
FMT_REV.1(1)	Unsuccessful revocation of security attributes.	Identity of individual attempting to revoke security attributes.
FMT_REV.1(2)	Unsuccessful revocation of security attributes.	Identity of individual attempting to revoke security attributes.
FMT_SMF.1(1)	Use of the management functions.	Identity of the administrator performing these functions.
FMT_SMR.1	Modifications to the group of users that are part of a role.	Identity of authorized administrator modifying the role definition
FPT_ITD_(EXP).1	None	
FPT_SEP_(EXP).1	None	
FPT_TRC_(EXP).1	Restoring consistency upon reconnection	
FPT_TST_(EXP).1	Execution of this set of TSF self tests.	The identity of the administrator performing the test, if initiated by an administrator.
FTA_MCS.1	Rejection of a new session based on the limitation of multiple concurrent sessions.	

Security Functional Requirement	Auditable Event(s)	Additional Audit Record Contents
FTA_TAB.1	None	
FTA_TAH.1	None	
FTA_TSE.1	Denial of a session establishment due to the session establishment mechanism.	Identity of the individual attempting to establish a session

5.1.1.2 User identity association (FAU_GEN.2-NIAP-0410)

FAU_GEN.2.1-NIAP-0410 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

5.1.1.3 Selective audit (FAU_SEL.1-NIAP-0407)

FAU_SEL.1.1-NIAP-0407 **Refinement**: The TSF shall **allow only the administrator** to include or exclude auditable events from the set of audited events based on the following attributes:

a) *user identity*,

b) *event type*,

c) *object identity*,

d) [selection: “subject identity”, “host identity”, “none”];

e) [success of auditable security events;

f) failure of auditable security events; and

g) [selection: [assignment: list of additional criteria that audit selectivity is based upon], “no additional criteria”].]

6 *Application Note: “event type” is to be defined by the ST author; the intent is to be able to include or exclude classes of audit events.*

5.1.2 User data protection (FDP)

5.1.2.1 Subset access control (FDP_ACC.1)

FDP_ACC.1.1 The TSF shall enforce the [Discretionary Access Control policy] on [all subjects, all DBMS-controlled objects and all operations among them].

5.1.2.2 Security attribute based access control (FDP_ACF.1-NIAP-0407)

7 *Interp Note: The following element was modified per CCIMB Interpretation 103.*

FDP_ACF.1.1-NIAP-0407 The TSF shall enforce the [Discretionary Access Control policy] to objects based on the following:

- [the authorized user identity associated with a subject, and
- access operations implemented for DBMS-controlled objects].

8 *Application Note: DBMS-controlled objects may be implementation-specific objects that are presented to authorized users at the user interface to the DBMS. They may include, but are not limited to tables, records, files, indexes, views, constraints, stored queries, and metadata. Data structures that are not presented to authorized users at the DBMS user interface, but are used internally are internal TSF data structures. Internal TSF data structures are not controlled according to the rules specified in FDP_ACF.1-NIAP-0407.*

FDP_ACF.1.2-NIAP-0407 **Refinement**: The TSF shall enforce the following rules to determine if an operation among controlled subjects and **DBMS-**controlled objects is allowed:

- **The Discretionary Access Control policy mechanism shall, either by explicit authorized user action or by default, provide that database management system controlled objects are protected from unauthorized access according to the following ordered rules**:

a) [If the requested mode of access is denied to that authorized user, deny access.

b) If the requested mode of access is permitted to that authorized user, permit access.

c) Else deny access].

FDP_ACF.1.3-NIAP-0407 **Refinement**: The TSF shall explicitly authorize access of subjects to **DBMS-controlled** objects based on the following additional rules: [*Authorized administrators must follow the above-stated Discretionary Access Control policy, except after taking the following specific actions:*] **[selection: [assignment: list of specific actions], "no additional actions"]**.

9 *Application Note: This element allows specifications of additional rules for authorized administrators to bypass the Discretionary Access Control policy for system management or maintenance (e.g., system backup).*

FDP_ACF.1.4-NIAP-0407 The TSF shall explicitly deny access of subjects to objects based on the following rules: [selection: [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects], "no additional explicit denial rules"].

5.1.2.3 Full residual information protection (FDP_RIP.2)

FDP_RIP.2.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the *allocation of the resource to* all objects.

5.1.3 Identification and authentication (FIA)

5.1.3.1 User attribute definition (FIA_ATD.1)

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

- [Database user identifier;
- Group memberships;
- Security-relevant database roles; and
- [assignment: list of security attributes]].

5.1.4 Security management (FMT)

5.1.4.1 Management of security functions behavior (FMT_MOF.1)

FMT_MOF.1.1 The TSF shall restrict the ability to *disable and enable* the functions [relating to the specification of events to be audited] to [authorized administrators].

5.1.4.2 Management of security attributes (FMT_MSA.1(1))

FMT_MSA.1.1(1) **Refinement**: The TSF shall enforce the [Discretionary Access Control policy] to restrict the ability to [*manage*] **all** the security attributes **of database users** to [authorized administrators].

10 *Application Note: The ST author should ensure that all attributes identified in FDP_ACF.1-NIAP-0407 are adequately managed and protected.*

5.1.4.3 Static attribute initialization (FMT_MSA.3(1))

11 *Interp Note: The following element is changed as a result of Interpretations 201 and 202.*

FMT_MSA.3.1(1) The TSF shall enforce the [Discretionary Access Control policy] to provide *restrictive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(1) The TSF shall allow the [authorized administrator] to specify alternative initial values to override the default values when an object or information is created.

5.1.4.4 Management of TSF data (FMT_MTD.1(1))

FMT_MTD.1.1(1) The TSF shall restrict the ability to [*include or exclude*] the [auditable events] to [authorized administrators].

5.1.4.5 Revocation (FMT_REV.1(1))

FMT_REV.1.1(1) The TSF shall restrict the ability to revoke security attributes associated with the *users* within the TSC to [the authorized administrator].

FMT_REV.1.2(1) The TSF shall enforce the rules [assignment: specification of revocation rules].

5.1.4.6 Revocation (FMT_REV.1(2))

FMT_REV.1.1(2) The TSF shall restrict the ability to revoke security attributes associated with the *subjects and objects* within the TSC to [the authorized administrator and database users as allowed by the Discretionary Access Control policy].

FMT_REV.1.2(2) The TSF shall enforce the rules [assignment: specification of revocation rules].

5.1.4.7 Specification of Management Functions (FMT_SMF.1(1))

FMT_SMF.1.1(1) The TSF shall be capable of performing the following security management functions: [assignment: list of security management functions to be provided by the TSF].

5.1.4.8 Security roles (FMT_SMR.1)

FMT_SMR.1.1 **Refinement**: The TSF shall maintain the roles:

- [authorized administrator]; **and**
- **[assignment: additional authorized identified roles]**.

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

12 *Application Note: This requirement identifies a minimum set of management roles. A ST or operational environment may contain a finer-grain decomposition of roles that correspond to the roles identified here (e.g., database non-administrative user or database operator). The ST writer may change the names of the roles identified above but the "new" roles must still perform the functions that the FMT requirements in this PP have defined.*

5.1.5 Protection of the TOE Security Functions (FPT)

5.1.5.1 SFP domain separation (FPT_ITD_(EXP).1)

FPT_ITD_(EXP).1.1 The TSF shall enforce separation between the security domains of subjects in the TSC.

5.1.5.2 TSF domain separation (FPT_SEP_(EXP).1)

FPT_SEP_(EXP).1.1 The TSF shall maintain a security domain that protects it from interference and tampering by untrusted subjects initiating actions through its own TSFI.

FPT_SEP_(EXP).2 The TSF shall enforce separation between the security domains of subjects in the TOE Scope of Control.

5.1.5.3 Internal TSF consistency (FPT_TRC_(EXP).1)

FPT_TRC_EXP.1.1 The TSF shall ensure that TSF data is consistent between parts of the TOE by providing a mechanism to bring inconsistent TSF data into a consistent state in a timely manner.

13 *Application Note: In general, it is impossible to achieve complete, constant consistency of TSF data that is distributed to remote portions of a TOE because distributed portions of the TSF may be active at different times or disconnected from one another. This requirement attempts to address this situation in a practical manner by acknowledging that there will be TSF data inconsistencies but that they will be corrected without undue delay. For example, a TSF could provide timely consistency through periodic broadcast of TSF data to all TSF nodes maintaining replicated TSF data. Another example approach is for the TSF to provide a mechanism to explicitly probe remote TSF nodes for inconsistencies and respond with action to correct the identified inconsistencies.*

5.1.5.4 TSF Testing (FPT_TST_(EXP).1)

FPT_TST_(EXP).1.1 The TSF shall provide administrator with the capability to verify the integrity of the following TSF data: [assignment: TSF data for which integrity validation is required].

FPT_TST_(EXP).1.2 The TSF shall provide administrator with the capability to verify the integrity of stored TSF executable code.

5.1.6 Toe Access (FTA)

5.1.6.1 Basic limitation on multiple concurrent sessions (FTA_MCS.1)

FTA_MCS.1.1 The TSF shall restrict the maximum number of concurrent sessions that belong to the same user.

FTA_MCS.1.2 The TSF shall enforce, by default, a limit of [assignment: default number] sessions per user.

5.1.6.2 Default TOE access banners (FTA_TAB.1)

FTA_TAB.1.1 Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorized use of the TOE.

14 *Application Note: A user session is an interactive persistent connection to the TOE, where a user is present to see the advisory warning message.*

5.1.6.3 TOE access history (FTA_TAH.1)

FTA_TAH.1.1 Upon successful session establishment, the TSF shall display the *date, time, method, and location* of the last successful session establishment to the user.

15 *Application Note: "Location" refers to what ever means the TOE uses to identify a point of entry for interactive user session establishment. The adequacy of this means is determined by other requirements (e.g., FPT_SEP, AVA_VLA).*

FTA_TAH.1.2 Upon successful session establishment, the TSF shall display the *date, time, method, and location* of the last unsuccessful attempt to session establishment and the number of unsuccessful attempts since the last successful session establishment.

FTA_TAH.1.3 The TSF shall not erase the access history information from the user interface without giving the user an opportunity to review the information.

5.1.6.4 TOE session establishment (FTA_TSE.1)

FTA_TSE.1.1 **Refinement**: The TSF shall be able to deny session establishment based on [attributes that can be set explicitly by authorized administrator(s), including user identity, port of entry, time of day, day of the week], **and [assignment: list of additional attributes]**.

5.2 Security Requirements for the IT Environment

This section contains the security functional requirements for the IT environment. With the TOE being a software-only TOE, the IT environment must provide protection of the TOE from tampering and interference. These requirements can also be satisfied by the TOE since the TOE is part of the IT environment. These requirements were drawn from the CC including NIAP and International Interpretations and explicit requirements.

Table 9 IT Environment Security Functional Requirements

IT Environment Security Functional Requirements	
FAU_SAR.1	Audit Review
FAU_SAR.2	Restricted Audit Review
FAU_SAR.3	Selectable Audit Review
FAU_STG.1-NIAP-0429	Protected audit trail storage
FAU_STG.NIAP-0414-1-NIAP-0429	Site-configurable prevention of audit data loss
FDP_IFC.1	Subset information flow control
FDP_IFF.1	Simple security attributes
FDP_ITT.1	Basic internal transfer protection
FIA_AFL.1	Authentication failure handling
FIA_UAU.1	Timing of authentication
FIA_UID.1	Timing of identification
FIA_USB.1	User-subject binding
FMT_MSA.1(2)	Management of security attributes
FMT_MSA.3(2)	Static attribute initialization
FMT_MTD.1(2)	Management of TSF data (Audit Records)
FMT_MTD.1(3)	Management of TSF data (User Authentication Data)
FMT_SMF.1(2)	Specification of management functions

IT Environment Security Functional Requirements	
FPT_RVM.1	Non-bypassability of the TSP
FPT_SEP_(ENV).1	TSF domain separation
FPT_STM.1	Reliable time stamps
FTA_SSL.1	TSF initiated session locking
FTA_SSL.2	User-initiated locking

5.2.1 Security audit (FAU)

5.2.1.1 Audit review (FAU_SAR.1)

FAU_SAR.1.1 **Refinement**: The **IT environment** shall provide [the authorized administrator] with the capability to read [all database audit information] from the audit records.

FAU_SAR.1.2 **Refinement**: The **IT environment** shall provide the audit records in a manner suitable for the **authorized administrator** to interpret the information.

5.2.1.2 Restricted Audit Review (FAU_SAR.2)

FAU_SAR.2.1 **Refinement**: The **IT environment** shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

5.2.1.3 Selectable Audit Review (FAU_SAR.3)

FAU_SAR.3.1 **Refinement**: The **IT environment** shall provide the ability to perform *searches and sorting* of audit data based on

- [User identity;
- Date of event;
- Time of event;
- Type of event;
- Event status (success/failure)]; **and**
- **[assignment: additional criteria with logical relations]**.

5.2.1.4 Protected audit trail storage (FAU_STG.1-NIAP-0429)

FAU_STG.1.1-NIAP-0429 **Refinement**: The **IT environment** shall **restrict the deletion of** stored audit records **in the audit trail to the authorized administrator**.

16 *Interp Note: The following element has been changed per CCIMB Interpretations 141 and 202.*

FAU_STG.1.2-NIAP-0429 **Refinement**: The **IT environment** shall be able to *prevent* unauthorized modifications to the audit records in the audit trail.

5.2.1.5 Site-configurable Prevention of audit data loss (FAU_STG.NIAP-0414-1-NIAP-0429)

17 *Interp Note: The following element has been changed per CCIMB Interpretations 202.*

FAU_STG.NIAP-0414-1.1-NIAP-0429 **Refinement**: The **IT Environment** shall **provide an authorized administrator with the capability to select one or more of the following actions** [selection: "ignore auditable events", "prevent auditable events, except those taken by the authorized user with special rights", "overwrite the oldest stored audit records"] and [assignment: other actions to be taken in case of audit storage failure] if the audit trail is full.

FAU_STG.NIAP-0414-1.2-NIAP-0429 **Refinement**: The **IT environment** shall [selection: choose one of: 'ignore auditable events', 'prevent auditable events, except those taken by the authorized user with special rights', 'overwrite the oldest stored audit records', [assignment: other actions to be taken in case of audit storage failure]] if the audit trail is full.

18 *Application Note: The TOE provides the administrator the option of preventing audit data loss by preventing auditable events from being logged. The administrator's actions under these circumstances are not required to be audited. The TOE also provides the administrator the option of overwriting "old" audit records rather than preventing auditable events, which may protect a denial-of-service attack.*

19 *Application Note: The ST writer should fill in other technology-specific actions that can be taken for audit storage failure (in addition to the two already specified), or select "no additional options" if there are no such technology-specific actions.*

5.2.2 User data protection (FDP)

5.2.2.1 Subset information flow control (FDP_IFC.1)

FDP_IFC.1.1 **Refinement**: The **IT environment** shall enforce the [Transfer Protection Policy] on [assignment: list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP].

5.2.2.2 Simple Security Attributes (FDP_IFF.1)

20 *Interp Note: The following element is changed as a result of Interpretation 104.*

FDP_IFF.1.1 **Refinement**: The **IT environment** shall enforce the [Transfer Protection Policy] based on the following types of subject and information security attributes: [assignment: list of subjects and information controlled under the indicated policy, and, for each, the security attributes].

FDP_IFF.1.2 **Refinement**: The **IT environment** shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: for each operation, the security attribute-based relationship that must hold between subject and information security attributes].

FDP_IFF.1.3 **Refinement**: The **IT environment** shall enforce the [assignment: additional information flow control policy rules].

FDP_IFF.1.4 **Refinement**: The **IT environment** shall provide the following [assignment: list of additional policy capabilities].

FDP_IFF.1.5 **Refinement**: The **IT environment** shall explicitly authorize an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly authorize information flows].

FDP_IFF.1.6 **Refinement**: The **IT environment** shall explicitly deny an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly deny information flows].

5.2.2.3 Basic internal transfer protection (FDP_ITT.1)

FDP_ITT.1.1 **Refinement**: The **IT environment** shall enforce the [Transfer Protection Policy] to prevent the [selection: disclosure, modification, loss of use] of user data when it is transmitted between physically-separated parts of the TOE.

5.2.3 Identification and authentication (FIA)

5.2.3.1 Authentication failure handling (FIA_AFL.1)

21 *Interp Note: The following element has been changed per CCIMB Interpretations 111.*

FIA_AFL.1.1 **Refinement**: The **IT environment** shall detect when *"an administrator configurable positive integer within [assignment: range of acceptable values]"* **of** unsuccessful authentication attempts occur related to [a user's authentication] **within [assignment: authorized administrator configurable amount of time].**

FIA_AFL.1.2 **Refinement**: When the defined number of unsuccessful authentication attempts has been met or surpassed, the **IT environment** shall [lock the device for an authorized administrator configurable amount of time].

22 *Application Note: At least one account should be exempted from the FIA_AFL.1.2 requirement in order to prevent denial of access.*

23 *Application Note: Note the use of "authorized administrator" in this requirement. Since this requirement may be met by the TOE or by a component in the IT environment, it is not possible to specify that the authorized individual be an authorized administrator.*

5.2.3.2 Timing of authentication (FIA_UAU.1)

FIA_UAU.1.1 **Refinement**: The **IT environment** shall allow [assignment: list of TSF mediated actions] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 **Refinement**: The **IT environment** shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

5.2.3.3 Timing of identification (FIA_UID.1)

FIA_UID.1.1 **Refinement**: The **IT environment** shall allow [assignment: list of TSF-mediated action] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 **Refinement**: The **IT environment** shall require each user to be **uniquely and** successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.2.3.4 User-subject binding (FIA_USB.1)

24 *Interp Note: This requirement was modified as a result of CCIMIB Interpretation 137.*

FIA_USB.1.1 **Refinement**: The **IT environment** shall associate the following user security attributes with subjects acting on the behalf of that user: [all attributes listed in FIA_ATD.1].

FIA_USB.1.2 **Refinement**: The **IT environment** shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [none].

FIA_USB.1.3 **Refinement**: The **IT environment** shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [only the authorized administrator can change security attributes].

5.2.4 Security management (FMT)

5.2.4.1 Management of security attributes (FMT_MSA.1(2))

FMT_MSA.1.1(2) **Refinement**: The **IT environment** shall enforce the [Transfer Protection Policy] to restrict the ability to [selection: change_default, query, modify, delete, [assignment: other operations]] the security attributes [assignment: list of security attributes] to [assignment: the authorized identified roles].

5.2.4.2 Static attribute initialization (FMT_MSA.3(2))

25 *Interp Note: The following element is changed as a result of Interpretations 201 and 202.*

FMT_MSA.3.1(2) **Refinement**: The **IT environment** shall enforce the [Transfer Protection Policy] to provide [selection: choose one of: restrictive, permissive, [assignment: other property]] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(2) **Refinement**: The **IT environment** shall allow the [assignment: the authorized identified roles] to specify alternative initial values to override the default values when an object or information is created.

5.2.4.3 Management of TSF data (audit records) (FMT_MTD.1(2))

FMT_MTD.1.1(2) **Refinement**: The **IT environment** shall restrict the ability to *query and clear* the [audit records] to [the authorized administrator].

5.2.4.4 Management of TSF data (user authentication data) (FMT_MTD.1(3))

FMT_MTD.1.1(3) **Refinement**: The **IT environment** shall restrict the ability to [*set and reset*] the [user authentication data] to [the authorized administrator].

5.2.4.5 Specification of Management Functions (FMT_SMF.1(2))

FMT_SMF.1.1(2) **Refinement**: The **IT environment** shall be capable of performing the following security management functions:

- [query and clearing audit records;
- set and resetting user authentication data; and
- [assignment: list of additional security management functions to be provided by the IT environment]].

5.2.5 Protection of the TSF (FPT)

5.2.5.1 Non-bypassability of the TSP (FPT_RVM.1)

FPT_RVM.1.1 **Refinement**: The **IT environment** shall ensure that **IT environment security policy** enforcement functions are invoked and succeed before each function within the **IT environment's scope of control** is allowed to proceed.

5.2.5.2 TSF domain separation (FPT_SEP_(ENV).1)

FPT_SEP_(ENV).1 The TSF Environment shall provide hardware that provides virtual memory management and at least two execution rings for executing software.

5.2.5.3 Reliable time stamps (FPT_STM.1)

FPT_STM.1.1 **Refinement**: The **IT environment** shall be able to provide reliable time stamps for its own use **and for the TOE**.

26 *Application note: The TOE referenced in this requirement is the TOE of the DBMS.*

5.2.6 Toe Access (FTA)

5.2.6.1 TSF initiated session locking (FTA_SSL.1)

FTA_SSL.1.1 **Refinement**: The **IT environment** shall lock an interactive session after **an authorized administrator specified time interval of user inactivity** by:

a) clearing or overwriting display devices, making the current contents unreadable;

b) disabling any activity of the user's data access/display devices other than unlocking the session.

FTA_SSL.1.2 **Refinement**: The **IT environment** shall require the following events to occur prior to unlocking the session: [user re-authentication].

5.2.6.2 User-initiated locking (FTA_SSL.2)

FTA_SSL.2.1 **Refinement**: The **IT environment** shall allow user-initiated locking of the user's own interactive session, by:

a) clearing or over-writing display devices, making the current contents unreadable;

b) disabling any activity of the user's data access/display devices other then unlocking the session.

FTA_SSL.2.2 **Refinement**: The **IT environment** shall require the following events to occur prior to unlocking the session: [user re-authentication].

5.3 TOE Security Assurance Requirements

The agreed upon Security Assurance Requirements drawn from the Common Criteria for Information Technology Security Evaluation, Part 3, dated Aug.99, Version 2.1 of CCIB-99-031 which collectively define "Basic Robustness" include the following:
All of the assurance requirements included in Evaluated Assurance Level (EAL) 2 augmented with the following additions:

- ALC_FLR.2: Flaw remediation
- AVA_MSU.1: Examination of guidance

The following is a list of the assurance requirements needed for Basic Robustness.

Table 10 Assurance Requirements

Assurance Class	Assurance Components	
Configuration Management	ACM_CAP.2	Configurations items
Delivery and Operation	ADO_DEL.1	Delivery procedures
	ADO_IGS.1	Installation, generation, and start-up procedures
Development	ADV_FSP.1	Informal functional specification
	ADV_HLD.1	Descriptive high-level design
	ADV_RCR.1	Informal correspondence demonstration
Guidance Documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Life Cycle Support	ALC_FLR.2	Flaw reporting procedures
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Vulnerability Assessment	AVA_MSU.1	Examination of guidance

Assurance Class	Assurance Components	
	AVA_SOF.1	Strength of TOE security functional evaluation
	AVA_VLA.1	Developer vulnerability analysis

5.3.1 Configuration Management (ACM)

5.3.1.1 Configuration items (ACM_CAP.2)

Developer action elements:

ACM_CAP.2.1D The developer shall provide a reference for the TOE.

ACM_CAP.2.2D The developer shall use a CM system.

ACM_CAP.2.3D The developer shall provide CM documentation.

Content and presentation of evidence elements:

ACM_CAP.2.1C The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.2.2C The TOE shall be labeled with its reference.

ACM_CAP.2.3C The CM documentation shall include a configuration list.

27 *Interp Note: The following element was added per CCIMB Interpretation 003.*

ACM_CAP.2.4C The configuration list shall uniquely identify all configuration items that comprise the TOE.

ACM_CAP.2.5C The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.2.6C The CM documentation shall describe the method used to uniquely identify the configuration items.

ACM_CAP.2.7C The CM system shall uniquely identify all configuration items.

Evaluator action elements:

ACM_CAP.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.2 Delivery and Operation (ADO)

5.3.2.1 Delivery procedures (ADO_DEL.1)

Developer action elements:

ADO_DEL.1.1D The developer shall document procedures for delivery of the TOE or parts of it to the user.

ADO_DEL.1.2D The developer shall use the delivery procedures.

Content and presentation of evidence elements:

ADO_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

Evaluator action elements:

ADO_DEL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.2.2 Installation, generation, and start-up procedures (ADO_IGS.1)

Developer action elements:

ADO_IGS.1.1D The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

Content and presentation of evidence elements:

28 *Interp Note: The following element was modified per CCIMB Interpretation 051.*

ADO_IGS.1.1C The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation and start-up of the TOE.

Evaluator action elements:

ADO_IGS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1.2E The evaluator shall determine that the installation, generation, and start-up procedures result in a security configuration.

5.3.3 Development (ADV)

5.3.3.1 Informal functional specification (ADV_FSP.1)

Developer action elements:

ADV_FSP.1.1D The developer shall provide a functional specification.

Content and presentation of evidence elements:

ADV_FSP.1.1C The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.1.2C The functional specification shall be internally consistent.

ADV_FSP.1.3C The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.

ADV_FSP.1.4C The functional specification shall completely represent the TSF.

Evaluator action elements:

ADV_FSP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements..

5.3.3.2 Descriptive high-level design (ADV_HLD.1)

Developer action elements:

ADV_HLD.1.1D The developer shall provide the high-level design of the TSF.

Content and presentation of evidence elements:

ADV_HLD.1.1C The presentation of the high-level design shall be informal..

ADV_HLD.1.2C The high-level design shall be internally consistent.

ADV_HLD.1.3C The high level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.1.4C The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.1.5C The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software..

ADV_HLD.1.6C The high-level design shall identify all interfaces to the subsystem of the TSF..

ADV_HLD.1.7C The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

Evaluator action elements:

ADV_HLD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_HLD.1.2E The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

5.3.3.3 Informal correspondence demonstration (ADV_RCR.1)

Developer action elements:

ADV_RCR.1.1D The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

Content and presentation of evidence elements:

ADV_RCR.1.1C For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

Evaluator action elements:

ADV_RCR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.4 Guidance Documents (AGD)

5.3.4.1 Administrator guidance (AGD_ADM.1)

Developer action elements:

AGD_ADM.1.1D The developer shall provide administrator guidance addressed to system administrative personnel.

Content and presentation of evidence elements:

AGD_ADM.1.1C The administrator guidance shall describe the administrative functions and interfaces available to the administer of the TOE.

AGD_ADM.1.2C The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3C The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4C The administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE.

AGD_ADM.1.5C The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6C The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7C The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8C The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

Evaluator action elements:

AGD_ADM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.4.2 User Guidance (AGD_USR.1)

Developer action elements:

AGD_USR.1.1D The developer shall provide user guidance.

Content and presentation of evidence elements:

AGD_USR.1.1C The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

AGD_USR.1.2C The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3C The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4C The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behavior found in the statement of TOE security environment.

AGD_USR.1.5C The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6C The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

Evaluator action elements:

AGD_USR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.5 Life Cycle Support (ALC)

5.3.5.1 Flaw reporting procedures (ALC_FLR.2)

29 *Interp Note: The following components were modified per CCIMB Interpretation 062 and 094.*

Developer action elements:

ALC_FLR.2.1D The developer shall provide flaw remediation procedures addressed to TOE developers.

ALC_FLR.2.2D The developer shall establish a procedure for accepting and acting upon all reports of security flaws and requests for corrections to those flaws.

ALC_FLR.2.3D The developer shall provide flaw remediation guidance addressed to TOE users.

Content and presentation of evidence elements:

ALC_FLR.2.1C The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

ALC_FLR.2.2C The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

ALC_FLR.2.3C The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

ALC_FLR.2.4C The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

ALC_FLR.2.5C The flaw remediation procedures shall describe a means by which the developer receives from TOE users reports and enquiries of suspected security flaws in the TOE.

ALC_FLR.2.6C The procedures for processing reported security flaws shall ensure that any reported flaws are corrected and the correction issued to TOE users.

ALC_FLR.2.7C The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.

ALC_FLR.2.8C The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE.

Evaluator action elements:

ALC_FLR.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.6 Tests (ATE)

5.3.6.1 Evidence of coverage (ATE_COV.1)

Developer action elements:

ATE_COV.1.1D The developer shall provide evidence of the test coverage.

Content and presentation of evidence elements:

ATE_COV.1.1C The evidence of the test coverage shall show the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

Evaluator action elements:

ATE_COV.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.6.2 Functional testing (ATE_FUN.1)

Developer action elements:

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation of evidence elements:

ATE_FUN.1.1C The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

ATE_FUN.1.3C The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.4C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.5C The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

Evaluator action elements:

ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.6.3 Independent testing – sample (ATE_IND.2)

Developer action elements:

ATE_IND.2.1D The developer shall provide the TOE for testing.

Content and presentation of evidence elements:

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

Evaluator action elements:

ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2E The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

ATE_IND.2.3E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

5.3.7 Vulnerability Assessment (AVA)

5.3.7.1 Validation of analysis (AVA_MSU.2)

Developer action elements:

AVA_MSU.2.1D The developer shall provide guidance documentation.

AVA_MSU.2.2D The developer shall document an analysis of the guidance documentation.

Content and presentation of evidence elements:

AVA_MSU.2.1C The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AVA_MSU.2.2C The guidance documentation shall be complete, clear, consistent and reasonable.

AVA_MSU.2.3C The guidance documentation shall list all assumptions about the intended environment.

AVA_MSU.2.4C The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).

AVA_MSU.2.5C The analysis documentation shall demonstrate that the guidance documentation is complete.

Evaluator action elements:

AVA_MSU.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_MSU.2.2E The evaluator shall repeat all configuration and installation procedures, and other procedures selectively, to confirm that the TOE can be configured and used securely using only the supplied guidance documentation.

AVA_MSU.2.3E The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.

AVA_MSU.2.4E The evaluator shall confirm that the analysis documentation shows that guidance is provided for secure operation in all modes of operation of the TOE.

5.3.7.2 Strength of TOE security function evaluation (AVA_SOF.1)

Developer action elements:

AVA_SOF.1.1D The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

Content and presentation of evidence elements:

AVA_SOF.1.1C For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level of SOF-basic.

AVA_SOF.1.2C For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric of SOF-basic.

Evaluator action elements:

AVA_SOF.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

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

5.3.7.3 Developer vulnerability analysis (AVA_VLA.1)

Developer action elements:

30 *Interp Note: The following element was modified per CCIMB Interpretation 051.*

AVA_VLA.1.1D The developer shall perform a vulnerability analysis.

31 *Interp Note: The following element was modified per CCIMB Interpretation 051.*

AVA_VLA.1.2D The developer shall provide vulnerability analysis documentation.

Content and presentation of evidence elements:

32 *Interp Note: The following element was modified per CCIMB Interpretation 051.*

AVA_VLA.1.1C The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for obvious ways in which a user can violate the TSP.

33 *Interp Note: The following element was modified per CCIMB Interpretation 051.*

AVA_VLA.1.2C The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities.

34 *Interp Note: The following element was modified per CCIMB Interpretation 051.*

AVA_VLA.1.3C The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

Evaluator action elements:

AVA_VLA.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VLA.1.2E The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure the identified vulnerabilities have been addressed.

6 RATIONALE

This section provides the rationale for the selection of the IT security requirements, objectives, assumptions, and threats. In particular, it shows that the IT security requirements are suitable to meet the security objectives, which in turn are shown to be suitable to cover all aspects of the TOE security environment.

6.1 Rationale for TOE Security Objectives

Table 11 Rationale for TOE Security Objectives

Threat/Policy	Objectives Addressing the Threat/Policy	Rationale
T. ACCIDENTAL_ADMIN_ERROR An administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.	O.ADMIN_GUIDANCE The TOE will provide administrators with the necessary information for secure management.	O.ADMIN_GUIDANCE helps to mitigate this threat by ensuring the TOE administrators have guidance that instructs them how to administer the TOE in a secure manner. Having this guidance helps to reduce the mistakes that an administrator might make that could cause the TOE to be configured in a way that is insecure.
T.MASQUERADE A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources.	O.TOE_ACCESS The TOE will provide mechanisms that control a user's logical access to the TOE.	O.TOE_ACCESS mitigates this threat by controlling the logical access to the TOE and its resources. By constraining how and when authorized users can access the TOE, and by mandating the type and strength of the authentication mechanism this objective helps mitigate the possibility of a user attempting to login and masquerade as an authorized user. In addition, this objective provides the administrator the means to control the number of failed login attempts a user can generate before an account is

Threat/Policy	Objectives Addressing the Threat/Policy	Rationale
		locked out, further reducing the possibility of a user gaining unauthorized access to the TOE.
T.POOR_DESIGN Unintentional errors in requirements specification or design of the TOE may occur, leading to flaws that may be exploited by a casually mischievous user or program.	O.CONFIGURATION_IDENTIFICATION The configuration of the TOE is fully identified in a manner that will allow implementation errors to be identified, corrected with the TOE being redistributed promptly.	O.CONFIGURATION_IDENTIFICATION plays a role in countering this threat by requiring the developer to provide control of the changes made to the TOE's design.
	O.DOCUMENTED_DESIGN The design of the TOE is adequately and accurately documented.	O.DOCUMENTED_DESIGN ensures that the design of the TOE is documented, permitting detailed review by evaluators and validators.
	O.VULNERABILITY_ANALYSIS The TOE will undergo some vulnerability analysis to demonstrate the design and implementation of the TOE does not contain any obvious flaws.	O.VULNERABILITY_ANALYSIS ensures that the design of the TOE is analyzed for design flaws.
T.POOR_IMPLEMENTATION Unintentional errors in implementation of the TOE design may occur, leading to flaws that may be exploited by a casually mischievous user or program.	O.CONFIGURATION_IDENTIFICATION The configuration of the TOE is fully identified in a manner that will allow implementation errors to be identified, corrected with the TOE being redistributed promptly.	O.CONFIGURATION_IDENTIFICATION plays a role in countering this treat by requiring the developer to provide control of the changes made to the TOE's design. Although the previous three objectives help minimize the introduction of errors into the implementation.

Threat/Policy	Objectives Addressing the Threat/Policy	Rationale
	O.PARTIAL_FUNCTIONAL_TEST The TOE will undergo some security functional testing that demonstrates the TSF satisfies some of its security functional requirements.	O.PARTIAL_FUNCTIONAL_TEST increases the likelihood that any errors that do exist in the implementation (with respect to the functional specification, high-level, and low-level design) will be discovered through testing.
	O.VULNERABILITY_ANALYSIS The TOE will undergo some vulnerability analysis to demonstrate the design and implementation of the TOE does not contain any obvious flaws.	O.VULNERABILITY_ANALYSIS helps reduce errors in the implementation that may not be discovered during functional testing. Ambiguous design documentation and the fact that exhaustive testing of the external interfaces is not required may leave bugs in the implementation undiscovered in functional testing.
T.POOR_TEST Lack of or insufficient tests to demonstrate that all TOE security functions operate correctly (including in a fielded TOE) may result in incorrect TOE behavior being discovered thereby causing potential security vulnerabilities.	O.DOCUMENTED_DESIGN The design of the TOE is adequately and accurately documented.	O.DOCUMENTED_DESIGN helps to ensure that the TOE's documented design satisfies the security functional requirements. In order to ensure the TOE's design is correctly realized in its implementation, the appropriate level of functional testing of the TOE's security mechanisms must be performed during the evaluation of the TOE.

Threat/Policy	Objectives Addressing the Threat/Policy	Rationale
	O.CORRECT_TSF_OPERATION The TOE will provide the capability to test the TSF to ensure the correct operation of the TSF at a customer's site.	O.CORRECT_TSF_OPERATION ensures that once the TOE is installed at a customer's location, the capability exists that the integrity of the TSF (hardware and software) can be demonstrated, and thus providing end users the confidence that the TOE's security policies continue to be enforced.
	O.PARTIAL_FUNCTIONAL_TEST The TOE will undergo some security functional testing that demonstrates the TSF satisfies some of its security functional requirements.	O.PARTIAL_FUNCTIONAL_TEST increases the likelihood that any errors that do exist in the implementation (with respect to the functional specification, high level, and low-level design) will be discovered through testing.

Threat/Policy	Objectives Addressing the Threat/Policy	Rationale
	O.VULNERABILITY_ANALYSIS The TOE will undergo some vulnerability analysis to demonstrate the design and implementation of the TOE does not contain any obvious flaws.	O.VULNERABILITY_ANALYSIS addresses this concern by requiring a vulnerability analysis be performed in conjunction with testing that goes beyond functional testing. This objective provides a measure of confidence that the TOE does not contain security flaws that may not be identified through functional testing. While these testing activities are a necessary activity for successful completion of an evaluation, this testing activity does not address the concern that the TOE continues to operate correctly and enforce its security policies once it has been fielded. Some level of testing must be available to end users to ensure the TOE's security mechanisms continue to operator correctly once the TOE is fielded.
T.RESIDUAL_DATA A user or process may gain unauthorized access to data through reallocation of TOE resources from one user or process to another.	O.RESIDUAL_INFORMATION The TOE will ensure that any information contained in a protected resource within its Scope of Control is not released when the resource is reallocated.	O.RESIDUAL_INFORMATION counters this threat by ensuring that TSF data and user data is not persistent when resources are released by one user/process and allocated to another user/process.

Threat/Policy	Objectives Addressing the Threat/Policy	Rationale
T.TSF_COMPROMISE A user or process may cause, through an unsophisticated attack, TSF data, or executable code to be inappropriately accessed (viewed, modified, or deleted).	O.RESIDUAL_INFORMATION The TOE will ensure that any information contained in a protected resource within its Scope of Control is not released when the resource is reallocated.	O.RESIDUAL_INFORMATION is necessary to mitigate this threat, because even if the security mechanisms do not allow a user to explicitly view TSF data, if TSF data were to inappropriately reside in a resource that was made available to a user, that user would be able to inappropriately view the TSF data.
	O.PARTIAL_SELF_PROTECTION The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure through its own interfaces.	O.PARTIAL_SELF_PROTECTION ensures the TOE is capable of protecting itself from attack.
	O.MANAGE The TOE will provide all the functions and facilities necessary to support the authorized administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.	O.MANAGE is necessary because an access control policy is specified to control access to TSF data. This objective is used to dictate who is able to view and modify TSF data, as well as the behavior of TSF functions.
	O.INTERNAL_TOE_DOMAINS The TSF will maintain internal domains for separation of data and queries belonging to concurrent users.	O.INTERNAL_TOE_DOMAINS ensures the TOE will establish separate domains for data belonging to users.

Threat/Policy	Objectives Addressing the Threat/Policy	Rationale
T.UNAUTHORIZED_ACCESS A user may gain unauthorized access to user data for which they are not authorized according to the TOE security policy.	O.MEDIATE The TOE must protect user data in accordance with its security policy.	O.MEDIATE ensures that all accesses to user data are subject to mediation, unless said data has been specifically identifies as public data. The TOE requires successful authentication to the TOE prior to gaining access to any controlled-access content. By implementing strong authentication to gain access to these services, an attacker's opportunity to successfully conduct a man-in-the-middle and/or password guessing attack is greatly reduced. Lastly, the TSF will ensure that all configured enforcement functions (authentication, access control rules, etc.) must be invoked prior to allowing a user to gain access to TOE or TOE mediated services. The TOE restricts the ability to modify the security attributes associated with access control rules, access to authenticated and unauthenticated services, etc to the administrator. This feature ensures that no other user can modify the information flow policy to bypass the intended TOE security policy.

Threat/Policy	Objectives Addressing the Threat/Policy	Rationale
	O.ACCESS_HISTORY The TOE will display information (to authorized users) related to previous attempts to establish a session.	O.ACCESS_HISTORY is important to mitigate this threat because it ensures the TOE will advise the user of the last successful login attempt and performed actions without their knowledge.
T.UNIDENTIFIED_ACTIONS Failure of the authorized administrator to identify and act upon unauthorized actions may occur.	O.ADMIN_GUIDANCE The TOE will provide administrators with the necessary information for secure management.	The threat of an authorized administrator failing to know about malicious audit events produces the objectives of the authorized administrator having the facilities and knowing how to use them (O.ADMIN_GUIDANCE).
	O.MANAGE The TOE will provide all the functions and facilities necessary to support the authorized administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.	The threat of an authorized administrator failing to know about malicious audit events produces the objectives of the authorized administrator having the capability to use the mechanisms (O.MANAGE) to review audit records.
P.ACCESS_BANNER The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.	O.DISPLAY_BANNER The TOE will display an advisory warning regarding use of the TOE.	O.DISPLAY_BANNER satisfies this policy by ensuring that the TOE displays an authorized administrator configurable banner that provides all interactive users with a warning about the unauthorized use of the TOE.

Threat/Policy	Objectives Addressing the Threat/Policy	Rationale
P.ACCOUNTABILITY The authorized users of the TOE shall be held accountable for their actions within the TOE.	O.AUDIT_GENERATION The TOE will provide the capability to detect and create records of security relevant events associated with users.	O.AUDIT_GENERATION addresses this policy by providing the authorized administrator with the capability of configuring the audit mechanism to record the actions of a specific user, or review the audit trail based on the identity of the user. Additionally, the administrator's ID is recorded when any security relevant change is made to the TOE (e.g., access rule modification, start-stop of the audit mechanism, establishment of a trusted channel, etc.).
	OE.TIME_STAMPS The IT environment will provide reliable time stamps.	OE.TIME_STAMPS plays a role in supporting this policy by requiring the TOE to provide a reliable time stamp. The audit mechanism is required to include the current date and time in each audit record. All audit records that include the user ID, will also include the date and time that the event occurred.
	O.TOE_ACCESS The TOE will provide mechanisms that control a user's logical access to the TOE.	O.TOE_ACCESS supports this policy by requiring the TOE to identify and authenticate all authorized users prior to allowing any TOE access or any TOE mediated access on behalf of those users.

Threat/Policy	Objectives Addressing the Threat/Policy	Rationale
P.ROLES The TOE shall provide an authorized administrator role for secure administration of the TOE. This role shall be separate and distinct from other authorized users.	O.ADMIN_ROLE The TOE will provide authorized administrator roles to isolate administrative actions.	The TOE has the objective of providing an authorized administrator role for secure administration. The TOE may provide other roles as well, but only the role of authorized administrator is required (O.ADMIN_ROLE).

6.2 Rationale for the Security Objectives and Security Functional Requirements for the Environment

Table 12 Rational for IT Environmental Objectives

Assumption	Environmental Objective Addressing the Assumption	Rationale
A.AUDIT_REVIEW The IT environment will provide the proper mechanisms to handle review of the TOE audit logs.	OE.AUDIT_REVIEW The IT environment will contain mechanisms to allow the authorized administrator to view and sort the audit logs.	OE.AUDIT_REVIEW provide the TOE will mechanisms to review the audit logs. These requirements will ensure the data is in a suitable manner for the administrator to interpret as well as giving the administrator a way to search and sort within the log to find appropriate data.
A.AUDIT_STORAGE The IT environment will provide a means for secure storage of the TOE audit logs and management of that data.	OE.AUDIT_STORAGE The IT environment will contain mechanisms to provide secure storage and management of the audit log.	OE.AUDIT_STORAGE ensures the IT environment will provide a secure mechanism for storing and managing the TOE audit log.

Assumption	Environmental Objective Addressing the Assumption	Rationale
A.DOMAIN_SEPARATION The IT environment will provide a separate domain for the TOE's operation.	OE.DOMAIN_SEPARATION The IT environment will provide an isolated domain for the execution of the TOE.	OE.DOMAIN_SEPARATION ensures the IT environment will provide an isolated domain for the TOE's execution.
A.I_AND_A It is assumed that the IT environment will provide identification and authentication mechanisms for the TOE.	OE.I_AND_A The IT environment will contain identification and authentication mechanisms for users to login to the TOE.	OE.I_AND_A ensures the IT environment will provide mechanisms for users of the TOE to be authenticated before any actions within the TOE may be taken. This includes management of user password data as well as being able to unlock a session that was locked by the environment or the user.
A.NO_BYPASS The IT environment will ensure the TSF cannot be bypassed in order to gain access to TOE data.	OE.NO_BYPASS The IT environment shall ensure the TOE security mechanisms cannot be bypassed in order to gain access to the TOE resources.	OE.NO_BYPASS ensures the TOE cannot be bypassed in order to gain unauthorized access of TOE resources.
A.NO_EVIL Administrators are non-hostile, appropriately trained, and follow all administrator guidance.	OE.NO_EVIL Sites using the TOE shall ensure that authorized administrators are non-hostile, appropriately trained and follow all administrator guidance.	All authorized administrators are trustworthy individuals, having background investigations commensurate with the level of data being protected, have undergone appropriate admin training, and follow all admin guidance.

Assumption	Environmental Objective Addressing the Assumption	Rationale
	OE.CONFIG The TOE will be installed, configured, managed and maintained in accordance with its guidance documentation and applicable security policies and procedures	Authorized administrators are trusted to properly configure the TOE so it enforces its security policies.
A.NO_GENERAL_PURPOSE There are no general-purpose computing or storage repository capabilities (e.g., compilers or user applications) available on DBMS servers, other than those services necessary for the operation, administration and support of the DBMS.	OE.NO_GENERAL_PURPOSE There will be no general-purpose computing capabilities (e.g., compilers or user applications) available on DMBS servers, other than those services necessary for the operation, administration and support of the DBMS.	The DBMS server must not include any general-purpose commuting or storage capabilities. This will protect the TSF data from malicious processes.
A.PHYSICAL Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the IT environment.	OE.PHYSICAL Physical security will be provided within the domain for the value of the IT assets protected by the TOE and the value of the stored, processed, and transmitted information.	The TOE, the TSF data, and protected user data is assumed to be protected from physical attack (e.g., theft, modification, destruction, or eavesdropping). Physical attack could include unauthorized intruders into the TOE environment, but it does not include physical destructive actions that might be taken by an individual that is authorized to access the TOE environment.

Assumption	Environmental Objective Addressing the Assumption	Rationale
A.ROBUST_ENVIORNMENT It is assumed that the IT environment is at least as robust as the TOE.	OE.ROBUST_ENVIORNMENT The IT environment that supports the TOE for enforcement of its security objectives will be of at least the same level of robustness as the TOE.	The TOE shall only be installed in an IT environment that is at least as robust as the TOE. The TOE is basic robustness, therefore, all elements in the environment the TOE depends on for enforcement of its security objectives are also assumed to be basic robustness. These elements could include the operating system, encryption devices, and/or boundary protection devices.
	OE.TRUST_IT Each IT entity the TOE relies on for security functions will be installed, configured, managed and maintained in a manner appropriate to the IT entity, and consistent with the security policy of the TOE and the relationship between them.	The IT entities in the environment are correctly installed, configured, managed and maintained.
A.SECURE_COMMS It is assumed that the IT environment will have a secure line of communications between the remote user and the TOE.	OE.SECURE_COMMS The IT environment will provide a secure line of communications between the remote user and the TOE.	The environment must provide a secure line of communication for transfer of TSF data. This is necessary because the TOE may be distributed geographically with users and authorized administrators in different locations. It may also be the case that the TOE is a distributed architecture, with database servers in different

Assumption	Environmental Objective Addressing the Assumption	Rationale
		geographic locations. The objective OE.SECURE_COMMS does not necessarily mandate that the communications between the remote administrator and the TOE be encrypted. Remote administration implies administration from any location other than the TOE console. In many implementations, remote administration will be done from another workstation on the same LAN as the TOE, but within a protected enclave. In this case, there is no need for cryptographic protection of the communications between the authorized administrator and the TOE.
A.TIME_STAMPS It is assumed that the IT environment will provide the TOE with the necessary reliable timestamps.	OE.TIME_STAMPS The IT environment will provide reliable time stamps.	OE.TIME_STAMPS states that the environment will maintain reliable timestamps and those will be used by the TOE to stamp each audit record with a date and time.

6.3 Rationale for TOE Security Requirements

Table 13 Rationale for TOE Security Requirements

Objective	Requirements Addressing the Objective	Rationale
O.ACCESS_HISTORY The TOE will display information (to authorized users) related to previous attempts to establish a session.	FTA_TAH.1	Users are notified about previous unauthorized login attempts and how many times it was attempted every time they log into their account. They are also notified about the last successful authorized login. This information will include the date, time, method, and location of the attempts. This will allow the user to detect if another user is attempting to access their account. These records cannot be deleted until after the user has been notified of their access history. (FTA_TAH.1)
O.ADMIN_GUIDANCE The TOE will provide administrators with the necessary information for secure management.	ADO_DEL.1	ADO_DEL.1 ensures that the administrator is provided documentation that instructs them how to ensure the delivery of the TOE, in whole or in parts, has not been tampered with or corrupted during delivery. This requirement ensures the administrator has the ability to begin their TOE installation with a clean (e.g., malicious code has not been inserted once it has left the developer's control) version of the TOE, which is necessary for secure management of the TOE.

Objective	Requirements Addressing the Objective	Rationale
	ADO_IGS.1	ADO_IGS.1 ensures the administrator has the information necessary to install the TOE in the evaluated configuration. Often times a vendor's product contains software that is not part of the TOE and has not been evaluated. The Installation, Generation, and Startup (IGS) documentation ensures that once the administrator has followed the installation and configuration guidance the result is a TOE in a secure configuration.
	AGD_ADM.1	AGD_ADM.1 mandates the developer provide the administrator with guidance on how to operate the TOE in a secure manner. This includes describing the interfaces the administrator uses in managing the TOE, security parameters that are configurable by the administrator, how to configure the TOE's rule set and the implications of any dependencies of individual rules. The documentation also provides a description of how to setup and review the auditing features of the TOE.
	AGD_USR.1	AGD_USR.1 is intended for non-administrative users, but could be used to provide guidance on security that is common to both administrators and non-administrators (e.g., password management guidelines).

Objective	Requirements Addressing the Objective	Rationale
	AVA_MSU.1	AVA_MSU.1 ensures that the guidance documentation is complete and consistent, and notes all requirements for external security measures.
O.ADMIN_ROLE The TOE will provide authorized administrator roles to isolate administrative actions.	FMT_SMR.1	The TOE will establish, at least, a authorized administrator role. The ST writer may choose to specify more roles. The authorized administrator will be given privileges to perform certain tasks that other users will not be able to perform. These privileges include, but are not limited to, access to audit information and security functions. (FMT_SMR.1)
O.AUDIT_GENERATION The TOE will provide the capability to detect and create records of security relevant events associated with users.	FAU_GEN.1-NIAP-0410	FAU_GEN.1-NIAP-0410 defines the set of events that the TOE must be capable of recording. This requirement ensures that the administrator has the ability to audit any security relevant events that takes place in the TOE. This requirement also defines the information that must be contained in the audit record for each auditable event. This requirement also places a requirement on the level of detail that is recorded on any additional security functional requirements an ST author adds to this PP.
	FAU_GEN.2-NIAP-0410	FAU_GEN.2-NIAP-0410 ensures that the audit records associate a user identity with the auditable event. In the case of authorized users, the association is accomplished with the userid.

Objective	Requirements Addressing the Objective	Rationale
	FAU_SEL.1-NIAP-0407	FAU_SEL.1-NIAP-0407 allows the administrator to configure which auditable events will be recorded in the audit trail. This provides the administrator with the flexibility in recording only those events that are deemed necessary by site policy, thus reducing the amount of resources consumed by the audit mechanism.
O.CONFIGURATION_IDENTIFICATION The configuration of the TOE is fully identified in a manner that will allow implementation errors to be identified, corrected with the TOE being redistributed promptly.	ACM_CAP.2	ACM_CAP.2 addresses this objective by requiring that there be a unique reference for the TOE, and that the TOE is labeled with that reference. It also requires that there be a CM system in place, and that the configuration items that comprise the TOE are uniquely identified. This provides a clear identification of the composition of the TOE.
	ALC_FLR.2	ALC_FLR.2 addresses this objective by requiring that there be a mechanism in place for identifying flaws subsequent to fielding, and for distributing those flaws to entities operating the system.
O.CORRECT_TSF_OPERATION The TOE will provide the capability to test the TSF to ensure the correct operation of the TSF at a customer's site.	FPT_TST_(EXP).1	FPT_TST_(EXP).1 is necessary to ensure the correctness of the TSF configuration files and TSF data. This requirement includes the critical nature and specific handling of the cryptographic related TSF data.

Objective	Requirements Addressing the Objective	Rationale
O.DISPLAY_BANNER The TOE will display an advisory warning regarding use of the TOE.	FTA_TAB.1	FTA_TAB.1 meets this objective by requiring the TOE display an administrator defined banner before a user can establish an authenticated session. This banner is under complete control of the administrator in which they specify any warnings regarding unauthorized use of the TOE and remove any product or version information if they desire.
O.DOCUMENTED_DESIGN The design of the TOE is adequately and accurately documented.	ADV_FSP.1	ADV_FSP.1 requires that the interfaces to the TOE be documented and specified.
	ADV_HLD.1	ADV_HLD.1 requires the high level design of the TOE be documented and specified and that said design be shown to correspond to the interfaces.
	ADV_RCR.1	ADV_RCR.1 requires that there be a correspondence between adjacent layers of the design decomposition.
O.MANAGE The TOE will provide all the functions and facilities necessary to support the authorized administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.	FMT_MOF.1	FMT_MOF.1 requires that the ability to use particular TOE capabilities be restricted to the administrator.
	FMT_MSA.1(1)	FMT_MSA.1(1) requires that the ability to perform operations on security attributes be restricted to particular roles.
	FMT_MSA.3(1)	FMT_MSA.3(1) requires that default values used for security attributes are restrictive, and that the administrator has the ability to override those values.

Objective	Requirements Addressing the Objective	Rationale
	FMT_MTD.1(1)	FMT_MTD.1(1) requires that the ability to manipulate TOE content is restricted to administrators.
	FMT_REV.1(1) FMT_REV.1(2)	FMT_REV.1 restricts the ability to revoke attributes to the administrator.
	FMT_SMF.1(1)	FMT_SMF.1(1) identifies the management functions that are available to the authorized administrator.
	FMT_SMR.1	FMT_SMR.1 defines the specific security roles to be supported.
O.MEDIATE The TOE must protect user data in accordance with its security policy.	FDP_ACC.1	The FDP requirements were chosen to define the policies, the subjects, objects, and operations for how and when mediation takes place in the TOE. FDP_ACC.1 defines the Access Control policy that will be enforced on a list of subjects acting on the behalf of users attempting to gain access to a list of named objects. All the operation between subject and object covered are defined by the TOE's policy.
	FDP_ACF.1-NIAP-0407	FDP_ACF.1-NIAP-0407 defines the security attribute used to provide access control to objects based on the TOE's access control policy.

Objective	Requirements Addressing the Objective	Rationale
	FPT_TRC_(EXP).1	Replicated TSF data that specifies attributes for access control must be consistent across distributed components of the TOE. The requirement is to maintain consistency of replicated TSF data.
O.INTERNAL_TOE_DOMAINS The TSF will maintain internal domains for separation of data and queries belonging to concurrent users.	FPT_SEP_(EXP).1	FPT_SEP_(EXP).1 requires the TOE to maintain a separate domain for its own execution separate from other processes.
	FPT_ITD_(EXP).1	FPT_ITD_(EXP).1 requires the domains be internal for separation of data belonging to concurrent users.
O.PARTIAL_FUNCTIONAL_TEST The TOE will undergo some security functional testing that demonstrates the TSF satisfies some of its security functional requirements.	ATE_COV.1	ATE_COV.1 requires that there be a correspondence between the tests in the test documentation and the TSF as described in the functional specification.
	ATE_FUN.1	ATE_FUN.1 requires that the developer provide test documentation for the TOE, including test plans, test procedure descriptions, expected test results, and actual test results. These need to identify the functions tested, the tests performed, and test scenarios. There require that the developer run those tests, and show that the expected results were achieved.
	ATE_IND.2	ATE_IND.2 requires that the evaluators test a subset of the TSF to confirm correct operation, on an equivalent set of resources to those used by the developer for testing. These sets should include a subset of the developer run tests.

Objective	Requirements Addressing the Objective	Rationale
O.PARTIAL_SELF_PROTECTION The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure through its own interfaces.	FPT_SEP_(EXP).1	The explicitly specific component FPT_SEP_(EXP).1 was chosen to ensure the TSF provides a domain that protects itself from untrusted users. If the TSF cannot protect itself it cannot be relied upon to enforce its security policies. The explicitly specified version was used to distinguish the aspects of FPT_SEP provided by the TOE vs. the aspects provided by the IT environment.
O.RESIDUAL_INFORMATION The TOE will ensure that any information contained in a protected resource within its Scope of Control is not released when the resource is reallocated.	FDP_RIP.2	FDP_RIP.2 is used to ensure the contents of resources are not available to subjects other than those explicitly granted access to the data.
O.TOE_ACCESS The TOE will provide mechanisms that control a user's logical access to the TOE.	FIA_ATD.1	FIA_ATD.1 defines the attributes of users, including a userid that is used by the TOE to determine a user's identity and enforce what type of access the user has to the TOE.
	FTA_MCS.1	FTA_MCS.1 ensures that users may only have a maximum of a specified number of active sessions open at any given time.
	FTA_TSE.1	FTA_TSE.1 allows the TOE to restrict access to the TOE based on certain criteria.

Objective	Requirements Addressing the Objective	Rationale
	AVA_SOF.1	AVA_SOF.1 requirement is applied to the password mechanism used by the local administrator (The single use authentication mechanism supplies by the IT environment (i.e., authentication server) has this same assurance requirement levied against it to ensure a consistent level of assurance.) For this TOE, the strength of function specified is basic. This requirement ensures the developer has performed an analysis of the password mechanism to ensure the probability of guessing a local administrator's password would require a high-attack potential, as defined in Annex B of the CEM. This analysis takes into account the password spaces, as well as any feature of the password mechanism that plays a role in limiting the number of failed authentication attempts within a given time period.
O.VULNERABILITY_ANALYSIS The TOE will undergo some vulnerability analysis to demonstrate the design and implementation of the TOE does not contain any obvious flaws.	AVA_VLA.1	The AVA_VLA.1 component provides the necessary level of confidence that vulnerabilities do not exist in the TOE that could cause the security policies to be violated. AVA_VLA.1 requires the developer to perform a systematic search for potential vulnerabilities in all the TOE deliverables. For those vulnerabilities that are not eliminated, a rationale must be provided that describes why these vulnerabilities cannot be exploited by a threat agent with a low attack potential, which is in keeping with

Objective	Requirements Addressing the Objective	Rationale
		the desired assurance level of this TOE. As with the functional testing, a key element is this component is that an independent assessment of the completeness of the developer's analysis is made, and more importantly, an independent vulnerability analysis coupled with testing of the TOE is performed. This component provides the confidence that security flaws do not exist in the TOE that could be exploited by a threat agent or moderate (or lower) attack potential to violate the TOE's security policies.

The following table includes the rationale for the IT Environment Requirements.

Table 14 Rationale for IT Environment Requirements

Environmental Objective	Requirements Addressing the Objective	Rationale
OE.AUDIT_REVIEW The IT environment will contain mechanisms to allow the authorized administrator to view and sort the audit logs.	FAU_SAR.1	FAU_SAR.1 requires that only the authorized administrator has the capability to read the audit records which must be presented in a manner suitable for the administrator to interpret them.
	FAU_SAR.2	FAU_SAR.2 prohibits all other users read access of the audit records.
	FAU_SAR.3	FAU_SAR.3 requires the IT environment to provide a mechanism for the administrator to search and sort through the audit records.

Environmental Objective	Requirements Addressing the	Rationale
OE.AUDIT_STORAGE The IT environment will contain mechanisms to provide secure storage and management of the audit log.	FAU_STG.1-NIAP-0429	FAU_STG.1-NIAP-0429 requires that only the authorized administrator may delete the audit records ensuring that no malicious users may compromise the data stored within the audit records.
	FAU_STG.NIAP-0414-1-NIAP-0429	FAU_STG.NIAP-0414-1-NIAP-0429 allows the authorized administrator to manage the audit logs when they trail becomes full.
	FMT_MTD.1(2)	FMT_MTD.1(2) allows only the authorized administrator to query the logs and clear the logs.
	FMT_SMF.1(2)	FMT_SMF.1(2) lists the mechanisms available to the administrator for managing the audit records.
OE.DOMAIN_SEPARATION The IT environment will provide an isolated domain for the execution of the TOE.	FPT_SEP_(ENV).1	FPT_SEP_(ENV).1 ensures the IT environment will provide the TOE's with an isolated domain for it's execution.
OE.I_AND_A The IT environment will contain identification and authentication mechanisms for users to login to the TOE.	FIA_AFL.1	FIA_AFL.1 ensures a user cannot keep entering an invalid password in attempts to login, this will prevent a brute force attack to crack a users password.
	FIA_UAU.1	FIA_UAU.1 requires the IT environment must authenticate all users before they are given access to the TOE.

Environmental Objective	Requirements Addressing the	Rationale
	FIA_UID.1	FIA_UID.1 requires the IT environment must uniquely identify all users before they are given access to the TOE.
	FIA_USB.1	FIA_USB.1 binds all subjects in the TOE to the user who is performing them.
	FMT_MTD.1(3)	FMT_MTD.1(3) allows only the authorized administrator to set and reset all users passwords.
	FMT_SMF.1(2)	FMT_SMF.1(2) lists the mechanisms available to the administrator for managing the audit records.
	FTA_SSL.1	FTA_SSL.1 requires authentication and identification mechanisms in order to unlock a user's session.
	FTA_SSL.2	FTA_SSL.2 requires authentication and identification mechanisms in order to unlock a user's session.
OE.NO_BYPASS The IT environment shall ensure the TOE security mechanisms cannot be bypassed in order to gain access to the TOE resources.	FPT_RVM.1	FPT_RVM.1 ensures the TOE cannot be bypassed in order to gain unauthorized access of TOE resources.
OE.NO_EVIL Sites using the TOE shall ensure that authorized administrators are non-hostile, appropriately trained and follow all administrator guidance.	N/A	This objective does not contain any IT security requirements because it is a non-IT related objective. Thus, the CC does not mandate it map to any requirements.

Environmental Objective	Requirements Addressing the	Rationale
OE.CONFIG The TOE will be installed, configured, managed and maintained in accordance with its guidance documentation and applicable security policies and procedures.	N/A	This objective does not contain any IT security requirements because it is a non-IT related objective. Thus, the CC does not mandate it map to any requirements.
OE. NO_GENERAL_ PURPOSE There will be no general-purpose computing capabilities (e.g., compilers or user applications) available on DMBS servers, other than those services necessary for the operation, administration and support of the DBMS.	N/A	This objective does not contain any IT security requirements because it is a non-IT related objective. Thus, the CC does not mandate it map to any requirements.
OE.PHYSICAL Physical security will be provided within the domain for the value of the IT assets protected by the TOE and the value of the stored, processed, and transmitted information.	N/A	This objective does not contain any IT security requirements because it is a non-IT related objective. Thus, the CC does not mandate it map to any requirements.
OE.ROBUST_ENVIORN MENT The IT environment that supports the TOE for enforcement of its security objectives will be of at least the same level of robustness as the TOE.	N/A	This objective does not contain any IT security requirements because it is a non-IT related objective. Thus, the CC does not mandate it map to any requirements.

Environmental Objective	Requirements Addressing the	Rationale
OE.SECURE_COMMS The IT environment will provide a secure line of communications between the remote user and the TOE.	FDP_IFC.1	FDP_IFC.1 defines the scope of the information flow control policy, Transfer Protection Policy.
	FDP_IFF.1	FDP_IFF.1 defines the security attributes and rules associated with the Transfer Protection Policy.
	FDP_ITT.1	FDP_ITT.1 requires the IT environment to protect all user data being transferred from one physically separated part of the TOE to another.
	FMT_MSA.1(2)	FMT_MSA.1(2) allows the Security Target Author to assign the management of security attributes to a particular role.
	FMT_MSA.3(2)	FMT_MSA.3(2) allows the Security Target Author to choose the strength of the initial security attributes.
OE.TIME_STAMPS The IT environment will provide reliable time stamps.	FPT_STM.1	FPT_STM.1 requires the IT environment to provide reliable time stamps to the TOE to use for audit generation.
OE.TRUST_IT Each IT entity the TOE relies on for security functions will be installed, configured, managed and maintained in a manner appropriate to the IT entity, and consistent with the security policy of the TOE and the relationship between them.	N/A	This objective does not contain any IT security requirements because it is a non-IT related objective. Thus, the CC does not mandate it map to any requirements.

6.4 Rationale for Assurance Requirements

This protection profile is developed at the basic robustness level. The assurance requirements are those recommended in instruction 4 from the *Consistency Instruction Manual for Development of US Government Protection Profiles for Use in Basic Robustness Environments*, Version 2.0, dated 1 March 2004.
Flaw Remediation is the only requirement not included in any EAL level because it does not add any assurance to the current system, but to subsequent releases. Therefore the PPRB decided to augment EAL2 with ALC_FLR.2 to instruct the vendors on proper flaw remediation techniques. AVA_MSU.1 is not incorporated until EAL3. Therefore the PPRB needed to augment EAL2 in order to ensure the user and admin guidance is clear and not misleading.

6.5 Rationale for Strength of Function Claim

The TOE minimum strength of function is SOF-basic. The evaluated TOE is intended to operate in DoD basic robustness environments processing classified information. Users in a DoD environment will have a clearance to access all data processed by the TOE, but not necessarily the need to know. All users are assumed to be cooperative and non-malicious. In commercial environments, company sensitive information may be processed, with users being cooperative, and not likely to attempt sophisticated attacks at data for which they are not authorized.

6.6 Rationale for Satisfying all Dependencies

Table 15 Functional Requirement Dependencies

Requirement	Dependency	Satisfied
FAU_GEN.1-NIAP-0410	FPT_STM.1	Satisfied by the IT environment with FPT_STM.1.
FAU_GEN.2-NIAP-0410	FAU_GEN.1-NIAP-0410 FIA_UID.1	FIA_UID.1 is satisfied by the IT environment with FIA_UID.1.
FAU_SEL.1-NIAP-0407	FAU_GEN.1-NIAP-0410 FMT_MTD.1(1)	Satisfied
FDP_ACC.1	FDP_ACF.1-NIAP-0407	Satisfied.
FDP_ACF.1-NIAP-0407	FDP_ACC.1 FMT_MSA.3(1)	Satisfied.
FDP_RIP.2	None	N/A

Requirement	Dependency	Satisfied
FIA_ATD.1	None	N/A
FMT_MOF.1	FMT_SMF.1(1)[1] FMT_SMR.1	Satisfied.
FMT_MSA.1(1)	[FDP_ACC.1 or FDP_IFC.1] FMT_SMF.1(1) [1] FMT_SMR.1	Dependency satisfied by FDP_ACC.1.
FMT_MSA.3(1)	FMT_MSA.1(1) FMT_SMR.1	Satisfied.
FMT_MTD.1(1)	FMT_SMF.1(1)[1] FMT_SMR.1	Satisfied.
FMT_REV.1(1)	FMT_SMR.1	Satisfied.
FMT_REV.1(2)	FMT_SMR.1	Satisfied.
FMT_SMF.1(1)	None	N/A
FMT_SMR.1	FIA_UID.1	FIA_UID.1 is satisfied by the IT environment with FIA_UID.1.
FPT_ITD_(EXP).1	None	N/A
FPT_SEP_(EXP).1	None	N/A
FPT_TRC_(EXP).1	FPT_ITT.1	This dependency is satisfied by the secure communication link (A.SECURE_COMMS) assumed to be present in the IT environment.
FPT_TST_(EXP).1	None	N/A

[1] This list of dependency has been modified per CCIMB Interpretation 065.

Requirement	Dependency	Satisfied
FTA_MCS.1	FIA_UID.1	FIA_UID.1 is satisfied by the IT environment with FIA_UID.1.
FTA_TAB.1	None	N/A
FTA_TAH.1	None	N/A
FTA_TSE.1	None	N/A

Table 16 Functional Requirement Dependencies for IT Environment

Requirement	Dependency	Satisfied
FAU_SAR.1	FAU_GEN.1-NIAP-0410	This dependency is satisfied by FAU_GEN.1-NIAP-0410 in Section 5.1.
FAU_SAR.2	FAU_SAR.1	Satisfied.
FAU_SAR.3	FAU_SAR.1	Satisfied.
FAU_STG.1-NIAP-0429	FAU_GEN.1-NIAP-0410	This dependency is satisfied by FAU_GEN.1-NIAP-0410 in Section 5.1.
FAU_STG.NIAP-0414-1-NIAP-0429	FAU_STG.1-NIAP-0429 FMT_MTD.1(2)	Satisfied.
FDP_IFC.1	FDP_IFF.1	Satisfied.
FDP_IFF.1	FDP_IFC.1 FMT_MSA.3(2)	Satisfied.
FDP_ITT.1	[FDP_ACC.1 or FDP_IFC.1]	Dependency satisfied by FDP_IFC.1.
FIA_AFL.1	FIA_UAU.1	Satisfied.
FIA_UAU.1	FIA_UID.1	Satisfied.
FIA_UID.1	None	N/A

Requirement	Dependency	Satisfied
FIA_USB.1	FIA_ATD.1	This dependency is satisfied by FAU_ATD.1 in Section 5.1.
FMT_MSA.1(2)	[FDP_ACC.1 or FDP_IFC.1] FMT_SMF.1(1) [1] FMT_SMR.1	Dependency satisfied by FDP_IFC.1.
FMT_MSA.3(2)	FMT_MSA.1(2) FMT_SMR.1	This dependency is satisfied by FMT_SMR.1 in Section 5.1.
FMT_MTD.1(2)	FMT_SMF.1(2)[1] FMT_SMR.1	This dependency is satisfied by FMT_SMR.1 in Section 5.1.
FMT_MTD.1(3)	FMT_SMF.1(2)[1] FMT_SMR.1	This dependency is satisfied by FMT_SMR.1 in Section 5.1.
FMT_SMF.1(2)	None	N/A
FPT_RVM.1	None	N/A
FPT_SEP_(ENV).1	None	N/A
FPT_STM.1	None	N/A
FTA_SSL.1	FIA_UAU.1	Satisfied.
FTA_SSL.2	FIA_UAU.1	Satisfied.

Table 17 Assurance Requirement Dependencies

Requirement	Dependency	Satisfied
ACM_CAP.2	None	N/A
ADO_DEL.1	None	N/A
ADO_IGS.1	AGD_ADM.1	Yes

Requirement	Dependency	Satisfied
ADV_FSP.1	ADV_RCR.1	Yes
ADV_HLD.1	ADV_FSP.1 ADV_RCR.1	Yes
ADV_RCR.1	None	N/A
AGD_ADM.1	ADV_FSP.1	Yes
AGD_USR.1	ADV_FSP.1	Yes
ALC_FLR.2	None	N/A
ATE_COV.1	ADV_FSP.1 ATE_FUN.1	Yes
ATE_FUN.1	None	N/A
ATE_IND.2	ADV_FSP.1 AGD_ADM.1 AGD_USR.1 ATE_FUN.1	Yes
AVA_MSU.1	ADO_IGS.1 ADV_FSP.1 AGD_ADM.1 AGD_USR.1	Yes
AVA_SOF.1	ADV_FSP.1 ADV_HLD.1	Yes
AVA_VLA.1	ADV_FSP.1 ADV_HLD.1 AGD_ADM.1 AGD_USR.1	Yes

6.7 Rationale for Explicit Requirements

Table 18 presents the rationale for the inclusion of the explicit functional and assurance requirements found in this PP. The explicit requirements that are included as NIAP interpretations do not require a rationale for their inclusion per CCEVS management.

Table 18 Rationale for Explicit Requirements

Explicit Requirement	Identifier	Rationale
FPT_TRC_(EXP).1		FPT_TRC_(EXP).1 has been created to require timely consistency of replicated TSF data. Although there is a Common Criteria Requirement that attempts to address this functionality, it falls short of the needs of the environment in this protection profile. Specifically, FPT_TRC.1.1 states that "The TSF shall ensure that TSF data is consistent when replicated between parts of the TOE." In the widely distributed environment of this PP's TOE, this is an infeasible requirement. For TOEs with a very large number of components, 100 percent TSF data consistency is not achievable and is not expected at any specific instant in time. Another concern lies in FPT_TRC.1.2 which states that when replicated parts of the TSF are "disconnected", the TSF shall ensure consistency of the TSF replicated data upon "reconnection". Upon first inspection, this seems reasonable, however, when applying this requirement it becomes clear that it dictates specific mechanisms to determine when a component is "disconnected" from the rest of the TSF and when it is "reconnected". This is problematic in this PP's environment in that it is not the intent of the authors to dictate that distributed TSF components keep track of connected/disconnected components. In general, to meet the needs of this PP, it is acceptable to simply require a

Explicit Requirement	Identifier	Rationale
		mechanism that provides TSF data consistency in a timely manner after it is determined that it is inconsistent.
FPT_ITD_(EXP).1		Subjects under the control of the software-only TOE must also have their security domains isolated from one another. Concurrent users of the database management system must be sure that their data is not observed or modified by other users of the same system.
FPT_SEP_(EXP).1		Given the nature of a PP compliant OTE that is described in the TOE Description, the objectives and functional requirements must ultimately reflect this description. Software Only Toe properties are instantiated in Section 3 of the PP (i.e., the Functional Requirements section) by creating explicitly stated requirements in place of FPT_SEP.1. The need for explicitly stated requirements is that when invoked, the current FPT_SEP.1 Common Criteria Requirement requires the TOE (not its environment) to protect itself from external interference and tampering. Typically, "Software Only" technology cannot fully meet these requirements as written. Software Only TOEs should be expected to work in the context of their hardware environment to aid in enforcing domain separation but cannot be required to fully counter the threats without hardware. Therefore, the PP authors chose to use explicitly stated requirements for domain separation when attempting to accommodate the "Software Only" TOE.

Explicit Requirement	Identifier	Rationale
FPT_TST_(EXP).1		The Protection Profile Review Board (PPRB) recommends that TSF testing be specified in all Basic Robustness PPs in order to validate aspects of the TSF prior to or while it is operating. However, there are two issues with FPT_TST.1 as it appears in the Common Criteria. First, the wording of FPT_TST.1.1 appears to make sense only if the TOE includes hardware; it is difficult to imagine what software TSF "self-tests" would be run. Secondly, some TOE data are dynamic (e.g., data in the audit trail, passwords) and so interpretation of "integrity" for FPT_TST.1.2 is required, leading to potential inconsistencies amongst Basic Robustness TOEs.

The following requirements were modified to refer to the IT environment. Throughout each requirement 'TSF' was replaced with 'IT Environment', 'TSC' was replaces with 'IT Environment Scope of Control', etc.

Table 19 Rationale for Environmental Requirements

Environmental Requirement	Identifier	Rationale
FPT_SEP_(ENV).1	TSF domain separation	This is an explicit requirement written to handle domain separation for software-only TOE's

6.8 Rationale for Not Addressing Consistency Instructions

This protection profile does not follow consistency instruction 15 because assignments were filled in for events that must be audited. Also, NIAP Interpretation 0410 is more recent then Interpretation 0407.
Instruction 16 was not followed because an additional selection was chosen, 'object identity'.
Instruction 17 was not followed because 'unauthorized' was added into the second element. Some deletions may be permitted, like removing the audit log to store it on another storage device for routine maintenance.

Instruction 18 was not incorporated into the protection profile because FAU_STG.NIAP-0414-1-NIAP-0429 was used instead. This requirement was based upon FAU_STG.NIAP-0414-1-NIAP-0429, which is hierarchical to FAU_STG.3.
Instruction 19 was not followed because the labelling is not consistent in the manual and this requirement was placed on the IT environment so 'TSF' was replaced with 'IT environment'.
Instruction 20 was not incorporated because cryptography is not required for the protection profile.
Instruction 22 was not incorporated because information flow requirements are not needed for this protection profile.
Instruction 23 was not followed because NIAP interpretation 0425 has been superseded by CCIMB Interpretation 111.
Instruction 24 was not followed because NIAP Interpretation 0425 has been superseded by CCIMB Interpretation 137.

7 APPENDICES

The following sections are the appendices for this Protection Profile.

A REFERENCES

[1] Common Criteria Implementation Board, Common Criteria for Information Technology Security Evaluation, CCIB-98-026, Version 2.1, August 1999

[2] Department of Defense Chief Information Officer, Guidance and Policy for Department of Defense Information Assurance Memorandum No. 6-8510 dated 16 June 2000

[3] National Security Agency, Protection Profile For Single-level Operating Systems In Environments Requiring Medium Robustness Version 1.22, 23 May 2001

[4] Department of Defense Standard, Department of Defense Trusted Computer System Evaluation Criteria (Orange Book), December 1985

[5] Trusted Product Evaluation Program (TPEP) Trusted Computer System Evaluation Criteria (TCSEC) Interpretations

[6] National Computer Security Center, Trusted Database Management System Interpretation of the Trusted Computer System Evaluation Criteria, NCSC-TG-021 Version-1, April 1991

[7] Security Agency Information Assurance Solutions Technical Directors, Information Assurance Technical Framework, Release 3.0, National September 2000

[8] Protection Profile for Operating Systems Implementing Commercial Security, Version 1.0, dated 27 December 2001

[9] Protection Profile Review Board, Protection Profile Consistency Guidance for Basic Robustness, Version 2.0, dated 1 March 2004

B GLOSSARY

Access – Interaction between an entity and an object that results in the flow or modification of data.

Access Control – Security service that controls the use of resources[2] and the disclosure and modification of data.[3]

Accountability – Property that allows activities in an IT system to be traced to the entity responsible for the activity.

Administrator – A user who has been specifically granted the authority to manage some portion or all of the TOE and whose actions may affect the TSP. Administrators may possess special privileges that provide capabilities to override portions of the TSP.

Assurance – A measure of confidence that the security features of an IT system are sufficient to enforce its' security policy.

Attack – An intentional act attempting to violate the security policy of an IT system.

Authentication – Security measure that verifies a claimed identity.

Authentication data – Information used to verify a claimed identity.

Authorization – Permission, granted by an entity authorized to do so, to perform functions and access data.

Authorized Administrator – An Authorized Administrator is the authorized person in contact with the Target of Evaluation who is responsible for maintaining its operational capability.

Authorized user – An authenticated user who may, in accordance with the TSP, perform an operation.

Availability – Timely[4], reliable access to IT resources.

Compromise – Violation of a security policy.

Confidentiality – A security policy pertaining to disclosure of data.

Conformant Product – A Target of Evaluation that satisfied all the functional security requirements in Section 5.1. The requirements in Section 5.2 are satisfied by its IT

[2] Hardware and software.
[3] Stored or communicated.
[4] According to a defined metric.

environment. Furthermore, a conformant TOE satisfies all the TOE security assurance requirements in section 5.3 of this document.

Critical Security Parameters (CSP) – Security-related information (e.g., cryptographic keys, authentication data such as passwords and pins, and cryptographic seeds) appearing in plaintext or otherwise unprotected form and whose disclosure or modification can compromise the security of a cryptographic module or the security of the information protected by the module.

Database Management System (DBMS) – A suite of programs that typically manage large structured sets of persistent data, offering ad hoc query facilities to many users. They are widely used in business applications.

Defense-in-Depth (DID) – A security design strategy whereby layers of protection are utilized to establish an adequate security posture for an IT system.

Discretionary Access Control (DAC) – A means of restricting access to objects based on the identity of subjects and/or groups to which they belong. Those controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject.

Enclave – A collection of entities under the control of a single authority and having a homogeneous security policy. They may be logical, or may be based on physical location and proximity.

Entity – A subject, object, user or another IT device, which interacts with TOE objects, data, or resources.

External IT entity – Any trusted Information Technology (IT) product or system, outside of the TOE, which may, in accordance with the TSP, perform an operation.

Identity – A representation (e.g., a string) uniquely identifying an authorized user, which can either be the full or abbreviated name of that user or a pseudonym.

Integrity – A security policy pertaining to the corruption of data and TSF mechanisms.

Named Object – An object that exhibits all of the following characteristics:

- The object may be used to transfer information between subjects of differing user identities within the TSF.
- Subjects in the TOE must be able to requires a specific instance of the object.
- The name used to refer to a specific instance of the object must exist in a context that potentially allows subjects with different user identities to requires the same instance of the object.

Object – An entity within the TSC that contains or receives information and upon which subjects perform operations.

Operating Environment – The total environment in which a TOE operates. It includes the physical facility and any physical, procedural, administrative and personnel controls.

Public Object – An object for which the TSF unconditionally permits all entities "read" access. Only the TSF or authorized administrators may create, delete, or modify the public objects.

Robustness – A characterization of the strength of a security function, mechanism, service or solution, and the assurance (or confidence) that it is implemented and functioning correctly. DoD has three levels of robustness:

Basic: Security services and mechanisms that equate to good commercial practices.

Medium: Security services and mechanisms that provide for layering of additional safeguards above good commercial practices.

High: Security services and mechanisms that provide the most stringent protection and rigorous security countermeasures.

Secure State – Condition in which all TOE security policies are enforced.

Security attributes – TSF data associated with subjects, objects, and users that are used for the enforcement of the TSP.

Security level – The combination of a hierarchical classification and a set of non-hierarchical categories that represent the sensitivity of the information.

Sensitive information – Information that, as determined by a competent authority, must be protected because its unauthorized disclosure, alteration, loss, or destruction will at least cause perceivable damage to someone or something.

Subject – An entity within the TSC that causes operation to be performed.

Threat – Capabilities, intentions and attack methods of adversaries, or any circumstance or event, with the potential to violate the TOE security policy.

Threat Agent – Any human user or Information Technology (IT) product or system, which may attempt to violate the TSP and perform an unauthorized operation with the TOE.

Unauthorized user – A user who may obtain access only to system provided public objects if any exist.

User – Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

Vulnerability – A weakness that can be exploited to violate the TOE security policy.

C ACRONYMS

CC	Common Criteria
CCIMB	Common Criteria Interpretations Management Board
CM	Configuration Management
DoD	Department of Defense
EAL	Evaluation Assurance Level
IATF	Information Assurance Technical Framework
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards Technology
NSA	National Security Agency
PP	Protection Profile
SFP	Security Functional Policies
SFR	Security Functional Requirement
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TOE Scope of Control
TSE	TOE Security Environment
TSF	TOE Security Functions
TSFI	TSF interfaces
TSP	TOE Security Policy
TTAP/CCEVS	Trust Technology Assessment Program/ Common Criteria Evaluation and Validation Scheme

D ROBUSTNESS ENVIRONMENT CHARACTERIZATION

D.1 General Environmental Characterization

In trying to specify the environments in which TOEs with various levels of robustness are appropriate, it is useful to first discuss the two defining factors that characterize that environment: value of the resources and authorization of the entities to those resources.
In general terms, the environment for a TOE can be characterized by the authorization (or lack of authorization) the least trustworthy entity has with respect to the highest value of TOE resources (i.e. the TOE itself and all of the data processed by the TOE).
Note that there are an infinite number of combinations of entity authorization and value of resources; this conceptually "makes sense" because there are an infinite number of potential environments, depending on how the resources are valued by the organization, and the variety of authorizations the organization defines for the associated entities. In the next section, these two environmental factors will be related to the robustness required for selection of an appropriate TOE.

D.1.1 Value of Resources

Value of the resources associated with the TOE includes the data being processed or used by the TOE, as well as the TOE itself (for example, a real-time control processor). "Value" is assigned by the using organization. For example, in the DoD low-value data might be equivalent to data marked "FOUO", while high-value data may be those classified Top Secret. In a commercial enterprise, low-value data might be the internal organizational structure as captured in the corporate on-line phone book, while high-value data might be corporate research results for the next generation product. Note that when considering the value of the data one must also consider the value of data or resources that are accessible through exploitation of the TOE. For example, a firewall may have "low value" data itself, but it might protect an enclave with high value data. If the firewall was being depended upon to protect the high value data, then it must be treated as a high-value-data TOE.

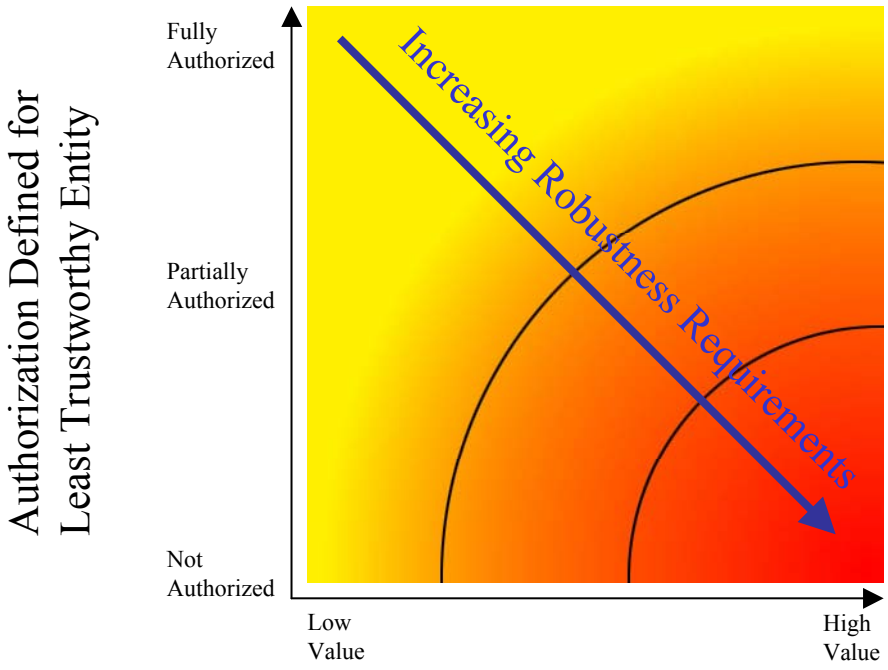
D.1.2 Authorization of Entities

Authorization that entities (users, administrators, other IT systems) have with respect to the TOE (and thus the resources of that TOE, including the TOE itself) is an abstract concept reflecting a combination of the trustworthiness of an entity and the access and privileges granted to that entity with respect to the resources of the TOE. For instance, entities that have total authorization to all data on the TOE are at one end of this spectrum; these entities may have privileges that allow them to read, write, and modify anything on the TOE, including all TSF data. Entities at the other end of the spectrum are those that are authorized to few or no TOE resources. For example, in the case of a router, non-administrative entities may have their packets routed by the TOE, but that is the extent of their authorization to the TOE's resources. In the case of an OS, an entity may not be allowed to log on to the TOE at all (that is, they are not valid users listed in the OS's user database).

It is important to note that authorization **does not** refer to the **access** that the entities actually have to the TOE or its data. For example, suppose the owner of the system determines that no one other than employees was authorized to certain data on a TOE, yet they connect the TOE to the Internet. There are millions of entities that are not **authorized** to the data (because they are not employees), but they actually have connectivity to the TOE through the Internet and thus can attempt to access the TOE and its associated resources.
Entities are characterized according to the value of resources to which they are authorized; the extent of their authorization is implicitly a measure of how trustworthy the entity is with respect to compromise of the data (that is, compromise of any of the applicable security policies; e.g., confidentiality, integrity, availability). In other words, in this model the greater the extent of an entity's authorization, the more trustworthy (with respect to applicable policies) that entity is.

D.1.3 Selection of Appropriate Robustness Levels

Robustness is a characteristic of a TOE defining how well it can protect itself and its resources; a more robust TOE is better able to protect itself. This section relates the defining factors of IT environments, authorization, and value of resources to the selection of appropriate robustness levels.
When assessing any environment with respect to Information Assurance the critical point to consider is the likelihood of an attempted security policy compromise, which was characterized in the previous section in terms of entity authorization and resource value. As previously mentioned, robustness is a characteristic of a TOE that reflects the extent to which a TOE can protect itself and its resources. It follows that as the likelihood of an attempted resource compromise increases, the robustness of an appropriate TOE should also increase.
It is critical to note that several combinations of the environmental factors will result in environments in which the likelihood of an attempted security policy compromise is similar. Consider the following two cases:
The first case is a TOE that processes only low-value data. Although the organization has stated that only its employees are authorized to log on to the system and access the data, the system is connected to the Internet to allow authorized employees to access the system from home. In this case, the least trusted entities would be unauthorized entities (e.g. non-employees) exposed to the TOE because of the Internet connectivity. However, since only low-value data are being processed, the likelihood that unauthorized entities would find it worth their while to attempt to compromise the data on the system is low and selection of a basic robustness TOE would be appropriate.
The second case is a TOE that processes high-value (e.g., classified) information. The organization requires that the TOE be stand-alone, and that every user with physical and logical access to the TOE undergo an investigation so that they are authorized to the highest value data on the TOE. Because of the extensive checks done during this investigation, the organization is assured that only highly trusted users are authorized to use the TOE. In this case, even though high value information is being processed, it is unlikely that a compromise of that data will be attempted because of the authorization and trustworthiness of the users and once again, selection of a basic robustness TOE would be appropriate.
The preceding examples demonstrated that it is possible for radically different combinations of entity authorization/resource values to result in a similar likelihood of an attempted compromise. As mentioned earlier, the robustness of a system is an indication of the protection being provided to counter compromise attempts. Therefore, a basic robustness system should be sufficient to



counter compromise attempts where the likelihood of an attempted compromise is low. The following chart depicts the "universe" of environments characterized by the two factors discussed in the previous section: on one axis is the authorization defined for the least trustworthy entity, and on the other axis is the highest value of resources associated with the TOE.

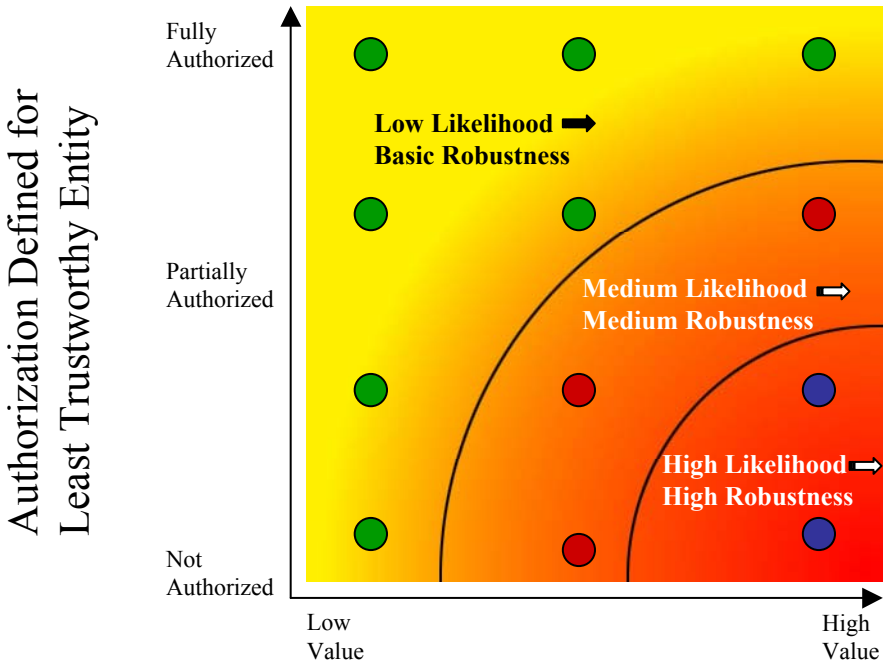
As depicted in the following figure, the robustness of the TOEs required in each environment steadily increases as one goes from the upper left of the chart to the lower right; this corresponds to the need to counter increasingly likely attack attempts by the least trustworthy entities in the environment. Note that the shading of the chart is intended to reflect- the notion that different environments engender similar levels of "likelihood of attempted compromise", signified by a similar color. Further, the delineations between such environments are not stark, but rather are finely grained and gradual.

While it would be possible to create many different "levels of robustness" at small intervals along the "Increasing Robustness Requirements" line to counter the increasing likelihood of attempted compromise due to those attacks, it would not be practical nor particularly useful. Instead, in order to implement the robustness strategy where there are only three robustness levels: Basic, Medium, and High, the graph is divided into three sections, with each section corresponding to a set of environments where the likelihood of attempted compromise is roughly similar. This is graphically depicted in the following chart.

In this second representation of environments and the robustness plane below, the "dots" represent given instantiations of environments; like-colored dots define environments with a similar likelihood of attempted compromise. Correspondingly, a TOE with a given robustness

should provide sufficient protection for environments characterized by like-colored dots. In choosing the appropriateness of a given robustness level TOE PP for an environment, then, the user must first consider the lowest authorization for an entity as well as the highest value of the resources in that environment. This should result in a "point" in the chart above, corresponding to the likelihood that that entity will attempt to compromise the most valuable resource in the environment. The appropriate robustness level for the specified TOE to counter this likelihood can then be chosen.

The difficult part of this activity is differentiating the authorization of various entities, as well as determining the relative values of resources; (e.g., what constitutes "low value" data vs. "medium value" data). Because every organization will be different, a rigorous definition is not possible. In Section 3 of this PP, the targeted threat level for a Basic robustness TOE is characterized. This information is provided to help organizations using this PP -ensure that the functional requirements specified by this Basic robustness PP are appropriate for their intended application of a compliant TOE.



E REFINEMENTS

This section contains refinements where text was omitted. Omitted text is shown as bold text within parenthesis. The actual text of the functional requirements as presented in Section 5 has been retained.

FAU_SEL.1.1-NIAP-0407 **Refinement**: The TSF shall **(be able to) allow only the administrator** to include or exclude auditable events from the set of audited events based on the following attributes:

a) *user identity*,

b) *event type*,

c) *object identity*,

d) [selection: "subject identity", "host identity", "none"];

e) [success of auditable security events;

f) failure of auditable security events; and

g) [selection: [assignment: list of additional criteria that audit selectivity is based upon], "no additional criteria"].]

FMT_MSA.1.1(1) **Refinement**: The TSF shall enforce the [Discretionary Access Control policy] to restrict the ability to [*manage*] **all** the security attributes (**[assignment: list of security attributes]) of database users** to [authorized administrators].

The following requirements are from the requirements on the IT environment in Section 5.2.

FAU_SAR.1.1 **Refinement**: The **(TSF) IT environment** shall provide [the authorized administrator] with the capability to read [all database audit information] from the audit records.

FAU_SAR.1.2 **Refinement**: The **(TSF) IT environment** shall provide the audit records in a manner suitable for the **(user) authorized administrator** to interpret the information.

FAU_SAR.2.1 **Refinement**: The **(TSF) IT environment** shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

FAU_SAR.3.1 **Refinement**: The **(TSF) IT environment** shall provide the ability to perform *searches and sorting* of audit data based on

- [User identity;
- Date of event;
- Time of event;
- Type of event;
- Event status (success/failure)]; **and**
- **[assignment: additional criteria with logical relations]**.

FAU_STG.1.1-NIAP-0429 **Refinement**: The **(TSF) IT environment** shall **(protect the) restrict the deletion of** stored audit records **(from unauthorized deletion) in the audit trail to the authorized administrator**.

FAU_STG.1.2-NIAP-0429 **Refinement**: The **(TSF) IT environment** shall be able to *prevent* unauthorized modifications to the audit records in the audit trail.

FAU_STG.NIAP-0414-1.1-NIAP-0429 **Refinement**: The **(TSF) IT Environment** shall **provide an authorized administrator with the capability to select one or more of the following actions** [selection: "ignore auditable events", "prevent auditable events, except those taken by the authorized user with special rights", "overwrite the oldest stored audit records"] and [assignment: other actions to be taken in case of audit storage failure] if the audit trail is full.

FAU_STG.NIAP-0414-1.2-NIAP-0429 **Refinement**: The **(TSF) IT environment** shall [selection: 'ignore auditable events', 'prevent auditable events, except those taken by the authorized user with special rights', 'overwrite the oldest stored audit records', [assignment: other actions to be taken in case of audit storage failure]] if the audit trail is full. **(and no other action has been selected.)**

FDP_IFC.1.1 **Refinement**: The **(TSF) IT environment** shall enforce the [Transfer Protection Policy] on [assignment: list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP].

FDP_IFF.1.1 **Refinement**: The **(TSF) IT environment** shall enforce the [Transfer Protection Policy] based on the following types of subject and information security attributes: [assignment: list of subjects and information controlled under the indicated policy, and, for each, the security attributes].

FDP_IFF.1.2 **Refinement**: The **(TSF) IT environment** shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: for each operation, the security attribute-based relationship that must hold between subject and information security attributes].

FDP_IFF.1.3 **Refinement**: The **(TSF) IT environment** shall enforce the [assignment: additional information flow control policy rules].

FDP_IFF.1.4 **Refinement**: The **(TSF) IT environment** shall provide the following [assignment: list of additional policy capabilities].

FDP_IFF.1.5 **Refinement**: The **(TSF) IT environment** shall explicitly authorize an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly authorize information flows].

FDP_IFF.1.6 **Refinement**: The **(TSF) IT environment** shall explicitly deny an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly deny information flows].

FDP_ITT.1.1 **Refinement**: The **(TSF) IT environment** shall enforce the [Transfer Protection Policy] to prevent the [selection: disclosure, modification, loss of use] of user data when it is transmitted between physically-separated parts of the TOE.

FIA_AFL.1.1 **Refinement**: The **(TSF) IT environment** shall detect when *"an administrator configurable positive integer within [assignment: range of acceptable values]"* **of** unsuccessful authentication attempts occur related to [a user's authentication] **within [assignment: authorized administrator configurable amount of time]**.

FIA_AFL.1.2 **Refinement**: When the defined number of unsuccessful authentication attempts has been met or surpassed, the **(TSF) IT environment** shall [lock the device for an authorized administrator configurable amount of time].

FIA_UAU.1.1 **Refinement**: The **(TSF) IT environment** shall allow [assignment: list of TSF mediated actions] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 **Refinement**: The **(TSF) IT environment** shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UID.1.1 **Refinement**: The **(TSF) IT environment** shall allow [assignment: list of TSF-mediated action] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 **Refinement**: The **(TSF) IT environment** shall require each user to be **uniquely and** successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FIA_USB.1.1 **Refinement**: The **(TSF) IT environment** shall associate the following user security attributes with subjects acting on the behalf of that user: [all attributes listed in FIA_ATD.1].

FIA_USB.1.2 **Refinement**: The **(TSF) IT environment** shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [none].

FIA_USB.1.3 **Refinement**: The **(TSF) IT environment** shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [only the authorized administrator can change security attributes].

FMT_MSA.1.1(2) **Refinement**: The **(TSF) IT environment** shall enforce the [Transfer Protection Policy] to restrict the ability to [selection: change_default, query, modify, delete, [assignment: other operations]] the security attributes [assignment: list of security attributes] to [assignment: the authorized identified roles].

FMT_MSA.3.1(2) **Refinement**: The **(TSF) IT environment** shall enforce the [Transfer Protection Policy] to provide [selection: choose one of: restrictive, permissive, [assignment: other property]] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(2) **Refinement**: The **(TSF) IT environment** shall allow the [assignment: the authorized identified roles] to specify alternative initial values to override the default values when an object or information is created.

FMT_MTD.1.1(2) **Refinement**: The **(TSF) IT environment** shall restrict the ability to *query and clear* the [audit records] to the [authorized administrator].

FMT_MTD.1.1(3) **Refinement**: The **(TSF) IT environment** shall restrict the ability to [*set and reset*] the [user authentication data] to [the authorized administrator].

FMT_SMF.1.1(2) **Refinement**: The **(TSF) IT environment** shall be capable of performing the following security management functions:

- [query and clearing audit records;
- set and resetting user authentication data; and
- [assignment: list of additional security management functions to be provided by the IT environment]].

FPT_RVM.1.1 **Refinement**: The **(TSF) IT environment** shall ensure that **(TSP) IT environment security policy** enforcement functions are invoked and succeed before each function within the **IT environment's scope of control (TSC)** is allowed to proceed.

FPT_STM.1.1 **Refinement**: The **(TSF) IT environment** shall be able to provide reliable time stamps for its own use **and for the TOE**.

FTA_SSL.1.1 **Refinement**: The **(TSF) IT environment** shall lock an interactive session after **an authorized administrator specified time interval of user inactivity** by:

a) clearing or overwriting display devices, making the current contents unreadable;

b) disabling any activity of the user's data access/display devices other than unlocking the session.

FTA_SSL.1.2 **Refinement**: The **(TSF) IT environment** shall require the following events to occur prior to unlocking the session: [user re-authentication].

FTA_SSL.2.1 **Refinement**: The **(TSF) IT environment** shall allow user-initiated locking of the user's own interactive session, by:

a) clearing or over-writing display devices, making the current contents unreadable;

b) disabling any activity of the user's data access/display devices other then unlocking the session.

FTA_SSL.2.2 **Refinement**: The **(TSF) IT environment** shall require the following events to occur prior to unlocking the session: [user re-authentication].