Vanguard
Integrity
Professionals, Inc.

Vanguard Enforcer™ Version 7.1
Common Criteria Security Target

Version:	1.39
Status:	Approved
Last Update:	2006-12-01

Document History

Version	Date	Summary	Author
0.01	2005-09-02	Initial Draft	Gordon McIntosh (atsec)
0.1	2005-09-30	First review draft	Gordon McIntosh (atsec)
0.2	2005-10-04	Integration of comments from Stephen Mueller	Gordon McIntosh (atsec)
0.3	2005-10-05	Integration of comments from Lou Losee	Gordon McIntosh (atsec)
0.4	2005-10-14	Integration of changes from Eldon	Gordon McIntosh (atsec)
0.5	2005-10-19	Integration of Helmut, Lou comments	Gordon McIntosh (atsec)
0.6	2005-10-24	Added VIO filters to SFR and TSF	Gordon McIntosh (atsec)
0.7	2005-10-27	Added Trademarks supplied by Vanguard	Gordon McIntosh (atsec)
0.71	2005-10-27	Additional trademarks per email from Jackson Baker, Vanguard	Gordon McIntosh (atsec)
0.8	2005-11-01	Add restrictions for environment to include CAPP only, no LSPP	Gordon McIntosh (atsec)
0.9	2005-11-06	Add rational	Gordon McIntosh (atsec)
1.0	2005-11-16	Add more to rationale and add threat	Gordon McIntosh (atsec)
1.1	2005-11-17	Changes to the Critical general Resource Sensor descriptions in FAU_ARP.1 (!) and F.AU.1.5.8 per email from Eldon Worley	Gordon McIntosh (atsec)
1.2	2005-12-01	Cleanup and removal of : FAU_SAA.5-RACF.2, item a)a.a. FAU_SAA.5-RACF.2, item a)f.a. FAU_SAA.5-RACF.2, item a)g.a. FAU_SAA.5-RACF.2, item a)n.a.	Gordon McIntosh (atsec)
1.3	2005-12-15	Removal of Active Alerts functionality throughout document	Gordon McIntosh (atsec)
1.4	2005-12-17	Update management function TSF	Gordon McIntosh (atsec)
1.5	2005-12-19	Cleanup with Lou's comments	Gordon McIntosh (atsec)
1.6	2006-01-31	Cleanup of evaluator comments	Gordon McIntosh (atsec)
1.7	2006-02-08	Cleanup of evaluator comments	Gordon McIntosh (atsec)
1.8	2006-02-09	Minor cleanup of evaluator comments	Gordon McIntosh (atsec)
1.9	2006-02-10	Minor leanup of evaluator comments	Gordon McIntosh (atsec)
1.10	2006-02-10	Minor cleanup of evaluator comments	Gordon McIntosh (atsec)
1.11	2006-02-24	Cleanup of CB and evaluator comments	Gordon McIntosh (atsec)

		and minor spelling	
1.12	2006-03-02	Correct FMT_MSA.1-1 Correct sensor descriptions	Gordon McIntosh (atsec)
1.13	2006-03-02	Correct FMT_MSA.1-1 Correct sensor descriptions again	Gordon McIntosh (atsec)
1.14	2006-03-07	Changes to Section 2.3.1 per Eldon Worley Removal of references to SNMP	Gordon McIntosh (atsec)
1.15	2006-03-09	Changes to Figure 1	Gordon McIntosh (atsec)
1.16	2006-03-24	Removal of FAU_SAA.1 from Table 12	Gordon McIntosh (atsec)
1.17	2006-03-29	Addition of Installation Critical Data set Sensor Changed dataset to data set in document	Gordon McIntosh (atsec)
1.18	2006-04-03	Sensor Name changes	Gordon McIntosh (atsec) Eldon Worley (Vanguard)
1.19	2006-04-09	Removed TSF 1.6, 4.1 TSF numbering unchanged	Gordon McIntosh (atsec)
1.20	2006-04-14	Altered System Access List Expiration sensor to Access List Expiration Sensor Added F.AU.1.15.9 for consistency with Enforcer Admin Guide	Eldon Worley (Vanguard)
1.21	2006-04-17	Altered the text for the name of the Access List Expiration Sensor to be compatible with Enforcer Admin Guide	Eldon Worley (Vanguard)
1.22	2006-04-27	Changed OE.MANAGE from requirement for the non-IT environment to IT-environment. and mapped to FMT-MSA.1, FMT_MSA.3, FMT_SMF.1, and FMT_SMR.1	Gordon McIntosh (atsec)
1.23	2006-04-28	Altered the text for the name of the Access List Expiration Sensor to be consistent Clarify OE.ADMIN in Table 11 Clarify A.ADMINISTRATION and A.NO_EVIL_ADM rationales in Table 19	Gordon McIntosh (atsec)
1.24	2006-05-02	Clarification of OE.ADMIN Correction to Table 18, Clarification of A.NO_EVIL_ADM	Gordon McIntosh (atsec)
1.25	2006-05-02	Reword OE.ADMIN	Gordon McIntosh (atsec)
1.26	2006-05-22	In Section 2.3, moved Access List Expiration Sensor to its own area. Rename Access List Expiration Sensor to Access List Expiration Processing Sensor in document	Eldon Worley (Vanguard) Gordon McIntosh (atsec)

1.27	2006-06-07	Added statement excluding active alerts, user defined exits, and SNMP and added TOE documentation to TOE and shipping method in Section 2.2 Added A.TIMESTAMP in Section 3.6 Added OE.TIMESTAMP in Section 4.2.1 Added a dependency to FAU_SAA.5-RACF.1 in Section 5.1.1 for FPT_STM.1 Added IT Environment security functions, FPT_SEP.1, FPT_STM.1 To Section 5.5, 5.9.1 and 5.9.2 Added OE.MANAGE in Table 18 Added A.TIMESTAMP in Table 19 Modified PE.MANAGE in Table 20 Added rationale in Section 8.4 for addition of dependency on FPT_STM.1. Added OE.TIMESTAMP in Table 23 Added dependency for FUA_SAA.5-RACF in Table 24 Added FPT_STM.1 and FPR_SEP.1 in Table 25.	Gordon McIntosh (atsec)
1.28	2006-06-27	Update TOE guidance in Section 2.2	Gordon McIntosh (atsec)
1.29	2006-07-20	Revise wording on F.AU.1.3.4 Remove F.AU.1.15.6 as redundant	Gordon McIntosh (atsec)
1.30	2006-10-11	Make changes to F.AU.1.4.1, F.AU.1.4.2, and F.AU.1.4.3	Gordon McIntosh (atsec)
1.31	2006-10-18	Added reference to the Vanguard Cover Letter in Section 2.2 and Section 10.	Jackson Baker (Vanguard)
1.32	2006-11-01	Make changes to F.AU.1.5.1 and section 5.3.2, FAU_ARP.1.1	Eldon Worley (Vanguard)
1.33	2006-11-03	Update version number and date	Gordon McIntosh (atsec)
1.34	2006-11-10	Updated section 5.3.2, items b) and o) to restore text about error messages Added list of PTFs for TOE in sections 1.1 and 2.6.1	Eldon Worley (Vanguard)
1.35	2006-11-10	Updated Table 1 to place the list of PTFs in the TOE Identification row Updated the Enforcer version value in section 2.6.1 to be 7.1.1	Eldon Worley (Vanguard)
1.36	2006-11-14	Updated Vanguard Enforcer Administrator Guide Document Number and corrected type on section 5.3.2, FAU_ARP.1.1 b) b	Jackson Baker (Vanguard)
1.37	2006-11-15	Document numbers in Reference Section updated and changed from dynamic updating.	Jackson Baker (Vanguard)
1.38	2006-11-16	Final document numbers entered to Reference Section.	Jackson Baker (Vanguard)
1.39	2006-12-01	Corrected PTF numbers in TOE identification section and updated document numbers in Reference Section.	Jackson Baker (Vanguard)

Table of Contents

1 Introduction 8
1.1 ST Identification 8
1.2 ST Overview 8
1.3 CC Conformance Claim 9
1.4 Strength of Function Claim 9
1.5 Structure 9
1.6 Terminology 9
1.7 Trademarks 9
1.7.1 Vanguard Trademarks 10
1.7.2 IBM Trademarks 11
2 TOE Description 12
2.1 Product Overview 12
2.2 TOE Overview 13
2.2.1 Startup and Option Interface Components 15
2.3 Sensor Component 15
2.3.1 Sensor Task Log Functions 18
2.4 Subjects, Objects, Security Attributes, TSF and user data 19
2.4.1 Subjects and users 19
2.4.2 Objects 19
2.4.3 Security Attributes 19
2.4.4 TSF and User Data 19
2.5 Summary of Security Features 20
2.5.1 Audit 20
2.5.2 Security Management 20
2.6 Configurations 20
2.6.1 Software Configuration 20
2.6.2 TOE Exclusions in the Evaluated Configuration 21
2.6.3 Hardware Configuration 21
3 TOE Security Environment 22
3.1 Introduction 22
3.2 Assumptions 22
3.3 Administrative Assumptions 22
3.4 Physical Assumptions 22
3.5 Personnel Assumptions 23
3.6 Procedural Assumptions 23
3.7 Threats 23
3.8 Threats addressed by TOE 23
3.8.1 Threats to be countered by the TOE 24
3.9 Organizational Security Policies (OSP) 24
3.10 OSP addressed by the TOE 24
3.11 OSP addressed by the TOE environment 24
4 Security Objectives 26
4.1 TOE Security Objectives 26
4.2 TOE Environmental Security Objectives 26
4.2.1 TOE Operational Environment 26
5 Security Requirements 28
5.1 Extended Components Definition 28
5.1.1 FAU_SAA.5-RACF RACF Potential Violation Analysis 28
5.2 TOE Security Functional Requirements 28
5.3 Security audit (FAU) 29
5.3.1 RACF Potential Violation Analysis (FAU_SAA.5-RACF) 29
5.3.2 Security audit automatic response in Sensor (FAU_ARP.1) 31
5.4 Security Management (FMT) 34

5.4.1 FMT_SMF.1 Specification of Management Functions 34
5.5 TOE Environment Security Functional Requirements 35
5.6 User Data Protection (FDP) 35
5.6.1 Subset access control (FDP_ACC.1) 35
5.6.2 Security attribute based access control (FDP_ACF.1) 36
5.7 Identification and Authentication (FIA) 36
5.7.1 Timing of authentication (FIA_UAU.1) 36
5.7.2 Timing of identification (FIA_UID.1) 36
5.8 Security Management (FMT) 36
5.8.1 Management of Security Attributes (FMT_MSA.1) 36
5.8.2 Static Attribute Initialization (FMT_MSA.3) 37
5.8.3 Specification of management functions (FMT_SMF.1) 37
5.8.4 Security roles (FMT_SMR.1) 37
5.9 Protection of the TSF 37
5.9.1 Domain Seperation (FPT_SEP.1) 37
5.9.2 Reliable Time Stamps (FPT_STM.1) 37
5.10 TOE Security Assurance Requirements 38
6 TOE Summary Specification 39
6.1 TOE Security Functions 39
6.1.1 Introduction 39
6.1.2 Audit (F.AU) 39
6.1.2.1 Sensor violation analysis and automatic response (F.AU.1) 39
6.1.3 TOE Management (F.MGMT) 45
6.2 Assurance Measures 45
7 Protection Profile Claims 48
7.1 PP Reference 48
8 Rationale 49
8.1 Security Objectives Rationale 49
8.2 Security Objectives Coverage 49
8.3 Security Objectives Sufficiency 50
8.4 Explicit Security Functional Requirements Rationale 52
8.5 Security Functional Requirements Rationale 52
8.6 Security Requirements Dependency Analysis 54
8.7 TOE Summary Specification Rationale 55
8.7.1 Security Functions Justification 55
8.7.2 Mutual Support of Security Functions 55
8.8 Assurance Measures Rationale 55
8.9 Strength of Function Rationale 56
9 Abbreviations 57
10 References 58

List of Tables

Table 1 - ST Identification Information 8
Table 2 - Administrative Assumptions 22
Table 3 - Physical Assumptions 22
Table 4 - Personnel Assumptions 23
Table 5 - Procedural Assumptions 23
Table 6 – Threats Countered by the TOE 24
Table 7 - TOE Organizational Security Policy 24
Table 8 - TOE Environment Organizational Security Policy 24
Table 9 - TOE Security Objectives 26
Table 10 - IT Environmental Security Objectives 26
Table 11 – Non - IT Environmental Security Objectives 27

Table 12 -Security Functional Requirements of the TOE 29
Table 13 - Security Functional Requirements of the TOE Operational Environment 35
Table 14 - Sensor violation analysis and automatic response TSF 39
Table 15 - TOE Management TSF 45
Table 16 - Mapping Assurance Components to Assurance Measures 45
Table 17 - Mapping Objectives to Threats and Policies 49
Table 18 - Mapping Objectives for the Environment to Threats, Assumptions, and Policies 49
Table 19 - Assumptions to Objectives Rationale 50
Table 20 - Organizational Security Policy to Objectives Rationale 51
Table 21 - Mapping Security Functional Requirements to Objectives 52
Table 22 - Mapping TOE Objectives to SFRs for the TOE 53
Table 23 - Mapping IT Environment Objectives to SFRs for the IT Environment 53
Table 24 - Dependencies between TOE Security Functional Requirements 54
Table 25 - Dependencies between IT Environment Security Functional Requirements 54
Table 26 - Mapping of TOE SFRs to TSF 55
Table 27 - Abbreviations and Acronyms 57
Table 28 - References 58

List of Figures

Figure 1 - TOE and TOE Environment 14

1 Introduction

1.1 ST Identification

The following table contains the Security Target (ST) identification information.

Table 1 - ST Identification Information

Attribute	Description
ST Title	Vanguard Enforcer Version 7.1 Common Criteria Security Target
TOE Identification	Vanguard Enforcer Version 7.1.1 PTFs *Program Temporary Fixes) to be applied are: VED6306 VED6301 VED6300 VED6299 VED6298 VED6297 VED6296 VED6294 VED6293 VED6291 VED6290 VED6285 VED6284 VED6283 VED6279 VED6277 VED6272 VED6259
CC Version	[CC], [CEM]
Keywords	Enforcer, z/OS, RACF

1.2 ST Overview

This document is the Security Target (ST) for the Vanguard Enforcer product Version 7.1. The Vanguard Enforcer [VEAG] provides administrative support for the IBM Resource Access Control Facility (RACF) Security Server [RACFAG], running on the IBM z/OS V1R6 operating system on an IBM zSeries processor

This evaluation is for the product running on IBM zSeries hardware, using the zSeries operating systems, z/OS V1R6, in the configuration equivalent to that evaluated under the Common Criteria (CC) as described in the Security Target for IBM z/OS Version 1 Release 6 [ZOS_ST], restricted to the Controlled Access Protection Profile (CAPP). This refers to the product certified under ID BSI-DSZ-CC-0247-2005 by the German Certification Body BSI on March 9, 2005. See http://www.bsi.de/zertifiz/zert/reporte/0247a.pdf for a copy of the certificate and the certification report.

The z/OS Security Target is included as a reference [ZOS_ST] and should be used to understand the environment in which the TOE is intended.

The Security Target has been developed in accordance with [CC] and [CEM], for a claimed Evaluation Assurance Level 3 (EAL3) augmented with flaw remediation ALC_FLR.1.

This Security Target assumes the user is familiar with the IBM zSeries Operating System, z/OS, as well as the IBM zSeries Security Server, RACF.

1.3 CC Conformance Claim

This ST is based upon the Common Criteria [CC] and Common Evaluation Methodology [CEM].

This ST claims the following CC conformance:

- Part 2 extended
- Part 3 conformant

Evaluation Assurance Level (EAL) 3 augmented by ALC_FLR.1.

This ST does not claim conformance to any Protection Profile (PP).

1.4 Strength of Function Claim

No SOF claims are made for this evaluation.

1.5 Structure

The structure of this document is as defined by [CC] Part 1 Annex C.

- Section 2 is the TOE Description.
- Section 3 provides the statement of TOE Security Environment.
- Section 4 provides the statement of Security Objectives.
- Section 5 provides the statement of Security Requirements.
- Section 6 provides the TOE Summary Specification, which includes the detailed specification of the IT Security Functions.
- Section 7 provides the Protection Profile Claims
- Section 8 provides the Rationale for the security objectives, security requirements and the TOE summary specification.

1.6 Terminology

This section contains definitions of technical terms that are used with a meaning specific to this document. Terms defined in the [CC] are not reiterated here, unless stated otherwise. Readers should be aware that some terms are used differently in other Vanguard documents. The following glossary points out different usage where appropriate:

Authorization
: If an *authorized administrator* is granted a requested service, the *user* is said to have authorization to the requested service.

Authorized User
: An authorized user is a *user* who has been properly identified and authenticated. These *users* are considered legitimate *users* of the TOE.

Authorized Administrator
: An authorized administrator is an *authorized user* who has been granted the authority to manage the TOE. These *users* are expected to use this authority only in the manner prescribed by the guidance given them.

User
: An individual attempting to invoke a service offered by the TOE

1.7 Trademarks

1.7.1 Vanguard Trademarks

The following terms are trademarks of the Vanguard in the United States and/or other countries:

- Vanguard Integrity Professionals
- Vanguard Security Solutions
- Vanguard Security Suite
- Vanguard Security on Demand
- Security on Demand
- ez/Security on Demand
- RioVision
- Vanguard Administrator
- Administrator
- Vanguard Advisor
- Advisor
- Vanguard Analyzer
- Analyzer
- Vanguard Enforcer
- Enforcer
- Vanguard SecurityCenter
- SecurityCenter
- Vanguard INCompliance
- INCompliance
- Vanguard PasswordReset
- PasswordReset
- Vanguard ez/AccessControl
- ez/AccessControl
- Vanguard ez/SignOn
- ez/SignOn
- Vanguard ez/Integrator
- ez/Integrator
- Vanguard ez/SignOn Deploy
- ez/SignOn Deploy
- Vanguard ez/Token
- ez/Token
- Vanguard Identity Manager
- Quality Security Framework
- Quality Security/390 Suite
- QS/390
- Vanguard Registration Manager
- Registration Manager
- SmartPanel
- SmartLink
- Find-it-Fix-it-Fast
- RiskMinder
- SmartAssist
- eDistribution
- AutoPilot
- QuickGen
- Pathway to Profitability
- Enterprise-Wise
- Knowledge Expo

1.7.2 IBM Trademarks

The following terms are trademarks of the IBM Corporation in the United States and/or other countries:

- ACF/VTAM
- Advanced Function Printing (AFP)
- DFSMS
- DFSMSdfp
- DFSMSdss
- DFSMShsm
- DFSMSrmm
- DFSMSvts
- DFSMS/MVS
- Enterprise Systems Architecture/370
- Enterprise Systems Architecture/390
- ESCON
- ES/9000
- IBM
- IBMLink
- MVS/DFP
- MVS/ESA
- MVS/SP
- PR/SM
- PSF/MVS
- RACF
- Sysplex Timer
- TSO/E
- VTAM
- 3090
- z/OS

2 TOE Description

This section describes the Target of Evaluation (TOE) in terms of the class of product, the operational environment, and the provided security functionality. This chapter provides a general description of the product, which also covers the features that are not part of the evaluated configuration. Features that are not part of the evaluated configuration are explicitly identified as such.

2.1 Product Overview

The Vanguard Enforcer [VEAG] provides administrative support for the IBM Resource Access Control Facility (RACF) Security Server [RACFAG], running on the IBM z/OS V1R6 operating system executing in an abstract machine on an IBM zSeries processor.

The product is intended to provide the following administrative support:

1. Provides automated surveillance and optional control of the z/OS RACF profiles and settings. Enforcer monitors the RACF configuration settings and modifies them (using the RACF SETROPTS command) via the 'Security Server Options Settings'. This includes RACF configuration settings, RACF profile definitions, and select system configurations (APF list, Link List, Program properties table, SVC definitions).

Vanguard Enforcer [VEAG] monitors selected installation defined settings and operating system settings. Should Enforcer detect an exception to a predefined set of settings, it will notify the administrators defined in the Enforcer configuration and optionally take automatic corrective action. When discrepancies are found Enforcer will perform one or more of the following operations:

1. Log the discrepancy.
2. Notify pre-determined administrators of the discrepancy.
3. Optionally take automatic corrective action to restore the system to the baseline configuration, where a “baseline” is a set of the values that represent the system settings in the correct configuration.

Vanguard Enforcer is accessed via the following interfaces:

1. z/OS Operator Console
    a. The MVS operator command interface is used to start, stop and modify the operating characteristics of Enforcer.

.

2. Interactive System Productivity Facility (ISPF) Interface
    a. The ISPF interface allows the administrator to perform the operations needed to configure Enforcer. The privileges required are:
        1. At least READ authority to the data set containing the Vanguard date code information.
        2. At least the ability to create a data set that will contain the Enforcer Baseline information. Normally, this would be:
            1. ALTER authority in the case of a generic profile that covers the Enforcer Baseline data set or at least CREATE authority in the group that is the high-level qualifier of the Enforcer Baseline data set or at least UPDATE authority to an existing Enforcer Baseline data set.
            2. At least READ access to the data sets needed for ISPF access to the various Enforcer ISPF dialogs.

2.2 TOE Overview

The TOE is comprised of startup code, Option Interface code, Sensor code, Vanguard Date Code Software, and guidance documentation. The TOE intended use is as an audit tool in an IBM zSeries z/OS system.

The Sensor Task is used to monitor the system wide options and the RACF security server database, detect changes to selected profiles, and by default, rollback changes, where possible, to the settings contained in a data set that is generated specifically to establish a “baseline” set of the values that represent the system settings in the correct configuration.

Multiple TOE Sensor Tasks (or sessions) may be run concurrently; however, each must maintain its own required baseline data set. Figure 1 below shows only one Sensor Task, as all TOE Sensor tasks act independently without knowledge of or communication to others. The administration of multiple TOE Sensor tasks must ensure each is monitoring different aspects of the system and overlap is eliminated.

The TOE software is comprised of the following major components:

1. Startup and Option Interface Components
    a. Enforcer REXX execs (Restructured Extended Executor executable code)
    b. Enforcer ISPF Dialogs
2. Sensor Component
    a. The Sensor Task
3. Vanguard Date Code Software

The TOE requires that Vanguard Date Code Software validate the Enforcer software license prior to and during execution, and although it is part of the TOE, it has no security functionality.

The TOE guidance is comprised of the following:

- [VEAG] - Vanguard Enforcer™ Administrator Guide
- [VEIGS] - Vanguard Security Solutions™ Installation Guide
- [VECC] - Vanguard Enforcer™ Secure Installation and Operations for Common Criteria
- [VECCL] – Vanguard Enforcer™ Cover Letter for Common Criteria

Figure 1 - TOE and TOE Environment shows the major components of TOE software within its intended environment, although it is not intended to be a detailed representation of the product, but is intended to show the general structure only.

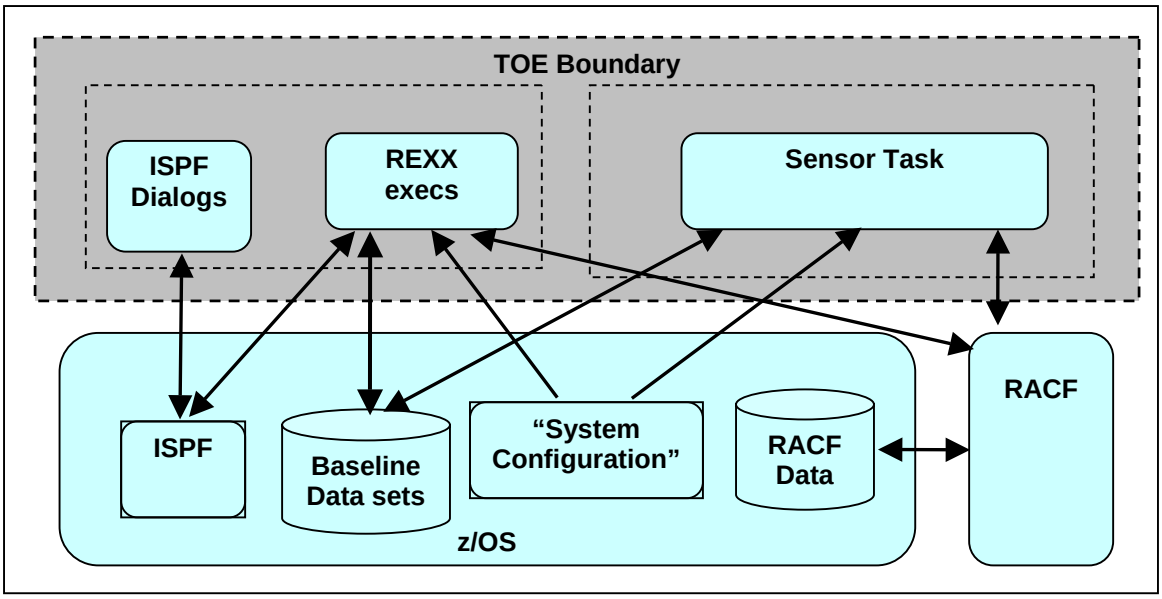

Figure 1 - TOE and TOE Environment

The TOE Environment is comprised of the IBM zSeries z/Operating System and IBM zSeries RACF Security Server. The TOE environment provides storage for the baseline data sets, the RACF data set, and the security functions to prevent bypass and/or corruption of the TOE. The Baseline Data sets in Figure are comprised of the following:

- Enforcer data set
- VANOPTS Library data set

The Enforcer data set is a collection of information from RACF configuration settings and profiles read from the RACF database as well as information from certain system configuration data sets, including APF lists, Link List, Program properties table and SVC definitions.

The VANOPTS Library data set contains:

- Notification data for email and TSO send
- Pathname strings for log data sets
- Name of the SMTP server

The block "System Configuration" in Figure 1 refers to any of the following:

- Current Authorized Program Facility (APF) data set definitions
- Current LNKLST (Link List) definitions
- Current (Link Pack Area) LPA definitions
- Current Supervisor call (SVC) definitions
- Current Program Properties Table (PPT) definitions
- DASD volume definitions (UCB - Unit Control Block)
- Information from system operator commands:
    - System Managed Storage (SMS) configuration information
    - RACF Remote Sharing Facility (RRSF) configuration information
    - System log recording data set for both software and hardware exceptions (LOGREC) information
    - System Management Facility (SMF) data set information
    - Unix System Services file system names

- Paging system data set names
- System DUMP data set names
- WLM (Workload Manager) configuration data set names

The RACF data set is maintained by RACF and shown for clarity, no assumptions are made for this database.

2.2.1 Startup and Option Interface Components

The TOE is started using Job Control language (JCL) that may be generated using the Enforcer ISPF Panel Interface “Options” menu. This JCL contains all information necessary to start/operate the started tasks, such as the location of the load modules, the location of necessary data sets, and options libraries.

The REXX code is invoked from normal ISPF services to do the following:

- Display the various ISPF panels associated with configuring the Enforcer Sensor task
- Invoke other REXX execs that interact with various system and RACF commands to retrieve RACF and system data set information that will be placed in the Enforcer Baseline data set.

The initial startup of the TOE requires a “baseline” data set be generated using the ISPF panel interface. This baseline is a collection of information from Resource Access Control Facility (RACF) configuration settings and profiles read from the RACF database as well as information from certain system configuration data sets, including APF lists, Link List, Program properties table and SVC definitions. Once this baseline has been generated, it is stored in a z/OS data set for use by the Sensor task.

The Startup and Option Interface Component performs security management functions that are a part of the claimed SFRs.

The Sensor Task is run as a started task, is required to execute as Authorized Program Facility (APF) “Authorized” program. These requirements are specified in the Installation, Generation and Secure Installation guidance.

2.3 Sensor Component

The Sensor task monitors the current state of the RACF database. The Sensor task is comprised of multiple Sensors. A sensor is a function within the Enforcer Sensor started task operation that performs the following basic operations:

- For system sensors (monitoring e.g., APF (Authorized Program Facility data set(s)), LNKLST (Link List data sets), LPA (Link Pack Area data sets), PPT (Program Properties Table), SVC (Supervisor Calls), RACF Security Configuration Options, System Started Task definitions) information is retrieved from the z/OS system and RACF using standard interfaces documented by IBM. This information is then compared with the Enforcer Baseline information.
- Installation sensors process installation selectable information related to data sets or RACF General Resource definitions.
- For sensors (both system and installation) that deal with data set and General Resource definition authorities, the Enforcer Baseline information is compared to the RACF Security information For those access list members/identifiers that are group names, the sensor does additional checks for each group member.
- Results from a sensor operation are always sent to the Enforcer LOG plus optional destinations such as Email, TSO SEND, and the Automated Operations Console. The

convention used for a message identifier is to prefix the message with (VEE + a sensor dependent suffix). e.g The Link List message prefix is VEELNK.

Sensors are separated into 'System' and 'Installation' sensors, system sensors are those predetermined by the TOE software and are not changeable by the administrator, installation sensors are those chosen by the administrator of each “installation”. In addition, there is an Access List Expiration Processing sensor that processes the Access Lists of the Data Set and General Resource profiles contained in the Enforcer Baseline.

This ST lists all available installation sensors; however, as stated above, each installation has the option of using these sensors. Sensors perform audit functions that are a part of the claimed SFRs. In the following discussion, **“**Unauthorized” refers to a change made to a RACF profile or system configuration that is not in the Enforcer baseline data set, i.e. a change that was made to a RACF profile or system configuration after the baseline was generated.

The System, Installation and Access List Processing Sensors are:

System Sensors (Predetermined by system):

1. System APF Sensor
   The APF Sensor is used to ensure that additions to or deletions from the system APF list are detected and logged. It also allows an administrator to ensure that all APF libraries are protected. Finally, the APF Sensor is used to ensure that the protection in place for APF libraries does not change. This sensor may make corrections to the RACF profiles but not to the system configurations.
2. System Critical Data Sets Sensor
   The Critical Data Sets Sensor is used to ensure that changes to the security profiles protecting selected data sets are detected and rolled back to the values preserved in the Enforcer baseline data set. The sensor also ensures that changes to selected fields within the protecting profile are detected and rolled back to the values preserved in the Enforcer baseline data set. This provides the administrator a reassurance and constant audit presence to detect changes that have occurred accidentally.
3. System Link List Sensor
   The Link List Sensor is used to ensure that unauthorized changes made to the system link list are detected and rolled back to the values preserved in the Enforcer baseline data set. In addition, it ensures the libraries that comprise the link list are protected and that the protection in place for those libraries has not changed.
4. System LPA Sensor
   The LPA Sensor is used to ensure that unauthorized changes made to the systems LPA List are detected and rolled back to the values preserved in the Enforcer baseline data set. In addition, it ensures the libraries that comprise the LPA list are protected and that the protection in place for those libraries has not changed.
5. System Privileged Users Sensor
   The Privileged Users Sensor is used to monitor those users that have been defined to RACF with privileges at either the system or the group level. The sensor will ensure that additional users have not been granted privileges not in the Enforcer baseline and that users defined to the baseline have not lost privileges.
6. System Program Properties (PPT) Sensor
   The Program Properties (PPT) Sensor allows the administrator to receive notification in the event that either the programs listed in the program properties table or the attributes of those programs have changed. Enforcer provides continuous monitoring which helps to ensure overall system security and integrity. This sensor does not make corrections to the Program Properties Table (PPT) information; the only action taken is to provide notifications.
7. System Security Server Options Sensor

The Security Server Options Sensor is used to maintain control of the Security Server's options that can be set using the RACF SETROPTS command. The SETROPTS parameters are divided into six groups that allow the user to select the level of compliance that the Enforcer Security Server Options sensor will provide.

8. System Started Task Sensor
   The Started Task Sensor is used to maintain control of the list of started procedures defined to RACF via the STARTED General Resource class or the started procedure table. For the purpose of this ST, a started procedure and started task are identical references.
9. System SVC Sensor
   The SVC Sensor is used to ensure that the SVCs on the system have not been activated or deactivated. It also monitors whether the SVC requires the calling program to be APF authorized.

Installation Sensors (Administrator decides what to check):

1. Installation Critical General Resource Profiles Sensor
   The Installation Critical General Resource Profiles Sensor can be used to ensure that the security profiles protecting selected general resources have not changed. The sensor also ensures that selected fields within the profile have not been altered form the values saved in the baseline. This provides the administrator a reassurance and constant audit presence to detect changes that have occurred.
2. Installation Restricted Utilities in Link List Sensor
   The Restricted Utilities in Link List Sensor allows the administrator to receive notification in the event that a program become generally available, i.e. it is no longer maintained under RACF program control. This sensor does not make corrections to the profiles; the only action taken is to provide notifications.
3. Installation Critical DASD Volumes Sensor
   The Installation Critical DASD Volume Sensor allows the user to specify volumes considered critical for the installation. The sensor allows the administrator to receive notification in the event that a data set on those volumes are no longer RACF protected with appropriate Universal Access (less than UPDATE) or that the data sets are not included in the Installation Critical Data Sets Baseline.
4. Installation Critical Groups Sensor
   The Installation Critical Groups Sensor can be used to ensure that the group level administrative span of control has not changed. It also ensures that the list of users connected to the group has not been altered.
5. Installation Critical Data Set Profiles Sensor
   The Installation Critical Data Sets Profiles Sensor can be used to ensure that changes to the security profiles protecting installation-selected data sets are detected and rolled back to the values preserved in the Enforcer™ baseline data set. The sensor also ensures that changes to selected fields within the protecting profile are detected and rolled back to the values preserved in the Enforcer™ baseline data set. This provides the administrator a reassurance and constant audit presence to detect changes that have occurred accidentally.

Access List Expiration Processing Sensor (administrator decides what to check):

1. Expiration Processing for Data Set Access Lists
   This portion of the Access List Expiration Processing sensor allows the administrator to set expiration dates for zero or more of the Access List entries associated with data set profiles contained in Baseline members associated with data sets. This processing is applicable to the data set profiles associated with the System and Installation sensors.
2. Expiration Processing for General Resource Access Lists
   This portion of the Access List Expiration Processing sensor allows the administrator to set expiration dates for zero or more of the Access List entries associated with General Resource profiles contained in Baseline members associated with General Resources. .

This processing is applicable to the General Resource profiles associated with the System and Installation sensors.

The Sensor task monitors the RACF database by making RACF queries for current profile information and information about the current state of the RACF configuration, compares to a known baseline, detects differences between these and takes action based on the profile and action designated in options. The sensor task also monitors that the definition of APF libraries, Link List libraries, the Program Properties table and SVC definitions do not change; these are not stored in the RACF database

If a delta between the baseline and current RACF database is detected and rollback has been selected, Enforcer uses normal RACF commands to update the RACF database, thus leaving an audit trail if the RACF audit settings are configured appropriately.

The Sensor performs these comparisons:

1. Profile comparison – Profile in both baseline data set and RACF
    a. Profiles inconsistencies are noted or corrected.
2. Forward comparison – A profile is in baseline data set, but not in RACF
    a. A profile was removed from RACF, either noted or profile replaced
3. Backward comparison – A profile is in RACF, but not in baseline data set

An additional function is the Restricted Utility Sensor operation as described below.

The Restricted Utility sensor processes a list of Installation supplied program names (assumed to be in the system link list). This processing is an attempt to load, but not execute, each program name. There is no examination of the possible RACF profiles and access lists that could be associated with the various program names.

The following actions are taken:

- When a load is successful,
    - A message is issued to the Enforcer LOG, and optional other message destinations, that the program is generally available. This assumes that the userid associated with the Enforcer sensor started task has no specific authority to the particular program. This is why the userid associated with the Enforcer sensor started task must not have either the TRUSTED or the PRIVILEGED attribute.
- When a load attempt fails
    - Access to the program is examined and if it is a *not authorized* condition, then it is *assumed* that the correct protection is in place for the program.

2.3.1 Sensor Task Log Functions

The Sensor task creates a log file (Enforcer Log) for all messages generated; it is a fixed size file with time and date encoded into the filename. If the log file does not exist, it is created; if it cannot be created, the Sensor task is terminated. This data set contains all of the messages issued by the Enforcer sensor started task. The Sensor Log functions do not implement any claimed SFRs and do not contribute to the TSF.

If for some reason, the Enforcer Log cannot be created by the Enforcer sensor started task, one or more messages will be issued to the system console and the Enforcer sensor started task will be terminated. Normally the message issued to the system console will also be available using the IBM Spool Display and Search Facility (SDSF) SYSLOG stream. This stream is visible from

an ISPF TSO session, however, there is an IBM system messages exit/definition that can suppress various messages.

If the Enforcer Log data set becomes full a new data set is allocated and if the allocation is successful logging continues. If allocation is unsuccessful, the sensor task will terminate and report to pre-defined e-mail destinations as well as on the system console (SYSLOG). Additionally, if the log file creation fails when a MODIFY command is issued, the Enforcer sensor task is terminated.

The following actions are taken with respect to the message logs:

1. Upon initialization the sensor task outputs messages to the console that contain:
    a. Log file name
    b. Name of options library
    c. Name of baseline data set
    d. Version and release of code
    e. List of currently active sensors
    f. Error messages (if an error occurs during initialization)
2. A log file is always created
    a. Upon initial startup
    b. When the existing log is full, full a new log file is created
    c. If the MODIFY command is issued with the NEWLOG operand

2.4 Subjects, Objects, Security Attributes, TSF and user data

2.4.1 Subjects and users

The TOE does not differentiate roles but depends on the profiles set in the RACF Security Server database to enable those individuals that are assigned to perform security administration i.e. those management tasks related to security of the TOE. The OSP set forth in this ST requires that the TOE environment limit access to the TOE to those authorized. Additionally, the TOE itself acts as a subject on behalf of a defined user ID.

2.4.2 Objects

The following are objects the TOE user (administrator or TOE on behalf of the administrator) can operate:

- Management objects
  The TOE processes configuration information stored as part of the baseline data sets maintained by the IT environment.
- Profile Data Objects
  The TOE processes profile data stored in the Enforcer Baseline data set and RACF data set

2.4.3 Security Attributes

The TOE Security Policy depends on the security attributes of the management objects and the security attributes of the profile data. These attributes are those configuration parameters specified under FMT_SMF.1defined in Section 5 for management objects, and the attributes of the profile data as detailed in Tables in Section 6 of this ST.

2.4.4 TSF and User Data

The following TSF data is used by the TOE to make TSP decisions:

- Configuration parameters derived during product installation or administrator interaction stored in the VANOPTS Library data set.
- Profile data stored in the Enforcer baseline data set derived from the RACF Security Server data set and System Configuration.

The TOE does not operate on user data in any form.

2.5 Summary of Security Features

The primary security features of the product are:

- Audit
- Security management

2.5.1 Audit

The TOE provides an audit tool to monitor the security settings of the z/OS RACF Security Server database. Selected security settings of the RACF Security Server database and configuration settings are sampled and compared to a baseline data set, if the monitored settings have been altered, notifications can be sent to selected administrators, and optionally the settings may be automatically returned to the value stored in the baseline data

2.5.2 Security Management

Enforcer provides a set of commands and options to manage the TOE security functions. The TOE does not differentiate roles but depends on the profiles set in the RACF Security Server database to enable those individuals that are assigned to perform security administration i.e. different management tasks related to security of the TOE.

Security administrators may perform the following security management functions:

- Enforcer installation and customization
- Enforcer ISPF panel customization to enable access to Enforcer ISPF dialogs
- Define RACF profiles monitored and if automatic correction is used.
- Determine which sensors are to run and the frequency that they are run
- Manage the selection of notification recipients.
-

2.6 Configurations

2.6.1 Software Configuration

The Target of Evaluation, Vanguard Enforcer Version 7.1.1, requires the following software elements to be installed:

- Vanguard Date Code Software

Additionally, the TOE is required to run on the Common Criteria evaluated configuration of the zSeries operating system as described in [ZOS_ST], restricted to the Discretionary Access Control mode of operation. All required, optional, and restricted software configurations described in that document must be followed.

Vanguard Enforcer Version 7.1.1 includes the following PTFs (Program Temporary Fixes):

VED6306
VED6301
VED6300
VED6299

VED6298
VED6297
VED6296
VED6294
VED6293
VED6291
VED6290
VED6285
VED6284
VED6283
VED6279
VED6277
VED6272
VED6259

2.6.2 TOE Exclusions in the Evaluated Configuration

The following are not supported in the evaluated configuration

- Active Alerts
  - Data Collection Facilities
  - Notification Facilities
- SNMP features of Enforcer
- Enforcer Optional Baseline Build Exits
- Vanguard COPYLIB utility for converting RECFM=FB CLIST and REXX libraries to RECFM=VB libraries

2.6.3 Hardware Configuration

The TOE runs on IBM zSeries hardware running the Common Criteria evaluated configuration of the zSeries operating system as described in [ZOS_ST]. All required, optional, and restricted hardware configurations described in that document must be followed.

3 TOE Security Environment

3.1 Introduction

The statement of TOE security environment describes the security aspects of the environment in which the TOE is intended to be used and the manner in which it is expected to be deployed.
To this end, the statement of TOE security environment identifies the list of assumptions made on the operational environment (including physical and procedural measures) and the intended method of use of the product, defines the threats that the product is designed to counter, and the organizational security policies with which the product is designed to comply.

3.2 Assumptions

This section describes the security aspects of the environment in which the TOE is intended to be used. This includes information about the administrative, physical, personnel, and procedural aspects of the environment.
The TOE is assured to provide effective security measures in a cooperative non-hostile environment only if it is installed, managed, and used correctly. The operational environment must be managed in accordance with user/administrator guidance documentation. The following specific conditions are assumed to exist in an environment where the TOE is employed.

3.3 Administrative Assumptions

Table 2 - Administrative Assumptions

Assumptions	Description
A.MULTIPLE_SENSOR_SESSION	The administration of multiple TOE Sensor sessions must ensure each is session monitors different aspects of the system and that overlap between sessions is eliminated.
A.UNAUTHORIZED_ACCESS	The TOE code, configuration, audit files, log files, and baseline data sets are protected from unauthorized access using the access control functions of the underlying operating system.
A.CAPP_MODE	z/OS as part of the IT environment is operated using only Discretionary Access Control (as defined by the z/OS Security Target); the use of Mandatory Access Control is not allowed.

3.4 Physical Assumptions

The TOE is intended for application in user areas that have physical control and monitoring. It is assumed that the following physical conditions will exist:

Table 3 - Physical Assumptions

Assumptions	Description
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access to the TOE hardware.
A.PROTECT	The TOE software, which is critical to security policy enforcement, will be protected from unauthorized modification.

3.5 Personnel Assumptions

It is assumed that the following personnel conditions will exist:

Table 4 - Personnel Assumptions

Assumptions	Description
A.ADMINISTRATION	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains, however, no assumption is made that an administrator cannot make errors.
A.NO_EVIL_ADM	The personnel responsible for the administration of the TOE are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the administrator documentation.
A.SECURITY_ADMINISTRATOR	There will be an individual assigned to administer TOE security that is different that the individual assigned to administer IT environment security. The intention is to have the administration of TOE security functions separated from that of the IT environment security administration, thereby preventing one administrator from duplicating errors made in the setup of the IT environment RACF database and the TOE baseline data set.

3.6 Procedural Assumptions

The ability of the TOE to enforce the intent of the organizational security policy is dependent upon the establishment of procedures. It is assumed that the following procedural controls exist.

Table 5 - Procedural Assumptions

Assumptions	Description
A.AUTHORIZE	Procedures exist for granting only authorized users access to TOE controls.
A.TIMESTAMP	The environment will provide reliable timestamps.

3.7 Threats

3.8 Threats addressed by TOE

This section describes the threat model for the TOE and identifies the individual threats that are assumed to exist in the TOE environment.

Although administrators of the TOE environment are assumed to be trustworthy, trained and to follow the instructions provided to them with respect to the secure configuration and operation of the systems under their responsibility, there is the possibility of an error being made. An error made in the RACF Security Server or security relevant configuration parameters may allow access to assets otherwise protected by the TOE IT Environment.

The TOE specifically does not counter threats to the TOE Environment by threat agents attempting unauthorized access to assets protected by the IT Environment; the TOE counters the threat of an administrative error that allows unauthorized access to this information

The **assets** to be protected indirectly by the TOE are comprised of information stored and processed by the TOE IT Environment from disclosure, modification, and destruction.

The **threat agent** that the TOE protects against is an administrator that makes an inadvertent error that allows an attack against the TOE Environment to succeed.

3.8.1 Threats to be countered by the TOE

Table 6 – Threats Countered by the TOE

Threat	Description
T.ADMINISTRATIVE_ERROR	Administrators of the TOE IT environment security are assumed trustworthy, trained to follow the instructions provided to them with respect to the secure configuration and operation of the systems under their responsibility. The operating environment of the TOE, z/OS and RACF, is extremely complex and changes to RACF profiles or z/OS system configurations occur on an ongoing daily basis, therefore, there is the possibility of an error being made that is relevant to system security. The purpose of the TOE is to provide a baseline data set of the security settings that can used to make comparisons to RACF profiles and system configurations on an ongoing basis so changes may be detected. The baseline data set and associated parameters need to be managed using the management facilities provide by the TOE.

3.9 Organizational Security Policies (OSP)

An Organizational Security Policy is a set of rules or procedures imposed by an organization using the TOE upon its operations to protect its sensitive data.

3.10 OSP addressed by the TOE

The TOE must comply with the following OSP:

Table 7 - TOE Organizational Security Policy

OSP	Description
P.RACF_MONITOR_ROLLBACK	The RACF Security Server database profiles and select system configurations shall be monitored for changes from the predefined baseline; the default action for detected changes shall be to roll back changes to a known state as defined in the baseline data set.
P.RACF_MONITOR_NOTIFY	The RACF Security Server database shall be monitored for changes from the predefined baseline; notices of detected changes shall be sent to the designated administrator.

3.11 OSP addressed by the TOE environment

The TOE environment must comply with the following OSP:

Table 8 - TOE Environment Organizational Security Policy

OSP	Description
PE.AUTHORIZED_USERS	The TOE environment must ensure only those users who have

OSP	Description
	been authorized to access the information within the system may access the system and the TOE code and configuration data sets are protected from unauthorized access.
PE.AUTHENTICATE	The TOE environment must ensure that all users are identified and authenticated before being granted access to the TOE mediated resources. Such limited access to the TOE is configured by the administrator and should be conformant with the security policies of the organization responsible for the operations of the TOE.
PE.MANAGE	Those responsible for the TOE environment must ensure that the underlying operating system and hardware is configured and managed in a secure way.
PE.INSTALL	Those responsible for the TOE environment must ensure that the TOE is installed in a secure manner, as specified in the Installation, Generation, and Secure Installation guidance.

4 Security Objectives

This section defines the security objectives of the TSF and its supporting environment. Security objectives, categorized as either IT security objectives or non-IT security objectives, reflect the stated intent to counter identified threats, cover assumptions, and/or comply with any organizational security policies identified. All of the identified threats and organizational policies are addressed under one of the categories below.

4.1 TOE Security Objectives

The following are the TOE security objectives:

Table 9 - TOE Security Objectives

Objective	Description
O.RACF.MONITOR	The TOE must monitor selected RACF Security Server settings and selected system configurations for differences with a baseline data set. The selection of the RACF settings and system configurations to be monitored is done by the security administrator.
O.RACF.CORRECT	The TOE must correct selected changes detected between the monitored RACF Security Server profiles, the selected system configurations and the baseline data set by returning to a known state to those profiles and system configurations where possible.
O.RACF.NOTIFY	The TOE must notify the Administrator that changes have been detected between the monitored RACF Security Server profiles or the select system configurations and the baseline data set
O.MANAGE	Those responsible for the TOE must ensure that the TOE is managed in a secure manner, which maintains the security of the TOE, including the TSF data and user data of the TOE, as described in the accompanying Installation, Generation, and Secure Installation guidance.

4.2 TOE Environmental Security Objectives

4.2.1 TOE Operational Environment

Some security needs are beyond the capability of the TOE to satisfy, so the TOE must depend on support from the TOE operational environment. The following environmental security objectives are derived from the TOE's dependencies on its environment.

OE – **O**bjective **E**nvironment

Table 10 - IT Environmental Security Objectives

Objective	Description
OE.AUTHENTICATE	The TOE environment must ensure that all users are identified and authenticated before being granted access to the TOE mediated resources. Such limited access to the TOE is configured by the administrator and should be conformant with the security policies of the organization responsible for the operations of the TOE.
OE.AUTHORIZE	The TOE environment must provide the ability to specify and manage access rights to objects and services by user and system process and the TOE code, configuration, and baseline data sets are protected from unauthorized access. Additionally, the TOE environment must allow the TOE access to the configuration and baseline data sets as well to System

Objective	Description
	Configuration parameters.
OE.MANAGE	The TOE environment must provide the ability to configure and managed the underlying operating system and hardware is in a secure way.
OE.TIMESTAMP	The environment must provide reliable timestamps.

The following are the non-IT security objectives:

Table 11 – Non - IT Environmental Security Objectives

Objective	Description
OE.ADMIN	Those responsible for the administration of the TOE must be trained such that they are capable of managing the TOE security functions; those responsible for managing the TOE environment must ensure the underlying operating system and hardware is configured and managed in a secure way. Administrators are trustworthy.
OE.INSTALL	Those responsible for the TOE must ensure that the TOE is installed in a secure manner, which maintains the security of the TOE, including the TSF data and user data of the TOE as specified in the Installation, Generation, and Secure Installation guidance.
OE.PHYSICAL	Those responsible for the TOE must ensure that the TOE and its underlying hardware and software are physically protected from unauthorized physical access and tampering.
OE.CAPP_MODE	The TOE environment must limit the operating mode to CAPP compliant mode defined in the z/OS Security Target [ZOS_ST].
OE.SECURITY_ADMIN	Those responsible for the TOE must assign an individual to administer TOE security that is different that the individual assigned to administer IT environment security.

5 Security Requirements

This chapter contains the Extended Components Definition as well as the security functional requirements for the TOE, the security assurance requirements for the TOE, and the security functional requirements for the IT environment.

Functional requirement components in this Security Target were drawn from Part 2 of the CC and from the ECD in Section 5.1. CC-defined operations for assignment, selection, and refinement were used to tailor the requirements to the level of detail necessary to meet the stated security objectives.

The following formatting styles have been used for the SFRs:

- **Assignments and selections**: bold text
- **Refinements**: bold and italic text

5.1 Extended Components Definition

5.1.1 FAU_SAA.5-RACF RACF Potential Violation Analysis

Management: FAU_SAA.5-RACF

The following actions could be considered for the management functions in FMT:

a) Maintenance of the rules by (adding, modifying, deletion) of rules from the set of rules

Audit: FAU_SAA.5-RACF

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: Enabling and disabling of any of the analysis mechanisms;

b) Basic: Automated responses performed by the tool.

Hierarchical to: No other components

Dependencies: FPT_STM.1 Reliable time stamps

FAU_SAA.5-RACF.1 The TSF shall be able to apply a set of rules in monitoring RACF profiles and system configurations, and based upon these rules, indicates a potential violation of the TSP.

FAU_SAA.5-RACF.2 The TSF shall enforce the following rules for monitoring RACF profiles and system configurations:

a) Comparison of [assignment: *subset of defined RACF profiles and system configurations*] known to indicate a potential security violation to predefined baseline configuration data;

b) [assignment: *any other rules*].

.

5.2 TOE Security Functional Requirements

Table 12 -Security Functional Requirements of the TOE

Security Functional Class	Security Functional Components
Security Audit (FAU)	FAU_ARP.1 Security audit automatic response FAU_SAA.5-RACF RACF Potential Violation Analysis
Security Management (FMT)	FMT_SMF.1 Specification of Management Functions

5.3 Security audit (FAU)

5.3.1 RACF Potential Violation Analysis (FAU_SAA.5-RACF)

FAU_SAA.5-RACF.1 The TSF shall be able to apply a set of rules in monitoring RACF profiles and system configurations, and based upon these rules, indicates a potential violation of the TSP.
FAU_SAA.5-RACF.2 The TSF shall enforce the following rules for monitoring RACF profiles and system configurations:

a) Comparison of **one or more of the following events as specified by an authorized administrator for each designated active sensor**
   - **a. System APF Sensor**
     a. **Incorrect UACC (greater than READ)**
     b. **Any of the following conditions:**
        1. **A data set found in the in-core APF table NOT specified in the APF Baseline data set.**
        2. **A data set specified in the APF Baseline NOT in the APF Data set Baseline with the same volume specification.**
        3. **A data set specified in the APF Baseline data set NOT cataloged on the volume specified in the APF table.**
        4. **A data set specified in the APF Baseline data set does NOT reside on the volume specified in that baseline.**
        5. **A data set listed in the APF Baseline data set NOT contained in the in-core APF table.**
   - **b. System Critical Data Sets Sensor**
     a. **Incorrect covering profile**
     b. **No covering profile**
     c. **RACF profile attribute incorrect**
     d. **Baseline user not in access list**
     e. **Baseline user has incorrect access,**
     f. **User in access list not in baseline,**
     g. **Global Table access different from profile UACC**
     h. **Global Table access different from baseline UACC**
   - **c. Installation Critical Groups Sensor**
     a. **Superior group changed,**
     b. **Owner changed,**
     c. **User connected to group but not in baseline, or**
     d. **Any of the following conditions:**
        1. **Group profile not found**
        2. **User in baseline but not connected to group**
   - **d. Access List Expiration Processing Sensor**
     a. **Expiration in Expire_Warning_1 option days,**
     b. **Expiration in Expire_Warning_2 option days,**
     c. **Access expired**
   - **e. Installation Critical General Resource Profiles Sensor**
     a. **Covering profile does not exist,**
     b. **UACC incorrect,**

c. **Audit setting incorrect,**
d. **NOTIFY incorrect,**
e. **OWNER incorrect,**
f. **WARNING mode on**
g. **Baseline user has incorrect access,**
h. **User in profile access list but not in baseline or**
i. **Any of the following conditions:**
    1. **Baseline user not in profile access list**
    2. **Global Table access different from profile UACC**

f. System Link List Sensor
a. **Incorrect UACC (greater than READ), or**
b. **Any of the following conditions:**
    1. **LNKLST data set not cataloged**
    2. **Incorrect SMS status**
    3. **LNKLST data set not in Critical Data set Baseline**
    4. **LNKLST data set not marked APF**
    5. **Baseline data set not marked APF**
    6. **Incorrect volume for data set in Critical Data set Baseline**
    7. **LNKLST data set out of sequence**
    8. **Global table grants access greater than READ**
    9. **Global table grants access different from profile UACC**

g. System LPA Sensor
a. **UACC is incorrect, or**
b. **Any of the following conditions for each LPA list data set:**
    1. **Not cataloged**
    2. **Not SMS**
    3. **Not in LPA table**
    4. **Not in baseline**
    5. **Not in Critical Data set Baseline**
    6. **Incorrect volume in Critical Data set Baseline**

h. System Program Properties (PPT) Sensor
a. **For all detected changes**

i. System Privileged Users Sensor
a. **User has unauthorized RACF system privilege (user in baseline),**
b. **Unauthorized User has RACF system privilege (user not in baseline),**
c. **User has unauthorized RACF group privilege (user in baseline),**
d. **Unauthorized User has RACF group privilege (user not in baseline), or**
e. **Any of the following conditions:**
    1. **User lost RACF authorized system privilege**
    2. **User lost RACF authorized group privilege**

j. Installation Restricted Utilities in Link List Sensor
a. **Any monitored program is generally accessible**

k. System Security Server Options Sensor
a. **Setting of the current Security Server option does not match the setting found in the baseline,**

l. System Started Task Sensor
a. **Started Procedure user ID has a RACF User profile TSO segment,**
b. **Started Procedure user ID is not connected to the RACF started task group,**
c. **Started procedure is defined in the STARTED class and has gained the trusted or privileged or trace attribute,**
d. **User id associated with a started procedure defined in STARTED class has changed,**

e. **Group associated with a started procedure defined in STARTED class has changed, or**
f. **Any of the following conditions:**
1. **Started Procedure definition not in baseline**
2. **Baseline Started Procedure not defined to system**

m. System SVC Sensor
a. **SVC active when baseline indicates inactive, or**
b. **Any of the following conditions:**
1. **SVC inactive when baseline indicates active**
2. **SVC requires APF authorization when baseline indicates no APF authorization required**
3. **SVC does not require APF authorization when baseline indicates APF authorization required**

n. Installation Critical DASD Volumes Sensor
a. **Any of the following conditions for each critical volume:**
1. **the DATA SET profile protecting the data set has a UACC greater than READ**
2. **the SMS status of a data set on the volume does not match the baseline**
3. **the VSAM status of a data set on the volume does not match the baseline**

o. Installation Critical Data Set Profiles Sensor
a. **Incorrect covering profile**
b. **No covering profile**
c. **RACF profile attribute incorrect**
d. **Baseline user not in access list**
e. **Baseline user has incorrect access,**
f. **User in access list not in baseline,**
g. **Global Table access different from profile UACC**
h. **Global Table access different from baseline UACC**

known to indicate a potential security violation to predefined baseline configuration data;

b) **None**

Application Note: For this security function, an event is defined as the results of a comparison made at a point in time. The time period between comparisons is configurable for each sensor.

Application Note: For this security function, **"**unauthorized" refers to a change made to a RACF profile or system configuration that is not in the Enforcer baseline data set, i.e. a change that was made to a RACF profile or system configuration after the baseline was generated.

5.3.2 Security audit automatic response in Sensor (FAU_ARP.1)

FAU_ARP.1.1 The TSF shall take **the following action (corresponding to the detected non-conformities between monitored profiles and configurations as specified in FAU_SAA.5-RACF and predefined baseline configurations) for each designated active sensor**

a) **System APF Sensor**
a. If covered by a fully qualified generic or a discrete profile then the UACC is set to READ, otherwise create a new fully qualified generic profile. The profile fields are set according to the baseline data sets and the UACC set to READ, and write a VEEAPF error message to the sensor log

b. Write a VEEAPF error message to the sensor log and (optionally) send notification(s) to selected administrator(s).

b) **System Critical Data Sets Sensor**
   a) **Write a VEECDC error message to the sensor log**
   b) **Create a DATA SET profile with the profile fields set according to the baseline data sets and write a VEECDC error message to the sensor log**
   c) **Alter the RACF profile to correct the attribute, and write a VEECDC error message to the sensor log**
   d) **Write an error to the Sensor log, and write a VEECDC error message to the sensor log**
   e) **Correct the access level in the access list, and write a VEECDC error message to the sensor log**
   f) **Remove the user from the access list, and write a VEECDC error message to the sensor log**
   g) **Write an error message to the Sensor log, and write a VEECDC error message to the sensor log**
   h) **Write a VEECDC error message to the sensor log and (optionally) send notification(s) to selected administrator(s).**

c) **Installation Critical Groups Sensor**
   a) **Reset the Superior Group to the baseline value, and write an error to the Sensor log**
   b) **Reset the owner to the baseline value, and write an error to the Sensor log**
   c) **Remove the user from the group, and write an error to the Sensor log**
   d) **Write error to Sensor log and (optionally) send notification to selected administrator(s).**

d) **Access List Expiration Processing Sensor**
   a) **Issue a message to the predefined administrator(s) via TSO SEND, and write an error to the Sensor log**
   b) **Issue a message to predefined administrator(s) via the TSO SEND command, and write an error to the Sensor log**
   c) **Issue a RACF PERMIT DELETE command, optionally, based on the Expire_Notice option, issue a message to predefined administrator(s) via the TSO SEND command, and write an error to the Sensor log**

e) **Installation Critical General Resource Profiles Sensor**
   a) **Create a new profile and setting all checked attributes including the access list to baseline values, and write an error to the Sensor log and (optionally) send notification to selected administrator(s).**
   b) **Set the correct UACC in the profile, and write an error to the Sensor log and (optionally) send notification to selected administrator(s).**
   c) **Set the correct audit values in the profile, and write an error to the Sensor log and (optionally) send notification to selected administrator(s).**
   d) **Set the correct NOTIFY value in the profile, and write an error to the Sensor log and (optionally) send notification to selected administrator(s).**
   e) **Set the correct OWNER value in the profile, and write an error to the Sensor log and (optionally) send notification to selected administrator(s).**
   f) **Turn off WARNING mode in the profile, and write an error to the Sensor log and (optionally) send notification to selected administrator(s).**
   g) **Correct the access level in the profile access list, and write an error to the Sensor log and (optionally) send notification to selected administrator(s).**
   h) **Remove the user/group from the profile access list if not:**
      a) **Connected to a started task group or**
      b) **One of the started task groups or**
      c) **A userid that has the PROTECTED attribute or**
      d) **A userid that is a member of one of the started task groups**

and write an error to the Sensor log and (optionally) send notification to selected administrator(s).

i) **Write an error message to the Sensor log and (optionally) send notification to selected administrator(s).**

f) **System Link List Sensor**
   a) **If the profile is a discrete or fully qualified generic then correct the profile UACC else add a new fully qualified generic profile with the correct UACC, and write an error to the Sensor log**
   b) **Write an error to Sensor log and (optionally) send notification to selected administrator(s).**

g) **System LPA Sensor**
   a) **If the profile is a discrete or fully qualified generic then alter the profile UACC; else add a new fully qualified profile setting the profile fields from the values in the baseline data sets including the UACC, write an error to the Sensor log and (optionally) send notification to selected administrator(s)**
   b) **Write an error message to the Sensor log and (optionally) send notification to selected administrator(s)**

h) **System Program Properties (PPT) Sensor**
   a) **Write an error message to the Sensor log and (optionally) send notification to selected administrator(s).**

i) **System Privileged Users Sensor**
   a) **Remove any unauthorized system privilege from the user, write an error to the Sensor log and (optionally) send notification to selected administrator(s)**
   b) **Remove any unauthorized system privilege from the user, write an error to the Sensor log and (optionally) send notification to selected administrator(s).**
   c) **Remove any unauthorized group privilege, write error to Sensor log and (optionally) send notification to selected administrator(s).**
   d) **Remove any unauthorized group privilege, write an error to the Sensor log and (optionally) send notification to selected administrator(s).**
   e) **Write an error to the Sensor log and (optionally) send notification to selected administrator(s).**

j) **Installation Restricted Utilities in Link List Sensor**
   a) **Write an error to the Sensor log and (optionally) send notification to selected administrator(s).**

k) **System Security Server Options Sensor**
   a) **Issue the SETROPTS command to change the option to the baseline value, write error to Sensor log and (optionally) send notification to selected administrator(s).**

l) **System Started Task Sensor**
   a) **Remove the TSO segment from the profile, write an error to the Sensor log, and (optionally) send notification to selected administrator(s).**
   b) **Connect the user to started task group, write an error to Sensor log, and (optionally) send notification to selected administrator(s).**
   c) **Remove the attribute from the profile, write an error to the Sensor log, and (optionally) send notification to selected administrator(s).**
   d) **Correct the user id in the STDATA segment of the STARTED class profile, write an error to the Sensor log, and (optionally) send notification to selected administrator(s).**
   e) **Correct the group id defined in the STDATA segment of the STARTED class profile, write an error to the Sensor log, and (optionally) send notification to selected administrator(s).**

f) **Write an error to the Sensor log and (optionally) send notification to selected administrator(s).**

m) **System SVC Sensor**
   a) **Alter the SVC table to invoke IGCERROR and write an error to the Sensor log and (optionally) send notification to selected administrator(s)**
   b) **Write an error to the Sensor log and (optionally) send notification to selected administrator(s).**

n) **Installation Critical DASD Volumes Sensor**
   a) **Write an error to the Sensor log and (optionally) send notification to selected administrator(s).**

o) **Installation Critical Data Set Profiles Sensor**
   a) **Write a VEECDC error message to the sensor log**
   b) **Create a DATA SET profile with the profile fields set according to the baseline data sets , and write a VEECDC error message to the sensor log**
   c) **Alter the RACF profile to correct the attribute, and write a VEECDC error message to the sensor log**
   d) **Write an error to the Sensor log, and write a VEECDC error message to the sensor log**
   e) **Correct the access level in the access list, and write a VEECDC error message to the sensor log**
   f) **Remove the user from the access list, and write a VEECDC error message to the sensor log**
   g) **Write an error to the Sensor log, and write a VEECDC error message to the sensor log**
   h) **Write a VEECDC error message to the sensor log and (optionally) send notification(s) to selected administrator(s).**

upon detection of a potential security violation.

Application Note: For this security function**, "**unauthorized" refers to a change made to a RACF profile or system configuration that is not in the Enforcer baseline data set, i.e. a change that was made to a RACF profile or system configuration after the baseline was generated.

5.4 Security Management (FMT)

5.4.1 FMT_SMF.1 Specification of Management Functions

.

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

- **Enforcer customization (VANOPTS Library data set)**
- **Define and select RACF profiles monitored (Enforcer baseline data set)**
- **Select or deselect options for automatic RACF profile correction (Enforcer baseline data set)**
- **Select notification recipients (VANOPTS Library data set)**

Application Note: Management functions are administered using the ISPF panel interface or z/OS console, either during installation of the TOE or during its operation. The parameters are stored either in the VANOPTS Library data set or in the Enforcer baseline data set.

5.5 TOE Environment Security Functional Requirements

The SFRs for the TOE environment have to be satisfied by the TOE environment. They have all been taken from CC part 2 [CC]. Where appropriate, the SFRs have been rephrased to clearly indicate that the TOE environment (not the TOE) must meet the requirements. This is allowed and described in Part 1, B.2.6 and C 2.6, as "a special kind of refinement and not subject to the assessment requirements associated with modified CC components".

As explained in section 2.4.3 this evaluation of Vanguard Enforcer is based on the use of z/OS V1R6 operating in CAPP mode as the operating system in the TOE environment. The LSPP mode of operation is not allowed. The security functional requirements for the IT environment are to a large part addressed by the operating system under which the evaluated version of Enforcer is installed.

In the case of z/OS V1R6 all security functional requirements for the IT environment have been subject to the Common Criteria evaluation

The following formatting styles have been used for the SFRs:

- **Assignments and selections**: bold text,
- **Refinements**: bold and italic text,
- **Special kind of refinements (SFR re-phrasing, see above)**: italic text.

Table 13 - Security Functional Requirements of the TOE Operational Environment

Security Functional Class	Security Functional Components
User Data Protection (FDP)	FDP_ACC.1: Subset access control FDP_ACF.1: Security attribute based access control
Identification and Authentication (FIA)	FIA_UAU.1: Timing of authentication FIA_UID.1: Timing of identification
Security Management (FMT)	FMT_MSA.1: Management of security attributes FMT_MSA.3: Static Attribute Initialization FMT_SMF.1: Specification of management functions FMT_SMR.1: Security roles
Protection of the TSF (FPT)	FPT_SEP.1 Domain Seperation FPT_STM.1 Reliable Time Stamps

5.6 User Data Protection (FDP)

5.6.1 Subset access control (FDP_ACC.1)

FDP_ACC.1.1 The *IT environment* shall enforce the **user access control SFP** on **user access**.

Application note: This is the protection provided by the operating system (part of TOE environment) assuring that only authorized users may access the TOE.

5.6.2 Security attribute based access control (FDP_ACF.1)

FDP_ACF.1.1 The *IT environment* shall enforce the **user access control SFP** to objects based on the following:

access rights as security attributes for users as subject and TOE code, TSF data, TOE services, buffer space memory, and data sets as objects.

FDP_ACF.1.2 The *IT environment* shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

By default, access to the objects must be denied. Only explicitly authorized subjects may access the objects.

FDP_ACF.1.3 The *IT environment* shall explicitly authorize access of subjects to objects based on the following additional rules:

none.

FDP_ACF.1.4 The *IT environment* shall explicitly deny access of subjects to objects based on the **following rules:**

none.

Application note: The IT environment is left freedom on how to fulfill the needed security functionality.

5.7 Identification and Authentication (FIA)

5.7.1 Timing of authentication (FIA_UAU.1)

FIA_UAU.1.1 The *IT environment* shall allow ***no execution of a program or command for all users except pseudo-users of Started Procedures (Tasks)*** on behalf of the user to be performed before the user is authenticated.

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

5.7.2 Timing of identification (FIA_UID.1)

FIA_UID.1.1 The *IT environment* shall allow ***no TSF-mediated actions*** on behalf of the user to be performed before the user is identified.

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

5.8 Security Management (FMT)

5.8.1 Management of Security Attributes (FMT_MSA.1)

FMT_MSA.1.1 The *IT environment* shall enforce the **access control SFP** to restrict the ability to **modify** the ***access control attributes*** **associated with a named object** to **users with the SPECIAL attribute or the appropriate group-SPECIAL attribute, users who have ALTER authority to the object and the owner of the resource profile of the named object.**

5.8.2 Static Attribute Initialization (FMT_MSA.3)

FMT_MSA.3.1 The *IT environment* shall enforce the ***access control SFP*** to provide ***restrictive*** default values for security attributes that are used to enforce the ***SFP***.

FMT_MSA.3.2 The *IT environment* shall allow the ***users with the SPECIAL attribute and the owner of the profile protecting the object*** to specify alternative initial values to override the default values when an object or information is created.

5.8.3 Specification of management functions (FMT_SMF.1)

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

- **object security attributes management**
- **user security attribute management**
- **authentication data management**

5.8.4 Security roles (FMT_SMR.1)

FMT_SMR.1.1 The *IT environment* shall maintain the roles **User, Administrator, and Security Administrator**.

FMT_SMR.1.2 The *IT environment* shall be able to associate users with roles.

Application Note: The requirement for a security administrator is made to separate the duties of a normal administrator that administrates RACF from that of a security administrator. This distinction is made such that the person administrating the RACF database is not the same as the administrator of the TOE (security administrator). In this manner, errors made by the normal administrator can be countered by the TOE, otherwise, errors made in the RACF database may be replicated in the TOE baselines.

5.9 Protection of the TSF

5.9.1 Domain Seperation (FPT_SEP.1)

FPT_SEP.1.1 The *IT environment* shall maintain a security domain for *the TSF's* execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The *IT environment* shall enforce separation between the security domains of subjects in the TSC.

Application Note: The second refinement in FPT_SEP.1.1 from "its own" to "the TSF's" is needed because of the SFR rephrasing which refines "TSF" to "IT environment". The SFR states that the IT environment (namely the product deploying the TOE) is required to protect the TOE.

5.9.2 Reliable Time Stamps (FPT_STM.1)

FPT_STM.1.1 The *IT environment* shall be able to provide reliable time stamps for *the TSF's* use.

Application Note: The second refinement in FPT_STM.1.1 from "its own" to "the TSF's" is needed because of the SFR rephrasing which refines "TSF" to "IT

environment". The SFR states that the IT environment (namely the product deploying the TOE) is required to protect the TOE.

5.10 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the Evaluation Assurance Level 3 components as specified in [CC] part 3 augmented by ALC_FLR.1. No operations are applied to the assurance components.

6 TOE Summary Specification

6.1 TOE Security Functions

6.1.1 Introduction

This chapter describes the security functions of Vanguard Enforcer that are subject to this evaluation.

6.1.2 Audit (F.AU)

The TOE provides a mechanism that monitors the security status of an IBM z/OS system that is using a RACF Security Server.

6.1.2.1 Sensor violation analysis and automatic response (F.AU.1)

The TOE monitors the RACF Security Server database for security relevant events that may result in potential security violations. If a potential violation is detected, the default action taken is to set a secure state as specified by the security administrator as well as sending notifications to security administrators. The areas monitored are referred to as sensors.

The following sensors are monitored for the listed violations.

Table 14 - Sensor violation analysis and automatic response TSF

TSF	Security Attribute	Required automatic response
System APF Sensor		
F.AU.1.1.1	Incorrect UACC	If covered by a fully qualified generic or a discrete profile then the UACC is set to READ, otherwise a new fully qualified generic profile is created with the UACC set to READ, and write VEEAPF error message to sensor log and (optionally) send notification to selected administrator(s).
F.AU.1.1.2	A data set found in the in-core APF table NOT specified in the APF Baseline data set.	Write VEEAPF error message to sensor log and (optionally) send notification to selected administrator(s).
F.AU.1.1.3	A data set specified in the APF Baseline NOT in the APF Data set Baseline with the same volume specification.	Write VEEAPF error message to sensor log and (optionally) send notification to selected administrator(s).
F.AU.1.1.4	A data set specified in the APF Baseline data set NOT cataloged on the volume specified in the APF table.	Write VEEAPF error message to sensor log and (optionally) send notification to selected administrator(s).
F.AU.1.1.5	A data set specified in the APF Baseline data set does NOT reside on the volume specified in that baseline	Write VEEAPF error message to sensor log and (optionally) send notification to selected administrator(s).
F.AU.1.1.6	A data set listed in the APF Baseline data set NOT contained in the in-core APF table.	Write VEEAPF error message to sensor log and (optionally) send notification to selected administrator(s).
System Critical Data Sets Sensor		

TSF	Security Attribute	Required automatic response
F.AU.1.2.1	Incorrect covering profile	Write VEECDC error message to sensor log and (optionally) send notification to selected administrator(s).
F.AU.1.2.2	No covering profile	Add profile, write VEECDC error message to sensor log and (optionally) send notification to selected administrator(s).
F.AU.1.2.3	RACF profile attribute incorrect	Change attribute, write VEECDC error message to sensor log and (optionally) send notification to selected administrator(s).
F.AU.1.2.4	Baseline user not in access list	Write error to sensor log, write VEECDC error message to sensor log and (optionally) send notification to selected administrator(s).
F.AU.1.2.5	Baseline user has incorrect access,	Correct access level in access list, write VEECDC error message to sensor log and (optionally) send notification to selected administrator(s).
F.AU.1.2.6	User in access list not in baseline,	Remove user from access list, write VEECDC error message to sensor log and (optionally) send notification to selected administrator(s).
F.AU.1.2.7	Global Table access different from profile UACC	Write error to sensor log, write VEECDC error message to sensor log and (optionally) send notification to selected administrator(s).
F.AU.1.2.8	Global Table access different from baseline UACC	Write VEECDC error message to sensor log and (optionally) send notification to selected administrator(s).
Installation Critical Groups Sensor		
F.AU.1.3.1	Superior group changed,	Reset Superior Group to baseline value, write VEECGC error message to sensor log and (optionally) send notification to selected administrator(s).
F.AU.1.3.2	Owner changed,	Reset owner to baseline value, write VEECGC error message to sensor log and (optionally) send notification to selected administrator(s).
F.AU.1.3.3	User connected but not in baseline	Remove user from group, write VEECGC error message to sensor log and (optionally) send notification to selected administrator(s).
F.AU.1.3.4	RACF profile not found for group	Write VEECGC error message to sensor log and (optionally) send notification to selected administrator(s).
F.AU.1.3.5	User in baseline but not connected	Write VEECGC error message to sensor log and (optionally) send notification to selected administrator(s).
Access List Expiration Processing Sensor		
F.AU.1.4.1	Expiration in Expire_Warning_1 option days,	Writes VEEEXP Enforcer LOG data set, and optionally writes the following: • TSO SEND messages to userids • Console messages for use by an automated operations processing program
F.AU.1.4.2	Expiration in Expire_Warning_2 option days,	Writes VEEEXP Enforcer LOG data set, and optionally writes the following: • TSO SEND messages to userids • Console messages for use by an automated operations processing

TSF	Security Attribute	Required automatic response
		program
F.AU.1.4.3	Access expired	Issue permit delete, writes VEEEXP Enforcer LOG data set, and optionally writes the following: • TSO SEND messages to userids • Console messages for use by an automated operations processing program
Installation Critical General Resource Profiles Sensor		
F.AU.1.5.1	Covering profile does not exist,	Add profile, write VEEGRC error message to sensor log and (optionally) send notification to selected administrator(s).
F.AU.1.5.2	UACC incorrect,	Set correct UACC, write VEEGRC error message to sensor log and (optionally) send notification to selected administrator(s).
F.AU.1.5.3	Audit setting incorrect,	Set correct audit values, write VEEGRC error message to sensor log and (optionally) send notification to selected administrator(s).
F.AU.1.5.4	NOTIFY incorrect,	Set correct NOTIFY value, write VEEGRC error message to sensor log and (optionally) send notification to selected administrator(s).
F.AU.1.5.5	OWNER incorrect,	Set correct OWNER value, write VEEGRC error message to sensor log and (optionally) send notification to selected administrator(s).
F.AU.1.5.6	WARNING mode on	Turn off WARNING mode, write VEEGRC error message to sensor log and (optionally) send notification to selected administrator(s).
F.AU.1.5.7	Baseline user has incorrect access,	Correct the access level in the access list, write VEEGRC error message to sensor log and (optionally) send notification to selected administrator(s).
F.AU.1.5.8	User/group in access list not in baseline	Remove the user/group from the profile access list if not: • Connected to a started task group or • One of the started task groups or • A userid that has the PROTECTED attribute or • A userid that is a member of one of the started task groups Write VEEGRC error message to sensor log and (optionally) send notification to selected administrator(s).
F.AU.1.5.9	Baseline user not in access list	Write VEEGRC error message to sensor log and (optionally) send notification to selected administrator(s).
F.AU.1.5.10	Global Table access different from UACC	
System Link List Sensor		
F.AU.1.6.1	Incorrect UACC	If profile is discrete or fully qualified generic, then correct the UACC, else add fully qualified generic profile with the correct UACC, write VEELNK error message to sensor log and (optionally) send notification to selected administrator(s).

TSF	Security Attribute	Required automatic response
F.AU.1.6.2	Not cataloged	Write VEELNK error message to sensor log and (optionally) send notification to selected administrator(s).
F.AU.1.6.3	Incorrect SMS status	
F.AU.1.6.4	LNKLST data set not in Critical Data set Baseline	
F.AU.1.6.5	LNKLST data set not marked APF	
F.AU.1.6.6	Baseline data set not marked APF	
F.AU.1.6.7	Incorrect volume for data set in Critical Data set Baseline	
F.AU.1.6.8	LNKLST data set out of sequence	
F.AU.1.6.9	Global table grants access greater than READ	
F.AU.1.6.10	Global table grants access different from profile UACC	
System LPA Sensor		
F.AU.1.7.1	UACC incorrect	If profile is discrete or fully qualified, alter the UACC; else add fully qualified profile and alter UACC, write VEELPA error message to sensor log and (optionally) send notification to selected administrator(s).
F.AU.1.7.2	LPA list data set not cataloged	Write VEELPA error message to sensor log and (optionally) send notification to selected administrator(s).
F.AU.1.7.3	LPA list data set not SMS	
F.AU.1.7.4	LPA list data set not in LPA table	
F.AU.1.7.5	LPA list data set not in baseline	
F.AU.1.7.6	LPA list data set not in Critical Data	
F.AU.1.7.7	LPA list data set has incorrect volume in Critical Data set Baseline	
System Program Properties (PPT) Sensor		
F.AU.1.8.1	For all detected changes	Write VEEPPT error message to sensor log and (optionally) send notification to selected administrator(s).
System Privileged Users Sensor		
F.AU.1.9.1	User has unauthorized system privilege (user in baseline),	Remove any unauthorized system privilege, write VEEPUC error message to sensor log and (optionally) send notification to selected administrator(s).
F.AU.1.9.2	Unauthorized User has system privilege (user not in baseline),	Remove any unauthorized system privilege, write VEEPUC error message to sensor log and (optionally) send notification to selected administrator(s).
F.AU.1.9.3	User has unauthorized group privilege (user in baseline),	Remove any unauthorized group privilege, write VEEPUC error message to sensor log and (optionally) send notification to selected administrator(s).
F.AU.1.9.4	Unauthorized User has group privilege (user not in baseline), or	Remove any unauthorized group privilege, write VEEPUC error message to sensor log and (optionally) send notification to selected

TSF	Security Attribute	Required automatic response
		administrator(s).
F.AU.1.9.5	User lost authorized system privilege	Write VEEPUC error message to sensor log and (optionally) send notification to selected administrator(s).
F.AU.1.9.6	User lost authorized group privilege	
Installation Restricted Utilities in Link List Sensor		
F.AU.1.10.1	If any monitored program is generally accessible	Write VEERUS error message to sensor log and (optionally) send notification to selected administrator(s).
System Security Server Options Sensor		
F.AU.1.11.1	If the setting of the current Security Server option does not match (comply) the setting found in the baseline,	Issue the SETROPTS command to change the option to the baseline value, write VEESET error message to sensor log and (optionally) send notification to selected administrator(s).
System Started Task Sensor		
F.AU.1.12.1	Started Procedure user ID has a RACF User profile TSO segment,	Remove the TSO segment, write VEESTC error message to sensor log and (optionally) send notification to selected administrator(s).
F.AU.1.12.2	Started Procedure user ID is not connected to the RACF started task group,	Connect user to started task group, write VEESTC error message to sensor log and (optionally) send notification to selected administrator(s).
F.AU.1.12.3	Started procedure is defined in the STARTED class and has gained the trusted or privileged or trace attribute	Remove the attribute from the profile, write VEESTC error message to sensor log and (optionally) send notification to selected administrator(s).
F.AU.1.12.4	User id associated with started procedure defined in STARTED class has changed,	Correct user id in STDATA segment of STARTED class profile, write VEESTC error message to sensor log and (optionally) send notification to selected administrator(s).
F.AU.1.12.5	Group is associated with started procedure defined in STARTED class has changed	Correct group id defined in STDATA segment of STARTED class profile, write VEESTC error message to sensor log and (optionally) send notification to selected administrator(s).
F.AU.1.12.6	Started Procedure definition not in baseline	Write VEESTC error message to sensor log and (optionally) send notification to selected administrator(s).
F.AU.1.12.7	Baseline Started Procedure not defined to system	
System SVC Sensor		
F.AU.1.13.1	SVC active when baseline indicates inactive	Alter SVC table to invoke IGCERROR, write VEESVC error message to sensor log and (optionally) send notification to selected administrator(s).
F.AU.1.13.2	SVC inactive when baseline indicates active	Write VEESVC error message to sensor log and (optionally) send notification to selected administrator(s).
F.AU.1.13.3	SVC requires APF authorization when baseline indicates no APF authorization.	
F.AU.1.13.4	SVC does not require APF authorization when baseline indicates APF authorization required	
Installation Critical DASD Volumes Sensor		

TSF	Security Attribute	Required automatic response
F.AU.1.14.1	Profile protecting data set has UACC greater than READ	Write VEEVOL error message to sensor log and (optionally) send notification to selected administrator(s).
F.AU.1.14.2	SMS status of data set does not match baseline	
F.AU.1.14.3	VSAM status of data set does not match baseline	
Installation Critical Data Set Profiles Sensor		
F.AU.1.15.1	Incorrect covering profile	Write VEECDC error message to sensor log and (optionally) send notification to selected administrator(s).
F.AU.1.15.2	No covering profile	Add profile, write VEECDC error message to sensor log and (optionally) send notification to selected administrator(s).
F.AU.1.15.3	RACF profile attribute incorrect	Change attribute, write VEECDC error message to sensor log and (optionally) send notification to selected administrator(s).
F.AU.1.15.4	Baseline user not in access list	Write error to sensor log, write VEECDC error message to sensor log and (optionally) send notification to selected administrator(s).
F.AU.1.15.5	Baseline user has incorrect access,	Correct access level in access list, write VEECDC error message to sensor log and (optionally) send notification to selected administrator(s).
F.AU.1.15.6	Deleted	Deleted
F.AU.1.15.7	Global Table access different from profile UACC	Write error to sensor log, write VEECDC error message to sensor log and (optionally) send notification to selected administrator(s).
F.AU.1.15.8	Global Table access different from baseline UACC	Write VEECDC error message to sensor log and (optionally) send notification to selected administrator(s).
F.AU.1.15.9	User/group in access list not in baseline	Remove the user/group from the profile access list if not: • Connected to a started task group or • One of the started task groups or • A userid that has the PROTECTED attribute or • A userid that is a member of one of the started task groups Write VEEGRC error message to sensor log and (optionally) send notification to selected administrator(s).

The corresponding SFRs are FAU_SAA.5-RACF and FAU_ARP.1.

6.1.3 TOE Management (F.MGMT)

The administration of the TOE management functions uses the ISPF panel interface or the z/OS console, either during installation of the TOE or during its operation. The parameters entered via these interfaces are stored either in the VANOPTS Library data set or in the Enforcer baseline data set.

Table 15 - TOE Management TSF

TSF	Description
F.MGMT.1 – Security Administrators may perform Enforcer customization.	
F.MGMT.1.1	Customize Sensors
F.MGMT.1.2	Customize Data Collection and Notification
F.MGMT.1.3	Allocate an initial Baseline data set
F.MGMT.1.4	Create the JCL for the Started Tasks
F.MGMT.1.5	Establish Enforcer started task JCL PARM options
F.MGMT.1.6	UNUSED (This TSF has been removed.)
F.MGMT.1.7	Build a baseline
F.MGMT.1.8	Set up Enforcer Execution options
F.MGMT.2 – Security Administrators define and select RACF profiles monitored.	
F.MGMT.2.1	Select critical data sets monitored
F.MGMT.2.2	Select critical general resources monitored
F.MGMT.3 – Security Administrators may select or deselect options for automatic RACF profile correction	
F.MGMT.3.1	Select warning or correct mode for each sensor
F.MGMT.4 – Security Administrators may select general security options	
F.MGMT.4.1	UNUSED (This TSF has been removed.)
F.MGMT.5 – Security Administrators may select notification recipients	
F.MGMT.5.1	Set up Sensor Email Notification Addresses
F.MGMT.5.2	Set up Sensor TSO SEND Notification Addresses

The corresponding SFR is FMT_SMF.1.

6.2 Assurance Measures

The following table provides an overview, how the assurance measures of EAL3 augmented by ALC_FLR.1 are met by Vanguard Enforcer
.

Table 16 - Mapping Assurance Components to Assurance Measures

Assurance Component	Documentation describing how the requirements are met
ACM_CAP.3	Vanguard Enforcer is developed at single site using a well defined

Assurance Component	Documentation describing how the requirements are met
	configuration management system following a detailed description of how configuration management is performed.
ACM_SCP.1	Source code, generated binaries, documentation, test plan, test cases and test results are all maintained under configuration management.
ADO_DEL.1	Vanguard Enforcer is delivered via sales channels controlled by Vanguard.
ADO_IGS.1	Guidance for installation and system configuration is provided.
ADV_FSP.1	The functional specification for Enforcer consists of the description of the commands provided to users, and the security administrators to use and manage the security functions and the description of the system configuration data sets.
ADV_HLD.2	A high-level design of the security functions of Enforcer will be provided by the developer. This document provides an overview of the implementation of the security functions within the subsystems of Enforcer and points to other existing documents for further details where appropriate.
ADV_RCR.1	The correspondence information is provided in the form of a spreadsheet showing the correspondence between the TOE summary specification and the functional specification and the functional specification and the high level design.
AGD_ADM.1	A number of documents exist that provide guidance for the system administrator.
AGD_USR.1	User Guidance is provided in a number of documents related to the usage of Enforcer. Those documents explain in detail the security functions a normal user can use and manage.
ALC_DVS.1	Vanguard has a set of guidance documents for physical, logical and procedural security measures that all Vanguard facilities have to use in their specific implementation of a Security Plan.
ALC_FLR.1	The Enforcer development within vanguard has a well-defined system for reporting flaws and tracing the status of the corrective actions for those flaws.
ATE_COV.2	Vanguard has detailed test plans to test the functions of Enforcer. Those test plans include an analysis of the test coverage, an analysis of the functional interfaces tested and an analysis of the testing against the high-level design.
ATE_DPT.1	Testing of internal interfaces is defined and described in the test plan documents and the test case descriptions.
ATE_FUN.1	Testing has been performed on the platforms that are defined in the Security Target. Test results are documented such that the tests can be

Assurance Component	Documentation describing how the requirements are met
	repeated.
ATE_IND.2	All the required resources to perform their own tests will be provided to the evaluation facility to perform their test. The evaluation facility will perform and document the tests they have created and performed as part of the evaluation technical report for testing.
AVA_MSU.1	A Misuse Analysis will be provided by the developer.
AVA_SOF.1	The Strength of Function Analysis will not be required because there are no functions based on permutational or probabilistic algorithms.
AVA_VLA.1	The developer will provide a vulnerability analysis and document the activities and findings.

7 Protection Profile Claims

7.1 PP Reference

This Security Target does not claim conformance with any Protection Profile that has been registered and / or evaluated.

8 Rationale

The rationale section provides additional information and demonstrates that the security objectives and the security functions defined in the previous chapter are consistent and sufficient to counter the threats defined in chapter 2.

8.1 Security Objectives Rationale

8.2 Security Objectives Coverage

The following table provides a mapping of TOE objectives to threats and policies, showing that each objective is at least covered by one threat or policy.

Table 17 - Mapping Objectives to Threats and Policies

Objective	Threat/Policy
O.RACF.MONITOR	T.ADMINISTRATIVE_ERROR P.RACF_MONITOR_NOTIFY
O.RACF.CORRECT	T.ADMINISTRATIVE_ERROR P.RACF_MONITOR_ROLLBACK
O.RACF.NOTIFY	T.ADMINISTRATIVE_ERROR P.RACF_MONITOR_NOTIFY
O.MANAGE	T.ADMINISTRATIVE_ERROR

The threat of administrative error, T.ADMINISTRATIVE_ERROR, is countered by the objectives, O.RACF.MONITOR, O.RACF.CORRECT, O.RACF.NOTIFY, and O.MANAGE. These objectives, if met, manage the TOE in a secure manner, monitor the RACF database, and system configurations for changes, correct these changes, and send notifications to a predefined list of administrators. These actions are sufficient to counter the threat identified.

The following table provides a mapping of the objectives for the TOE environment to assumptions, threats, and policies, showing that each objective is at least covered by one assumption, threat, or policy.

Table 18 - Mapping Objectives for the Environment to Threats, Assumptions, and Policies

Environmental Objective	Threat/Assumption/Policy
OE.ADMIN	A.ADMINISTRATION A.NO_EVIL_ADM A.MULTIPLE_SENSOR_SESSION
OE.AUTHENTICATE	PE.AUTHENTICATE
OE.AUTHORIZE	A.UNAUTHORIZED_ACCESS PE.AUTHORIZED_USERS
OE.CAPP_MODE	A.CAPP_MODE
OE.INSTALL	PE.INSTALL
OE.MANAGE	PE.MANAGE
OE.PHYSICAL	A.LOCATE A.PROTECT
OE.SECURITY_ADMIN	A.SECURITY_ADMINISTRATOR
OE.TIMESTAMP	A.TIMESTAMP

8.3 Security Objectives Sufficiency

The following rationale provides justification that the security objectives are suitable to cover each individual assumption. Each security objective that traces back to an assumption about the use of the TOE, when achieved, actually contributes to the TOE achieving consistency with the assumption, and that if all security objectives that trace back to an assumption are achieved, the intended usage is supported.

Table 19 - Assumptions to Objectives Rationale

Assumption	Rationale for Objective
A.MULTIPLE_SENSOR_SESSION	This assumption is addressed by the environment objective, OE.ADMIN, those responsible for the administration of the TOE must be trained such that they are capable of managing the TOE and the security of the information it contains and that the underlying operating system and hardware is configured and managed in a secure way..
A.UNAUTHORIZED_ACCESS	This assumption is addressed by the environment objective, OE.AUTHORIZE, which states the TOE environment must provide the ability to specify and manage access rights to objects and services by user and system process and the TOE code and configuration data sets are protected from unauthorized access.
A.CAPP_MODE	This assumption is addressed by the environment objective, OE.CAPP_MODE, which states that the TOE environment must limit the operating mode to CAPP compliant operations.
A.LOCATE	This assumption is addressed by the environment objective, OE. PHYSICAL, this states that those responsible for the TOE environment must ensure that the TOE and its underlying hardware and software are physically protected from unauthorized physical access and tampering.
A.PROTECT	This assumption is addressed by the environment objective, OE. PHYSICAL, which states that those responsible for the TOE environment must ensure that the TOE and its underlying hardware and software are physically protected from unauthorized physical access and tampering.
A.ADMINISTRATION	This assumption is addressed by the environment objective, OE.ADMIN, which states those responsible for the administration of the TOE must be trained such that they are capable of managing the TOE and the security of the information it contains and that the underlying operating system and hardware is configured and managed in a secure way.
A.NO_EVIL_ADM	This assumption is addressed by the environment objective, OE.ADMIN, which states those responsible for the administration of the TOE must be trained such that they are capable of managing the TOE and the security of the information it contains and that the underlying operating system and hardware is configured and managed in a secure way.. Administrators are trustworthy..

Assumption	Rationale for Objective
A.AUTHORIZE	This assumption is addressed by the environment objectives, OE.AUTHORIZE, which states the TOE environment must provide the ability to specify and manage access rights to objects and services by user and system process and the TOE code and configuration data sets are protected from unauthorized access.
A.SECURITY_ADMINISTRATOR	This assumption is addressed by the environment objective, OE.SECURITY_ADMIN, which states that those responsible for the TOE environment must assign an individual to administer TOE IT environment security that is different that the individual assigned to perform normal IT environment administration.
A.TIMESTAMP	This assumption is addressed by the environment objective, OE.TIMESTAMP, that states that the environment must provide reliable timestamps. The timestamp function provides timing for the sampling interval for selected security settings of the RACF Security Server database and configuration settings comparisons against the baseline dataset.

The following rationale provides justification that the security objectives are suitable to cover each individual organizational security policy, that each security objective that traces back to an OSP, when achieved, actually contributes to the implementation of the OSP, and that if all security objectives that trace back to an OSP are achieved, the OSP is implemented:

Table 20 - Organizational Security Policy to Objectives Rationale

OSP	Rationale for Objective
P.RACF_MONITOR_NOTIFY	This policy is implemented by the objectives, O.RACF.MONITOR and O.RACF.NOTIFY, which states that the TOE must monitor selected RACF Security Server settings and profiles for changes that may result in potential security violations and the TOE must notify the Administrator that RACF security profile changes may violate system security policy.
P.RACF_MONITOR_ROLLBACK	This policy is implemented by the objectives, O.RACF.CORRECT, which states the TOE must correct changes detected to the monitored RACF Security Server profiles by returning to a known secure state.
PE.AUTHORIZED_USERS	This policy is implemented by the environmental objective, OE.AUTHORIZE, which states the TOE environment must provide the ability to specify and manage access rights to objects and services by user and system process and the TOE code and configuration data sets are protected from unauthorized access.
PE.AUTHENTICATE	This policy is implemented by the environmental objective, OE.AUTHENTICATE, which states the TOE environment must ensure that all users are identified and authenticated before being granted access to the

OSP	Rationale for Objective
	TOE mediated resources. Such limited access to the TOE is configured by the administrator and should be conformant with the security policies of the organization responsible for the operations of the TOE.
PE.MANAGE	This policy is implemented by the environmental objective, OE.MANAGE, those responsible for the TOE environment must ensure that the underlying operating system and hardware is configured and managed in a secure way.
PE.INSTALL	This policy is implemented by the environmental objective, OE.INSTALL, which states those responsible for the TOE environment must ensure that the TOE is installed in a secure manner, which maintains the security of the TOE, including the TSF data and user data of the TOE.

8.4 Explicit Security Functional Requirements Rationale

One explicit security functional requirements is defined in this Security Target:

- FAU_SAA.5-RACF

This security functional requirement has been defined as an extension to part 2 of the Common Criteria to address a situation where a TOE needs to monitor a change in state of a security database. This database contains the security settings for the underlying operating system that in large installations may become very complex, and because of this complexity, may give rise to an administrative error that would allow a vulnerability to be exposed.

In normal systems, the FAU_SAA SFR is dependent on the generation of audit records, however in this TOE, the database settings are the equivalent of audit records, and changes to the state of the database is used for the potential violation analysis. As stated in Section 2.5.1, “Selected security settings of the RACF Security Server database and configuration settings are sampled…”. The requirement for an accurate time interval at which sampling occurs creates a dependency on a timing source, which is satisfied by a tme stamp provided by the environment.

8.5 Security Functional Requirements Rationale

The following table provides a mapping of security functional requirements to objectives, showing that that each security functional requirement covers at least one objective and that each objective is covered by at least one security functional requirement.

Table 21 - Mapping Security Functional Requirements to Objectives

SFR	Objective
FAU_SAA.5-RACF	O.RACF.MONITOR
FAU_ARP.1	O.RACF.NOTIFY, O.RACF.CORRECT
FMT_SMF.1	O.MANAGE

The following rationale provides justification for each security objective for the TOE, showing that the TOE security function requirements are suitable to meet and achieve the security objectives.

Table 22 - Mapping TOE Objectives to SFRs for the TOE

Objective for the TOE	Security Functional Requirement
O.RACF.MONITOR	The objective to monitor selected RACF Security Server settings and profiles for changes that may result in potential security violations is met by requirements for violation analysis FAU_SAA.5-RACF. Supportive management functions have been specified in FMT_SMF.1.
O.RACF.CORRECT	The objective to correct changes detected to the monitored RACF Security Server profiles by returning to a known secure state is met by requirements for automatic response FAU_ARP.1. Supportive management functions have been specified in FMT_SMF.1.
O.RACF.NOTIFY	The objective to notify the Administrator that RACF security profile changes may violate system security policy is met by requirements for automatic response FAU_ARP.1. Supportive management functions have been specified in FMT_SMF.1.
O.MANAGE	The objective to ensure that the TOE is managed in a secure manner, which maintains the security of the TOE, including the TSF data and user data of the TOE, as described in the accompanying Secure Installation and Configuration Guide is met by requirements for security management FMT_SMF.1

The objective, O.RACF.MONITOR, is satisfied using the security function FAU_SAA.5-RACF that is supported by the management function FMT_SMF.1.

The objectives, O.RACF.CORRECT and O.RACF.NOTIFY, are satisfied using FAU_ARP.1 and supported by the management function FMT_SMF.1

The objective, O.MANAGE, is satisfied using the management function FMT_SMF.1.

These objectives, if met, monitor the RACF database and system configurations for changes, correct these changes, and send notifications to a predefined list of administrators. These actions are sufficient to meet the objectives identified.

The following rationale provides justification for each security objective for the IT environment, showing that the security functional requirements for the IT environment are suitable to meet and achieve the security objectives.

Table 23 - Mapping IT Environment Objectives to SFRs for the IT Environment

Objective	Security Functional Requirement
OE.AUTHENTICATE	The objective that the TOE environment must ensure that all users are identified and authenticated before being granted access to the TOE mediated resources is met by the requirement for FIA_UAU.1 and FIA_UID.1.
OE.AUTHORIZE	The objective that the TOE environment must provide the ability to specify and manage access rights to objects and

Objective	Security Functional Requirement
	services by user and system process and the TOE code and configuration data sets are protected from unauthorized access. FDP_ACC.1, FDP_ACF.1, and FPT_SEP.1
OE.MANAGE	The objective that the TOE environment must provide the ability to configure and manage the underlying operating system and hardware in a secure way is met by the requirements for FMT_MSA.1, FMT_MSA.3, FMT_SMF.1, and FMT_SMR.1.
OE.TIMESTAMP	The objective that the TOE environment must provide reliable timestamps is met by the requirements for FPT_STM.1.

8.6 Security Requirements Dependency Analysis

The following table shows the dependencies between the security functional requirements for the TOE and their resolution in this Security Target.

SFRs in italic type setting show dependent SFRs that have not been resolved.

The following table shows that the TOE security functions specified in the TOE summary specification meet all the security functional requirements for the TOE and work together to satisfy the TOE security functional requirements.

Table 24 - Dependencies between TOE Security Functional Requirements

SFR	Dependencies	Resolved
FAU_SAA.5-RACF	FPT_STM.1	Yes
FAU_ARP.1	*FAU_SAA.1*	No
FMT_SMF.1	None	Yes

The dependency for FAU_ARP.1 is shown unresolved in the table above, however, a custom SFR has been created that will fulfill this dependency. This custom SFR is FAU_SAA.5-RACF and provides the violation analysis to detect changes necessary for FAU_ARP.1.

The following tables contain the dependency analyses for the IT environment SFRs.

Table 25 - Dependencies between IT Environment Security Functional Requirements

SFR	Dependencies	Resolved
FDP_ACC.1	FDP_ACF.1	Yes
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	Yes Yes
FIA_UAU.1	FIA_UID.1	Yes
FIA_UID.1	None	Yes
FMT_MSA.1	FDP_ACC.1 FMT_SMF.1 FMT_SMR.1	Yes Yes Yes

SFR	Dependencies	Resolved
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	Yes Yes
FMT_SMF.1	None	Yes
FMT_SMR.1 FPT_STM.1 FPT_SEP.1	FIA_UID.1 None None	Yes Yes Yes

There are no unresolved IT Environment SFRs, therefore no rationale.

8.7 TOE Summary Specification Rationale

8.7.1 Security Functions Justification

The following table shows that the IT security functions specified in the TOE summary specification meet all the security functional requirements for the TOE and work together to satisfy the TOE security functional requirements.

Chapter 6 demonstrates that security function F.AU.1 supports the security function requirements FAU_SAA.5-RACF and FAU_ARP.1 and F.MGMT supports FMT_SMF.1. By showing this, it is clearly shown that the IT security functions specified in the TOE summary specification meet all the security functional requirements for the TOE

Table 26 - Mapping of TOE SFRs to TSF

SFR	Security Function
FAU_SAA.5-RACF	F.AU.1
FAU_ARP.1	F.AU.1
FMT_SMF.1	F.MGMT

8.7.2 Mutual Support of Security Functions

The TOE intended use is to provide administrative support for the IBM z/OS system:

1. Automated surveillance and optional control of the z/OS RACF profiles and settings.

As such, the goal to provide this support is satisfied by the audit security functions, F.AU, and the necessary management functions, F.MGMT and together provides the mutual support necessary.

8.8 Assurance Measures Rationale

Dependencies within the EAL3 package selected for the security assurance requirements have been considered by the authors of CC Part 3 and are not analyzed here again. The included component on flaw remediation, ALC_FLR.1, has no dependencies on other requirements.

The evaluation assurance level (EAL) 3 was chosen as a medium level of assurance reflecting the expected assurance requirements of commercial customers using the target of evaluation (TOE) to protect against administrator errors. The TOE is intended to provide a reasonable level of protection against this as compared to the lack of protection provided by the operating system itself. This is reflected as well in the definition of the TOE environment in chapter 2 and the security objectives for the TOE in chapter 4 of this ST.

The assurance level EAL3 was augmented with ALC_FLR.1 to address the flaw remediation process used for the product. Since the evaluation methodology for ALC_FLR.1 has been harmonized and is covered by the Mutual Recognition Arrangement, this was considered a useful augmentation for the assurance level chosen.

The assurance measures are explained in Table 16 - Mapping Assurance Components to Assurance Measures.

8.9 Strength of Function Rationale

This Security Target makes no claims for Strength of Function, as there are no probabilistic or permutational mechanisms in the TOE.

9 Abbreviations

Table 27 - Abbreviations and Acronyms

Abbreviation	Description
APF	Authorized Program Facility (IBM zSeries z/OS)
CC	Common Criteria
CCIMB	Common Criteria Interpretations Management Board
DAC	Discretionary Access Control
DASD	Direct Access Storage Device
ID	Identification
IOCDS	Input/Output Configuration Data set
ISPF	Interactive System Productivity Facility (IBM zSeries z/OS)
LOGREC	Log recording data set for both software and hardware exceptions
LPA	Link Pack Area
MAC	Mandatory Access Control
PP	Protection Profile
PR/SM	Processor Resource/Systems Manager (IBM zSeries z/OS)
RACF	Resource Access Control Facility (IBM zSeries z/OS)
RRSF	RACF Remote Sharing Facility
SDSF	System Display and Search Facility (IBM zSeries z/OS)
SFR	Security Functional Requirement
SMF	System Management Facility (IBM zSeries z/OS)
SMS	System Managed Storage
ST	Security Target
SVC	Supervisor call
TOE	Target of Evaluation
TSO	Time Share Option (IBM zSeries z/OS)
TSP	TOE Security Policy
UACC	Universal access (IBM zSeries z/OS)
VSAM	Virtual Storage Access Method

10 References

Table 28 - References

Reference	Reference Description	Version
[CC]	Common Criteria for Information Technology Security Evaluation, CCMB-2005-08-001, 2, 3,	Version 2.3, August 2005, Parts 1 to 3.
[CEM]	Common Methodology for Information Technology Security Evaluation, CCMB-2005-08-004, Evaluation Methodology,	Version 2.3, August 2005. Part 4
[ZOS_ST]	Security Target for IBM z/OS Version 1 Release 6 http://www.commoncriteriaportal.org/public/files/epfiles/0247b.pdf	V1.15 February, 2005
[RACFAG]	z/OS V1R6.0 Security Server RACF Security Administrator's Guide Document number SA22-7683-06	Seventh Edition, March 2005
[VEAG]	Vanguard Enforcer™ Administrator Guide Document Number VENF-120106-710U	Version 7.1 December 2006
[VECC]	Vanguard Enforcer™ Secure Installation and Operations for Common Criteria Document Number EAL3 VENF-120106-710I	Version 7.1 December 2006
[VEIGS]	Vanguard Security Solutions™ Installation Guide Document Number VSS-111606-710I	Version 7.1 November 2006
[VECCL]	Vanguard Enforcer™ Cover Letter for Common Criteria Document Number VSS-120106-710C	Version 7.1 December 2006

