

National Information Assurance Partnership



Common Criteria Evaluation and Validation Scheme Validation Report

BMC Software, Inc.

BMC CONTROL-SA

Report Number: CCEVS-VR-05-0107
Dated: 22 July 2005
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

VALIDATION REPORT
BMC CONTROL-SA

ACKNOWLEDGEMENTS

Validation Team

**Paul Bicknell
The MITRE Corporation
Bedford, MA**

**Shaun Gilmore
NSA
Ft. Meade, MD**

Common Criteria Testing Laboratory

**Science Applications International Corporation
Columbia, Maryland**

Table of Contents

1	Executive Summary	1
1.1	Interpretations	2
1.2	Threats to Security	2
2	Identification	3
3	Security Policy	4
4	Assumptions.....	5
5	Architectural Information	6
6	Documentation.....	10
	Design documentation	10
	Guidance documentation	10
	Configuration Management documentation	11
	Delivery and Operation documentation	11
	Test documentation.....	11
	Vulnerability Assessment documentation.....	11
	Security Target.....	12
7	IT Product Testing	12
7.1	Developer Testing.....	12
7.2	Evaluation Team Independent Testing	12
7.3	Evaluation Team Penetration Testing.....	12
8	Evaluated Configuration	13
9	Results of the Evaluation	13
10	Validator Comments/Recommendations	14
11	Annexes.....	14
12	Security Target.....	14
13	Glossary	15
14	Bibliography	15

VALIDATION REPORT
BMC CONTROL-SA

1 Executive Summary

The evaluation of the BMC CONTROL-SA was performed by Science Applications International Corporation (SAIC) in the United States and was completed on 8 July 2005. The evaluation was conducted in accordance with the requirements of the Common Criteria, Version 2.2 and the Common Methodology for IT Security Evaluation (CEM), Version 2.2.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 2.2) for conformance to the Common Criteria for IT Security Evaluation (Version 2.2). This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This Validation Report is not an endorsement of the BMC CONTROL-SA product by any agency of the US Government and no warranty of the product is either expressed or implied.

The validation team monitored the activities of the evaluation team, reviewed evaluation-testing documentation, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The SAIC evaluation team concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL 2) have been met.

The technical information included in this report was obtained from the Evaluation Technical Report (ETR) Part 1 (non-proprietary) produced by SAIC.

1.1 Interpretations

This evaluation used the Common Criteria for Information Technology Security Evaluation Parts 2 and 3, Version 2.2, Revision 256, January 2004, which incorporated all applicable interpretations at the time the evaluation started.

1.2 Threats to Security

The Security Target identified the following threats that the evaluated product addresses:

T.AUDIT A user may perform unauthorized actions that go undetected.

T.TRANSMIT An unauthorized user may eavesdrop on communications between separate parts of the TOE allowing the unauthorized user to intercept and modify transmitted information.

T.SYNC An unauthorized user may cause the data (security administration data and access control permissions) on the ESS and Managed System to become unsynchronized, as a result obsolete access controls, including old authentication data may be exploited.

T.UNAUTH An unauthorized user may gain access to and/or modify the TOE data.

1.3 Use of Cryptography

The TOE utilizes cryptography to protect TSF data in transmission between distributed parts of the TOE. However, that cryptography was not analyzed or tested to conform to cryptographic standards during the evaluation.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;
- The organizations and individuals participating in the evaluation, etc.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE:	BMC CONTROL-SA <ul style="list-style-type: none">• ESS v3.3 SP1• CONTROL-SA/Solaris Agent v3.1.0• ESS Web Console v2.1.01 SP1• CONTROL-SA/RACF Agent v3.2.01• ESS Console v3.8.01 SP1 CONTROL-SA/Active Directory (AD) Agent v3.1.07 SP2
Protection Profile	Not applicable.
ST:	<i>BMC CONTROL-SA Security Target, Version 1.0, July 8,</i>

VALIDATION REPORT
BMC CONTROL-SA

Item	Identifier
	2005.
Evaluation Technical Report	<i>Evaluation Technical Report For BMC CONTROL-SA, Version 1.0, July 8, 2005</i>
CC Version	Common Criteria for Information Technology Security Evaluation, Version 2.2, Revision 256, January 2004
Conformance Result	CC Part 2 conformant, CC Part 3 conformant
Sponsor	BMC Software, Inc.
Developer	BMC Software, Inc
Common Criteria Testing Lab (CCTL)	SAIC, Columbia, MD
CCEVS Validator	Paul Bicknell, The MITRE Corporation Shaun Gilmore, National Security Agency

3 Security Policy

The TOE provides the following security functions: Security Audit, Cryptographic Support, User Data Protection, Identification and Authentication, Security Management. And Protection of the TSF.

Each is discussed in more detail as follows:

- **Security audit** - Audit records are generated when security related auditable events occur. The information that is recorded in the audit record includes the date/time, the responsible user, the event, the outcome of the event, and if applicable, the unique identification of the Managed System (see Section 5 below for an explanation of Managed System). The TOE provides the functionality necessary for authorized administrators to review audit logs.
- **Cryptographic support** - The TOE supports cryptographic operations such as data encryption/decryption of the data that is transmitted between components of the TOE.
- **User data protection** - The TOE enforces an Access Control policy, which restricts access to the TOE and its functions (i.e. administering attributes of Managed

VALIDATION REPORT
BMC CONTROL-SA

Systems). This protection requires that users (authorized administrator) of the TOE be identified and authenticated before any access to Managed Systems' attributes is granted. Access is granted based on privileges defined by the TOE granted to the user (authorized administrator) that allow access to specific Managed System attributes.

- **Identification and authentication** - All users must be identified and authenticated before access to the TSF is allowed. The user is required to provide a user ID and password, if the verification is successful, access into the TOE is granted.
- **Security management** - The TOE is managed through the Enterprise SecurityStation (ESS) Server (see Section 5 below for an explanation of the ESS), which is the central point of control through which administrators can perform all key security administration tasks including:
 - Management of Audit Data
 - Management of ESS Access Control
 - Management of ESS and Managed System data
- **Protection of the TSF** - The TOE implements a set of security mechanisms to protect the transmission and integrity of its data. The TOE uses data encryption to protect the data transmitted between components of the TOE. The TOE also ensures the consistency of TSF data when replicated between components of the TOE.

4 Assumptions

The following secure usage assumptions about the intended environment of the TOE are identified in the Security Target:

- A.ADMIN The authorized administrators are competent, not careless, willfully negligent, or hostile and will adhere to the guidance and instructions provided in the TOE documentation. The authorized administrators are also trained for proper TOE operation.
- A.BACKUP The authorized administrator follows the computer system backup and recovery procedures, to enable the computer system and product to be restored to a secure state after a failure of the computer system or product.
- A.INSTALL Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.
- A.LOCATE The components of the TOE critical to security policy enforcement must be located within controlled access facilities that will be protected from unauthorized physical access and modification.

VALIDATION REPORT
BMC CONTROL-SA

- A.MANAGE There will be one or more individuals assigned to manage the TOE and the security of information it contains.
- A.OS It is assumed that the underlying operating system and associated DBMS will provide capabilities and be configured appropriately to protect TSF data and functions (logically as well as physically).
- A.TIME The operating environment will provide a reliable system time.

5 Architectural Information

The BMC CONTROL-SA provides security administration for an entire enterprise, regardless of number and variety of platforms, is performed from a central point of control. This central point of control, Enterprise SecurityStation, enables the security administrator to manage different environments via a console interface.

Using Enterprise SecurityStation, the administrator can perform key security administration tasks such as: define new entities (for example, Accounts or Groups), connect users to their organizational roles, inquire about entities, set enterprise-wide security policies and standards, and identify security alerts.

The TOE consists of the following components:

Enterprise SecurityStation (ESS) Server - is the central point of control. The ESS receives data from Open Services, ESS Console, and Command line batch update files and updates the ESS database accordingly. The ESS also instructs the gateways to communicate with the Managed Systems.

Router - directs communications among the ESS Server-gateway and SA-Agent-gateway pairs

ESS Console - The ESS Console provides comprehensive, interactive access to the ESS database. ESS Console is the administrator's primary interface to ESS data, which is maintained in the ESS database. The ESS Console displays ESS database information, collects administrator input and passes this input to ESS for execution. The ESS Console is an element of the ESS server and is a separate executable.

Web Console (GUI) - Web Console provides view and controller functionality. The Web Console enables end users to interact with Open Services, and it sends data to the end user in the form of Web pages displayed in the client browser.

Open Services - Open Services provides the CONTROL-SA system with an open, common, application-programming interface (API) for connecting CONTROL-SA service providers with CONTROL-SA service consumers. Open Services connects Enterprise SecurityStation, a back-end service provider to various front-end applications and clients.

VALIDATION REPORT
BMC CONTROL-SA

The Open Services component collects input from the Web Console and other clients (for example, SPML Form Generator) and passes this input to the ESS component. Open Services connects to ESS Server using the ESS-API.

Command line batch update files - The command line batch update files contain commands for ESS execution. These files are read directly by ESS. ESS Server also accepts input from a batch update file. This capability is most often used when the TOE is installed, in order to build the TOE database from existing information.

Application and System Gateways – The Gateways represent a process, which handles communication with one or more Managed System Agents and updates the ESS database. Gateways communicate with each other. On the Managed System, the gateway communicates with the ESS gateway on the one hand and the Managed System agent on the other. The ESS gateway is used for communication between the Managed System Gateways and the ESS Server. Application and system gateways communicate with the Managed System agents to pass commands received from ESS to the Managed System agents for execution by the Managed System and to receive notification from the Managed System agents of local modifications that affect the ESS database (for example, a change to user access permissions).

Managed System Agents - Managed System agents, residing on the Managed System receive commands from ESS for execution by the Managed System, execute the commands on the Managed System, and notify the gateway of local modifications that affect the ESS database (for example, a change to user access permissions).

The underlying operating systems that support the TOE are as follows:

TOE Component	OS Version
ESS v3.3 SP1	Solaris 9
CONTROL-SA/Solaris Agent v3.1.0	Solaris 9
ESS Web Console v2.1.01 SP1	Solaris 9
CONTROL-SA/RACF Agent v3.2.01	RACF
ESS Console v3.8.01 SP1	Windows 2000, XP, Server 2003
CONTROL-SA/Active Directory (AD) Agent v3.1.07 SP2	Windows Server 2003

In addition, the following third-party components are also required for the functioning of the TOE, and comprise the environment in which the TOE components execute.

Product	Version	Notes
WebLogic	7	J2EE Web Application Server – runs Java Runtime; includes servlet containers
WebSphere	5.0.2.3	J2EE Web Application Server – runs Java Runtime; includes servlet containers

VALIDATION REPORT
BMC CONTROL-SA

Product	Version	Notes
JBoss	3.0.4	Open source J2EE Web Application Server, provided with SA-Control; does not include servlet containers
Tomcat	4.1.24	Servlet container (required only for JBoss)
Wasp		Development toolkit and runtime component; Wasp server executes Web Services requests
Sun JDK	1.4.1_02	Java runtime component
IBM JDK	On Solaris: (Sun + IBM added library) 1.3.1_09	Java runtime component
JCE	7	Java encryption services
Orbix/OrbixSSL	3.3.6	CORBA standard middleware; provides session management, including secure channels between applications on different computers
Oracle	8.1.7.0 through 9.2.4	Stores the ESS data, including audit logs
Adaptive Server Enterprise (Sybase)	12.0.0.6 through 12.5.01	
TCL/Tk	8.3.4	

Notes related to Third Party Components

- WebLogic, WebSphere, and JBoss all perform the same functionality. The customer is free to choose among them.
- WebLogic and WebSphere include the functionality provided by Tomcat; JBoss does not.
- SunJDK and IBM JDK provide the same functionality, and the customer is free to choose between them.
- Oracle and Sybase provide the same functionality, and the customer is free to choose between them.

5.1 Physical Boundaries

Each component of the TOE is a software application that operates within a specified environment. The TOE physical boundaries are the external interfaces and the interfaces to the IT environment. The interfaces to the IT environment refer to interfaces that provide any necessary services to the TOE that are necessary for the TOE to function properly. The operating systems and third party components are not part of the TOE.

The TOE consists of the components illustrated below. These components work together to provide centralized security administration for an entire enterprise.

VALIDATION REPORT
BMC CONTROL-SA

BMC CONTROL -SA

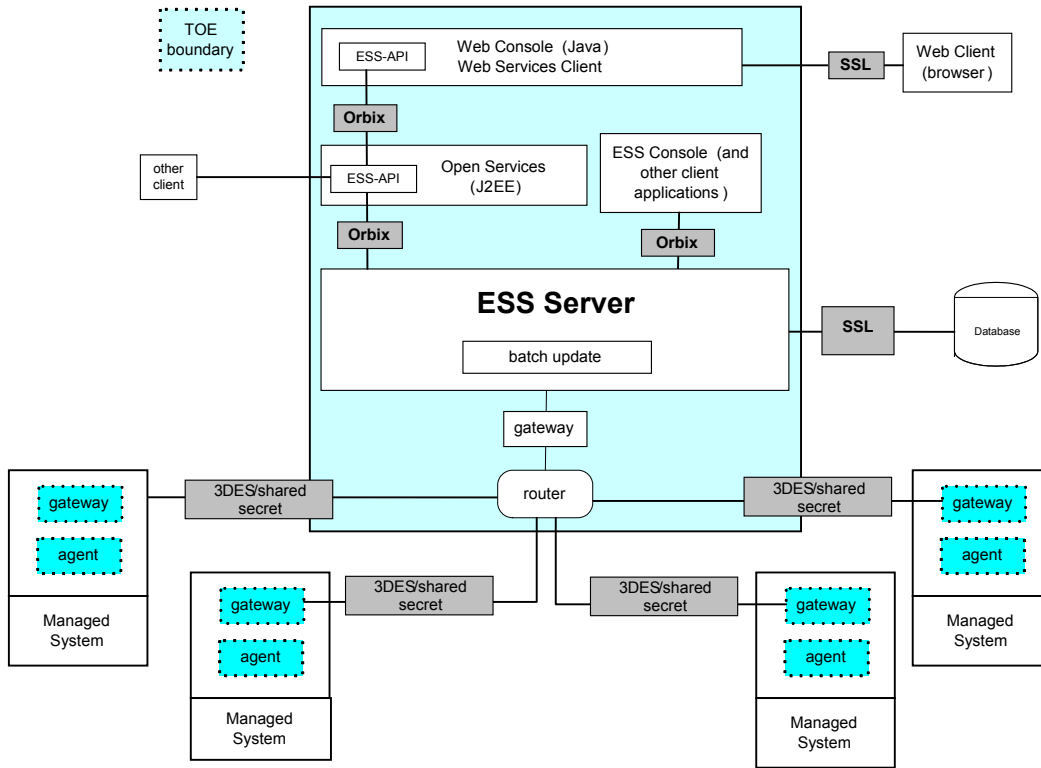


Figure 1 TOE Architecture

As illustrated in Figure 1, many SA-Agent platforms can communicate with ESS via the ESS gateways. SA-Agent does not replace the security provided by the individual Managed System. Together with the features of ESS, SA-Agent enables enterprise-wide management and security administration of multiple Managed Systems.

Interaction between SA-Agent and the Managed Systems is achieved through the USA-API. Since each Managed System has different facilities and operates using its own unique terminology, SA-Agent is provided with a dedicated USA-API for each type of Managed System supported. The use of dedicated USA-APIs enables SA-Agent to handle the unique features and operations of each Managed System.

Although the SA-Agents runs on any number of managed platforms or networks throughout an organization, the SA-Agents included in the evaluated configuration are: CONTROL-SA/Agent for Solaris v3.1.07, CONTROL-SA/Agent for Microsoft Active Directory v3.1.07, and CONTROL-SA/Agent for RACF v3.2.01.

6 Documentation

Design documentation

Document	Version	Date
BMC Control-SA Functional Specification / High Level Design / Representation Correspondence	1.3	March 21, 2005

Guidance documentation

Document	Version	Date
BMC CONTROL-SA Administrator and User Guidance, Version 1.0, 21 January 2005	Version 1.0	January 21, 2005
CONTROL-SA®/Agent for RACF Administrator Guide Release Notes: CONTROL-SA®/Agent for RACF, February 2, 2005	Version 3.2.01	December 26, 2004
CONTROL-SA®/Agent for Solaris Administrator Guide Release Notes: CONTROL-SA®/Agent for Solaris, December 31, 2003	Version 3.1.07	December 31, 2003
CONTROL-SA®/Web Console (Tomcat Deployment) Administrator Guide	Version 2.1.01	September 20, 2004
CONTROL-SA Web Console® User's Guide Release Notes: CONTROL-SA®/Web Console, September 23, 2004 CONTROL-SA®/Web Console, Service Pack 1, December 22, 2004	Version 2.1.01	September 20, 2004
Enterprise SecurityStation® (Oracle Database) Installation Guide	Version 3.3.00	October 20, 2004
Enterprise SecurityStation® Administration Guide Release Notes: Enterprise SecurityStation® December 2, 2004 Enterprise SecurityStation® Service Pack 1, March 1, 2005	Version 3.3.00	October 20, 2004
Enterprise SecurityStation® Console Installation	Version	May 10, 2004

VALIDATION REPORT
BMC CONTROL-SA

Document	Version	Date
Guide	3.8.01	
Enterprise SecurityStation® Console Administration Guide	Version 3.8.01	May 10, 2004
Enterprise SecurityStation® Console User Guide Release Notes: Enterprise SecurityStation® Console, June 6, 2004 Enterprise SecurityStation® Console, Service Pack 1, October 3, 2004	Version 3.8.01	February 26, 2004

Configuration Management documentation

Document	Version	Date
Identity Management BU Configuration Management Guide, Version 1.0	Version 1.0	November 11, 2004
Identity Management BU Configuration Management User Guide	Version 1.0	November 16, 2004
BMC CONTROL-SA Configuration Management	Version 1.1	May 11, 2005

Delivery and Operation documentation

Document	Version	Date
BMC Control-SA Secure Delivery	Version 1.0	January 21, 2005

Test documentation

Document	Version	Date
BMC CONTROL-SA Test Plan, WECO.zip, ESS Console.zip, 26 Oct Test File.zip	Version 1.1	May 11, 2005

Vulnerability Assessment documentation

Document	Version	Date
BMC CONTROL-SA Vulnerability and Strength of Function Analysis	Version 1.0	December 26, 2004

VALIDATION REPORT
BMC CONTROL-SA

Security Target

Document	Version	Date
BMC CONTROL-SA Security Target	Version 1.0	July 8, 2005

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team.

7.1 Vender Testing

The vendor ran the documented test procedures before the evaluation team's Independent Testing Activity began. The vendor provided a complete set of test results for analysis.

The evaluation team analyzed the vendor test procedures to ensure adequate coverage and to determine if the interfaces between subsystems were behaving as expected.

The Evaluation Team determined that the vendor's actual test results matched the vendor's expected results.

The evaluation test team installed the TOE in the vendor's test lab. Some issues were noted during the set up and testing. Updates to the vendor documentation have corrected the cause of these issues.

7.2 Evaluation Team Independent Testing

The Evaluation Team chose to run a subset of the tests that the vendor performed. The subset was chosen to ensure adequate coverage for all security functional requirements. This ensured that the Evaluation Team adequately addressed all the security functions. The Evaluation Team used the vendor's test configurations to perform the tests.

In addition, the Evaluation Team also tested the installation, generation, and start-up procedures to determine that those procedures result in a secure configuration.

However, the evaluation team did not test any cryptographic mechanism for compliance with any standards.

7.3 Evaluation Team Penetration Testing

For its penetration tests, the Evaluation Team used a combination of open-source information and the vendor's test report documentation and procedures to identify a set of

VALIDATION REPORT
BMC CONTROL-SA

penetration test cases. The Evaluation Team used the vendor's test configuration to successfully perform its penetration tests.

The Evaluation Team's ETR, Part 2, provides a detailed description of the tests, the results, and the effects, if any, on the information presented in the ST or other evaluation evidence.

8 Evaluated Configuration

The evaluated configuration consists of a BMC CONTROL-SA system composed of the following components:

BMC CONTROL-SA

- ESS v3.3 SP1
- CONTROL-SA/Solaris Agent v3.1.0
- ESS Web Console v2.1.01 SP1
- CONTROL-SA/RACF Agent v3.2.01
- ESS Console v3.8.01 SP1
- CONTROL-SA/Active Directory (AD) Agent v3.1.07 SP2

The evaluated configuration executes on the following platforms: Solaris 9 for the BMC CONTROL-SA ESS component and Solaris 9, Microsoft Windows Server 2003, and RACF for the respective BMC CONTROL-SA agents. Note that a DBMS (Oracle or Sybase) must also be provided by the environment.

9 Results of the Evaluation

The Evaluation Team conducted the evaluation based on the Common Criteria (CC) Version 2.2 and the Common Evaluation Methodology (CEM) Version 2.2. There were no applicable National and International Interpretations in effect.

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL 2 assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of the issue that needed to be resolved or the clarification that needed to be made to the particular evaluation evidence.

The Evaluation Team accomplished this by providing Notes, Comments, or Vendor Actions in the draft ETR sections for an evaluation activity (e.g., ASE, ADV) that recorded the Evaluation Team's evaluation results and that the Evaluation Team provided to the developer. The Evaluation Team also communicated with the developer by telephone and electronic mail. If applicable, the Evaluation Team re-performed the work unit or units affected. In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict. Verdicts were not assigned to assurance classes.

VALIDATION REPORT BMC CONTROL-SA

Section 5, Results of Evaluation, in the Evaluation Team's ETR, Part 1, states:

“The evaluation determined the BMC CONTROL-SA TOE to be Part 2 conformant, and to meet the Part 3 Evaluation Assurance Level 2 (EAL2) requirements.”

For further details, the reader is encouraged to consult the non-proprietary ETR, Part 1, for this product.

The validation team followed the procedures outlined in the Common Criteria Evaluation and Validation Scheme (CCEVS) publication number 3 for Technical Oversight and Validation Procedures. The validation team has observed the evaluation and all of its activities were in accordance with the Common Criteria, the Common Evaluation Methodology, and the CCEVS. The validation team therefore concludes that the evaluation and its results of pass are complete.

10 Validator Comments/Recommendations

In addition to the information presented in other sections of this document, the validator has the following comments:

External storage of TOE data: The fact that TSF data is stored on a database server outside of TOE control requires surety that environmental controls will be adequate for its protection.

Cryptography: The cryptography used in this product has not been FIPS certified nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.

11 Annexes

Not applicable.

12 Security Target

The Security Target is identified as *BMC CONTROL-SA Security Target*, Version 1.0, July 8, 2005.

The document identifies the security functional requirements (SFRs) necessary to implement Access Control and TOE Self Protection security policies. These include TOE

VALIDATION REPORT
BMC CONTROL-SA

SFRs and IT Environment SFRs. Additionally, the Security Target specifies the security assurance requirements necessary for EAL 2.

13 Glossary

The following definitions are used throughout this document:

Hardware: the physical equipment used to process programs.

Software: the programs and associated data that can be dynamically written and modified.

Target of Evaluation (TOE) - An information technology product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

TOE Security Functions (TSF) – The portions of the TOE that are relied on for correct enforcement of the TOE security policies.

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

- *Common Criteria for Information Technology Security Evaluation*, Version 2.2, Revision 256, January 2004, Parts 1, 2, and 3.
- Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 1.0, February 2002.
- *Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model*, Version 0.6, 11 January 1997.
- *Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology*, Version 2.2 Revision 256, January 2004.
- *BMC CONTROL-SA Security Target*, Version 1.0, July 8, 2005.
- ETR Part 1 (Non-Proprietary), Version 1.0, July 8, 2005.