Certification Report

Buheita Fujiwara, Chairman
Information-technology Promotion Agency, Japan

Target of Evaluation

Application date/ID	June 19, 2006 (ITC-6084)
Certification No.	C0075
Sponsor	Konica Minolta Business Technologies, Inc.
Name of TOE	bizhub 350 / bizhub 250 / bizhub 200 / ineo 350 / ineo 250 (Ver.2) Control Software
Version of TOE	4040-0100-G10-52-000
PP Conformance	None
Conformed Claim	EAL3
TOE Developer	Konica Minolta Business Technologies, Inc.
Evaluation Facility	Mizuho Information & Research Institute, Inc. Center for Evaluation of Information Security

This is to report that the evaluation result for the above TOE is certified as follows.
January 24, 2007

Haruki Tabuchi, Technical Manager
Information Security Certification Office
IT Security Center
Information-technology Promotion Agency, Japan

Evaluation Criteria, etc.: This TOE is evaluated in accordance with the following criteria prescribed in the "IT Security Evaluation and Certification Scheme".

- Common Criteria for Information Technology Security Evaluation Version 2.3
- Common Methodology for Information Technology Security Evaluation Version 2.3

Evaluation Result: Pass

"bizhub 350 / bizhub 250 / bizhub 200 / ineo 350 / ineo 250 (Ver.2) Control Software" has been evaluated in accordance with the provision of the "IT Security Certification Procedure" by Information-technology Promotion Agency, Japan, and has met the specified assurance requirements.

Notice:
This document is the English translation version of the Certification Report published by the Certification Body of Japan Information Technology Security Evaluation and Certification Scheme.

Table of Contents

1. Executive Summary 1
1.1 Introduction 1
1.2 Evaluated Product 1
1.2.1 Name of Product 1
1.2.2 Product Overview 1
1.2.3 Scope of TOE and Overview of Operation 2
1.2.4 TOE Functionality 3
1.3 Conduct of Evaluation 5
1.4 Certification 6
1.5 Overview of Report 6
1.5.1 PP Conformance 6
1.5.2 EAL 6
1.5.3 SOF 6
1.5.4 Security Functions 6
1.5.5 Threat 11
1.5.6 Organisational Security Policy 12
1.5.7 Configuration Requirements 12
1.5.8 Assumptions for Operational Environment 13
1.5.9 Documents Attached to Product 13
2. Conduct and Results of Evaluation by Evaluation Facility 14
2.1 Evaluation Methods 14
2.2 Overview of Evaluation Conducted 14
2.3 Product Testing 14
2.3.1 Developer Testing 14
2.3.2 Evaluator Testing 16
2.4 Evaluation Result 18
3. Conduct of Certification 19
4. Conclusion 20
4.1 Certification Result 20
4.2 Recommendations 20
5. Glossary 21
6. Bibliography 23

1. Executive Summary

1.1 Introduction

This Certification Report describes the content of certification result in relation to IT Security Evaluation of “bizhub 350 / bizhub 250 / bizhub 200 / ineo 350 / ineo 250 (Ver.2) Control Software” (hereinafter referred to as “the TOE”) conducted by Mizuho Information & Research Institute, Inc. Center for Evaluation of Information Security (hereinafter referred to as “Evaluation Facility”), and it reports to the sponsor, Konica Minolta Business Technologies, Inc.

The reader of the Certification Report is advised to read the corresponding ST and manuals (please refer to “1.5.9 Documents Attached to Product” for further details) attached to the TOE together with this report. The assumed environment, corresponding security objectives, security functional and assurance requirements needed for its implementation and their summary specifications are specifically described in ST. The operational conditions and functional specifications are also described in the document attached to the TOE.

Note that the Certification Report presents the certification result based on assurance requirements conformed to the TOE, and does not certify individual IT product itself.

Note: In this Certification Report, IT Security Evaluation Criteria and IT Security Evaluation Method prescribed by IT Security Evaluation and Certification Scheme are named CC and CEM, respectively.

1.2 Evaluated Product

1.2.1 Name of Product

The target product by this Certificate is as follows:

Name of Product:	bizhub 350 / bizhub 250 / bizhub 200 / ineo 350 / ineo 250 (Ver.2) Control Software
Version:	4040-0100-G20-52-000
Developer:	Konica Minolta Business Technologies, Inc.

1.2.2 Product Overview

This TOE is the embedded software that is installed on the Konica Minolta Business Technologies, Inc. digital MFP (bizhub 350, bizhub 250, bizhub 200, ineo 350, and ineo 250) (Hereinafter referred to as “MFP”). This TOE is on the flash memory on the MFP controller carried in MFP, and this controls the whole operation of MFP such as the operation control processing and the image data management received from the panel of MFP body or the network.
This TOE offers the protection from exposure of the highly confidential document stored in the MFP, and aims at protecting the data which may be exposed against a user’s intention. In order to realize it, this offers the functions such as the function that limits the operation to the specific document only to the authorized user, the function that performs the overwrite deletion of the data domain which became unnecessary and the function that deletes the confidential information including a setting value. Moreover, this has the mechanism using the unauthorized access protection function (HDD Lock Function) with which HDD is equipped against the risk of taking out HDD (option part) unjustly which is

a medium for storing image data in MFP. And this offers the encryption key generation function to encrypt the data written to the HDD when the encryption board (option part) is installed on the MFP controller.

1.2.3 Scope of TOE and Overview of Operation

This TOE exists on the flash memory on the MFP controller, which built in the body of the MFP, and is loaded and run on the RAM. Figure1-1 shows the relationship between this TOE and the MFP. Shaded region on the figure1-1 indicates the TOE and "*" shows the option parts of MFP.

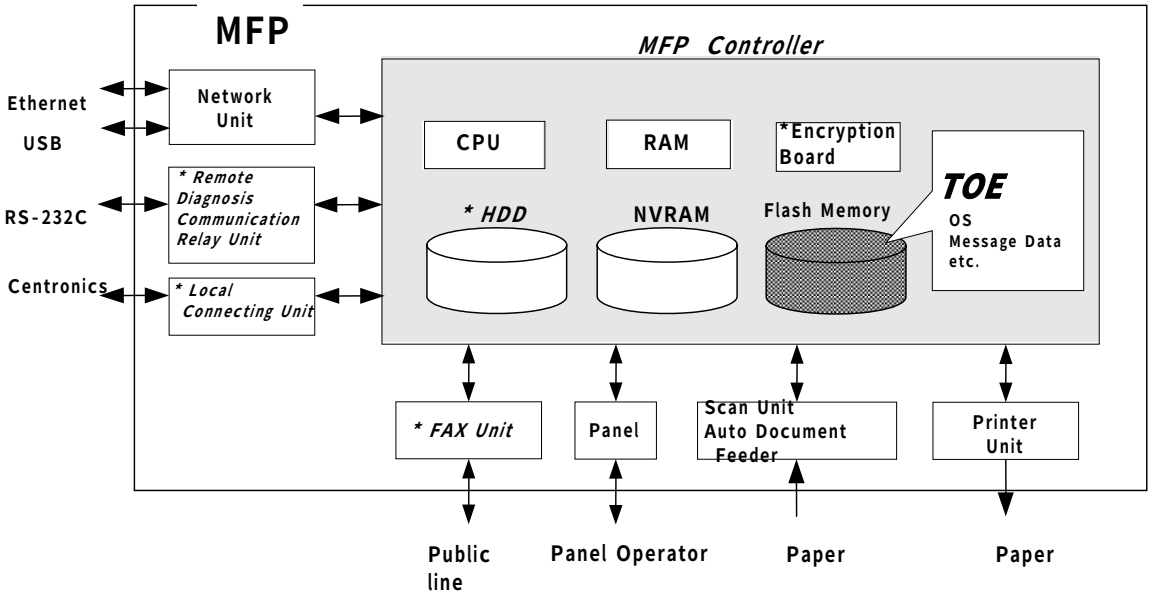


Figure 1-1: Hardware structure that relates to TOE

Flash memory is the storage medium that stores the object code of this TOE and it also stores the message data of each country's language to display the response accessed through the panel and network, OS, and so on.
NVRAM is the nonvolatile memory and it stores various setting values (administrator password, transmission addresses data, etc).
HDD is provided as option parts. HDD stores the image data as the file, and is also used for the storage area for swapping the image data which exceeds the capacity of RAM processing area. Also, this TOE has the HDD lock function that can prohibit the unauthorized reading or unauthorized writing to HDD by setting the password in HDD.
The encryption board is provided as option parts. The encryption function is installed on the encryption board to encrypt the data written to the HDD as the hardware-based function.

Next, the logical structure of this TOE is shown. MFP includes the function that is not associated with the security directly such as basic function, user choice function, and remote diagnosis function other than the function that is indicated in "1.2.4 TOE functionality".
Basic function is a series of function for the office work concerning the image such as copy, print, scan, and fax and TOE performs the core control in the operation of these functions.
User choice function is used for that the user can freely set the image quality

adjustment (magnification and print density etc), the standard layout, the power saving shift time and the auto reset time (function that the display of the operation panel returns to a basic screen if it doesn't operate it during the fixed time), which are needed to use the basic function.
Remote diagnosis function is used for managing the operation status of MFP, setup information, and the device information like the number of prints by using the several methods for the connection, such as the modem connection via RS-232C, the FAX unit, the E-Mail, etc, and communicating with the support center run by the subsidiaries of the Konica Minolta Business Technologies, Inc..

MFP user who can use these functions uses each function that TOE provides, via the panel or the network.
The roles of the personnel that relate to the use of the MFP are defined as follows.

1. User
A person who does copying, scanning, etc. with MFP.(In general, the employee in the office is assumed.)

2. Administrator
MFP's user who carries out the management of the operation of MFP. An administrator performs the operation management of MFP and the management of user box. (In general, it is assumed that the person elected from the employees in the office plays this role.)

3. Service Engineer
A user who performs management of maintenance for the MFP. Service Engineer performs the repair and adjustment of MFP. (In general, the person in charge at the sales companies that performs the maintenance service of MFP and is in cooperation with Konica Minolta Business Technologies, Inc. is assumed.)

4. Person in charge at the organization that uses the MFP
A person in charge at the organization that manages the office where the MFP is installed. This person assigns an administrator who carries out the management of the operation of the MFP.

5. Person in charge at the organization that manages the maintenance of the MFP
A person in charge at the organization that carries out management of the maintenance for the MFP. This person assigns service engineers who perform the maintenance management for the MFP.

Besides this, though not a user of TOE, a person who goes in and out in the office are assumed as an accessible person to TOE.

1.2.4 TOE Functionality

This TOE provides the following functions.

1. Secure Print Function
When the secure print password is received with the printing data, the image data is stored as the standby status. And the print command and password input from the panel allows printing.

2. User Box Function
The directory named a user box can be created as an area to store the image file in

HDD. Two types of user box exist; one is the user box with fixed name "Public" with user box ID “1” which all users can use, and the other is the user box used by setting password which can be used individually or among users with sharing password.
TOE offers the functions to the image file in a user box such as downloading from the client PC, deleting, and setting of the period to keep (delete automatically by the fixed time passed), and also the change of user box name, the change of the password and the deletion of the user box, from the panel or the network unit. (Upon request via the network from the client PC.)
If HDD is not equipped, the user box cannot be created.

3. Administrator Function
TOE provides the functions such as the management of the user boxes and management of various settings of the network, image quality, etc in the administrator mode that only authenticated administrator can operate. Also, it offers the operation setting function related to the behavior of the other function.

4. Service Engineer Function
TOE provides a management function of administrator and a maintenance function, such as adjusting the device for Scan/Print etc, within the service mode that only a service engineer can operate.

5. Enhanced Security Function
Various setting functions related to the behavior of the security function for the Administrator function and the Service engineer function can be set collectively to the secure values by the operation settings of the “Enhanced Security Function”. Each value set is prohibited changing itself into the vulnerable one individually.

6. Overwrite delete function of the remaining information
It performs the overwrite deletion of the unneeded image files made by the job termination, the deleting operation by the job management function, the deletion of image files saved in the user box, and the deletion after a lapse of the storage period of image file. Overwriting data is 0x00 ⇒ 0x00 ⇒ 0x00 and performs the overwriting in this order.

7. HDD Lock Function
HDD has the HDD lock function as measure against the illegal taking out, when the password is set. The administrator function does the operation setting of this function. As for the starting operation of MFP, the access to HDD is permitted by the matching of the HDD lock password set to the HDD and the one set on the MFP. (Even if HDD is taken out, it is impossible to use it excluding the MFP that the concerned HDD installed.)

8. Encryption Key Generation Function
It generates the encryption key to encrypt the data written to HDD based on the Konica Minolta encryption specification standard.

The protected assets of this TOE are image files (secure print file) that are registered by the secure print and image files (user box file) that are stored in the user box except “Public”.
Moreover, when the stored data have physically been separated from the jurisdiction of a user, such as the use of MFP ended by the lease return or being disposed, or the case of an HDD theft, a user has concerns about leak possibility of every remaining data. Therefore, in this case, the following data files become protected assets.

1. All User Box Files
The image files which are stored in all types of user boxes including "Public" user box.

2. Swap Data File
A file to constitute an image that is a big size that does not fit into an RAM area occurring by a copy and a PC print (including secure print file).

3. Overlay Image File
A background image file. This registered image file can be set as wallpaper and used for copying, etc.

4. HDD accumulation image file
A file stored in an HDD from a PC print, and printed by the operation from a panel.

5. Remaining Image file
The file which remains in the HDD data area that is not deleted only by general deletion operation (deletion of a file management area).

6. Transmission address data file
The file included an address transmitting an image, such as an E-mail address, a phone number, etc.

1.3 Conduct of Evaluation

Based on the IT Security Evaluation/Certification Program operated by the Certification Body, TOE functionality and its assurance requirements are being evaluated by evaluation facility in accordance with those publicized documents such as “IT Security Evaluation and Certification Scheme”[2], “IT Security Certification Procedure”[3] and “Evaluation Facility Approval Procedure”[4].

Scope of the evaluation is as follow.

- Security design of the TOE shall be adequate;
- Security functions of the TOE shall be satisfied with security functional requirements described in the security design;
- This TOE shall be developed in accordance with the basic security design;
- Above mentioned three items shall be evaluated in accordance with the CC Part 3 and CEM.

More specific, the evaluation facility examined “bizhub 350 / bizhub 250 / bizhub 200 / ineo 350 / ineo 250 (Ver.1) Control Software Security Target ver.1.09” as the basis design of security functions for the TOE (hereinafter referred to as “the ST”)[1], the evaluation deliverables in relation to development of the TOE and the development, manufacturing and shipping sites of the TOE. The evaluation facility evaluated if the TOE is satisfied both Annex C of CC Part 1 (either of [5], [8] or [11]) and Functional Requirements of CC Part 2 (either of [6], [9] or [12]) and also evaluated if the development, manufacturing and shipping environments for the TOE is also satisfied with Assurance Requirements of CC Part 3 (either of [7], [10] or [13]) as its rationale. Such evaluation procedure and its result are presented in bizhub 350 / bizhub 250 / bizhub 200 / ineo 350 / ineo 250 (Ver.1) Control Software Evaluation Technical Report” (hereinafter referred to as “the Evaluation Technical Report”) [17]. Further, evaluation methodology should comply with the CEM (either of [14], [15] or [16]).

1.4 Certification

The Certification Body verifies the Evaluation Technical Report and Observation Report prepared by the evaluation facility and evaluation evidence materials, and confirmed that the TOE evaluation is conducted in accordance with the prescribed procedure. Certification review is also prepared for those concerns found in the certification process. Evaluation is completed with the Evaluation Technical Report dated January, 2007 submitted by the evaluation facility and those problems pointed out by the Certification Body are fully resolved and confirmed that the TOE evaluation is appropriately conducted in accordance with CC and CEM. The Certification Body prepared this Certification Report based on the Evaluation Technical Report submitted by the evaluation facility and concluded fully certification activities.

1.5 Overview of Report

1.5.1 PP Conformance

There is no PP to be conformed.

1.5.2 EAL

Evaluation Assurance Level of TOE defined by this ST is EAL3 conformance.

1.5.3 SOF

This ST claims a minimum strength of function level of “SOF-basic”.
This TOE assumes the use in the general office environment protected from the attack of the external network.
Access which went via the panel to TOE, or access which went via the internal network is under management by an administrator, and a complicated attack is not assumed.
Therefore, SOF-foundations are enough.

1.5.4 Security Functions

Security functions of the TOE are as follow.

1. Administrator Function (F.ADMIN)
This is a series of security function that administrator operates, such as an administrator identification and authentication function in an administrator mode accessing from a panel or through a network, and a security management function that includes a change of an administrator password and a lock cancellation of a locked user box.

   a. Administrator Identification and Authentication Function
   It identifies and authenticates the accessing user as the administrator in response to the access request to the administrator mode.

   b. Function offered in Administrator Mode
   When a user is identified and authenticated as an administrator by the administrator identification authentication function at the accessing request to the administrator mode, the administrator authority is associated with the task substituting the user.

The following operations and the use of the functions are permitted.

1) Change of the administrator password
When a user is re-authenticated as an administrator, and the new password satisfies the quality, the password is changed.
Administrator password is set with 8-digit by using 0 to 9. (A total of 10 characters are selectable.)
It returns "*" for each character as feedback for the entered administrator password if it's the access from the panel.
Also, it shall not be composed of one kind of character.
It resets the number of authentication failure when the authentication is successful
When the authentication failure that becomes the third times at total in each authentication function by using the administrator password is detected, it locks all the authentication functions to use the administrator password. (The access to the administrator mode is refused.)
Lock of Authentication function is released with F.RESET function operated.

2) Change of User box password
A user box password other than the "Public" user box is changed. Verify that the new user box password satisfies the following qualities.
User box password is set with 8-digit by using ASCII code (0x20 - 0x7E, except 0x22, 0x5E, 0x2B) (A total of 92 characters are selectable).
Also, it shall not be composed of one kind of character.

3) Change of User box ID
A user box ID other than the "Public" user box is changed. It verifies that the new box ID is not matched to any of the registered user box ID.

4) Release of Lock
It resets (0 clear) the number of authentication failure for all secure prints and for all user boxes. If a secure print or user box that access locked exists, the lock is released.

5) Setting and execution of all area overwrite deletion function
It performs the overwrite deletion of all area. (F.OVERWRITE-ALL is executed.)

6) Network setting
A setup operation for a series of setup data (IP address, etc) that relates to MFP address, SMTP server and DNS server are performed.

7) Password setting function of HDD lock function
It changes the HDD lock password. By using the HDD lock password currently set, when it is re-authenticated as an administrator, and the new password satisfies the quality, it is changed.
HDD lock password is set with 20-digit by using ASCII code (0x20 - 0x7E, except 0x20, 0x22, 0x28, 0x29, 0x2C, 0x3A, 0x3B, 0x3C, 0x3E, 0x5B, 0x5C, 0x5D, 0x5E) (A total of 82 characters are selectable).
It returns, in verification, "*" for each character as feedback for the entered HDD lock password.
Also, it shall not be composed of one kind of character.
OFF/ON of HDD lock function is set. To set it ON, it verifies that the HDD lock password satisfies the quality as well as the time of changing the HDD lock password. To set it OFF, it requires the re-authentication as the administrator as well as the change of HDD lock password.

8) Operation setting of Encryption setting
It changes the encryption pass phrase. By using the encryption pass phrase currently set, when it is re-authenticated as an administrator, and the new password satisfies the quality, it is changed.
Encryption pass phrase is set with 20-digit by using ASCII code (0x20 - 0x7E, except 0x20, 0x22, 0x28, 0x29, 0x2C, 0x3A, 0x3B, 0x3C, 0x3E, 0x5B, 0x5C, 0x5D, 0x5E) (A total of 82 characters are selectable).
It returns, in verification, "*" for each character as feedback for the entered encryption pass phrase.
Also, it shall not be composed of one kind of character.
OFF/ON of encryption function is set. To set it ON, it verifies that the encryption pass phrase satisfies the quality as well as the time of changing the encryption pass phrase. To set it OFF, it requires the re-authentication as the administrator as well as the change of encryption pass phrase.

9) Operation setting of Enhanced security function
The function that influences the setting of the enhanced security function operated by the administrator is as follows.
-Operation setting of enhanced security function
Function to set enhanced security function valid or invalid.
-Overwrite deletion function for all area
The settings of enhanced security function are invalidated by executing the overwrite deletion of all area.

2. Service Mode Function (F.SERVICE)
This is a series of security function that the service engineer operates, such as the service engineer identification and authentication function in service mode accessing from a panel, and a security management function that includes a change in the service code and the administrator password.

a. Service Engineer Identification and Authentication Function
It identifies and authenticates the accessing user as the service engineer in response to the access request to the service mode from panel.

b. Function offered in service mode
The following function is allowed to use when a user is identified and authenticated as a service engineer by the service engineer identification authentication function at the accessing request to the service mode.

1) Change of the service code
When a user is re-authenticated as a service engineer, and the new password satisfies the quality, it is changed.
Service code is set with 8-digit by using 0 to 9 and # and *. (A total of 12 characters are selectable)
It returns "*" for each character as feedback for the entered service codes.
It resets the number of the authentication failure when succeeding in the authentication.
When the authentication failure that becomes the third times at total in each authentication function by using the service code is detected, it locks all the authentication functions to use the service code. (The access to the service mode is refused.)
Lock of authentication function is released with F.RESET function operated.
Also, it shall not be composed of one kind of character.

2) Transmission of administrator password
The device information of MFP is transmitted to MFP support center via FAX unit

or by E-mail.

3) Initialization of administrator password
The administrator password is changed to the factory default.

3. User Box Function (F.BOX)
This is a security function that relates to the user box such as the user box access control function, which identifies and authenticates that a person is a permitted user to use the user box in the accessing to the user box from a PC and controls the operation to the user box file.

a. Registration function of User box
The user box registration operation is offered by the user operation. The user box specified is registered by the ID and password of a user box appropriately identified.
It verifies that there is no user box already registered with the same user box ID.
It verifies the user box password satisfies the following requirements.

1) User box password is set with 8-digit by using ASCII code (0x20 - 0x7E, except 0x22, 0x5E, 0x2B) (A total of 92 characters are selectable.)

2) Also, it shall not be composed of one kind of character.

b. Identification and Authentication Function in access to user box
It authenticates that the accessing user is a user to whom the use of a user box concerned is permitted respectively in response to the access request to each user box.
This resets the number of authentication failure when succeeding in the authentication.
When the authentication failure is detected the third times at total for a user box concerned, it locks the authentication function to the user box.
The lock of the authentication function executes the lock release function to the user box of F.ADMIN or operates F.RESET function and releases the lock of the user box.
The followings are the function that the user who is permitted the use of the user box is offered in the user box identification authentication domain of the user box, and to execute it authentication is required for all.

1) Access Control to user box files in the user box
As for the task of substituting the user, "User Box ID" of the user box is related to the task as a user box attribute. This task is permitted to perform the download operation to the user box file of which a user box attributes match to the user box attributes of the subject attributes.

2) Change of user box password
It changes the user box password of the user box.
It verifies that the new user box password satisfies the following quality.
・User box password is set with 8-digit by using ASCII code (0x20 - 0x7E, except 0x22, 0x5E, 0x2B) (A total of 92 characters are selectable.).
・It shall not be composed of one kind of character.

4. Secure Print Function (F.PRINT)
This is a series of security function related to the secure print such as the access control function that allows the printing of the secure print file after authenticating if a user is the authorized user to use the secure print file for the access to the secure print file from the panel.

a. Authentication Function by secure print password

It authenticates that the accessing user is a user to whom the use of the secure print file concerned is permitted, in response to the access request to each secure print file.
Secure print password is set with 8-digit by using ASCII code (0x20 - 0x7E, except 0x22, 0x5E, 0x2B) (A total of 92 characters are selectable.).
It returns "*" for each character as feedback for the entered secure print password.
When the authentication failure is detected the third times at total for the secure print file concerned, it locks the authentication function to the concerned secure print file.
The lock status is released by executing the lock release function of F.ADMIN against the secure print file.

b. Access control function to secure print file
The secure print file access control activates when it is authenticated.
The task of substituting the user that is identified and authenticated has the secure print internal control ID of the secure print file authenticated as the file attribute.
This task is permitted to print the secure print file with the file attribute which matches to this file attribute.

c. Registration function of secure print file
1) Registration of secure print password
It verifies that the registering secure print password satisfies the following condition in the registration request of secure print file.
・Secure print password is set with 8-digit by using ASCII code (0x20 - 0x7E, except 0x22, 0x5E, 0x2B) (A total of 92 characters are selectable.).
・It shall not be composed of one kind of character.

2) Grant of secure print internal control ID
Secure print internal control ID that is identified uniquely sets to the concerned secure print file after verifying the secure print password in the registration request of secure print file.

5. Remaining information overwrite deletion function (F.OVERWRITE-FILE)
This is not only the general deletion (deletion of the management area for the file access), but also the overwrite deletion function of the HDD data domain when deleting a file in the following cases.
<Event that remaining information overwrite deletion starts>
-Job completion of copy and print.
Overwrite deletion object：Swap data file
-Deletion by user operation.
Overwrite deletion object：All user box files, overlay image file, and HDD accumulation image file
-Start of automatic deletion by time limit passage.
Overwrite deletion object：All user box file, swap data file(Only the swap data of the secure print file corresponds)
-When the power is turned on, after the power was turned off while the job is running.
Overwrite deletion object：Swap data file

The deletion method is "0x00⇒0x00⇒0x00" and overwrites the object area. As a result of the operation of this function, the remaining image file does not exist.

6. All area overwrite deletion function (F.OVERWRITE-ALL)
This executes the overwrite deletion at the HDD data area and deletes the transmission address data file installed in NVRAM as well. The object deleted or initialized is as follows.

<deletion object：HDD>
-All user box files
-Swap data file
-Overlay image file
-HDD accumulation image file
-User box password
<deletion object：NVRAM>
-Transmission address data file
-HDD lock password
-Encryption pass phrase
<initialization object：NVRAM>
-Administrator password
The deletion method for the data and the frequency written in HDD executes "0x00⇒ 0xFF⇒0x00⇒0xFF⇒0x00⇒0xFF⇒0xAA⇒ verification".
In addition, by the execution of this function, the enhanced security function becomes invalid. (Refer to the description of operation setting of the enhanced security function in F.ADMIN)

7. HDD Verification Function (F.HDD)
When the HDD lock password is set to HDD, it verifies the status of HDD, and if HDD lock password is not set, it does not permit the reading and the writing operations by assuming that the illegal HDD is set up.
Only when it is certain that the HDD lock password is set, HDD lock function is carried and it is considered as usable HDD. And it permits reading and writing to HDD as a checking function.
In addition, authentication using HDD lock password is realized by HDD lock function which is the function other than TOE (provided by HDD).

8. Authentication Failure Frequency Reset Function (F.RESET)
This is a function to reset the number of authentication failure counted in each authentication function including the administrator authentication. (Do not relate to the lock is valid or not.)
This function operates by activating TOE such that the main power supply of MFP is turned on, it returns from the power failure and so forth. When it starts, the following numbers of authentication failure are reset.
-The number of failure to authentication of administrator
-The number of failure to authentication of a service engineer
-The number of failure that is kept for each user box to authentication of a user box

9. Encryption key generation function (F.CRYPT)
This is a function to generate the encryption key to encrypt the data written to HDD by using the Konica Minolta HDD encryption key generation algorithm (SHA-1) that is regulated by the Konica Minolta encryption specification standard.
Konica Minolta HDD encryption key generation algorithm (SHA-1) is the algorithm that generates the encryption key by using SHA-1 that is regulated by FIPS 180-1. Once the encryption pass phrase is decided with the operational setting of the encryption function that restricts the access by F.ADMIN, it generates the encryption key of 128bit sizes using the Encryption pass phrase by applying the Konica Minolta HDD encryption key generation algorithm (SHA-1).

1.5.5 Threat

This TOE assumes such threats presented in Table 1-1 and provides functions for countermeasure to them.

Table 1-1 Assumed Threats

Identifier	Threat
T.DISCARD-MFP	-When the leaser returned or the discarded MFP were collected, all user box files, a swap data file, an overlay image file, an HDD accumulation image file, and a remaining image file can leak by the person with malicious intent taking out and analyzing an HDD in MFP. -When lease returned or the discarded MFP were collected, the person with malicious intent operates MFP and may find out concealment information such as a transmission address data file, various set passwords, etc.
T.BRING-OUT-STORAGE	-All user box files, a swap data file, an overlay image file, an HDD accumulation image file, and a remaining image file leak by a person or a user with malicious intent illegally taking out and analyzing an HDD in MFP. -A person or a user with malicious intent illegally replaces an HDD in MFP. In the replaced HDD, new files of the “user box” file, a swap data file, an overlay image file, an HDD accumulation image file, and a remaining image file are accumulated. A person or a user with malicious intent takes out and analyzes the replaced HDD and image files leak.
T.ACCESS-BOX	Exposure of the user box file when malicious person or user accesses this unpermitted user box and then download it, print it or transmit it.(E-mail transmission, FTP transmission and SMB transmission).
T.ACCESS-SECURE-PRINT	Exposure of secure print file when malicious person or user prints the file which is not permitted to use.
T.ACCESS-NET-SETTING	-When a malicious person or user changes a network setting related to transmission of a box file, even if the addressee is installed in it correctly, the box file can be transmitted (E-mail transmission or FTP transmission) to the entity where it is not meant to be sent, thus this box file can be exposed. <Network setting that relates to the user box file transmission> -Setting that relates to SMTP server -Setting that relates to DNS server -Malicious person or user changes the network settings of MFP with TOE to identify MFP and uses the setting value of the original MFP with TOE (NetBIOS name, AppleTalk printer name, IP address etc.) into the entity for another illegal MFP. The secure print file becomes sent to unauthorized MFP and the data is exposed.
T.ACCESS-SETTING	The possibility of leaking user box file and secure print file rises because malicious person or user changes the settings related to the enhanced security function.

1.5.6 Organisational Security Policy

There are no organisational security policies required for using the TOE.

1.5.7 Configuration Requirements

The TOE operates on the bizhub 350, bizhub 250, bizhub 200, ineo 350, ineo 250 which is the digital MFP provided by the Konica Minolta Business Technologies, Inc. HDD and the encryption board are option parts and are not equipped as a standard. When option parts HDD and the encryption board are not installed, the function that requires the each of them cannot be used.

1.5.8 Assumptions for Operational Environment

Assumptions required in environment using this TOE presents in the Table 1-3.
The effective performance of the TOE security functions are not assured unless these preconditions are satisfied.

Table 1-3 Assumptions in Use of the TOE

Identifier	Assumptions
A.ADMIN	Administrators, in the role given to them, will not carry out a malicious act during the series of permitted operations given to them.
A.SERVICE	Service engineers, in the role given to them, will not carry out a malicious act during series of permitted operations given to them.
A.NETWORK	-The intra-office LAN where the MFP with the TOE will be installed is not intercepted. -When the intra-office LAN where the MFP with the TOE will be installed is connected to an external network, access from the external network to the MFP is not allowed.
A.SECRET	Each password and encryption pass phrase do not leak out from each user in the use of TOE.
A.SETTING	MFP with the TOE is used after enabling the enhanced security function.

1.5.9 Documents Attached to Product

Documents attached to the TOE are listed below.

<Document for administrator/general user>
1. bizhub 200 / ineo 350 User's Guide [Security Operations](Ver.1.02)(Japanese)
2. bizhub 200 / 250 / 350 User's Guide [Security Operations](Ver.1.02)(English)
3. ineo 250 / 350 User's Guide [Security Operations](Ver.1.02)(English)

<Document for service engineer>
1. bizhub 200 / 250 / 350 Service Manual [Security Function](Ver.1.01)(Japanese)
2. bizhub 200 / 250 / 350 ineo 250 / 350 Service Manual [Security Function] (Ver.1.01)(English)

2. Conduct and Results of Evaluation by Evaluation Facility

2.1 Evaluation Methods

Evaluation was conducted by using the evaluation methods prescribed in CEM in accordance with the assurance requirements in CC Part 3. Details for evaluation activities are report in the Evaluation Technical Report. It described the description of overview of the TOE, and the contents and verdict evaluated by each work unit prescribed in CEM.

2.2 Overview of Evaluation Conducted

The history of evaluation conducted was present in the Evaluation Technical Report as follows.

Evaluation has started on Jury, 2006 and concluded by completion the Evaluation Technical Report dated January, 2007. The evaluation facility received a full set of evaluation deliverables necessary for evaluation provided by developer, and examined the evidences in relation to a series of evaluation conducted. Additionally, the evaluation facility directly visited the development and manufacturing sites on August, September, and October, 2006 and examined procedural status conducted in relation to each work unit for configuration management, delivery and operation and lifecycle by investigating records and staff hearing. Further, the evaluation facility executed sampling check of conducted testing by developer and evaluator testing by using developer testing environment at developer site on October, and November, 2006.

Concerns found in evaluation activities for each work unit were all issued as Observation Report and were reported to developer. These concerns were reviewed by developer and all problems were solved eventually.

As for concerns indicated during evaluation process by the Certification Body, the certification review was sent to the evaluation facility. These were reflected to evaluation after investigation conducted by the evaluation facility and the developer.

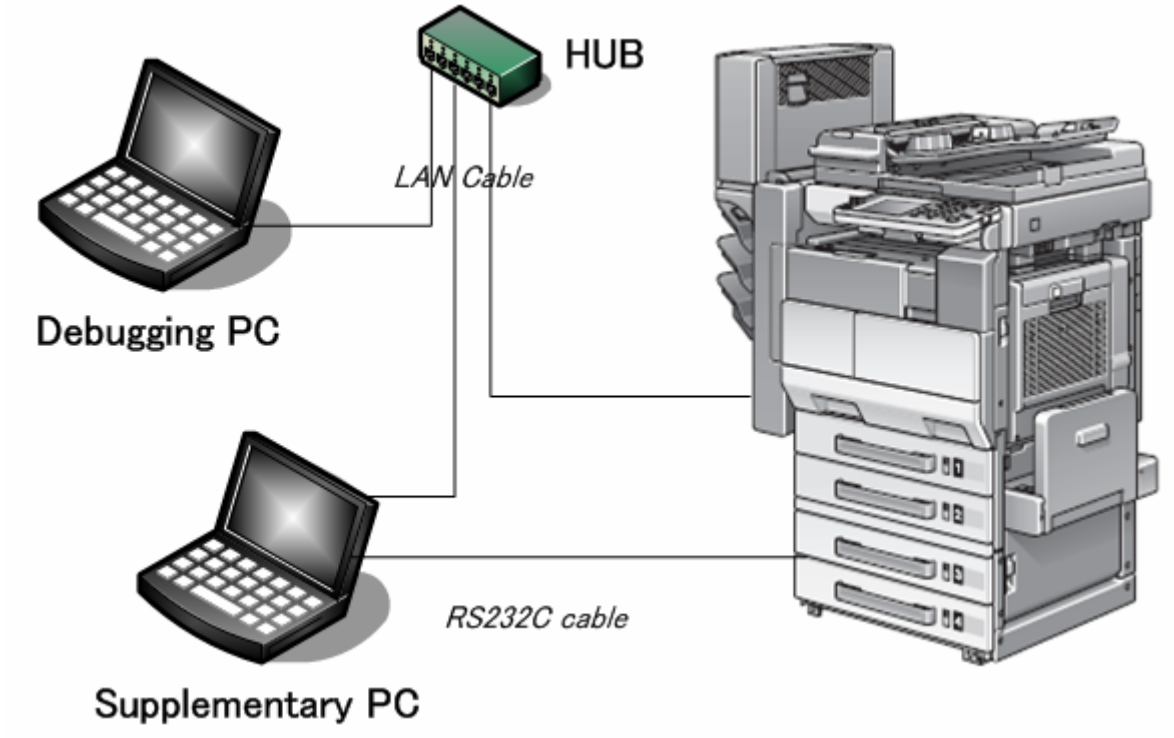
2.3 Product Testing

Overview of developer testing evaluated by evaluator and evaluator testing conducted by evaluator are as follows.

2.3.1 Developer Testing

1. Developer Test Environment

Figure 2-1 shows the test configurations used by the developer.



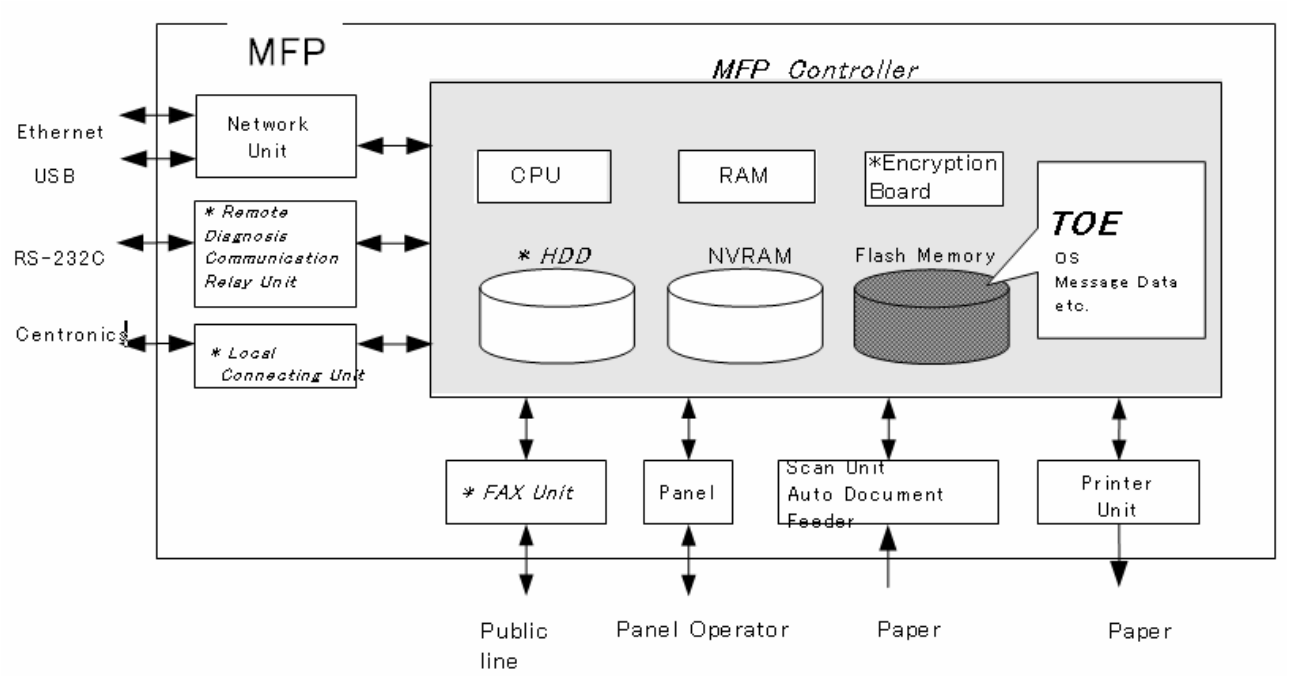


Figure 2-1 Developer test configuration

2. Outlining of Developer Testing

Outlining of the testing performed by the developer is as follow.

a. Test configuration

The configurations of the tests performed by the developer are shown in Figures 2-1. Developer testing is performed at the same TOE testing environment with the TOE configuration identified in ST. However, local connection unit (option parts) is eliminated from the configuration of MFP.

b. Testing Approach

For the testing, following approach was used.
1) Check the behavior of them such as the change of settings, the authentication method and the check of access control, by using the external interface (panel, Page Scope Web Connection (PSWC), and power supply OFF/ON).

2) For the function that cannot check the behavior by operating directly by user, it performs the test procedure for each and checks the adequacy of the behavior.

Outlining of the test is as follows.
-Retrieve the transmission data on the network for the function accessing via the interface of PC (PSWC) to TOE (MFP), and analyze.
-In order to check the operation of SNMPv1, use MIB browser software (GetIfVer2.3.1).
-To check the data transmitting by remote diagnosis operation (Remote maintenance system: RMS), set up the RMS on the supplementary PC and check that the data is transmitted from MFP via Fax line.
-Check if the “remaining information overwrite deletion function” and the “all area overwrite deletion function” operate correctly by using HDD dump display tool etc.
-Check the error occurrence by exchanging the HDD for the other HDD that the HDD lock password is not set up, in order to check that the HDD lock password is valid.
-Check the encryption key generation function is valid by referring to the data on the memory using the debug function installed by panel.

c. Scope of Testing Performed

Testing is performed about 37 items by the developer.
The coverage analysis is conducted and examined to testing satisfactorily all of the security functions described in the functional specification and the external interface. Then, the depth analysis is conducted and examined to testing satisfactorily all the subsystems described in the high-level design and the subsystem interfaces.

d. Result

The evaluator confirmed consistencies between the expected test results and the actual test results provided by the developer. The Evaluator confirmed the developer testing approach performed and legitimacy of items performed, and confirmed consistencies between the testing approach described in the test plan and the actual test results.

2.3.2 Evaluator Testing

1. Evaluator Test Environment

The evaluator used test configurations that are identical to those used by the developer and it was conducted as shown in Figure 2-1.

2. Outlining of Evaluator Testing

Outlining of testing performed by the evaluator is as follow.

a. Test configuration

The configurations of the tests performed by the evaluator are shown in figures 2-1. The evaluator tests were performed in TOE test environments identical to the TOE configuration identified by ST.

b. Testing Approach

For the testing, following approach was used.
1) Check the behavior of them such as the change of settings, the authentication method and the check of access control, by using the external interface (panel, Page Scope Web Connection (PSWC), and power supply OFF/ON).

2) For the function that cannot check the behavior by operating directly by user, it performs the test procedure for each and checks the adequacy of the behavior.

Outlining of the test is as follows.
-Retrieve the transmission data on the network for the function accessing via the interface of PC (PSWC) to TOE (MFP), and analyze.
-In order to check the operation of SNMPv1, use MIB browser software (GetIfVer2.3.1).
-To check the data transmitting by remote diagnosis operation (Remote maintenance system: RMS), set up the RMS on the supplementary PC and check that the data is transmitted from MFP via Fax line.
-Check if the “remaining information overwrite deletion function” and the “all area overwrite deletion function” operate correctly by using HDD dump display tool etc.
-Check the error occurrence by exchanging the HDD for the other HDD that the HDD lock password is not set up, in order to check that the HDD lock password is valid.
-Check the encryption key generation function is valid by referring to the data on the memory using the debug function installed by panel.

c. Scope of Testing Performed

The evaluator performed 24 tests in total: 10 independent tests and 14 sampled developer tests. As the selection criteria of the test, followings take into account.
1) Security function that is suspected to operate along the specifications by the developer test.
2) More important security function than other security function
3) Security function set as the object of strength of function.
4) Function that is used from different interface.

Also, intrusion tests performed by evaluator are conducted as follows.
TOE can perform three kinds of operations such as the operation by the panel, the operation through the network by PSWC (PageScope WebConnection), and the operation by power supply OFF/ON of MFP. The operation by the panel and by power supply OFF/ON of MFP can be considered impossible to perform unauthorized operations such as operation other than assumed usage because of the physical restriction of MFP and operation panel. On the other hand, the operation via the network has broad option and is easy to perform the operation other than expected input.
With a focus on the items related to the network, 6 intrusion tests were invented in consideration of the following 3 points.
1) Verify the truth of insistence based on the vulnerability analysis of developer.

2) Verify the response to the clear vulnerability, that evaluator thinks.
3) Verify the truth of insistence of the strength of function of developer.

Table 2-2 shows the intrusion test item list.

Table 2-2: Intrusion Test Item List

Test No.	Intrusion Testing name for vulnerability test based on [VLA]	Intrusion Test Perspective of idea
VLA-T1	Security objective situation assurance test of network I/F (1)	Perspective 1)
VLA-T2	Security objective situation assurance test of network I/F (2)	Perspective 1)
VLA-T3	Assurance test of official vulnerability	Perspective 1)
VLA-T4	Security function assurance test against HTTP request	Perspective 2)
VLA-T5	Assurance test of Web server function	Perspective 2)
VLA-T6	Assurance test related to the strength of function	Perspective 3)

d. Result

All evaluator testing conducted is completes correctly and could confirm the behavior of the TOE. The evaluator also confirmed that all the test results are consistent with the behavior.

2.4 Evaluation Result

The evaluator had the conclusion that the TOE satisfies all work units prescribed in CEM by submitting the Evaluation Technical Report.

3. Conduct of Certification

The following certification was conducted based on each materials submitted by evaluation facility during evaluation process.

1. Contents pointed out in the Observation Report shall be adequate.
2. Contents pointed out in the Observation Report shall properly be reflected.
3. Evidential materials submitted were sampled, its contents were examined, and related work units shall be evaluated as presented in the Evaluation Technical Report.
4. Rationale of evaluation verdict by the evaluator presented in the Evaluation Technical Report shall be adequate.
5. The Evaluator's evaluation methodology presented in the Evaluation Technical Report shall conform to the CEM.

Concerns found in certification process were prepared as certification review, which were sent to evaluation facility.

The Certification Body confirmed such concerns pointed out in Observation Report and certification review were solved in the ST and the Evaluation Technical Report.

4. Conclusion

4.1 Certification Result

The Certification Body verified the Evaluation Technical Report, the Observation Report and the related evaluation evidential materials submitted and confirmed that all evaluator action elements required in CC Part 3 are conducted appropriately to the TOE. The Certification Body verified the TOE is satisfied the EAL3 assurance requirements prescribed in CC Part 3.

4.2 Recommendations

None

5. Glossary

The abbreviations used in this report are listed below.

CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
PP	Protection Profile
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
MFP	Multiple Function Peripheral
HDD	Hard Disk Drive
LAN	Local Area Network
IP	Internet Protocol
FTP	File Transfer Protocol
SNMP	Simple Network Management Protocol
NVRAM	Non-Volatile Random Access Memory

The glossaries used in this report are listed below.

MFP Controller	Controller that controls all the operation of MFP including the operation control process received from the network or the MFP panel and the management of image data. TOE is the software that operates on that controller.
Flash Memory	Memory device that performs the high speed and high integration of EEPROM and carried the batch deletion mechanism
PC Print	Send the print data of file desired to print to MFP by using the printer driver from PC. MPF converts the data into image file and prints that image data.

Secure Print	This is the printing method that restricts by the password authentication. Specify the password by the printer driver and printing by MFP is allowed only when that password is authenticated.
User Box	Directory that is created in the HDD area in order to store the image files in the MFP.
Service Engineer	A user who performs the management of maintenance for the MFP. Performs the repair and adjustment of MFP. In general, it is the person in charge at the sales companies or agencies that performs the maintenance service of MFP and that is in cooperation with Konica Minolta Business Technologies, Inc.
Service Mode	Operation panel screen area which can operate MFP function that is prepared for the service engineer.
Service Code	Kind of password collating when entering the service mode.
Swap Data	Data to constitute a big size image that does not fit into an RAM area occurring by the copy and the PC print.
Overlay Image File	Image file that can be used as a background image of copy etc.
HDD Accumulation Image	Image file that is stored in HDD of MFP by PC print.
Remaining Image File	File that remains in the HDD data area. It is the image file that cannot be deleted by general deletion operation.
Transmission Address Data File	File including address transmitting an image, such as an E-mail address and a phone number etc.

6. Bibliography

[1] bizhub 350 / bizhub 250 / bizhub 200 / ineo 350 / ineo 250 (Ver.2) Control Software Version 1.09 (December 12, 2006) Konica Minolta Business Technologies, Inc

[2] IT Security Evaluation and Certification Scheme, July 2005, Information-technology Promotion Agency, Japan EC-01

[3] IT Security Certification Procedure, July 2005, Information-technology Promotion Agency, Japan EC-03

[4] Evaluation Facility Approval Procedure, July 2005, Information-technology Promotion Agency, Japan EC-05

[5] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Version 2.3 August 2005 CCMB-2005-08-001

[6] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements Version 2.3 August 2005 CCMB-2005-08-002

[7] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements Version 2.3 August 2005 CCMB-2005-08-003

[8] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Version 2.3 August 2005 CCMB-2005-08-001 (Translation Version 1.0 December 2005)

[9] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements Version 2.3 August 2005 CCMB-2005-08-002 (Translation Version 1.0 December 2005)

[10] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements Version 2.3 August 2005 CCMB-2005-08-003 (Translation Version 1.0 December 2005)

[11] ISO/IEC 15408-1:2005 - Information Technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model

[12] ISO/IEC 15408-2:2005 - Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements

[13] ISO/IEC 15408-3:2005 - Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements

[14] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology Version 2.3 August 2005 CCMB-2005-08-004

[15] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology Version 2.3 August 2005 CCMB-2005-08-004 (Translation Version 1.0 December 2005)

[16] ISO/IEC 18045:2005 Information technology - Security techniques - Methodology for IT security evaluation

[17] bizhub 350 / bizhub 250 / bizhub 200 / ineo 350 / ineo 250 (Ver.2) Control Software Evaluation Technical Report ,January 9, 2007, Mizuho Information & Research Institute, Inc. Center for Evaluation of Information Security