Perceptive Software, Inc.
ImageNow v5.42 SP3 and WebNow v3.42
Security Target

Version 1.0

01/10/07

Prepared for:

Perceptive Software, Inc.

22701 W. 68th Terr
Shawnee, KS 66226

Prepared By:

Science Applications International Corporation

Common Criteria Testing Laboratory

7125 Columbia Gateway Drive, Suite 300
Columbia, MD 21046

TABLE of CONTENTS

LIST OF TABLES

1. Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. The TOE is ImageNow v5.42 SP3 and WebNow v3.42 by Perceptive Software, Inc. The TOE is a document imaging, management and workflow solution based on a client/server architecture that provides a user the ability to scan, file, retrieve, print, fax or distribute electronic objects.

The Security Target contains the following additional sections:

- This section gives an overview of the TOE, describes the TOE in terms of its physical and logical boundaries, and states the scope of the TOE.
- Security Environment (Section 3)

  This section details the expectations of the environment, the threats that are countered by the TOE and it environment and the organizational policy that the TOE must fulfill.
- Security Objectives (Section 4)

  This section details the security objectives of the TOE and its environment.
- IT Security Requirements (Section 5)

  The section presents the security functional requirements (SFR) for TOE and IT Environment that supports the TOE, and details the assurance requirements for EAL 2, augmented with ALC_FLR.2 and AVA_MSU.1.
- TOE Summary Specification (Section 6)

  The section describes the security functions represented in the TOE that satisfy the security requirements
- Protection Profile Claims (Section 7)

  This section presents any protection profile claims
- Rationale (Section 8).

  This section closes the ST with the justifications of the security objectives, requirements and TOE summary specifications as to their consistency, completeness and suitability.

1.1 Security Target, TOE and CC Identification

ST Title – ImageNow v5.42 SP3 and WebNow v3.42 Security Target

ST Version – Version 1.0

ST Date – 01/10/07

TOE Identification – ImageNow v5.42 SP3 and WebNow v3.42

TOE Developer – Perceptive Software, Inc.

Evaluation Sponsor – Perceptive Software, Inc.

CC Identification – Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005

1.2 Conformance Claims

This TOE is conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 2.3, August 2005.
    - Part 2 Conformant
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, Version 2.3, August 2005.
    - Part 3 Conformant
    - Assurance Level: EAL 2 augmented with ALC_FLR.2 and AVA_MSU.1

1.3 Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
    - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a letter placed at the end of the component. For example FDP_ACC.1a and FDP_ACC.1b indicate that the ST includes two iterations of the FDP_ACC.1 requirement, a and b.
    - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]).
    - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
    - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

2. TOE Description

The Target of Evaluation (TOE) is ImageNow, version 5.42 SP3 and WebNow, version 3.42 from Perceptive Software, Inc.

The TOE includes an embedded Database (DB) component in the evaluated configuration, and the evaluated configuration supports third party databases. The TOE is a subset of the product in that the product includes subcomponents called agents that add to ImageNow server component functionality.

The remainder of this section summarizes the ImageNow architecture.

2.1 TOE Overview

The TOE is a document imaging, management and workflow solution based on a client/server architecture that provides a user the ability to scan, file, retrieve, print, fax or distribute electronic objects. Because the TOE can support widespread imaging within an entire network, it provides security auditing, thorough security management functionality, and secure data transfer when accessing stored images via WebNow or the ImageNow Client. Individual TOE components are depicted below and described in the sections that follow.

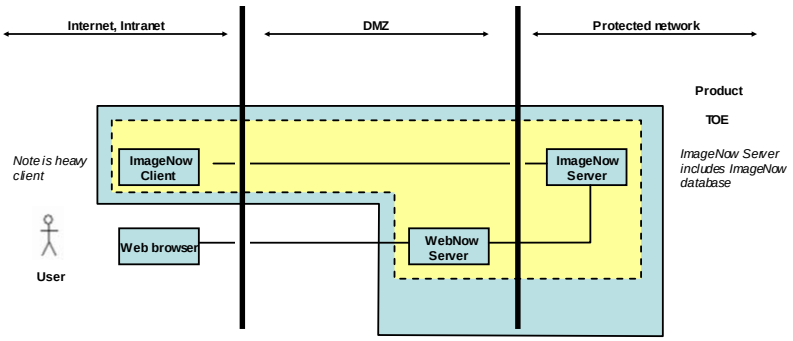

Figure 1: TOE boundary

In Figure 1, the communication between the ImageNow Server and the ImageNow Client, and the ImageNow Server and WebNow should be protected as deemed necessary. The TOE can be configured to use a Perceptive Software, Inc. implementation of 3DES over TCP/IP to help make the links more secure. However, that implementation has not been FIPS or otherwise certified. As such, this ST assumes that the links would be protected to the degree necessary by available external means (e.g., physical network protection or some VPN technology). Note that in a closed enterprise network enclave it may be the case that, if the network users are suitably trusted not to actively attempt to circumvent the security mechanisms of the TOE, the network communications would not need to be protected.

The TOE offers users the flexibility of deployment options and configurations that allow choices for distributed document capture, indexing, storage and management capabilities. ImageNow can simultaneously manage scanning along with the importing of object data from multiple sources, such as fax servers, mail servers, or a network location.

The TOE allows images to be indexed and tracked by 20 different data elements and six user-defined index values. An unlimited number of keywords can be assigned to a document, enabling the user to retrieve specific information. ImageNow also has a LearnMode to 'learn' the host application screen. From the host application screen, a user retrieves the desired transaction. The user presses the ImageNow icon from the windows system tray and ImageNow retrieves all associated documents linked to the current displayed transaction. The toolbars in

ImageNow provide the user with the ability to annotate key points on the document without altering original integrity, distribute the document via print, fax, or e-mail, and view multiple documents that are linked to the current displayed document.

2.2 TOE Architecture

The TOE is comprised of the following components: ImageNow Server (which contains ISA, Intool, the ImageNow database, and the Object Storage Manager, OSM), ImageNow Client, and WebNow. The following section contains an overview of each of the components.

2.2.1 ImageNow Server

The ImageNow Server subsystem contains the following modules: OSM, ImageNow database, ISA, and Intool. The ImageNow Server provides all user authorization, document capture, indexing, retrieval, and workflow functions and includes the ImageNow Server Administrator (ISA) to manage services, logging, and auditing. Although the ImageNow Server provides the overriding security functionality, the only function where a user must log on to ISA directly is to manage the logs (i.e., audit). All other security management functions are handled on the ImageNow Client.

In order to limit security management of the TOE, the ImageNow Server implements Owners and Managers. There is only one Owner which is created during the installation of the TOE. The Ownere is synonymious with the conventional notion of administrator and has full access to all security management functions of the TOE. Managers are users that have been assigned one or more security management privileges or the system-defined Manager role (granting all manager privileges). Depending on the specific combination of privileges granted, a Manager could potentially perform every security management function, except managing management privileges (i.e., a Manager cannot create or remove other Managers and cannot change their own management privileges).

2.2.1.1 OSM

The documents are stored in the Object Storage Manager (OSM) as document objects. The OSM requires a high capacity and high availability storage system, such as Redundant Array of Independent Disks (RAID) 5. The OSM needs to be directly accessible by the ImageNow Server. The OSM can be installed on a separate server because the object store for the scanned images and other documents can grow quite large.

2.2.1.2 ImageNow Database

The ImageNow database stores the metadata of each document. ImageNow includes an embedded database in one of its evaluated configurations. Third party databases can be used in additional supported evaluated configuration to provide the same functionality.

2.2.1.3 ISA

The ImageNow Server Administration (ISA) is the administrator console used to control the ImageNow Server. ISA enables an Owner, or a Manager given ISA privilege, to manage ImageNow Server on Microsoft Windows. Using ISA, users with the appropriate privileges can customize ImageNow Server configuration (.ini) files, manage and mirror storage locations, and monitor, audit, instant message, and disconnect users. ISA also provides a way to supervise specific ImageNow Clients or groups for auditing purposes, view all database tables, workflow queues, and locked documents, and monitor the number of user licenses being used compared with the number of licenses available. ISA can also be used to view real-time interaction between users and ImageNow Server for real-time troubleshooting, as well as view, save, print, and e-mail server log files using the Log and Activity Viewers.

2.2.1.4 Intool

This command-line tool is provided as a tool that provides information about the Owner outside of ISA. This tool provides a mechanism to change the Owner if needed. Intool provides many of the options available in ISA for ImageNow Servers running on UNIX platforms.

2.2.1.5 Auditing Scripts

ImageNow Server contains an auditing script called apply_cc_audit. This script establishes the auditing claimed in this evaluation.

2.2.2 WebNow

The WebNow component is a separate browser-based interface that works seamlessly with the ImageNow Server to provide web-based access to the stored images. The WebNow Server application enables users to view and work with ImageNow documents using a Web browser. The WebNow component enables ImageNow functionality to be used over a highly distributed Wide Area Network (WAN).

Users access WebNow from their client computer by supplying a URL to WebNow in a web browser. From their browser connection to WebNow, users can view and search documents stored in ImageNow, and participate in workflows created in the ImageNow Client. User permissions are set in the ImageNow Client.

2.2.3 ImageNow Client

The Client is a desktop interface that provides access to all ImageNow functions such as document capture, viewing, searching, indexing documents, and creating and participating in workflows. Users are created and permissions are granted using ImageNow Client.

ImageNow Client connects directly to the ImageNow Server Scanning, and indexing operations are conducted in the ImageNow Client. Third, Perceptive Software's LearnMode technology exists only in the ImageNow Client.

2.2.4 Physical Boundaries

The ImageNow Server component runs on the following platforms:

- Microsoft Windows 2000 and 2003
- Sun Microsystems Solaris 8, 9 and 10 (SPARC processor)
- The ImageNow Server requires an embedded C-Tree database, or an external database. Supported external databases include: Oracle 8i, 9i and 10g and MS SQL Server 2000 (Service Pack 3a or higher)

The ImageNow Client component runs on the following platforms:

- Microsoft Windows 2000 and XP Professional, version SP2

WebNow runs on the following platforms:

- Microsoft Windows 2000 and 2003
- Sun Microsystems Solaris 8, 9 and 10 (SPARC processor)
- Additionally, WebNow requires a J2EE Server. WebNow supports five J2EE Web application servers: Macromedia® JRun™ 4.0, BEA® WebLogic® 8.x, IBM® WebSphere 6.x, Apache Tomcat 5.x (open-source), and Oracle® Application Server 10.1.2.

Users who access WebNow with a web browser require the following configuration on their computer:

- An Internet Explorer 5.5 or Mozilla Firefox 1.0.1 (for Windows) web browser.
- Java 1.4x or higher Sun Microsystems® Java Runtime Environment (JRE), 32-Bit version.

Directories

- LDAP compliant directory products
- Microsoft Active Directory, as provided by supported Microsoft operating systems

The TOE relies on each of the components identified above to help protect the TOE in its environment. The operating systems and databases are expected to provide a secure execution environment and to protect the files that contain the TOE and its data, including the user data stores managed by the TOE and its generated audit records. The directory servers are expected to provide a reliable means of authentication and protect authentication data.

2.2.5 Logical Boundaries

The TOE logically supports the following security functions at its interfaces:

- Security audit
- User data protection
- Identification and authentication
- Security management

2.2.5.1 Security audit

ImageNow generates an audit record for audit mechanism start-up and shutdown events, as well as viewing, deleting, and re-indexing images. Each audit record includes the date and time of the event, type of event, subject identity, the IP and MAC addresses where the event occurred, and the outcome of the event. An Owner or Manager can review the audited records. In addition, ImageNow provides audit selection capabilities for reviewing audit data. The audit events are stored on the underlying operating system. The Information Technology (IT) environment provides a reliable timestamp for audit use and the protection of the audit records.

2.2.5.2 User data protection

ImageNow enforces rules-based access control on users and groups. The Owner or Manager has the ability to grant access (known as privileges) on the drawer objects that contain document pages.

2.2.5.3 Identification and authentication

ImageNow maintains a list of security attributes for users and requires users to be authorized prior to granted access to protected functions as security attributes are associated to users. The TOE relies on the IT environment to authenticate users using user and password mechanisms provided by directory services

2.2.5.4 Security management

ImageNow restricts the ability to manage user security policy rules. This is accomplished in a manner similar to that employed to control access to drawers – global privileges are required to successfully perform specific security management and other TOE functions. ImageNow provides the functions necessary for effective management of the security functions and all actions are accomplished on the Client with the exception of auditing, as that is accomplished via the ISA console.

2.3 TOE Documentation

Perceptive Software offers a series of documents that describe the installation process for the TOE as well as guidance for subsequent use and administration of the applicable security features. Refer to Section 6 for information about these and other documentation associated with the TOE.

3. Security Environment

This section summarizes the threats addressed by the TOE and assumptions about the intended environment of the TOE. Note that while the identified threats are mitigated by the security functions implemented in the TOE, the overall assurance level (EAL 2 augmented with ALC_FLR.2 and AVA_MSU.1) also serves as an indicator of whether the TOE would be suitable for a given environment.

3.1 Threats

T.AUTHENT	An authorized user may incorrectly change TOE data or functions they are authorized to modify.
T.MANAGE	An administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.
T.PROTECT	An attacker may be able to gain unauthorized access to TOE data or functions.

3.2 Assumptions

A.NO_EVIL	Authorized administrators are non-hostile, appropriately trained and follow all administrator guidance.
A.PHYSICAL	It is assumed that appropriate security is provided within the environment of the TOE for the value of the IT assets protected by the TOE and the value of the stored, processed, and transmitted information.

4. Security Objectives

This section summarizes the security objectives for the TOE and its environment.

4.1 Security Objectives for the TOE

O.ADMIN_ROLE	The TOE will provide authorized administrator roles to isolate administrative actions.
O.AUDIT_GENERATION	The TOE will provide the capability to detect and create records of security relevant events associated with users.
O.AUDIT_REVIEW	In a Windows configuration, the TOE will provide the capability to view audit information and ensure it is available only to authorized administrators.
O.DISCRETIONARY_ACCESS	The TOE will control access to resources based upon the identity of users or groups of users.
O.MANAGE	The TOE will provide all the functions and facilities necessary to support the authorized administrators in their management of the security of the TOE.
O.USER_IDENTIFICATION	The TOE will uniquely identify users.

4.2 Security Objectives for the IT Environment

OE.AUDIT_SUPPORT	The IT environment will protect audit data stored from unauthorized access and, in a Solaris configuration, the IT environment will provide the capability to view audit information and ensure it is available only to authorized administrators.
OE.TIME	The IT environment will provide a time source that provides reliable time stamps.
OE.PROTECT_TOE	The IT environment will provide protection to the TOE and its assets from external interference or tampering.
OE.USER_AUTHENTICATION	The IT environment will authenticate users.

4.3 Security Objectives for the Environment

OE.ADMIN_GUIDANCE	The TOE guidance documentation will provide authorized administrators with the necessary information for secure management of the TOE.
OE.CONFIG	The TOE will be installed, configured, managed and maintained in accordance with its guidance documentation and applicable security policies and procedures.

OE.INSTALL	The TOE will be delivered with the appropriate installation guidance to establish and maintain TOE security.
OE.PHYSICAL	Physical security will be provided within the domain for the value of the IT assets protected by the TOE and the value of the stored, processed, and transmitted information.
OE.SELF_PROTECTION	IT environment and its assets will be protected from external interference, tampering or unauthorized disclosure.

5. IT Security Requirements

This section defines the Security Functional Requirements (SFRs) for the TOE as well as the security assurance requirements against which the TOE has been evaluated. All of the requirements have been copied from version 2.2 of the applicable Common Criteria documents.

5.1 TOE Security Functional Requirements

The following table describes the Security Functional Requirements (SFRs) that are satisfied by ImageNow v5.42 SP3 and WebNow v3.42.

Requirement Class	Requirement Component
FAU: Security audit	FAU_GEN.1: Audit data generation
	FAU_SAR.1a: Audit review
	FAU_SAR.2a: Restricted audit review
FDP: User data protection	FDP_ACC.2: Complete access control
	FDP_ACF.1: Security attribute based access control
FIA: Identification and authentication	FIA_ATD.1: User attribute definition
	FIA_UID.2a: User identification before any action
FMT: Security management	FMT_MSA.1: Management of security attributes
	FMT_MSA.3: Static attribute initialization
	FMT_MTD.1a: Management of TSF data
	FMT_MTD.1b: Management of TSF data
	FMT_SMF.1: Specification of Management Functions
	FMT_SMR.1: Security roles

Table 1 TOE Security Functional Components

5.1.1 Security audit (FAU)

5.1.1.1 Audit data generation (FAU_GEN.1)

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events: a) Start-up and shutdown of the audit functions; b) All auditable events for the [***not specified***] level of audit; and c) [**copy, delete, move or view a document; delete, view, or insert a page in a document; add, delete, or update a drawer; add, delete, or update a group; add or delete users to or from a group; grant privileges to a user or group; and add, delete, or update users**].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information: a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [**user connection information (IP and MAC addresses)**].

5.1.1.2 Audit review (FAU_SAR.1a)

FAU_SAR.1a.1 **In a Windows configuration, t**he TSF shall provide **[Owner, Manager]** with the capability to read [**all audit information**] from the audit records.

FAU_SAR.1a.2 **In a Windows configuration, t**he TSF shall provide the audit records in a manner suitable for the user to interpret the information.

5.1.1.3 Restricted audit review (FAU_SAR.2a)

FAU_SAR.2a.1 **In a Windows configuration, t**he TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

5.1.2 User data protection (FDP)

5.1.2.1 Complete access control (FDP_ACC.2)

FDP_ACC.2.1 The TSF shall enforce the [**ImageNow Access Control SFP**] on [**subjects: users; objects: drawers**] and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP.

5.1.2.2 Security attribute based access control (FDP_ACF.1)

FDP_ACF.1.1 The TSF shall enforce the [**ImageNow Access Control SFP**] to objects based on the following: [**subject security attributes: user ID, group IDs, and privileges; object security attributes: drawer identifier**].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:
[
(a) if the user ID has been denied the privilege to perform the requested operation on the identified object, the operation is not allowed and no further rules are processed;
(b) if the user ID has been granted the privilege to perform the requested operation on the identified object, the operation is allowed and no further rules are processed;
(c) if the user ID belongs to any group where the associated group ID has been denied the privilege to perform the requested operation on the identified object, the operation is not allowed and no further rules are processed;
(d) if the user ID belongs to any group where the associated group ID has been granted the privilege to perform the requested operation on the identified object, the operation is allowed and no further rules are processed;
(e) otherwise, i.e., if the user ID and all applicable groups IDs have not been granted or denied the applicable privilege, the operation is not allowed
].

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [**no additional authorize access rules**].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the **[no additional rules**].

5.1.3 Identification and authentication (FIA)

5.1.3.1 User attribute definition (FIA_ATD.1)

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [**user ID, group ID, privileges**].

5.1.3.2 User identification before any action (FIA_UID.2a)

FIA_UID.2a.1 The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

5.1.4 Security management (FMT)

5.1.4.1 Management of security attributes (FMT_MSA.1)

FMT_MSA.1.1 The TSF shall enforce the [**ImageNow Access Control SFP**] to restrict the ability to [***query, modify, delete*****]** the security attributes [**user ID, group, and privileges**] to [**Owner or Manager with the applicable privilege**].

5.1.4.2 Static attribute initialization (FMT_MSA.3)

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

FMT_MSA.3.2 The TSF shall allow the [**Owner**] to specify alternative initial values to override the default values when an object or information is created.

5.1.4.3 Management of TSF data (FMT_MTD.1a)

FMT_MTD.1a.1 The TSF shall restrict the ability to [***modify, delete,*** [**create**]] the [**user accounts**] to [**Owner or Manager with the applicable privilege**].

5.1.4.4 Management of TSF data (FMT_MTD.1b)

FMT_MTD.1b.1 The TSF shall restrict the ability to [***modify***] the [**event auditing**] to [**Owner or Manager with the applicable privilege**].

5.1.4.5 Specification of Management Functions (FMT_SMF.1)

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [**management of user accounts and user attributes; which includes the ability to create, modify, and delete user accounts, management of object security attributes, and ability to determine the events that will be audited**].

5.1.4.6 Security roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the roles [**Owner, Manager, and User**].

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

5.2 IT Environment Security Functional Requirements

The following table describes the Security Functional Requirements (SFRs) that need to be satisfied by the IT environment of the TOE.

Requirement Class	Requirement Component
FAU: Security audit	FAU_SAR.1b: Audit review
	FAU_SAR.2b: Restricted audit review
	FAU_STG.1: Protected audit trail storage
FIA: Identification and authentication	FIA_UAU.2: User authentication before any action
	FIA_UID.2b: User identification before any action
FPT: Protection of the TSF	FPT_RVM.1: Non-bypassability of the TSP
	FPT_SEP.1: Domain separation
	FPT_STM.1: Reliable time stamps

Table 2 IT Environment Security Functional Components

5.2.1 Security audit (FAU)

5.2.1.1 Audit review (FAU_SAR.1b)

FAU_SAR.1b.1 **In a Solaris configuration, t**he ~~TSF~~ **IT Environment** shall provide **[Owner, Manager]** with the capability to read [**all audit information**] from the audit records.

FAU_SAR.1b.2 **In a Solaris configuration, t**he ~~TSF~~ **IT Environment** shall provide the audit records in a manner suitable for the user to interpret the information.

5.2.1.2 Restricted audit review (FAU_SAR.2b)

FAU_SAR.2b.1 **In a Solaris configuration, t**he ~~TSF~~ **IT Environment** shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

5.2.1.3 Protected audit trail storage (FAU_STG.1)

FAU_STG.1.1 The ~~TSF~~ **IT Environment** shall protect the stored audit records from unauthorized deletion.
FAU_STG.1.2 The ~~TSF~~ **IT Environment** shall be able to [***prevent***] unauthorized modifications to the audit records in the audit trail.

5.2.2 Identification and authentication (FIA)

5.2.2.1 User authentication before any action (FIA_UAU.2)

FIA_UAU.2.1 The ~~TSF~~ **IT Environment** shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

5.2.2.2 User identification before any action (FIA_UID.2b)

FIA_UID.2b.1 The ~~TSF~~ **IT Environment** shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

5.2.3 Protection of the TSF (FPT)

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

FPT_RVM.1.1 The ~~TSF~~ **IT Environment** shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

5.2.3.2 Domain separation (FPT_SEP.1)

FPT_SEP.1.1 The ~~TSF~~ **IT Environment** shall maintain a security domain for its own execution that protects it from interference and tampering from untrusted subjects.

FPT_SEP.2.1 The ~~TSF~~ **IT Environment** shall enforce separation between the security domains of subjects in the TSC.

5.2.3.3 Reliable time stamps (FPT_STM.1)

FPT_STM.1.1 The ~~TSF~~ **IT Environment** shall be able to provide reliable time stamps for its own use **and for use by the TOE**.

5.3 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the EAL 2 augmented with ALC_FLR.2 and AVA_MSU.1 components as specified in Part 3 of the Common Criteria. No operations are applied to the assurance components.

Requirement Class	Requirement Component
ACM: Configuration management	ACM_CAP.2: Configuration items
ADO: Delivery and operation	ADO_DEL.1: Delivery procedures
	ADO_IGS.1: Installation, generation, and start-up procedures
ADV: Development	ADV_FSP.1: Informal functional specification
	ADV_HLD.1: Descriptive high-level design
	ADV_RCR.1: Informal correspondence demonstration
AGD: Guidance documents	AGD_ADM.1: Administrator guidance
	AGD_USR.1: User guidance
ALC: Life cycle support	ALC_FLR.2: Flaw reporting procedures
ATE: Tests	ATE_COV.1: Evidence of coverage
	ATE_FUN.1: Functional testing
	ATE_IND.2: Independent testing - sample
AVA: Vulnerability assessment	AVA_MSU.1: Examination of guidance
	AVA_SOF.1: Strength of TOE security function evaluation
	AVA_VLA.1: Developer vulnerability analysis

Table 3 EAL 2 augmented with ALC_FLR.2 and AVA_MSU.1 Assurance Components

5.3.1 Configuration management (ACM)

5.3.1.1 Configuration items (ACM_CAP.2)

ACM_CAP.2.1d The developer shall provide a reference for the TOE.
ACM_CAP.2.2d The developer shall use a CM system.
ACM_CAP.2.3d The developer shall provide CM documentation.
ACM_CAP.2.1c The reference for the TOE shall be unique to each version of the TOE.
ACM_CAP.2.2c The TOE shall be labeled with its reference.
ACM_CAP.2.3c The CM documentation shall include a configuration list.
ACM_CAP.2.4c The configuration list shall uniquely identify all configuration items that comprise the TOE.
ACM_CAP.2.5c The configuration list shall describe the configuration items that comprise the TOE.
ACM_CAP.2.6c The CM documentation shall describe the method used to uniquely identify the configuration items.
ACM_CAP.2.7c The CM system shall uniquely identify all configuration items.
ACM_CAP.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.2 Delivery and operation (ADO)

5.3.2.1 Delivery procedures (ADO_DEL.1)

ADO_DEL.1.1d The developer shall document procedures for delivery of the TOE or parts of it to the user.
ADO_DEL.1.2d The developer shall use the delivery procedures.
ADO_DEL.1.1c The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

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

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

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

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

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

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

5.3.3 Development (ADV)

5.3.3.1 Informal functional specification (ADV_FSP.1)

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

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

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

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

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

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

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

5.3.3.2 Descriptive high-level design (ADV_HLD.1)

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

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

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

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

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

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

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

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

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

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

5.3.3.3 Informal correspondence demonstration (ADV_RCR.1)

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

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

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

5.3.4 Guidance documents (AGD)

5.3.4.1 Administrator guidance (AGD_ADM.1)

AGD_ADM.1.1d The developer shall provide administrator guidance addressed to system administrative personnel.
AGD_ADM.1.1c The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.
AGD_ADM.1.2c The administrator guidance shall describe how to administer the TOE in a secure manner.
AGD_ADM.1.3c The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.
AGD_ADM.1.4c The administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE.
AGD_ADM.1.5c The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.
AGD_ADM.1.6c The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.
AGD_ADM.1.7c The administrator guidance shall be consistent with all other documentation supplied for evaluation.
AGD_ADM.1.8c The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.
AGD_ADM.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.4.2 User guidance (AGD_USR.1)

AGD_USR.1.1d The developer shall provide user guidance.
AGD_USR.1.1c The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.
AGD_USR.1.2c The user guidance shall describe the use of user-accessible security functions provided by the TOE.
AGD_USR.1.3c The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.
AGD_USR.1.4c The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behavior found in the statement of TOE security environment.
AGD_USR.1.5c The user guidance shall be consistent with all other documentation supplied for evaluation.
AGD_USR.1.6c The user guidance shall describe all security requirements for the IT environment that are relevant to the user.
AGD_USR.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.5 Life cycle support (ALC)

5.3.5.1 Flaw reporting procedures (ALC_FLR.2)

ALC_FLR.2.1d The developer shall provide flaw remediation procedures addressed to TOE developers.
ALC_FLR.2.2d The developer shall establish a procedure for accepting and acting upon all reports of security flaws and requests for corrections to those flaws.
ALC_FLR.2.3d The developer shall provide flaw remediation guidance addressed to TOE users.
ALC_FLR.2.1c The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.
ALC_FLR.2.2c The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.
ALC_FLR.2.3c The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

ALC_FLR.2.4c The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.
ALC_FLR.2.5c The flaw remediation procedures documentation shall describe a means by which the developer receives from TOE users reports and enquiries of suspected security flaws in the TOE.
ALC_FLR.2.6c The procedures for processing reported security flaws shall ensure that any reported flaws are corrected and the correction issued to TOE users.
ALC_FLR.2.7c The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.
ALC_FLR.2.8c The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE.
ALC_FLR.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.6 Tests (ATE)

5.3.6.1 Evidence of coverage (ATE_COV.1)

ATE_COV.1.1d The developer shall provide evidence of the test coverage.
ATE_COV.1.1c The evidence of the test coverage shall show the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.
ATE_COV.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.6.2 Functional testing (ATE_FUN.1)

ATE_FUN.1.1d The developer shall test the TSF and document the results.
ATE_FUN.1.2d The developer shall provide test documentation.
ATE_FUN.1.1c The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.
ATE_FUN.1.2c The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.
ATE_FUN.1.3c The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.
ATE_FUN.1.4c The expected test results shall show the anticipated outputs from a successful execution of the tests.
ATE_FUN.1.5c The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.
ATE_FUN.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.6.3 Independent testing - sample (ATE_IND.2)

ATE_IND.2.1d The developer shall provide the TOE for testing.
ATE_IND.2.1c The TOE shall be suitable for testing.
ATE_IND.2.2c The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.
ATE_IND.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ATE_IND.2.2e The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.
ATE_IND.2.3e The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

5.3.7 Vulnerability assessment (AVA)

5.3.7.1 Examination of guidance (AVA_MSU.1)

AVA_MSU.1.1d The developer shall provide guidance documentation.
AVA_MSU.1.1c The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.
AVA_MSU.1.2c The guidance documentation shall be complete, clear, consistent and reasonable.
AVA_MSU.1.3c The guidance documentation shall list all assumptions about the intended environment.
AVA_MSU.1.4c The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).
AVA_MSU.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_MSU.1.2e The evaluator shall repeat all configuration and installation procedures to confirm that the TOE can be configured and used securely using only the supplied guidance documentation.
AVA_MSU.1.3e The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.

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

AVA_SOF.1.1d The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.
AVA_SOF.1.1c For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.
AVA_SOF.1.2c For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.
AVA_SOF.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_SOF.1.2e The evaluator shall confirm that the strength claims are correct.

5.3.7.3 Developer vulnerability analysis (AVA_VLA.1)

AVA_VLA.1.1d The developer shall perform a vulnerability analysis.
AVA_VLA.1.2d The developer shall provide vulnerability analysis documentation.
AVA_VLA.1.1c The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for obvious ways in which a user can violate the TSP.
AVA_VLA.1.2c The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities.
AVA_VLA.1.3c The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.
AVA_VLA.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_VLA.1.2e The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

6. TOE Summary Specification

This chapter describes the security functions and associated assurance measures.

6.1 TOE Security Functions

6.1.1 Security audit

The TOE provides its own audit mechanism that can generate audit records for audit mechanism start-up and shutdown events, as well as the following events:

- copy, delete, move or view a document
- delete, view, or insert a page in a document
- add, delete, or update a drawer
- add, delete, or update a group
- add or delete users to or from a group
- grant privileges to a user or group
- add, delete, or update users

Auditing is not enabled by default. An administrator must enable auditing in the evaluated configuration. To manage the auditable events, one of the following auditing scripts must be used: for Windows, apply_cc_audit.bat and for UNIX, apply_cc_audit.sh. These scripts configure the ImageNow Server to audit server events (both ImageNow Client and WebNow events) and agent events (all agents included in the evaluated configuration).

The audit trail is stored in files on the ImageNow Server. Each audit record identifies the event type, date and time of the event, type of event, and subject identity, and user connection information. Events are logged when successful. If an event is unsuccessful, it is trapped and corrected by the user interface. Similar events are audited in ImageNow Client and WebNow, except that WebNow does not have the ability to perform or audit the following events: insert page or delete page. When a new user is added, you must turn auditing on for that user.

In a Windows configuration, the audit trail can be accessed using ISA. Access to the audit trail using the TOE is restricted by the administrator console to either “Owner” or “Manager” roles. The administrator console and roles are both described in the security management function description below. Note that the TOE offers the abilities to review and delete audit records, but offers no functions that would allow audit records to be otherwise modified.

In a Solaris configuration, the audit trail can be access by viewing the appropriate files that are protected by the underlying Solaris operating system and hence the review capability is provided and protected by the IT environment in this case.

The Security audit function is designed to satisfy the following security functional requirements:

- FAU_GEN.1: The audit events as well as the audit record content enumerated above represent a superset of that required.
- FAU_SAR.1a: In Windows, users possessing “Owner” or “Manager” roles can log into the ISA (server) to view all audit records stored in the audit trail.
- FAU_SAR.2a: In Windows, users possessing “Owner” or “Manager” roles have viewing capability in the ISA (server) to view audit records stored in the audit trail.

6.1.2 User data protection

The TOE implements a discretionary access control (DAC) policy for object access based on:

- user identities,
- group memberships,

- and privileges.

The TOE objects subject to this policy are drawers. Other objects are part of the protected object (i.e., a scanned document image). The TOE implements an electronic filing system that is analogous to a paper filing cabinet scheme where the physical organization of documents is replaced with logical storage.

Objects

The TOE is able to store virtually any type of electronic file, or object. An object can be a scanned document image, a Microsoft Excel spreadsheet, a WordPerfect document, or a variety of other files. The difference between individual objects and documents is as follows: an image is a digital representation of a single piece of paper. The image consists of one and only one object. Similarly, an Excel spreadsheet is a single object. A document refers to an index value that uniquely identifies a single object or group of objects, as depicted in the figure below. The first DocKey is called the drawer.

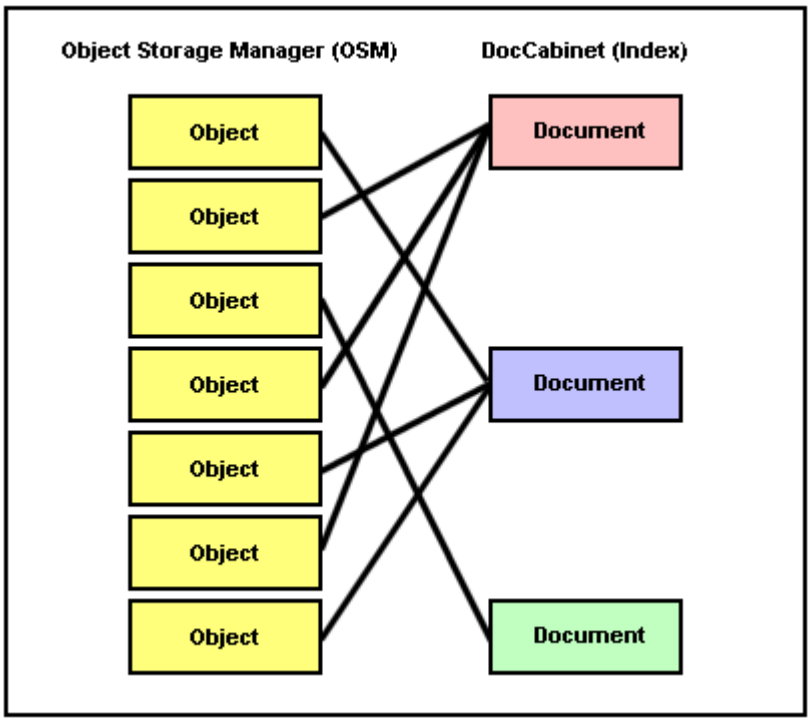

Figure 2: TOE objects

There are six index values (DocKeys) that identify any given object:

- Drawer
- Folder
- Tab
- Field3
- Field4
- Field5

Note that when an object is created the Field5 index value must be assigned a unique identifier for the corresponding document by either the object creator or the administrator.

User and Groups

Groups are used in ImageNow by users with management privileges, Managers, and the Owner to organize users, and assign and manage their privileges. Groups serve as a tool to help organize and manage privileges more

generally. For example, create a group called Accounting and add all of the users who will need access to the Accounting drawer, users who will scan documents into the Accounting drawer, users who create annotations on documents in the Accounting drawer, users who will create batches in the Accounting drawer, and so on. The privileges for all the accounting users can be set at once by assigning their privileges at the group level. To go further, it may be necessary to create different groups for different types of users in the Accounting department. For example, you might have a group of users who perform all of the scanning tasks and require privileges to scan documents into the Accounting Drawer but not copy or move the documents. Another group might be assigned privileges to create and process batches in the Accounting Drawer. A third group might be created with privileges to access documents in PowerView mode only. Both global privileges and drawer privileges can be assigned at the group level instead of at the user level to simplify assignment and management of privileges for several users at once.

Object Access

Access to stored images is restricted to authorized users. Access control is applied to the objects, i.e., 'drawers', implemented by the TOE. Users and/or groups are granted access to drawer and their contents by virtue of (drawer) privilege assignments. Note that the TOE implements *global* privileges which apply to security relevant (i.e., management) and other general operations of the TOE and *drawer* privileges which apply specifically to the operations related to drawers.

Privileges can be granted, denied or remain unassigned to individual users and to the groups to which they belong. Each user can utilize the privileges directly assigned as well as any privileges assigned to any of their groups. Note that users can belong to groups, but groups cannot belong to other groups. Since user and group privileges can potentially conflict, the TOE employs a priority scheme to resolve conflicts. User privileges take precedent over group privileges and denied privileges take precedent over granted privileges. Hence, if a user is either denied or granted a privilege, that is it and there is no need to examine any group privileges. However, if one group grants a privilege and another denies it, the denial will take precedent and the privilege would be denied.

Note that that there are (drawer) privileges associated with each operation that can be performed on a drawer (e.g., view, copy delete, move) and their contents (e.g., add notations, print). The administrator guide should be consulted for a complete list of privileges and the associated operations.

The User data protection function is designed to satisfy the following security functional requirements:

- FDP_ACC.2: The access control policy ensures that users can access drawers only when they are appropriately authorized to do so.
- FDP_ACF.1: When a user attempts to access a drawer, their identity and groups memberships are used to determine whether they have the privilege necessary to perform that operation and to enforce the result.

6.1.3 Identification and authentication

The TOE implements a DAC policy for object access based on the following subject security attributes:

- user identities,
- group memberships, and
- privileges.

The TOE defines user identities, group memberships, and privileges, but it does not authenticate users. Instead, the TOE relies on the IT environment to authenticate users. The TOE requires all users to supply user ID and password to access the system and data. Note that group memberships and privileges are described in the user data protection security function description above.

The user ID and password information is passed by the TOE to operating system of the local machine in the IT environment. Note that the product supports three types of authentication: System, LDAP, and SQL. By default, ImageNow is set to System user authentication, where users are authenticated against the native directory service for the operating system on which the ImageNow Server is running. For example, System authentication on Windows uses Microsoft Active Directory. In LDAP authentication, users are authenticated against an LDAP server. In SQL

authentication, users are authenticated against an ODBC SQL database. The authentication results are passed back to ImageNow. If the user is successfully identified and authenticated, ImageNow user rights and privileges are determined and assigned by the TOE.

The Identification and authentication function is designed to satisfy the following security functional requirements:

- FIA_ATD.1: The TOE defines user identities, group memberships, and privileges.
- FIA_UID.2a: ImageNow collects the user ID and password information and passes to the IT environment to perform identification and authentication. The TOE enforces the results provided by the IT environment and performs user identification for access control.

6.1.4 Security management

The components involved in managing TOE security functions are:

- ImageNow Server
  - provides interfaces (via its ISA Console application) to manage audit
- ImageNow Client
  - provides interfaces to manage users and user security attributes
  - provides interfaces to manage objects and object security attributes

ImageNow has predefined roles; Owner and Manager. The Owner in ImageNow is the top-level user role. There is exactly one Owner in an implementation of ImageNow. Creation of the Owner is done during the initial installation of ImageNow Server. The Owner creates user accounts and assigns privileges. A user can be assigned the system-defined Manager role. Note that a user is also considered a Manager if they have been granted some or all administrative or management type (global) privileges[1]. Owners and Managers create 'drawers' and assign privileges (including both drawer and global privileges) to users and groups. Any user that is not an Owner or Manager is considered to be a User.

User Role

A user is in the User role if they have no management (global) privileges within ImageNow. The user is assigned drawer (or non-security relevant global, e.g., print) privileges to perform tasks within ImageNow by a Manager or the Owner. The user can be promoted or demoted to the system-defined Manager role (see below) only by the Owner. Alternately, they can be made into a Manager by granted specific management privileges.

Users in the User role generally include those who scan documents, process batches, access documents in PowerView, link scanned documents to drawers, and the dozens of other features available in ImageNow.

Manager Role

The Manager Role is defined as a user that has been assigned one or more management (global) privileges and/or has been assigned the system-defined Manager Role explicitly.

Users in this role can be assigned any of the management (global) privileges as well as any drawer privileges, if necessary. A Manager may be able to add users, groups, drawers and assign privileges based on their management privileges. Though their functions can be more limited if the user has not been assigned the system-defined manager role and has not been granted all of the management privileges.

A user assigned the system-defined Manager Role user must be promoted to a manager by the Owner in ImageNow. The system-defined Manager can do almost everything that the Owner can do within the system. No Manager can

[1] Examples of management global privileges include: Users – allowing the creation, deletion, and modification of users (and assignment of their privileges); Groups – allowing the creation deletion, and modification of groups (and assignment of users and privileges); Drawers – allowing the creation, deletion and modification of drawers; and Security Administration – allowing the general ability to administer the server. The administrator guide should be consulted for a complete list of privileges and their meanings.

promote or demote users to the system-defined Manager role. There can be many Managers in an implementation of ImageNow. The Manager will define users and their abilities in the system by assigning privileges to them.

Owner Role

Every implementation of ImageNow must have one Owner. In ImageNow, the terms "Owner" and "Administrator" are synonymous. The owner can perform any ISA or ImageNow Client function.

The Security management function is designed to satisfy the following security functional requirements:

- FMT_MSA.1.1: Users are restricted by default – they have no privileges. Only an Owner can perform all security management; however, the Manager role or User role granted management privileges can also be granted certain administrative rights.
- FMT_MSA.3: By default, every drawer object is created without any user, group, or privilege assignments, although a user possessing the Owner role can create a new drawer with the same privilege assignments as an existing drawer using the ImageNow Client interfaces.
- FMT_MTD.1a: The ability to create, modify, or delete user accounts is restricted to a user possessing the Owner role or a user given specific Manager privileges through restrictions enforced by ImageNow Client interface.
- FMT_MTD.1b: The ability to modify events to be audited is restricted to a user possessing the Owner role or a user given specific Manager privileges through restrictions enforced by the ISA interface.
- FMT_SMF.1: The TOE provides the ImageNow Client interface to manage users and objects. The ISA interface enables users to manage the auditable events.
- FMT_SMR.1: The TOE provides three roles that can be assigned to users:
  - Owner – every implementation of the TOE must have an Owner role defined and only one is allowed. The Owner is the top level user role in the system with access to change all security privileges. Only the Owner can promote or demote users to the level of the Manager role.
  - Manager – the Manager can do almost everything that the Owner can do within the system. The Manager can define users and their purpose in the system by assigning privileges to them.
  - User – user who, by default, has no management privileges.

6.2 TOE Security Assurance Measures

6.2.1 Configuration management

The configuration management measures applied by Perceptive Software ensure that configuration items are uniquely identified, and that documented procedures are used to control and track changes that are made to the TOE. Perceptive Software ensures changes to the implementation representation are controlled. Perceptive Software performs configuration management on the TOE design documentation, tests and test documentation, user and administrator guidance, delivery and operation documentation, life-cycle documentation, vulnerability analysis documentation, and configuration management documentation.

These activities are documented in:

- Perceptive Software Configuration Management Plan

The Configuration management assurance measure satisfies the following EAL 2 augmented with ALC_FLR.2 and AVA_MSU.1 assurance requirements:

- ACM_CAP.2

6.2.2 Delivery and operation

Perceptive Software provides delivery documentation and procedures to identify the TOE, secure the TOE during delivery, and provide necessary installation and generation instructions. Perceptive Software delivery procedures describe all applicable procedures to be used to prevent in appropriate access to the TOE. Perceptive Software also provides documentation that describes the steps necessary to install the TOE in accordance with the evaluated configuration.

These activities are documented in:

- Perceptive Software Installation and Delivery Guide

The Delivery and operation assurance measure satisfies the following EAL 2 augmented with ALC_FLR.2 and AVA_MSU.1 assurance requirements:

- ADO_DEL.1
- ADO_IGS.1

6.2.3 Development

Perceptive Software has numerous documents describing all facets of the design of the TOE. In particular, they have a functional specification that describes the accessible TOE interfaces; a high-level design that decomposes the TOE architecture into subsystems and describes each subsystem and their interfaces; and, correspondence documentation that explains how each of the design abstractions correspond from the TOE summary specification in the Security Target to the subsystems.

These activities are documented in:

- ImageNow Functional Specification
- ImageNow High-level Design
- ImageNow Design Correspondence Analysis

The Development assurance measure satisfies the following EAL 2 augmented with ALC_FLR.2 and AVA_MSU.1 assurance requirements:

- ADV_FSP.1
- ADV_HLD.1
- ADV_RCR.1

6.2.4 Guidance documents

Perceptive Software provides administrator and user guidance on how to utilize the TOE security functions and warnings to administrators and users about actions that can compromise the security of the TOE.

These activities are documented in:

- ImageNow Administration Guide
- ImageNow User Guide
- ImageNow ISA Guide

The Guidance documents assurance measure satisfies the following EAL 2 augmented with ALC_FLR.2 and AVA_MSU.1 assurance requirements:

- AGD_ADM.1
- AGD_USR.1

6.2.5 Life cycle support

Perceptive Software ensures the adequacy of the procedures used during the development and maintenance of the TOE through its life-cycle. Perceptive Software includes security controls on the development environment that are adequate to provide the confidentiality and integrity of the TOE design and implementation that is necessary to ensure the secure operation of the TOE. In addition, Perceptive Software identifies and tracks reported flaws, ensuring that they are addressed and corrections and corrective measures are made available as applicable.

These activities are documented in:

- ImageNow Life-cycle Plan

The Life cycle support assurance measure satisfies the following EAL 2 augmented with ALC_FLR.2 and AVA_MSU.1 assurance requirements:

- ALC_FLR.2

6.2.6 Tests

Perceptive Software has a test plan that describes how each of the necessary security functions is tested, along with the expected test results. Perceptive Software has documented each test as well as an analysis of test coverage and depth demonstrating that the security aspects of the design evident from the functional specification and high-level design are appropriately tested. Actual test results are created on a regular basis to demonstrate that the tests have been applied and that the TOE operates as designed.

These activities are documented in:

- ImageNow Test Plan
- ImageNow Test Coverage Analysis
- ImageNow Test Results

The Tests assurance measure satisfies the following EAL 2 augmented with ALC_FLR.2 and AVA_MSU.1 assurance requirements:

- ATE_COV.1
- ATE_FUN.1
- ATE_IND.2

6.2.7 Vulnerability assessment

The TOE administrator and user guidance documents describe the operation of the TOE and how to maintain a secure state. These guides also describe all necessary operating assumptions and security requirements outside the scope of control of the TOE. They have been developed to serve as complete, clear, consistent, and reasonable administrator and user references.

Perceptive Software performs regular vulnerability analyses of the entire TOE (including documentation) to identify obvious weaknesses that can be exploited in the TOE.

These activities are documented in:

- Perceptive Software Vulnerability Analysis Report

The Vulnerability assessment assurance measure satisfies the following EAL 2 augmented with ALC_FLR.2 and AVA_MSU.1 assurance requirements:

- AVA_MSU.1
- AVA_SOF.1 – note that there are no applicable security functions, there is no SOF claim
- AVA_VLA.1

7. Protection Profile Claims

There is no Protection Profile claim in this Security Target

8. Rationale

This section provides the rationale for completeness and consistency of the Security Target. The rationale addresses the following areas:

- Security Objectives;
- Security Functional Requirements;
- Security Assurance Requirements;
- Strength of Functions;
- Requirement Dependencies;
- TOE Summary Specification; and,
- PP Claims.

8.1 Security Objectives Rationale

This section shows that all secure usage assumptions, organizational security policies, and threats are completely covered by security objectives. In addition, each objective counters or addresses at least one assumption, organizational security policy, or threat.

8.1.1 Complete Coverage – Threats

This section shows that all secure usage assumptions, organizational security policies, and threats are completely covered by security objectives. In addition, each objective counters or addresses at least one assumption, organizational security policy, or threat.

	O.ADMIN_ROLE	O.AUDIT_GENERATION	O.AUDIT_REVIEW	O.DISCRETIONARY_ACCESS	O.USER_IDENTIFICATION	O.MANAGE	OE.AUDIT_SUPPORT	OE.TIME	OE.PROTECT_TOE	OE.USER_AUTHENTICATION
T.AUTHENT		x			x			x		x
T.MANAGE	x	x	x			x		x		
T.PROTECT				x			x		x	

Table 4 Threat to objective Correspondence

8.1.1.1 T.AUTHENT

An authorized user may incorrectly change TOE data or functions they are authorized to modify.

This Threat is satisfied by ensuring that:

- O.AUDIT_GENERATION: The TOE audits security-relevant events, including actions that might represent an error.
- O.USER_IDENTIFICATION: The TOE ensures authorized users are identified before allowing access to TOE data or functions they are authorized to modify.
- OE.USER_AUTHENTICATION: The TOE ensures authorized users are authenticated by the IT environment before allowing access to TOE data or functions they are authorized to modify.
- OE.TIME: The IT environment provides reliable time for use in audit records.

8.1.1.2 T.MANAGE

An administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.

This Threat is satisfied by ensuring that:

- O.ADMIN_ROLE: The TOE defines security management roles distinct from other non-security management roles related to use of the TOE.
- O.AUDIT_GENERATION: The TOE audits security-relevant events, including actions that might represent an error.
- O.AUDIT_REVIEW: The TOE provides administrator console interfaces to review the audit trail, including records of actions that might represent an error.
- O.MANAGE: The TOE provides administrator console interfaces to manage TOE security functions.
- OE.TIME: The IT environment provides reliable time for use in audit records.

8.1.1.3 T.PROTECT

An attacker may be able to gain unauthorized access to TOE data or functions.

This Threat is satisfied by ensuring that:

- O.DISCRETIONARY_ACCESS: The TOE protects drawer objects using a DAC mechanism.
- OE.AUDIT_SUPPORT: The IT environment supports the audit function by protecting audit records from unauthorized access.
- OE.PROTECT_TOE: The IT environment protects server components from unauthorized access and ensures the TOE can only be accessed using its interfaces.

8.1.2 Complete Coverage – Policy

There are no organization security policies.

8.1.3 Complete Coverage – Environmental Assumptions

This section provides evidence demonstrating coverage of the Non-IT security objectives by the environmental assumptions. The following table shows this assumption to objective mapping.

	OE.ADMIN_GUIDANCE	OE.CONFIG	OE.INSTALL	OE.PHYSICAL	OE.SELF_PROTECTION
A.NO_EVIL	x	x	x		
A.PHYSICAL				x	x

Table 5 Assumption to objective Correspondence

8.1.3.1 A.NO_EVIL

Authorized administrators are non-hostile, appropriately trained and follow all administrator guidance.

This Assumption is satisfied by ensuring that:

- OE.ADMIN_GUIDANCE: This objective ensures guidance is available to administrators.
- OE.CONFIG: This objective ensures administrators follow guidance when installing, configuring, and managing the TOE.
- OE.INSTALL: This objective ensures installation and delivery procedures are available to administrators.

8.1.3.2 A.PHYSICAL

It is assumed that appropriate security is provided within the environment of the TOE for the value of the IT assets protected by the TOE and the value of the stored, processed, and transmitted information.

This Assumption is satisfied by ensuring that:

- OE.PHYSICAL: This objective ensures the TOE is physically protected.
- OE.SELF_PROTECTION: This objective ensures the IT environment protects itself from applicable attacks..

8.2 Security Requirements Rationale

This section provides evidence supporting the internal consistency and completeness of the components (requirements) in the Security Target. Note that **Table 6** indicates the requirements that effectively satisfy the individual objectives. .

8.2.1 Security Functional Requirements Rationale

All SFRs identified in this Security Target are fully addressed in this section and each SFR is mapped to the objective for which it is intended to satisfy.

	O.ADMIN_ROLE	O.AUDIT_GENERATION	O.AUDIT_REVIEW	O.DISCRETIONARY_ACCESS	O.MANAGE	O.USER_IDENTIFICATION	OE.AUDIT_SUPPORT	OE.TIME	OE.PROTECT_TOE	OE.USER_AUTHENTICATION
FAU_GEN.1		x								
FAU_SAR.1			x							
FAU_SAR.2			x		x					
FDP_ACC.2				x						
FDP_ACF.1				x						
FIA_ATD.1				x						
FIA_UID.2a				x		x				
FMT_MSA.1					x					
FMT_MSA.3					x					
FMT_MTD.1a					x					
FMT_MTD.1b					x					
FMT_SMF.1					x					
FMT_SMR.1	x				x					
FAU_SAR.1b							x			
FAU_SAR.2b							x			
FAU_STG.1							x			
FIA_UAU.2										x
FIA_UID.2b										x
FPT_RVM.1									x	
FPT_SEP.1									x	
FPT_STM.1								x		

Table 6 Objective to Requirement Correspondence

8.2.1.1 O.ADMIN_ROLE

The TOE will provide authorized administrator roles to isolate administrative actions.

This TOE Security Objective is satisfied by ensuring that:

- FMT_SMR.1: The TOE provides three distinct roles that can be explicitly assigned to users.

8.2.1.2 O.AUDIT_GENERATION

The TOE will provide the capability to detect and create records of security relevant events associated with users.

This TOE Security Objective is satisfied by ensuring that:

- FAU_GEN.1: The audit events as well as the audit record content enumerated above represent a superset of that required.
- FAU_STG.1: The IT environment is relied on to protect the audit trail from unauthorized access.

- FPT_STM.1: The IT environment is relied on to provide a reliable time source.

8.2.1.3 O.AUDIT_REVIEW

In a Windows configuration, the TOE will provide the capability to view audit information and ensure it is available only to authorized administrators.

This TOE Security Objective is satisfied by ensuring that:

- FAU_SAR.1a: In a Windows configuration users possessing "Owner" or "Manager" roles can log into the ISA (server) to view audit records stored in the audit trail.
- FAU_SAR.2a: In a Windows configuration users possessing "Owner" or "Manager" roles have viewing capability in the ISA (server) to view audit records stored in the audit trail.

8.2.1.4 O.DISCRETIONARY_ACCESS

The TOE will control access to resources based upon the identity of users or groups of users.

This TOE Security Objective is satisfied by ensuring that:

- FDP_ACC.2: Access controls are applied at the drawer level where individual pages (documents) are filed.
- FDP_ACF.1: Drawer objects have owners, ACLs, and can define groups and privileges, and these attributes are compared against user identities in order to determine whether the request operation should be allowed.
- FIA_ATD.1: The DAC policy uses user identities, group memberships, and privileges.
- FIA_UID.2a: The DAC policy relies on users to be individually identified by the TOE.

8.2.1.5 O.MANAGE

The TOE will provide all the functions and facilities necessary to support the authorized administrators in their management of the security of the TOE.

This TOE Security Objective is satisfied by ensuring that:

- FAU_SAR.2a: In a Windows configuration[2], only the Owner (e.g., top-level administrator) has viewing capability in the ISA (server) to view audit records stored in the audit trail.
- FMT_MSA.1.1: Users are restricted by default – they have no privileges. Only an Owner can perform all security management; however, the Manager role can also be granted certain administrative rights.
- FMT_MSA.3: By default every drawer object is created without any user, group, or privilege assignments, although a user possessing the Owner role can create a new drawer with the same privilege assignments as an existing drawer using the ImageNow Client interfaces.
- FMT_MTD.1a: The ability to create, modify, or delete user accounts is restricted to a user possessing the Owner role or a user given specific Manager privileges through restrictions enforced by ImageNow Client interface.
- FMT_MTD.1b: The ability to modify events to be audited is restricted to a user possessing the Owner role or a user given specific Manager privileges through restrictions enforced by the ISA interface.
- FMT_SMF.1: The TOE provides the ImageNow Client interface to manage users and objects. To manage the auditable events, run one of the following auditing scripts: for Windows, run apply_cc_audit.bat and for UNIX, run apply_cc_audit.sh.

[2] Note that in a Solaris configuration this capability is required to be provided by the environment.

- FMT_SMR.1: The TOE provides three roles that can be assigned to users.

8.2.1.6 O.USER_IDENTIFICATION

The TOE will uniquely identify users.

This TOE Security Objective is satisfied by ensuring that:

- FIA_UID.2a: ImageNow collects the user ID and password information and passes to the IT environment to perform identification and authentication. The TOE enforces the results provided by the IT environment and performs user identification for access control.

8.2.1.7 OE.AUDIT_SUPPORT

The IT environment will protect audit data stored from unauthorized access and, in a Solaris configuration, the IT environment will provide the capability to view audit information and ensure it is available only to authorized administrators.

This IT environment Security Objective is satisfied by ensuring that:

- FAU_SAR.1b: In a Solaris configuration, users possessing “Owner” or “Manager” roles can view audit records stored in files containing the audit trail.
- FAU_SAR.2b: In a Solaris configuration, users possessing “Owner” or “Manager” roles have viewing access to the files containing the audit trail.
- FAU_STG.1: The IT environment is relied on to protect the audit trail from unauthorized access.

8.2.1.8 OE.TIME

The IT environment will provide a time source that provides reliable time stamps.

This IT environment Security Objective is satisfied by ensuring that:

- FPT_STM.1: The IT environment is relied on to provide a reliable time source.

8.2.1.9 OE.PROTECT_TOE

The IT environment will provide protection to the TOE and its assets from external interference or tampering.

This IT environment Security Objective is satisfied by ensuring that:

- FPT_RVM.1: The IT environment ensures the TOE can only be accessed using its interfaces.
- FPT_SEP.1: The IT environment protects server components from unauthorized access.

8.2.1.10 OE.USER_AUTHENTICATION

The IT environment will authenticate users.

This IT environment Security Objective is satisfied by ensuring that:

- FIA_UID.2b: The IT environment is relied on to authenticate user identities provided by the TOE.
- FIA_UAU.2: The IT environment is relied on to authenticate user identities provided by the TOE.

8.3 Security Assurance Requirements Rationale

The base assurance level was augmented to EAL 2 augmented with ALC_FLR.2 and AVA_MSU.1, because flaw remediation procedures provide greater assurance that security-related bugs will be fixed in a widely distributed commercial product.

EAL2 was selected as the assurance level because the TOE is a commercial product whose users require a low to moderate level of independently assured security. ImageNow v5.42 SP3 and WebNow v3.42 is targeted at a relatively benign environment with good physical access security and competent administrators. Within such environments it is assumed that attackers will have little attack potential. As such, EAL2 is appropriate to provide the assurance necessary to counter the limited potential for attack.

8.4 Strength of Functions Rationale

There are no applicable security functions, the TOE does not for example authenticate users.

8.5 Requirement Dependency Rationale

The following table demonstrates that all dependencies among the claimed security requirements are satisfied and therefore the requirements work together to accomplish the overall objectives defined for the TOE.

ST Requirement	CC Dependencies	ST Dependencies
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FAU_SAR.1a	FAU_GEN.1	FAU_GEN.1
FAU_SAR.1b	FAU_GEN.1	FAU_GEN.1
FAU_SAR.2a	FAU_SAR.1	FAU_SAR.1a
FAU_SAR.2b	FAU_SAR.1	FAU_SAR.1b
FDP_ACC.2	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 and FMT_MSA.3	FDP_ACC.2 and FMT_MSA.3
FIA_ATD.1	none	none
FIA_UID.2a	none	none
FIA_UID.2b	none	none
FMT_MSA.1	FMT_SMR.1 and FMT_SMF.1 and (FDP_ACC.1 or FDP_IFC.1)	FMT_SMR.1 and FMT_SMF.1 and FDP_ACC.2
FMT_MSA.3	FMT_MSA.1 and FMT_SMR.1	FMT_MSA.1 and FMT_SMR.1
FMT_MTD.1a	FMT_SMR.1 and FMT_SMF.1	FMT_SMR.1 and FMT_SMF.1
FMT_MTD.1b	FMT_SMR.1 and FMT_SMF.1	FMT_SMR.1 and FMT_SMF.1
FMT_SMF.1	none	none
FMT_SMR.1	FIA_UID.1	FIA_UID.2
FPT_RVM.1	none	none
FPT_SEP.1	none	none
FPT_STM.1	none	none
ACM_CAP.2	none	none
ADO_DEL.1	none	none
ADO_IGS.1	AGD_ADM.1	AGD_ADM.1
ADV_FSP.1	ADV_RCR.1	ADV_RCR.1
ADV_HLD.1	ADV_FSP.1 and ADV_RCR.1	ADV_FSP.1 and ADV_RCR.1
ADV_RCR.1	none	none
AGD_ADM.1	ADV_FSP.1	ADV_FSP.1
AGD_USR.1	ADV_FSP.1	ADV_FSP.1
ALC_FLR.2	none	none
ATE_COV.1	ADV_FSP.1 and ATE_FUN.1	ADV_FSP.1 and ATE_FUN.1
ATE_FUN.1	none	none

ATE_IND.2	ADV_FSP.1 and AGD_ADM.1 and AGD_USR.1 and ATE_FUN.1	ADV_FSP.1 and AGD_ADM.1 and AGD_USR.1 and ATE_FUN.1
AVA_MSU.1	ADO_IGS.1 and ADV_FSP.1 and AGD_ADM.1 and AGD_USR.1	ADO_IGS.1 and ADV_FSP.1 and AGD_ADM.1 and AGD_USR.1
AVA_SOF.1	ADV_FSP.1 and ADV_HLD.1	ADV_FSP.1 and ADV_HLD.1
AVA_VLA.1	ADV_FSP.1 and ADV_HLD.1 and AGD_ADM.1 and AGD_USR.1	ADV_FSP.1 and ADV_HLD.1 and AGD_ADM.1 and AGD_USR.1

Table 7 Security Requirement Dependencies

8.6 Explicitly Stated Requirements Rationale

There are no explicitly stated requirements in this Security Target.

8.7 TOE Summary Specification Rationale

Each subsection in Section 6, the TOE Summary Specification, describes a security function of the TOE. Each description is followed with rationale that indicates which requirements are satisfied by aspects of the corresponding security function. The set of security functions work together to satisfy all of the security functions and assurance requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality.

This Section in conjunction with Section 6, the TOE Summary Specification, provides evidence that the security functions are suitable to meet the TOE security requirements. The collection of security functions work together to provide all of the security requirements. The security functions described in the TOE summary specification are all necessary for the required security functionality in the TSF. **Table 8 Security Functions vs. Requirements Mapping** demonstrates the relationship between security requirements and security functions.

	Security audit	**User data protection**	**Identification and authentication**	**Security management**
FAU_GEN.1	X			
FAU_SAR.1a	X			
FAU_SAR.2a	X			
FDP_ACC.2		X		
FDP_ACF.1		X		
FIA_ATD.1			X	
FIA_UID.2a			X	
FMT_MSA.1				X
FMT_MSA.3				X
FMT_MTD.1a				X
FMT_MTD.1b				X
FMT_SMF.1				X
FMT_SMR.1				X

Table 8 Security Functions vs. Requirements Mapping

8.8 PP Claims Rationale

See Section 7, Protection Profile Claims.