Common Criteria Security Target

For The

Promia Intelligent Agent Security Manager Version 1.2 (IASM)

Revision 3.3d
28 April 2006

Table of Contents

List of Figures

List of Tables

1 INTRODUCTION

This section contains document management and overview information necessary to allow a Security Target (ST) to be used in a U.S. CCEVS Common Criteria evaluation. The Overview summarizes the ST in narrative form and provides sufficient information for a potential user to determine whether the ST is of interest. The Conventions section provides an explanation the Common Criteria (CC) notation and formatting plus outlines how this document is organized. The Terms section gives a basic definition of terms, which are specific to this ST. Finally, the Related Profiles section identifies profiles directly related to this ST.

1.1 Security Target Identification

Title: Common Criteria Security Target for the Promia Intelligent Agent Security Manager Version 1.2 (IASM)

Sponsor: Promia, Inc

Author: David Chizmadia

CC Version: Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 2.2, January 2004, ISO/IEC 15408-2. Part 2 extended Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 2.2, January 2004, ISO/IEC 15408-3. Part 3 conformant Evaluation Assurance Level 3 (EAL 3) augmented with ALC_FLR.2 and ALC_LCD.1.

Security Target Version: Revision 3.3d, dated 28 April 2006

Keywords: Attack Sensing and Warning, Security Event Management, Security Incident Detection, Security Incident Response Management, Distributed System, Medium Robustness

1.2 Security Target Overview

1.2.1 Purpose

The purpose of this ST is to document the security assumptions, policies, threats, objectives, requirements, and rationale for the technical evaluation of the Promia security management product called the Intelligent Agent Security Manager Version 1.2 (IASM). Any unqualified references in this document to IASM or Intelligent Agent Security Manager shall be understood to refer to IASM Version 1.2. A detailed definition of the IASM product is provided in Section 2. It is intended that this IASM Security Target be used as the basis for a third party evaluation according to the Common Criteria (ISO/IEC 15408) and its associated Common Evaluation Methodology: as reflected, e.g., in the US Common Criteria Evaluation and Validation Scheme (CCEVS) administered by the US National Information Assurance Partnership (NIAP).

1.2.2 Scope

Type of system: The IASM TOE is a general-purpose platform for building and deploying security incident management systems (SIMS) that detect and react to security incidents in a specific monitored network. The SIMS of which the IASM TOE is a part becomes an integral part of the security countermeasures of an operational system. This Security Target applies to the IASM TOE, which is comprised of the following three distinct devices: each of which includes dedicated hardware running the IASM software:

The **IASM Master Server**, which is the core of the IASM product and provides: collection and consolidation of operational and security events; redistribution of those events to one or more Analytic Engines that are designed to detect security incidents on the monitored network; consolidation and management of security incidents detected by Analytic Engines; and user interfaces that the operations personnel of the monitored network employ to monitor and respond to detected security incidents;

The **IASM Database Server**, which implements the IASM TOE security incident management data model and provides scalable persistent storage for information collected or produced by an operational SIMS based on the IASM TOE;

The **IASM Console Server**, which is a software application that provides the human user interfaces for administering and operating the IASM.

Type of access: The IASM Master Server requires and uses access to the network infrastructure of the monitored network to exchange control messages and operational and security event data with external entities. The Human/Machine Interfaces to the IASM recognize four roles for people allowed access to the IASM: Operator, Analyst, Reporter, and Administrator.

Nature of use: The IASM TOE collects and consolidates operational and security event records from multiple sources, operating at different levels within the TCP/IP protocol stack, within the communications and computing architecture of the monitored system. It then redistributes those events to external Analytic Engines, which create security incidents that are in turn collected and consolidate by the IASM TOE. It also displays the security status of the monitored network to allow effective human intervention when security incidents are detected. Finally, it provides recommended responses to detected security incidents and can use a defined interface to invoke separate software components that automatically implement those responses.

1.3 Conventions

The notation, formatting, and conventions used in this ST are consistent with those used in version 2.2 of the CC.

The CC allows several operations to be performed on functional requirements; *refinement*, *selection*, *assignment*, and *iteration* are defined in section 4.4.1.3.2 of Part 1 of the CC. Each of these operations has been used in producing this ST.

> The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**.
>
> The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by *italicized text.*
>
> The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignment is indicated by showing the value in square brackets, [Assignment value].
>
> The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing the iteration number in parenthesis following the component identifier, (iteration number).

The CC paradigm also allows PP and ST authors to create their own requirements. Such requirements are termed 'explicitly stated requirements' and are permitted if the CC does not offer suitable requirements to meet the authors' needs. Explicitly stated requirements must be identified and are required to use the CC class/family/component model in articulating the requirements. In this PP, explicit requirements will be indicated with the "EXP" following the component name

1.4 Terminology

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

Access Control – A security service that mediates the use of computing, communication, and storage resources in order to enforce a defined security policy regarding the disclosure or modification those resources.

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

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

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

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

Authentication -- Security measure that verifies a claimed identity.

Authentication data -- Information used to verify a claimed identity.

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

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

Availability – Timely (according to some defined metric) and reliable access to IT resources.

Compromise -- Violation of a security policy.

Confidentiality -- A security policy pertaining to disclosure of data.

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

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

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

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

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

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

Monitored Network – The collection of computer nodes and network infrastructure from which an IASM collects operational and security events in order to detect security incidents.

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

The object may be used to transfer information between subjects of differing user identities within the TSF.

Subjects in the TOE must be able to request a specific instance of the object.

The name used to refer to a specific instance of the object must exist in a context that potentially allows subjects with different user identities to request the same instance of the object.

Non-Repudiation -- A security policy pertaining to providing one or more of the following:

To the sender of data, proof of delivery to the intended recipient,

To the recipient of data, proof of the identity of the user who sent the data.

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

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

Operating System (OS) **–** The software that provides the basic services for computer program execution, persistent data storage management, and network data communications.

Peer TOEs -- Mutually authenticated TOEs that interact to enforce a common security policy.

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

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

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

Security Incident **–** A detected attack against the monitored network or IASM TSF

Subject -- An entity within the TSC that causes operations to be performed. Subjects can come in two forms: trusted and untrusted. Trusted subjects are exempt from part or all of the TOE security policies. Untrusted subjects are bound by all TOE security policies.

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

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

User -- Any entity (human user or external IT entity) outside the TOE that interacts with the TOE. In the case of the Authorization Server protecting web resources, an “agent” acts on behalf of a user. Therefore, the “user” never truly interacts with the TOE. The authorization server software must have access to the “user’s” privilege attributes which are generally maintained in a separate data storage (not part of the TOE).

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

1.5 Related Protection Profiles

Intrusion Detection System System Protection Profile, Version 1.5, dated 3/2005

1.6 Security Target Organization

Section 1, ST Introduction, provides the document management and overview information necessary to identify the ST along with references to related PPs.

Section 2, TOE Description, defines the TOE and establishes the context for the TOE security environment.

Section 3, TOE Security Environment (TSE), describes the expected environment in which the TOE is to be used. This section defines the set of threats that are relevant to the secure operation of the TOE, organizational security policies with which the TOE must comply, and secure usage assumptions applicable to this analysis.

Section 4, Security Objectives, defines the set of security objectives to be satisfied by the TOE and by the TOE operating environment.

Section 5, IT Security Requirements, defines the security functional and assurance requirements derived from CC Parts 2 and 3, respectively, that must be satisfied by the TOE, the TOE IT environment, and the Non-IT environment.

Section 6, TOE Summary Specification, provides a brief description of the security-relevant subsystems that comprise the TOE and shows how the Security Function Requirements from Section 5 are allocated to those subsystems.

Section 7, Protection Profile Conformance Claims, identifies the protection profiles to which the IASM is claiming conformance.

Section 8, Rationale, provides rationale to demonstrate that the security objectives satisfy the threats and policies. This section also explains how the set of requirements are complete relative to the security objectives. This section includes a dependency analysis, Strength of Function (SOF) discussion, and rationale for the use of explicit requirements.

Section 9, References, provides background material for further investigation by users of the PP.

Section 10, Acronyms, provides a listing of acronyms used throughout the document.

2 TOE DESCRIPTION

2.1 IASM Target Of Evaluation Definition and Overview

Under an SBIR contract with the US Navy Computer Network Defense program, Promia has developed the IASM Suite, which integrates security countermeasures for security incident detection, management, and response into the Navy network operations centers to which it is deployed. The IASM Suite is an example of the relatively new class of *Security Incident Management System* (SIMS) products that automatically collect, normalize, and analyze the operational and security event logs of diverse kinds of security relevant devices on monitored networks in order to detect security incidents that are only visible when data available from multiple devices is considered. Having detected the incidents, the IASM Suite then identifies candidate responses based on site-specific policies and provides a unified operator interface for managing the incidents and responses. One of the goals of the SBIR program is to reduce the lifecycle costs of technology by generalizing government-specific systems into generally applicable commercial products. Along with this goal of commercializing the IASM Suite technology comes the obligation to comply with the policy that US Government organizations must favor the use of information assurance technologies that have been evaluated according to the Common Criteria (ISO 15488).

The IASM TOE (Target Of Evaluation), therefore, is the general purpose Security Incident Management Platform that provides the subset of IASM Suite functions that both are needed in an enterprise-specific SIMS – such as the Navy-specific IASM Suite – and can be successfully evaluated using the Common Criteria. One of the most important aspects of selecting the IASM TOE was determining which IASM Suite functions could be specified and tested without reference to detailed knowledge of a specific network. The set of functions chosen to comprise the IASM TOE consist of the following:

- Dedicated, commodity, IASM TOE hardware running a security-hardened OS, the Java Runtime Environment with Secure Socket Extensions, and CORBA middleware;
- A security incident management (SIM) repository that implements the abstractions needed for a SIMS – specifically: events, assets, incidents, and responses;
- User interfaces for monitoring and operating upon information in the SIM repository;
- Interfaces that devices on the monitored network can use to submit potentially security-relevant operational and security events to the IASM TOE for normalization and storage into the SIM repository and redistribution to analytic engines;
- Interfaces – used by enterprise-specific SIMS analytic software components that are outside the scope of IASM TOE – for registering an interest in redistributed events from the monitored network and creating and managing detected security incidents;
- Interfaces for managing IASM TOE and site-specific SIMS software components;
- An identified set of SIMS roles and interfaces for managing those roles;
- Interfaces for managing and identifying and authenticating authorized SIMS users.

The relative scopes of a complete SIMS (as represented by the IASM Suite developed specifically for the US Navy) and the IASM TOE are shown in **Figure 2-1** below. The scope of the full SIMS is circumscribed by the large dashed box labeled *Intelligent Agent Security Manager Suite*, while the IASM TOE is shown as the subset of IASM Suite components denoted by double solid lined boxes.

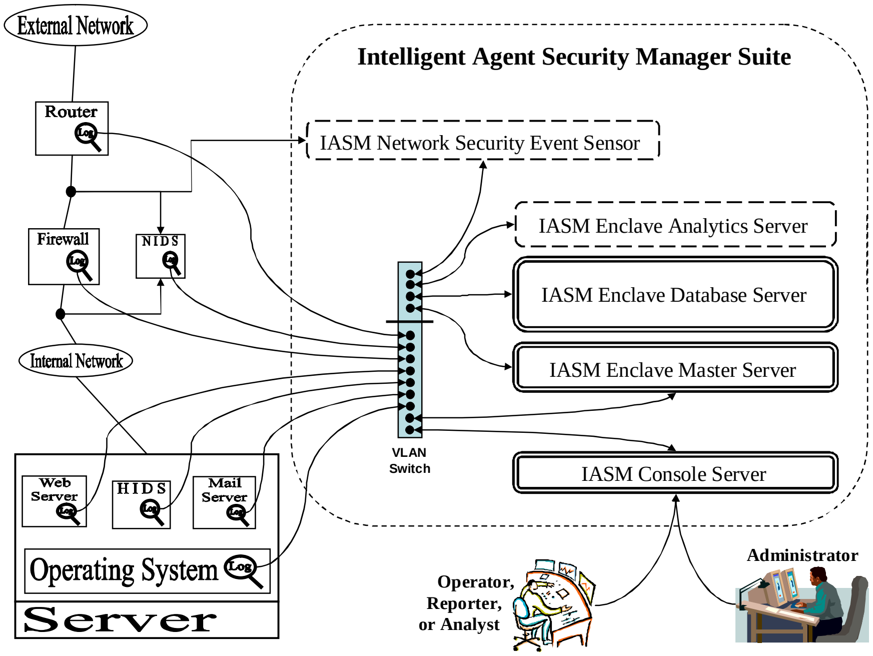
External Network
Router
Log
Firewall
Log
NIDS
Internal Network
Web Server
HIDS
Mail Server
Operating System
Server
Intelligent Agent Security Manager Suite
IASM Network Security Event Sensor
IASM Enclave Analytics Server
IASM Enclave Database Server
IASM Enclave Master Server
VLAN Switch
IASM Console Server
Operator, Reporter, or Analyst
Administrator

Figure 2-1 – The IASM Conceptual Approach

With reference to **Figure 2-1**, the IASM TOE provides the functions described above as follows:

2.1.1 Commodity hardware with a Secure OS, JRE/JSSE, and a CORBA ORB

The IASM TOE hardware for each of the three components shown in **Figure 2-1** is comprised of a commodity motherboard designed to support dual AMD Opteron 64-bit processors. The specific hardware used in the IASM TOE is specified below in section 2.2. Each hardware component runs a secure operating system that is based on Suse Linux 9.0, but which has been specialized for the IASM environment by eliminating extraneous software packages and using operational settings that provide a much higher degree of self protection (than the standard configuration) against both malicious local programs and network-based attackers. All IASM software is written in Java and therefore uses the Java Runtime Environment (JRE) version 1.5, including the JRE Secure Sockets Extensions (JSSE) implementation of the Secure Sockets layer version 3 (SSLv3) protocol. Over the OS and JRE is layered distributed communications and computing middleware that uses the CORBA Object Request Broker programming interfaces and the OMG protocol that uses SSLv3 to provide confidentiality and integrity protection for CORBA Internet Inter-ORB protocol messages (the SSL Inter-ORB protocol – SSLIOP) as the foundation of a secure, transparent, and standards-based specification and implementation of the IASM TOE external and internal programmatic interfaces.

2.1.2 Security Incident Management (SIM) Repository

One of the components shown in **Figure 2-1** is the IASM Enclave Database Server. The hardware for this component consists of the standard motherboard, as well as 1-4 Terabytes of hard disk storage capacity – enough for several months of operational and security event data – and an optional tape storage system for archiving older contents of the IASM TOE database. The more important aspect of the Database Server, though, is the security incident management data model embodied in the security incident management (SIM) repository database schema.

2.1.3 Interfaces between the IASM TOE and devices on the monitored network

The IASM TOE does not exist in a vacuum, specifically, it requires sources of the operational and security events that it analyzes to detect security incidents. The IASM TOE includes CORBA-based interfaces through which it can accept operational and security event data from devices on the monitored network.

2.1.4 Interfaces between the IASM TOE and Analytic Software Components

The IASM TOE specifically excludes analytic software components because the specification and operation of such components is intrinsically dependent on the operational characteristics of the monitored network and therefore cannot be effectively evaluated as a general-purpose product. The IASM TOE does, however, include a specific set of interfaces that allow each analytic engine deployed in a SIMS based on the IASM TOE both to receive copies of the events received by the IASM TOE from devices on the monitored network and to create and update incidents in the IASM TOE database. The strength of this architectural approach is that new analytic components can be added and old ones removed as appropriate for the SIMS deployed to each monitored network.

2.1.5 Interfaces for managing IASM TOE and associated SIMS software components

The IASM TOE includes a set of programmatic interfaces that specifically allow it to monitor the availability and operational health of running software components. All IASM TOE software components implement these interfaces and can therefore be managed using to standard IASM TOE tools and administrative user interfaces. In addition, any SIMS components that are outside of the IASM TOE, but implement these interfaces, can also be managed along with the IASM TOE components.

2.1.6 Identified SIMS Roles

The IASM TOE recognizes four roles that authorized users may assume and adjusts its behavior and the information that it makes available based on the role assumed by the user. The four roles are Administrator, Operator, Analyst, and Reporter. An **Administrator** performs initial installation and configuration of the IASM system, as well as ongoing administrative tasks, especially regular maintenance of the IASM operational and security settings and moves-adds-changes of the hardware and software components of the IASM. An **IASM Operator** performs ongoing monitoring of the network security, typically as a member of the network operations staff, with a primary focus on monitoring the network for intrusions, identifying attacks as they occur, and taking corrective action. An **IASM Analyst** performs strategic and global network traffic analysis, including specialized attacks such as low-and-slow. The Analyst performs IASM functions associated with the analysis of intrusion attacks, post-attack forensic analysis and development of new pattern specifications. An **IASM Reporter** is an administrative support person (e.g., an executive officer) who prepares security situation awareness summary reports pertaining to the monitored network for the senior IA management personnel.

2.1.7 Interfaces for User management and login

The IASM User Console provides a user interface for the Administrator role that includes functions for creating, modifying, and deleting user profiles. Interfaces are also provided to allow any user to change their authentication information.

With the exception of the user login dialog, all IASM TOE security functions require that users first identify and authenticate themselves at the Console. This identification and authentication is accomplished by requiring the user to enter both a user ID and a password, which are verified by comparing them to user attributes already established and stored by the IASM Administrator. If the user identity claimed is verified by the accompanying password the user is allowed to interact with security relevant interfaces, subject to the constraints the role assigned to that user account. If the user identity claimed is not verified by the accompanying password the user is simply returned to the user login dialog. If the user login dialog detects three consecutive unsuccessful login attempts, it enters a state in which it will refuse to accept any login attempts from any user for the next 6 minutes, at the end of which it resets and again accepts login attempts.

2.1.8 User interfaces to the SIM Repository

The IASM User Console is the link between the IASM and the operations staff of the monitored network. It consists of both the IASM Console Server – a Dell 1750 workstation running the version of Windows XP that has been evaluated to conform to the Controlled Access PP security requirements at EAL4 level of assurance – and the IASM user interface software components described below. The User Console is attached to the IASM through the monitored network port of the IASM Master Server. The primary User Console software component is the IASM Task Bar application, which initially displays user login dialog. Once a user is identified and authenticated, the initial user interface is replaced by the appropriate task bar for the role assumed by that user. The User Console has a specialized task bar for each of the IASM roles.

The IASM Operator Task Bar is the primary GUI application installed on the User Console and is available to all authorized user: though the specific functions available on the task bar are different according to the user's role. As indicated by its name, the Operator Task Bar is used primarily by a user acting as an IASM Operator to display the operational security status of the monitored network in real time. In addition to the security status, the Operator Task Bar also provides drill-down capabilities that can expose a tremendous amount of information about the topology and vulnerabilities of the network being monitored. For this reason, it is absolutely crucial that the Operator Task Bar only be available to authorized monitored network operations personnel who are properly trained to use it and known to be trustworthy.

A user who has assumed the Administrator role is also able to access the Administrator Task Bar, which is the privileged interface between the IASM Administrator and the IASM. Like the Operator Task Bar , the Administrator Task Bar is an IASM GUI application installed on the User Console workstation. The Administrator Task Bar provides a unified interface to the IASM functions for defining users, defining monitored network assets, defining filters for the events that should be acquired from the Network Security Event Sensor (NSES) and other external sensors, defining or viewing both operating and security policies, defining incident responses and the appropriate conditions under which to suggest them, and viewing and managing the running components of an IASM.

The User Console also has an Analyst Task Bar, which provides capabilities for more extensive analysis of the Event data collected and stored by the IASM. Finally, the User Console has a Reporter Task Bar that provides access to the restricted set of functions needed to perform the Reporter tasks.

2.2 Evaluation Configuration

2.2.1 Included In the TOE Evaluation

The following table summarizes the categories of configuration items that comprise the evaluated TOE. Since the IASM TOE is defined as a collection of appliances, the table includes both software and hardware configuration items. The table also shows the IASM components that are included in each category of configuration item.

Table 2-1 – TOE Software and Hardware Configuration Items

CI Categories	IASM Components
IASM Master Server	Hardware components • A dual Opteron (2-2.4Ghz) Motherboard, with 8-16 Gigabytes RAM, a single-channel 10/100Mb Ethernet NIC, and a dual-channel GigE NIC Software components • Suse Linux Enterprise Server 9.0 Operating System • IASM Version 1.2 Core Services
IASM Database Server	Hardware components • A dual Opteron (2-2.4Ghz) Motherboard, with 8-16 Gigabytes RAM, a single-channel 10/100Mb Ethernet NIC, and a dual-channel GigE NIC • 5 250GB drives in RAID configuration Software components • Suse Linux Enterprise Server 9.0 Operating System • IASM Multi-collector Agents
IASM Console Server	• A Dell 1750 workstation with Windows XP Professional installed in the CC evaluated configuration. • IASM User Console SW (1 per Enclave Server)

2.2.2 Excluded From the TOE Evaluation

The items listed below are specifically excluded from the TOE evaluation:

- The IASM Network Security Event Sensor (NSES) that performs Anomaly- and Signature-based analysis of monitored network traffic to detect and send potentially security-relevant events to the IASM and the additional forensic tools on the NSES that allow an Analyst to conduct more extensive in-place analysis of the traffic surrounding an NSES anomalous event.
- IASM SensorAgents that supply the events from various third party devices on the monitored network that are received normalized, and stored by IASM;
- Sensor Agent filters – both raw and normalized;
- The IASM Enclave Analytic Server and analytic software components that monitor and mine the stream of monitored network events to detect potential security incidents;

2.3 The IASM TOE Logical Boundary

The IASM TOE provides the following logical security functions:

- **Protected External Communications,** which provides the core capability for ensuring that the IASM TOE only communicates with the external entities that it intends and expects to communicate with;
- **Protection of Security Functions**, which provides the common self-protection capabilities upon which the implementations of the other security functions rely;
- **Security Functions Management**, which provides the interface through which an IASM Administrator establishes, monitors, and manages the security and operational configuration of the IASM;
- **User Identification & Authentication**, which provides the identification, authentication, and authentication secret (i.e., password) generation capabilities that provide a substantial proportion of the technical and operational assurance in the security of the TOE;
- **Security Information Consolidation**, which both accepts, normalizes, stores, and redistributes (to analytic software components) operational and security events from devices on the monitored network and allows analytic software components to create, modify, and store security incidents in the IASM TOE SIM repository;
- **Security Incident Management**, which provides the operational interface by which IASM Operators are alerted to newly detected or changed security incidents and provided with the tools to review and react to the incidents. The IASM_SIM subsystem also provides the related interfaces with which the IASM Analysts and IASM Reporters can accomplish their jobs.

3 TOE SECURITY ENVIRONMENT

3.1 Assumptions

This section contains assumptions regarding the security environment and the intended usage of the TOE. The specific conditions identified in Table 3-1 are assumed to exist at any site at which an IASM product is installed.

Table 3-1 – TOE Assumptions

IDENTIFICATION	DESCRIPTION
Intended Usage Assumptions	
A.DYNMIC	The TOE will be actively managed in a manner that allows it to appropriately address changes in the IT System.
A.EVENTS	The devices on the IT System that supply events to the TOE are protected from attacks on their integrity and availability and are designed and operated to correctly use the standard SSL/TLS technologies for protecting the in-transit confidentiality of the events they supply to the TOE.
A.ASCOPE	The average quantity and rate of events generated by the IT System being monitored fall within the specified capacity of the TOE.
A.COMMS	Adequate communications exist among the TOE components and between the TOE components and the IT System components.
A.NETSEP	The internal communications path between TOE components is separated from the external communications path between the TOE components and the IT System components using either physical (separate network switches) or logical (VLANs within a single network switch) techniques.
Physical Assumptions	
A.PROTCT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

IDENTIFICATION	DESCRIPTION
Personnel Assumptions	
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NOEVIL	The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
A.NOTRST	The TOE can only be accessed by authorized users

3.2 Threats Addressed by the IASM TOE

Table 3-2 identifies the threats for the TOE and the IT Environment. The TOE itself has threats and the TOE is also responsible for addressing threats to the environment in which it resides. The assumed level of expertise of the attacker varies from unsophisticated to sophisticated.

Table 3-2 – TOE Threats

IDENTIFICATION	DESCRIPTION
Threats to the TOE	
T.COMINT	An unauthorized user may attempt to change or delete the data collected and produced by the TOE by bypassing a security mechanism.
T.COMDIS	An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.
T.LOSSOF	An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.
T.NOHALT	An unauthorized user may attempt to compromise the continuity of the TOE's operation by halting its execution.
T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.
T.IMPCON	An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.
T.INFLUX	An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.

IDENTIFICATION	DESCRIPTION
T.FACCNT	Unauthorized attempts to access TOE data or security functions may go undetected.
Threats to the IT System Monitored by the TOE	
T.MISUSE	Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors.
T.INADVE	Inadvertent activity and access may occur on an IT System the TOE monitors.
T.MISACT	Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors.

3.3 Organizational Security Policies

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs. Table 3-3 includes the organizational security policies that would indicate the need for a Security Incident Management System in an organization.

Table 3-3 – TOE Policies

IDENTIFICATION	DESCRIPTION
P.DETECT	The TOE shall collect and store information from both the monitored system – about events that could indicate inappropriate activity resulting from misuse of, access to, or malicious activity on monitored system assets – and the analytic engines – about probable security incidents detected in the collected events.
P.RESPND	The TOE shall provide mechanisms for setting security incident response policies and displaying the policies that apply to detected security incidents
P.MANAGE	The TOE shall only be managed by authorized users.
P.ACCESS	All data collected and produced by the TOE shall only be used for authorized purposes.
P.ACCACT	Users of the TOE shall be accountable for their actions within the security incident management platform.
P.INTGTY	Data collected and produced by the TOE shall be protected from modification.

IDENTIFICATION	DESCRIPTION
P.PROTCT	The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.
P.USESTD	To the maximum extent possible, both the IT System and the TOE shall use networking and security technologies that are based on industry open standards.

4 SECURITY OBJECTIVES

This chapter describes the security objectives for the TOE and the TOE's operating environment. The security objectives are divided between TOE Security Objectives (i.e., security objectives addressed directly by the TOE) and Security Objectives for the Operating Environment (i.e., security objectives addressed by the IT domain or by non-technical or procedural means).

The security objectives identify the responsibilities of the TOE and its environment in meeting the security needs.

4.1 TOE Security Objectives

Table 4-1 defines the security objectives that are to be addressed by the IASM TOE.

Table 4-1 – TOE Security Objectives

IDENTIFICATION	DESCRIPTION
O.PROTCT	The TOE must protect itself from unauthorized modifications of and access to its functions and data.
O.EVENTS	The TOE must collect and store information about all events that might be useful for analysis of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets and the TOE.
O.INCDNT	The TOE must provide asset and event information to external analysis components, from which it must then collect and store information about past, present, or possible future incidents that those components detect.
O.RESPON	The TOE must collect and store predefined responses to detected incidents and rules for associating each response with a detected incident.
O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data.
O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
O.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.

IDENTIFICATION	DESCRIPTION
O.COMACC	The TOE must only communicate with external entities accessing the TOE through the network connection to the monitored network that can be positively and continuously identified and authenticated.
O.COMCON	The TOE must protect all communications with external entities accessing the TOE through the network connection to the monitored network from disclosure to any other external entities.
O.COMINT	The TOE must protect all communications with external entities accessing the TOE through the network connection to the monitored network from undetected modification or destruction by any other external entities.
O.OFLOWS	The TOE must appropriately handle potential audit and security incident management repository data storage overflows.
O.AUDITS	The TOE must record audit records for data accesses and use of the security incident management functions.
O.INTEGR	The TOE must ensure the integrity of all audit and security incident management repository data.

4.2 TOE Environment Security Objectives

The TOE's operating environment must satisfy the following objectives. These objectives do not levy any IT requirements but are satisfied by procedural or administrative measures.

Table 4-2 – TOE Environment Security Objectives

IDENTIFICATION	DESCRIPTION
O.INSTAL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and configured in accordance with the security administrative guidance.
O.PHYCAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
O.CREDEN	Those responsible for the TOE must ensure that all access credentials are protected by the users or authorized external entities in a manner which is consistent with IT security.

IDENTIFICATION	DESCRIPTION
O.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System.
O.INTROP	Those responsible for the TOE must ensure that the external entities with which the TOE intends and expects to communicate use the same technology(s) as the TOE to protect the communications.
O.SENSRS	Those responsible for the TOE must develop, install, configure, and manage external entities that collect, buffer, and send to the TOE events detected by sensors on the monitored network.
O.ANALYZ	Those responsible for the TOE must develop, install, configure, and manage external entities that analyze the events collected from sensors on the monitored network to detect security incidents and then send information about those detected security incidents back to the TOE.

5 IT SECURITY REQUIREMENTS

This section provides functional and assurance requirements that must be satisfied by a Security Target-compliant TOE. If necessary, it also provides functional requirements the IT environment must meet to deploy an IASM product in a secure manner to meet the policy objectives. These requirements consist of functional components from Part 2 of the CC, augmented by explicitly stated functional components that are unique to the IASM, and assurance components from Part 3 of the CC.

5.1 TOE Functional Security Requirements

This section identifies the functional (i.e., externally visible) behaviors that must be satisfied by an IASM TOE. These requirements consist of functional components from CC Part 2 that are incorporated into [IDSSYPP]. Table 5-1 summarizes the IASM Security Functional Requirements.

Table 5-1 – TOE Security Functional Requirements

FUNCTIONAL SECURITY CLASS	FUNCTIONAL SECURITY REQUIREMENT COMPONENTS
Security Audit, Audit Data Generation	FAU_GEN.1
Security Audit, Audit Review	FAU_SAR.1
Security Audit, Restricted Audit Review	FAU_SAR.2
Security Audit, Selectable Audit Review	FAU_SAR.3
Security Audit, Guarantees of Audit Data Availability	FAU_STG.2
Security Audit, Prevention of Audit Loss	FAU_STG.4
Identification & Authentication, Authentication Failure Handling	FIA_AFL.1
Identification & Authentication, User Attribute Definition	FIA_ATD.1
Identification & Authentication, TSF Generation of Secrets	FIA_SOS.2
Identification & Authentication, Timing of Authentication	FIA_UAU.1
Identification & Authentication, Timing of Identification	FIA_UID.1
Security Management, Management of Security Functions Behavior	FMT_MOF.1
Security Management, Management of TSF data	FMT_MTD.1
Security Management, Specification of Management Functions	FMT_SMF.1
Security Management, Security Roles	FMT_SMR.1

FUNCTIONAL SECURITY CLASS	FUNCTIONAL SECURITY REQUIREMENT COMPONENTS
Protection of TSF Functions, Non-Bypassability of the TSP	FPT_RVM.1
Protection of TSF Functions, TSF Domain Separation	FPT_SEP.1
Protection of TSF Functions, Reliable Time Stamps	FPT_STM.1
Trusted Path/Channels, Inter-TSF Trusted Channel	FTP_ITC.1

5.1.1 FAU_GEN.1 Audit Data Generation

Hierarchical to: No other components.

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 *basic* level of audit; and

c. [Access to the TSF.]

Table 5-2 – Auditable Events for the Basic Level of Audit

Component	Event	Details
FAU_GEN.1	Start-up and shutdown of audit functions	
FAU_GEN.1	Access to TSF	
FAU_SAR.1	Reading of information from the audit records	
FAU_SAR.2	Unsuccessful attempts to read information from the audit records	
FIA_UAU.1	All use of the authentication mechanism	**User identity, location**
FIA_UID.1	All use of the user identification mechanism	**User identity, location**
FMT_MOF.1	All modifications in the behavior of the functions of the TSF	
FMT_MTD.1	All modifications to the values of TSF data	
FMT_SMR.1	Modifications to the group of users that are part of a role	**User identity**

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 ST, [the additional information specified in the **Details** column of Table 5-2 – Auditable Events for the Basic Level of Audit].

Dependencies: FPT_STM.1 Reliable time stamps

5.1.2 FAU_SAR.1 Audit Review

Hierarchical to: No other components.

FAU_SAR.1.1: The TSF shall provide [IASM Administrators, IASM Reporters] with the capability to read [all information] from the audit records.

FAU_SAR.1.2: The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

Dependencies: FAU_GEN.1 Audit data generation

5.1.3 FAU_SAR.2 Restricted Audit Review

Hierarchical to: No other components.

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

Dependencies: FAU_SAR.1 Audit review

5.1.4 FAU_SAR.3 Selectable Audit Review

Hierarchical to: No other components.

FAU_SAR.3.1 (1): The TSF shall provide the ability to perform *searches* of audit data based on [date and time of event, IASM subject identity, type of event, and result of event].

FAU_SAR.3.1 (2): The TSF shall provide the ability to perform *sorting* of audit data based on [date and time of event, IASM subject identity, type of event, and result of event].

FAU_SAR.3.1 (3): The TSF shall provide the ability to perform *ordering* of audit data based on [date and time of event, IASM subject identity, type of event, and result of event].

Dependencies: FAU_SAR.1 Audit review

5.1.5 FAU_STG.2 Guarantees of Audit Data Availability

Hierarchical to: FAU_STG.1

FAU_STG.2.1: The TSF shall protect the stored audit records from unauthorized deletion.

FAU_STG.2.2: The TSF shall be able to *detect* unauthorized modifications to the audit records in the audit trail.

FAU_STG.2.3 (1): The TSF shall ensure that [all] audit records will be maintained when the following conditions occur: *audit storage exhaustion*.

FAU_STG.2.3 (2): The TSF shall ensure that [all] audit records will be maintained when the following conditions occur: *attack*.

Dependencies: FAU_GEN.1 Audit data generation

5.1.6 FAU_STG.4 Prevention of Audit Data Loss

Hierarchical to: FAU_STG.3

FAU_STG.4.1 The TSF shall *prevent auditable events, except those taken by the authorized user with special rights* if the audit trail is full.

Dependencies: FAU_STG.1 Protected audit trail storage (Actually satisfied by FAU_STG.2, which is hierarchical to FAU_STG.1, in this ST))

5.1.7 FIA_AFL.1 Authentication Failure Handling

Hierarchical to: No other components.

FIA_AFL.1.1 The TSF shall detect when *[3]* unsuccessful authentication attempts occur related to [user logon or change of user at the User Console].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts have been met or surpassed, the TSF shall [prevent any attempts to use the authentication facility at the User Console for 6 minutes].

Dependencies: FIA_UAU.1 Timing of authentication

5.1.8 FIA_ATD.1 User Attribute Definition

Hierarchical to: No other components.

FIA_ATD.1.1: The TSF shall maintain the following list of security attributes belonging to individual users: [user identity, IASM role, authentication data].

Dependencies: No dependencies

5.1.9 FIA_SOS.2 TSF Generation of secrets

Hierarchical to: No other components.

FIA_SOS.2.1: The TSF shall provide a mechanism to generate secrets that meet [at least the minimum quality implicit in the rules summarized in Section 6.6.3].

FIA_SOS.2.2: The TSF shall be able to enforce the use of TSF generated secrets for [all user authentication].

Dependencies: No dependencies

5.1.10 FIA_UAU.1 Timing of Authentication

Hierarchical to: No other components.

FIA_UAU.1.1: The TSF shall allow [no actions] on behalf of the user to be performed before the user is authenticated.

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

Dependencies: FIA_UID.1 Timing of identification

5.1.11 FIA_UID.1 Timing of Identification

Hierarchical to: No other components.

FIA_UID.1.1: The TSF shall allow [no actions] on behalf of the user to be performed before the user is identified.

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

Dependencies: No dependencies

5.1.12 FMT_MOF.1 Management of Security Functions Behavior

Hierarchical to: No other components.

FMT_MOF.1.1: The TSF shall restrict the ability to *determine the behavior of, disable, enable, or modify the behavior of* the functions of [audit record consolidation and security incident reaction] to [IASM Administrators].

Dependencies: FMT_SMF.1 Specification of management functions,
FMT_SMR.1 Security roles

5.1.13 FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1: The TSF shall restrict the ability to *change_default, query, modify, and delete* [all mutable TSF data] to [the IASM Administrator].

Dependencies: FMT_SMF.1 Specification of management functions,
FMT_SMR.1 Security roles

5.1.14 FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [modify system data collection behavior; modify system incident reaction behavior; and define, modify, and delete authorized user profiles].

Dependencies: No dependencies

5.1.15 FMT_SMR.1 Security Roles

Hierarchical to: No other components.

FMT_SMR.1.1: The TSF shall maintain the roles: [IASM Administrator, IASM Operator, IASM Analyst, and IASM Reporter].

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

Dependencies: FIA_UID.1 Timing of identification

5.1.16 FPT_RVM.1 Non-Bypassability of the TSP

Hierarchical to: No other components.

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

Dependencies: No dependencies

5.1.17 FPT_SEP.1 TSF Domain Separation

Hierarchical to: No other components.

FPT_SEP.1.1: The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2: The TSF shall enforce separation between the security domains of subjects in the TSC.

Dependencies: No dependencies

5.1.18 FPT_STM.1 Reliable Time Stamps

Hierarchical to: No other components.

FPT_STM.1.1: The TSF shall be able to provide reliable time stamps for its own use.

Dependencies: No dependencies

5.1.19 FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: No other components.

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2(1) The TSF shall permit *the TSF* to initiate communication via the trusted channel.

FTP_ITC.1.2(2) The TSF shall permit *the remote trusted IT product* to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [all communications with external entities].

Dependencies: No dependencies

5.2 TOE Environment Functional Security Requirements

This Security Target does not impose any Functional Security Requirements drawn from CC Part 2 on the TOE Environment.

5.3 Explicitly Stated TOE Functional Security Requirements

This section identifies the functional (i.e., externally visible) behaviors that are specific to a platform for security incident management systems and must therefore be satisfied by the IASM TOE. These requirements consist of explicitly stated functional components that have been adapted from [IDSSYPP], with some reference to the CC Part 2 FAU class. Table 5-3 summarizes these explicitly stated Security Requirements.

Table 5-3 – Explicitly Stated TOE Security Functional Requirements

FUNCTIONAL SECURITY CLASS	FUNCTIONAL SECURITY REQUIREMENT COMPONENTS
IDS System, System Data Collection	IDS_SDC_(EXP).1
IDS System, Analyzer React	IDS_RCT_(EXP).1
IDS System, Restricted SIM repository Data Review	IDS_RDR_(EXP).1

FUNCTIONAL SECURITY CLASS	FUNCTIONAL SECURITY REQUIREMENT COMPONENTS
IDS System, Guarantee of SIM repository Data Availability	IDS_STG_(EXP).1
IDS System, Prevention of SIM repository data loss	IDS_STG_(EXP).2

5.3.1 IDS_SDC_(EXP).1 System Data Collection

Hierarchical to: No other components.

IDS_SDC_(EXP).1.1 The System shall be able to collect the following information from the targeted IT System resource(s) **and external security incident detection analysis components and consolidate it into a unified security incident management repository:**

a. *Start-up and shutdown, service requests, security configuration changes*;

b. [Suspected security attack events detected by devices among the targeted IT System resource(s)];

c. [Suspected security incidents detected by an external security incident detection analysis component].

IDS_SDC_(EXP).1.2 At a minimum, the System shall collect and record the following information:

a. Date and time of the event, type of event, subject **(i.e., the targeted IT System resource that generated the event or the external security incident detection analysis component that detected the incident)** identity, and the outcome (success or failure) of the event; and

b. The following additional context-specific information:

1. Service Requests shall include: Specific service, apparent initiator, apparent target
2. Security configuration changes shall include: Apparent initiator, configuration parameter(s) being changed, and new configuration value(s);
3. **Suspected security attack events shall include: Information identifying the suspected security attack event;**
4. **Detected security incidents shall include: Information identifying the suspected security incident and the list of monitored system events in which the incident was detected.**

Dependencies: FPT_STM.1 Reliable Time Stamps,
FTP_ITC.1 Inter-TSF trusted channel

5.3.2 IDS_RCT_(EXP).1 Analyzer React

Hierarchical to: No other components.

IDS_RCT_(EXP).1.1 The System shall send an alarm to [IASM Operator and IASM Analyst console(s) that are initiated before the alarm has been acknowledged] and take [action to display a message identifying the potential security incident, make accessible the security attack event data in which the incident was detected, and list potential responses deduced from the System response policies in effect] when a **security incident** is detected.

Dependencies: No dependencies

5.3.3 IDS_RDR_(EXP).1 Restricted SIM repository Data Review

Hierarchical to: No other components.

IDS_RDR_(EXP).1.1 The System shall provide [IASM Operators, IASM Analysts, and IASM Reporters] with the capability to read [suspected security attack events and detected security incidents] from the **unified security incident management repository** data.

IDS_RDR_(EXP).1.2 The System shall provide the **unified security incident management repository** data in a manner suitable for the user to interpret the information.

IDS_RDR_(EXP).1.3 The System shall prohibit all users read access to the **unified security incident management repository** data, except those users that have been granted explicit read-access.

Dependencies: No dependencies

5.3.4 IDS_STG_(EXP).1 Guarantee of SIM repository Data Availability

Hierarchical to: No other components.

IDS_STG_(EXP).1.1 The System shall protect the stored **unified security incident management repository** data from unauthorized deletion.

IDS_STG_(EXP).1.2 The System shall protect the stored **unified security incident management repository** data from modification.

IDS_STG_(EXP).1.3 The System shall ensure that [all] stored **unified security incident management repository** data will be maintained when the following conditions occur: ***unified security incident management repository*** *data storage exhaustion or attack on the storage mechanism.*

Dependencies: No dependencies

5.3.5 IDS_STG_(EXP).2 Prevention of SIM repository data loss

Hierarchical to: No other components.

IDS_STG_(EXP).2.1 The System shall *prevent System data* ***collection actions****, except those taken by the authorized user with special rights* ***to archive and delete data in the unified***

security incident management repository and send an alarm if the storage capacity **of the unified security incident management repository** has been reached.

Dependencies: No dependencies

5.4 Other Explicitly Stated TOE Functional Security Requirements

There are no additional explicitly stated Security Requirements for the TOE.

5.5 Explicitly Stated Security Requirements for the TOE Environment

Table 5-4: Explicitly Stated Security Requirements for the TOE Environment

FUNCTIONAL SECURITY CLASS	FUNCTIONAL SECURITY REQUIREMENT COMPONENTS
IDS System, Analyzer analysis	IDS_ANL_(EXP).1

5.5.1 IDS_ANL_(EXP).1 Analyzer analysis

IDS_ANL.1.1 The **external security incident detection analysis components integrated with the** System shall perform the following analysis function(s) on all IDS **security attack event** data received:

a. *Statistical- and signature-* **based analysis of the security attack event data in the context of the specific network being monitored**.

IDS_ANL.1.2 The **external security incident detection analysis components integrated with the** System shall record within each analytical result **(i.e., detected security incident)** at least the following information:

a. Date and time of the result, type of result, identification of data source **(i.e., the external security incident detection analysis component that detected the incident)**; and

b. [A list of the IDS security attack events that caused the incident to be detected].

5.6 Strength of TOE Security Function Claims

The IASM TOE shall provide an overall Strength of Security Function (SOF) of SOF-Basic. To attain this overall SOF, the following specific requirements that necessarily rely on probabilistic or permutational mechanisms shall each meet, or exceed, the stated requirement-specific SOF level:

Table 5-5 – Strength of Function Claims

Security Requirement	Required SOF
FIA_SOS.2 & FIA_UAU.1	SOF-Basic

5.7 TOE Security Assurance Requirements

The TOE assurance requirements for this ST are EAL3+, where the plus is comprised of additional requirements for Flaw Remediation and Life Cycle Definition. All assurance requirements are enumerated in the table below.

Table 5-6 – EAL3+ Assurance Requirements Summary

Assurance Class	Assurance Component	
Configuration Management **(ACM)**	**ACM_CAP.3**	Authorization controls
	ACM_SCP.1	TOE CM coverage
Delivery and Operation (**ADO**)	**ADO_DEL.1**	Delivery procedures
	ADO_IGS.1	Installation generation and start-up procedures
Development (**ADV**)	**ADV_FSP.1**	Informal functional specification
	ADV_HLD.2	Security enforcing high-level design
	ADV_RCR.1	Informal correspondence demonstration
Guidance Documents (**AGD**)	**AGD_ADM.1**	Administrator guidance
	AGD_USR.1	User guidance
Life Cycle Support (**ALC**)	**ALC_DVS.1**	Identification of security measures
	***ALC_FLR.2**	Flaw Remediation: Flaw Reporting Procedures
	***ALC_LCD.1**	Life Cycle Definition: Developer Defined Life-Cycle Model
Tests (**ATE**)	**ATE_COV.2**	Analysis of coverage
	ATE_DPT.1	Testing: high-level design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Vulnerability Assessment (**AVA**)	**AVA_MSU.1**	Examination of guidance
	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.1	Developer vulnerability analysis

6 TOE SUMMARY SPECIFICATION

This chapter describes the TOE security functions and associated assurance measures.

Sections 6.1 through 6.6 each describe one of the TOE Security Functions (TSF). The description for each TSF consists of a detailed account of how the TSF specifically satisfies each of the security function requirements that have been allocated to it. This serves to both describe the security functions and rationalize that the security functions are suitable to satisfy the necessary requirements.

Section 6.7 describes the assurance measures that are used to satisfy the security assurance requirements.

6.1 TSF_PEC: Protected External Communications

6.1.1 FTP_ITC.1 Inter-TSF trusted channel

All information that is transmitted between the TOE and an Authorized External Entity – i.e., an entity accessing the TOE through the network connection to the monitored network and with which the TOE intends and expects to communicate securely – is protected from both disclosure and modification by using SSL version 3.0 as implemented in the standard Java Secure Sockets Extension implementation provided with the Java Runtime Environment version 1.5. The disclosure protection is accomplished by the symmetric encryption of the data being transferred using either the DESede (aka, Triple DES – defined in US FIPS-46-3) or AES (defined in US FIPS-197) ciphers and a per connection key generated as part of the SSLv3 protocol. The modification protection is accomplished by the use of the HMAC (Hashed Message Authentication Code – defined by IETF RFC2104) that is incorporated into the SSLv3 record transfer protocol.

6.2 TSF_PSF: Protection of Security Functions

6.2.1 FAU_GEN.1 Audit Data Generation

The IASM User Console maintains an activity log of all I&A or administrative actions performed through the User Console. Each activityLog event record is comprised of the following fields:

- **created**: The timestamp of the event.
- **userId**: The user identifier.
- **type**: The type of activity. See below.
- **what**: A short description of the activity.
- **sigValue**: A check sum of the record.

The **Type** field can take on the following values:

- **1:** Logged on
- **2:** Logged on and DoD PKI authenticated
- **3:** Logged off
- **5:** Invalid Logon
- **7:** InfoCon level change
- **10:** Process change
- **12:** Sensor agent controller change
- **20:** Administration change
- **30:** Password Generation
- **31:** Password Changed
- **42:** activityLog report generated

With the Types identified above, the activityLog is able to address all of the event types called out in Table 5-2 – Auditable Events for the Basic Level of Audit, except for the start up and shut down of the audit facility. That event type is handled separately by the underlying operating system component of the IASM, which is configured to log the creation and destruction of all processes, including those that execute the User Console software.

6.2.2 FPT_RVM.1 Non-Bypassability of the TSP

User Bypass of the TSP

The only way that users can access the IASM is through the User Console. As stated in assumption A.NOTRST (in section 3.1), only trusted users are allowed to access the User Console and they must first successfully authenticate themselves to the IASM before they are able to take any actions that can view or modify the TSF. No actions are allowed on the IASM TOE until after successful authentication, and the allowed actions are determined by the assigned user role. In addition, a trusted user (minimally, the IASM Administrator) must also log into underlying User Console OS (Windows XP Professional) before the User Console software can be started.

External Entity Bypass of the TSP

The IASM TOE is usually located, both logically and physically, deep inside the protected perimeter of the monitored network. This has the first order effect of limiting the access that true external entities might have to the IASM TOE. In addition, the IASM TOE is configured to not respond as a network device to any network packets except those that are part of an SSL connection originating from known Authorized External Entities. This is implemented with the intrinsic packet firewall features of the Suse Linux OS used in the IASM TOE Master and DBServer components.

The User Console is protected from external attempts to bypass the TSP primarily by the security features of the Console Server Operating System.

Malicious or Flawed Software Bypass of the TSP

In addition to all of the protection provided by careful network configuration, the IASM has also been designed so that neither maliciously subverted nor non-malicious, but flawed, IASM software components are able to circumvent the TSP. This is accomplished through the use of dedicated hardware components running operating system software (Windows XP Professional for the User Console and Suse Linux Enterprise Server v9 for everything else) that has been evaluated to the EAL4 level of assurance against CC STs that include the FPT_RVM.1 security function requirement. Building upon this solid technical foundation, the IASM TOE software components are designed and implemented such that they only transfer control and data across process and network node boundaries using well defined middleware (i.e., CORBA). Since the IASM software components have been partitioned so that most aspects of the TSP are enforced through the cooperation of two or more software components, the complexity of bypassing the TSP through intentional compromise of software components is rendered much more difficult.

6.2.3 FPT_SEP.1 TSF Domain Separation

The IASM architecture incorporates three levels of domain separation to provide protection against both external and internal threats. The coarsest level of domain separation is provided by the use of independent network nodes for critical subsystems within the TOE: specifically, the Master server for interaction with Authorized External Entities, the DBServer server for the SIM Repository, and the User Console for Audit review and security management functions. This level of separation is enforced by the components being physically disjoint and logically connected only through the TCP/IP protocol and augmented by the exclusive use of SSL connections among the TOE network nodes.

A medium level of domain separation is provided within the Master and DBServer components by using of multiple physical processors in each appliance. This level of separation allows related collections of software components within that component to be segregated in almost the same way as among the components, but without the additional protection from SSL.

The finest-grained level of domain separation is provided by the process abstraction of the CC-evaluated operating systems used by the IASM subsystems. By running each software subsystem in a separate process, the IASM is able to enforce a very fine-grain level of separation among the software components. This process-level separation is reinforced through the extensive use of CORBA IIOP as the mechanism for inter-process communication among most of the software components.

6.2.4 FPT_STM.1 Reliable Time Stamps

All hardware components (Master, DBServer, and Console) of each IASM TOE include hardware clocks that have been synchronized during the manufacturing process. These clocks are accessed via operating system software (Windows XP Professional for the User Console and Suse Linux Enterprise Server v9 for everything else) that has been evaluated to the EAL4 level of assurance against CC STs that include the FPT_STM.1 security function requirement. In addition, all IASM software components that must share a synchronized perception of time implement an application-layer protocol that compensates for differences in the time reported by local and remote clocks. This is supported by the incorporation of time coordination fields in the protocols used between those components.

6.3 TSF_SFM: Security Function Management

6.3.1 FMT_MOF.1 Management of Security Functions Behavior and FMT_MTD.1 Management of TSF data

With the exception of the user login dialog, all IASM security functions require that users first identify and authenticate themselves at the User Console. More specifically, only a user who has authenticated into the Administrator role is provided with the user interface to the administrative management functions, among which are the capabilities to "*determine, disable, enable, or modify the behavior of* the functions of [audit record consolidation, security incident detection analysis, and security incident reaction]". Likewise, only the Administrator user interface provides access to the capabilities to "*change_default, query, modify, and delete* [all mutable TSF data]".

6.3.2 FMT_SMF.1 Specification of Management Functions

The IASM provides interfaces that allow users to perform the following actions:

- Modify policies, including which events are detected, whether incidents are created for each event detected, and how the system will react when events are detected;
- Configure and tune the operational of parameters of running IASM components; and
- Manage the profiles for authorized users of the system.

6.3.3 FMT_SMR.1 Security Roles

The Security Function Management TSF implements the four security roles identified below. The IASM User Console login process associates one or more of these four roles with each identified and authenticated user. The IASM Administrator assigns the role or roles that will be associated with each user during the login process.

- **Administrator**: All functions. Administrators must manage themselves, as well as read, modify, delete and push policy. Administrators can also administer other administrators and their roles as part of adding, maintaining, and deleting users and role assignments.
- **Operator**: All functions related to managing security incidents, including generating pre-defined reports.
- **Analyst**: All Operator functions, as well as additional ones related to conducting more detailed analysis of the incidents.
- **Reporter**: All functions related to defining, running, and schedule periodic runs of reports.

6.4 TSF_SIC: Security Information Consolidation

6.4.1 IDS_SDC_(EXP).1 System Data Collection

The IASM presents a collection of interfaces by which a standard software component deployed to appropriate sensor devices on the monitored network is able to download and initialize the appropriate Sensor Agent for each sensor, allow that sensor agent to identify itself and download operating parameters, allow the IASM to monitor and manage the Sensor Agent, and (most importantly) accept the events generated by the sensor device for normalization into a common format and distribution to both the IASM SIM Repository and external analytic engines. Likewise, the same interfaces are used to bootstrap, configure, and manage the external analytic engines as well as distribute events received from sensor agents to and accept detected incidents back from the analytic engines. The foundation for the Security Information Consolidation TSF, however, is the security incident management (SIM) repository that implements the abstractions needed for a SIMS – specifically: events, assets, incidents, and responses.

6.4.2 FAU_STG.2 Guarantees of Audit Data Availability and IDS_STG_(EXP).1 Guarantee of System Data Availability

All IASM internal audit and System data is stored into the central SIM Repository. The contents of the Repository are then only disclosed to identified, authenticated, and authorized human users via the User Console. The Repository is specifically configured so that its internal audit and System data contents cannot be directly modified from the User Console. Taken together, these measures ensure that the internal audit and System data is always available to the human users with a verified need to see and act upon the internal audit and System data.

Further there is no TSF interface to disable audit or delete or modify audit records; however, there does exist an ability to back up and restore these audit logs. The internal audit function starts automatically when the TOE is installed. Once recorded, internal audit data cannot be modified or deleted except by direct manipulation of the underlying reporistory mechanism. The only TSF interfaces to the audit mechanism allow the creation of an audit log, viewing audit information, and copy the audit information to another media for back-up and restore purposes. The TSF ensures that [all already recorded] system events are maintained in the event of TOE failure, direct attack against the TSF attack, or storage exhaustion of the repository mechanism.

Audit data storage exhaustion can occur if the disk space allocated to the repository exceeds the storage allowed. If this unlikely event occurs, an alarm is triggered and an administrator must backup the internal audit and System alert tables. To prevent inadvertent audit data storage exhaustion, an IASM Administrative documentation instructed site Administrators to set a schedule by which audit and alert information is periodically saved to some form of external media.

6.4.3 FAU_STG.4 Prevention of Audit Loss and IDS_STG_(EXP).2 Prevention of System Data Loss

As described above, all internal audit and System data is stored into a unified IASM repository. The storage allocated to the IASM repository ranges from 1-4 Terabytes in order to provide 60-

120 days of storage for internal audit and System data. Especially for the internal audit, there is very little chance that storage would be exceeded. In the event that the repository storage is exceeded, the default system behavior is to halt all processing until the IASM Administrator backs up and removes the oldest internal audit and System data from the repository.

6.5 TSF_SIM: Security Incident Management

6.5.1 FAU_SAR.1 Audit Review, FAU_SAR.2 Restricted Audit Review, and FAU_SAR.3 Selectable Audit Review

Access to the IASM activityLog, which contains the record of all security relevant events performed by IASM users, is only possible by generating a report from the the User Console. The authority to access the activityLog records and therefore generate the report is only given to the IASM Administrator. Like all IASM reports, an extensive set of selection and sorting criteria can be used to acquire the relevant activityLog data, which can then be presented in the way desired by the Administrator.

6.5.2 IDS_RCT_(EXP).1 Analyzer React

The IASM includes a Response component that monitors all security incidents that are generated and inserted into the IASM repository by the external Analysis Engines and, based on policies configured by the IASM Administrator, decides on potential reactions. By default, the candidate reactions are presented to security personnel for their final decision and implementation. Examples of candidate reactions include simple e-mail notifications, defensive adjustments to sensors, or offensive measures against a source. The results of these actions, as documented by the human users, are then stored in an incident history log for future review. This same log also stores user interactions done within the incident management GUI component.

6.5.3 IDS_RDR_(EXP).1 Restricted Data Review

The IASM User Console provides the operational interface by which IASM Operators are alerted to newly detected or changed security incidents and provided with the tools to review and react to the incidents. The User Console also provides the interfaces with which the IASM Analysts and IASM Reporters can accomplish their jobs. All IASM data is protected from disclosure to and modification by any person who is not an authorized user of the IASM acting in one of the four identified IASM roles.

The ultimate goal of the IASM Security Incident Detection function is to ensure that Operators of the monitored network are made aware of the Security Incidents that are occurring on the monitored network and provided with enough time and information to react before any (or much) damage is done. The primary IASM component that implements this capability is the Response Engine, which monitors the Incidents that have been detected for ones with threat metrics that exceed an Administrator-defined threshold. When such an Incident is generated, the Response Engine first identifies one or more Administrator-defined candidate response actions that would mitigate damage from the identified incident. The Response Engine then forwards the Incident and candidate responses on to the User Console Operator GUI to for display to the monitored network Operators for review and action. The Operator Console component also provides a subset of its functions to IASM users who have logged in with the IASM Reporter role and a superset of its functions IASM users who have logged in with the IASM Analyst role.

6.6 TSF_UIA: User Identification & Authentication

6.6.1 FIA_UAU.1 Timing of Authentication, FIA_UID.1 Timing of Identification, and FIA_AFL.1 Authentication Failure Handling

With the exception of the user login dialog and viewing the Tactical Incident Summary of open incidents detected by the IASM, all IASM security functions require that users first identify and authenticate themselves at the User Console. This identification and authentication is accomplished by requiring the user to enter both a user ID and a password, which are verified by comparing them to user attributes already established and stored by the IASM Administrator. If the user identity claimed is verified by the accompanying password the user is allowed to interact with security relevant interfaces, subject to the constraints the role assigned to that user account. If the user identity claimed is not verified by the accompanying password the user is simply returned to the user login dialog. If the user login dialog detects three consecutive unsuccessful login attempts, it enters a state in which it will refuse to accept any login attempts from any user for the next 6 minutes, at the end of which it resets and again accepts login attempts.

6.6.2 FIA_ATD.1 User Attribute Definition

User accounts in the TOE have the following attributes: login id (identification data), password (authentication data), and assigned role (role association data).

6.6.3 FIA_SOS.2 TSF Generation of Secrets

An IASM Administrator creating a new user account and an existing user who is changing his or her password must use the IASM strong password generation facility. The facility forces the user to generate and select a password that satisfies the following rules:

1. The password shall be 8-200 ASCII characters in length.

2. The password shall contain four categories of English characters, including:

    - Upper case,
    - Lower case,
    - Numerals, and
    - Special ASCII symbols
      (~, `, !, @, #, $, %, ^, &, *, (,), _, +, -, =, [,], {, }, \, |, ;, : ", ', ,, ., <, >, ?, /)

3. The password shall have at least one special ASCII symbol character in the second through sixth position.

4. The password should appear as a sequence of random letters, numbers, and symbols. The password shall include all four different categories of characters (note in “2.” above) and shall contain no repeated characters.

5. The password shall withstand a Dictionary Attack or Brute Force Attack, as opposed to using a password from a pre-built list.

6. A Strong Password shall be randomly generated to assign an initial logon password to new authorized users. Upon successful initial logon the IASM system shall require the user to change the password to a new Strong Password.

7. The password SHALL NOT:
   - Contain ANY PART of a user logon id,
   - Use any actual word or name in ANY language,
   - Use numbers in place of similar letters,
   - Reuse any portion of a previous user password,
   - Use consecutive letters or numbers like "abcdefg" or "234567",
   - Use adjacent keys on your keyboard like "qwerty", and/or
   - Use the same user password, or previous 10 passwords.

6.7 Implementation of the IASM Security Assurance Requirements

Table 6-1 – Mapping of EAL3+ Assurance Requirements to TOE Assurance Measures

Assurance Component	Approach To Meeting The Requirement
ACM_CAP.3: Authorization controls	The vendor has provided the Configuration Management Plan and Configuration Items List, which describe the configuration management process used for development of the IASM TOE.
ACM_SCP.1: TOE CM coverage	The vendor has provided the Configuration Management Plan and Configuration Items List, which describe the configuration management system used for development of the IASM TOE.
ADO_DEL.1: Delivery procedures	The vendor has provided the Configuration Management Plan, which describes the normal IASM TOE delivery procedures.
ADO_IGS.1: Installation generation and start-up procedures	The vendor has provided the IASM Operations Manual, which describes the procedures for initial intallation and configuration of the IASM TOE.
ADV_FSP.1: Informal functional specification	The vendor has provided design documentation that includes the required informal functional specification.
ADV_HLD.2: Security enforcing high-level design	The vendor has provided design documentation that includes the required security enforcing high-level design.
ADV_RCR.1: Informal correspondence demonstration	The vendor has provided design documentation that includes the required informal correspondence demonstration.
AGD_ADM.1: Administrator guidance	The vendor has provided the User Console Manual documentation.
AGD_USR.1: User guidance	The vendor has provided the User Console Manual documentation.
ALC_DVS.1: Identification of security measures	The vendor has provided the Configuration Management Plan describing the IASM TOE development practices.
ALC_FLR.2: Flaw Remediation: Flaw Reporting Procedures	The vendor has provided the Configuration Management Plan, which describes the IASM TOE security flaw remediation process.
ALC_LCD.1: Life Cycle Definition: Developer Defined Life-Cycle Model	The vendor has provided the Configuration Management Plan, which describes the IASM TOE development practices.
ATE_COV.2: Analysis of coverage	The vendor has provided documentation for analysis of the IASM TOE functional security testing coverage.
ATE_DPT.1: Testing: high-level design	The vendor has provided documentation for testing of the high level design for the TSFs.
ATE_FUN.1: Functional testing	The vendor has provided documentation describing the functional security testing of the IASM TOE.
ATE_IND.2: Independent testing – sample	The laboratory used development evidence submitted by the vendor along with the functional testing evidence as a baseline for an independent test plan.
AVA_MSU.1: Examination of guidance	The vendor evidence provided for ADO_IGS, ADV_FSP, and AGD_ADM, was used to meet this requirement.
AVA_SOF.1: Strength of TOE security function evaluation	The vendor has provided documentation describing the technical basis for the IASM TOE Strength of Function claims.
AVA_VLA.1: Developer vulnerability analysis	The vendor has provided documentation describing the IASM TOE vulnerability analysis performed by the vendor.

7 PP COMPLIANCE

This ST does not claim compliance with any Protection Profile.

Vendor Application Note:
The SFRs in Chapter 5 have been specifically chosen so that when the IASM TOE is combined with external Sensor Agents that have been appropriately evaluated in their operating environments and one or more external Analytic Engines that have been appropriately evaluated in their operating environment (to determine that it (they) meet the explicitly stated SFR for the TOE Environment specified in section 5.5.1), the combined system would comply with [IDSSYPP].

8 RATIONALE

This section describes the rationale for the completeness and appropriateness of the Security Objectives and Security Functional Requirements as defined in Section 4 and 5.

8.1 Rationale for Security Objectives

8.1.1 Rationale for TOE Security Objectives

Table 8-1 – Rationale for TOE Security Objectives

Objective	Threats Mitigated By the Objective	Rationale
O.PROTCT	T.COMINT	O.PROTCT mitigates the T.COMINT threat by mandating TOE self-protection, which includes TOE data integrity-preserving, mechanisms.
	T.COMDIS	O.PROTCT mitigates the T.COMDIS threat by mandating TOE self-protection, which includes TOE data confidentiality-preserving, mechanisms.
	T.LOSSOF	O.PROTCT mitigates the T.LOSSOF threat by mandating TOE self-protection, which includes TOE data availability-preserving, mechanisms.
	T.PRIVIL	O.PROTCT mitigates the T.PRIVIL threat by mandating TOE self-protection mechanisms, which are indirectly the basis for trusting the mechanisms used to realize the O.IDAUTH and O.ACCESS objectives as well as a direct countermeasure against privilege escalation.
	T.IMPCON	O.PROTCT mitigates the T.IMPCON threat by mandating TOE self-protection mechanisms, which are indirectly the basis for trusting the mechanisms used to realize the O.IDAUTH and O.ACCESS objectives as well as a direct countermeasure against privilege escalation.
	P.MANAGE	O.PROTCT realizes the P.MANAGE policy by mandating TOE self-protection mechanisms, which are indirectly the basis for trusting the mechanisms used to realize the O.IDAUTH and O.ACCESS objectives as well as a direct countermeasure against privilege escalation.
	P.ACCESS	O.PROTCT realizes the P.ACCESS

Objective	Threats Mitigated By the Objective	Rationale
		policy by mandating TOE self-protection mechanisms, which are indirectly the basis for trusting the mechanisms used to realize the O.IDAUTH and O.ACCESS objectives as well as a direct countermeasure against privilege escalation.
	P.INTGTY	O.PROTCT realizes the P.INTGTY policy by mandating TOE self-protection, which includes TOE data integrity-preserving, mechanisms.
	P.PROTCT	O.PROTCT realizes the P.PROTCT policy by mandating TOE self-protection mechanisms, which are indirectly the basis for trusting the mechanisms used to realize the O.IDAUTH and O.ACCESS objectives as well as a direct countermeasure against privilege escalation.
O.EVENTS	T.NOHALT	O.EVENTS mitigates the T.NOHALT threat by mandating a capability for collecting events from the monitored system that might contain evidence of emerging or ongoing attacks that could halt execution of the TOE.
	T.MISUSE	O.EVENTS mitigates the T.MISUSE threat by mandating a capability to collect and store information about events from the monitored system that might contain evidence of inappropriate activity - including unauthorized access and misuse of system functions or resources - on the monitored system.
	T.INADVE	O.EVENTS mitigates the T.INADVE threat by mandating a capability to collect and store information about events from the monitored system that might contain evidence of inappropriate activity - including inadvertent activity and access - on the monitored system.
	T.MISACT	O.EVENTS mitigates the T.MISACT threat by mandating a capability to collect and store information about events from the monitored system that might contain evidence of inappropriate activity - including installation of malicious software - on the monitored system.
	P.DETECT	O.EVENTS realizes the P.DETECT

Objective	Threats Mitigated By the Objective	Rationale
		policy by mandating a capability to collect and store information about events from the monitored system that might contain evidence of inappropriate activity that may have resulted from misuse, access, or malicious activity of monitored system assets.
O.INCDNT	T.MISUSE	O.INCDNT mitigates the T.MISUSE threat by mandating interfaces for integrating analytic engines – one of which might be able to detect misuse of monitored network resources – with the TOE.
	T.INADVE	O.INCDNT mitigates the T.INADVE threat mandating interfaces for integrating analytic engines – one of which might be able to detect inadvertent activity or access on the monitored network – with the TOE.
	T.MISACT	O.INCDNT mitigates the T.MISACT threat by mandating interfaces for integrating analytic engines – one of which might be able to detect malicious activity on the monitored network – with the TOE.
	P.DETECT	O.INCDNT realizes the P.DETECT policy by mandating interfaces for integrating analytic engines that can analyze events collected from the monitored system to detect probable security incidents.
O.RESPON	P.RESPND	O.RESPON realizes the P.RESPND policy by mandating that the TOE provide a way to associate pre-defined response policies with specific detected security incidents.
O.EADMIN	T.IMPCON	O.EADMIN mitigates the T.IMPCON threat by mandating that the TOE have all the necessary administrator functions to manage the product.
	P.MANAGE	O.EADMIN realizes the P.MANAGE policy by mandating that there exist a set of functions that administrators can use to effectively manage the TOE.
O.ACCESS	T.COMINT	O.ACCESS mitigates the T.COMINT threat by mandating that only authorized users, who are trusted to only modify TOE data in accordance with appropriate security policies, can

Objective	Threats Mitigated By the Objective	Rationale
		access and change TOE data.
	T.COMDIS	O.ACCESS mitigates the T.COMDIS threat by mandating that only authorized users, who are trusted to protect the confidentiality of TOE data in accordance with appropriate security policies, can access and read TOE data.
	T.LOSSOF	O.ACCESS mitigates the T.LOSSOF threat by mandating that only authorized users, who are trusted to only delete TOE data in accordance with appropriate security policies, can access and delete TOE data.
	T.NOHALT	O.ACCESS mitigates the T.NOHALT threat by mandating that only authorized users, who are trusted to only stop TOE collection and analysis functions in accordance with appropriate security policies, can access and manage TOE collection and analysis functions.
	T.PRIVIL	O.ACCESS mitigates the T.PRIVIL threat by mandating an access control mechanism that can be used to limit the access that authorized users have to parts of the TOE.
	T.IMPCON	O.ACCESS mitigates the T.IMPCON threat by mandating an access control mechanism that can be used to limit the access that authorized users have to parts of the TOE.
	P.MANAGE	O.ACCESS realizes the P.MANAGE policy by mandating an access control mechanism that can be used to limit the access that authorized users have to the management functions of the TOE.
	P.ACCESS	O.ACCESS realizes the P.ACCESS policy by mandating that the TOE only provide authorized users with access to appropriate TOE functions and data.
	P.PROTCT	O.ACCESS realizes the P.PROTCT policy by mandating that only authorized users can access appropriate TOE functions and data.
O.IDAUTH	T.COMINT	O.IDAUTH mitigates the T.COMINT threat by mandating authentication of users prior to any TOE data access, which provides the basis for realizing

Objective	Threats Mitigated By the Objective	Rationale
		O.ACCESS.
	T.COMDIS	O.IDAUTH mitigates the T.COMDIS threat by mandating authentication of users prior to any TOE data access, which provides the basis for realizing O.ACCESS.
	T.LOSSOF	O.IDAUTH mitigates the T.LOSSOF threat by mandating authentication of users prior to any TOE data access, which provides the basis for realizing O.ACCESS.
	T.NOHALT	O.IDAUTH indirectly mitigates the T.NOHALT threat by mandating authentication of users prior to any TOE function accesses, which provides the basis for realizing O.ACCESS, which directly mitigates T.NOHALT.
	T.PRIVIL	O.IDAUTH mitigates the T.PRIVIL threat by mandating authentication of users prior to any TOE data access, which allows the TOE to distinguish between privileged and unprivileged users.
	T.IMPCON	O.IDAUTH mitigates the T.IMPCON threat by mandating authentication of users prior to any TOE data access, which allows the TOE to distinguish between privileged and unprivileged users.
	P.MANAGE	O.IDAUTH realizes the P.MANAGE policy by mandating authentication of users prior to permitting access to any TOE data or functions, which allows the TOE to distinguish between privileged and unprivileged users.
	P.ACCESS	O.IDAUTH realizes the P.ACCESS policy by mandating authentication of users prior to the TOE establishing their authorizations and performing any actions on their behalf, which provides the basis for realizing O.ACCESS.
	P.ACCACT	O.IDAUTH realizes the P.ACCACT policy by mandating authentication of users prior to the TOE establishing their authorizations and performing - and auditing - any actions on their behalf.
	P.PROTCT	O.IDAUTH realizes the P.PROTCT policy by mandating authentication of

Objective	Threats Mitigated By the Objective	Rationale
		users prior to the TOE establishing their authorizations and performing any actions on their behalf, which provides the basis for realizing O.ACCESS.
O.COMACC	T.COMDIS	O.COMACC mitigates the T.COMDIS threat by mandating that only authorized external entities can communicate with the TOE.
	T.COMINT	O.COMACC mitigates the T.COMINT threat by mandating that only authorized external entities can communicate with the TOE.
	T.LOSSOF	O.COMACC mitigates the T.LOSSOF threat by mandating that only authorized external entities can communicate with the TOE.
	T.NOHALT	O.COMACC mitigates the T.NOHALT threat by mandating that only authorized external entities can communicate with the TOE.
	T.PRIVIL	O.COMACC mitigates the T.PRIVIL threat by mandating that only authorized external entities can communicate with the TOE.
	P.ACCESS	O.COMACC realizes the P.ACCESS policy by mandating that only authorized, and presumably acting for authorized purposes, external entities can communicate with the TOE.
	P.PROTCT	O.COMACC realizes the P.PROTCT policy by mandating that only authorized users can access appropriate TOE functions and data.
	P.USESTD	O.COMACC realizes the P.USESTD policy by necessarily requiring use of a standard secure communication protocol for use with potentially arbitrary external entities.
O.COMCON	T.COMDIS	O.COMCON mitigates the T.COMDIS threat by mandating that the protocol used to communicate with external entities provide confidentiality of the data exchanged.
	P.PROTCT	O.COMCON realizes the P.PROTCT policy by mandating that data is only disclosed (which is a form of access) to the specific external entities with which the TOE is authorized to communicate.

Objective	Threats Mitigated By the Objective	Rationale
O.COMINT	T.COMINT	O.COMINT mitigates the T.COMINT threat by mandating that the protocol used to communicate with external entities detect changes to any of the data exchanged.
	T.LOSSOF	O.COMINT mitigates the T.LOSSOF threat by mandating that the protocol used to communicate with external entities detect loss of any of the data exchanged.
	P.INTGTY	O.COMINT realizes the P.INTGTY policy by mandating that the protocol used to communicate with external entities detect changes to any of the data exchanged.
O.OFLOWS	T.INFLUX	O.OFLOWS mitigates the T.INFLUX threat by mandating that the TOE handle data storage overflows.
	P.PROTCT	O.OFLOWS realizes the P.PROTCT policy by mandating that the TOE handle data storage overflows.
O.AUDITS	T.FACCNT	O.AUDITS mitigates the T.FACCNT threat by mandating that the TOE to audit attempts for data accesses and use of TOE functions.
	T.MISUSE	O.AUDITS mitigates the T.MISUSE threat by mandating that the TOE record audit records of TOE data accesses and use of TOE functions.
	T.INADVE	O.AUDITS mitigates the T.INADVE threat by mandating that the TOE record audit records of TOE data accesses and use of TOE functions.
	T.MISACT	O.AUDITS mitigates the T.MISACT threat by mandating that the TOE record audit records of TOE data accesses and use of TOE functions.
	P.DETECT	O.AUDITS realizes the P.DETECT policy by mandating that the TOE record audit records of TOE data accesses and use of TOE functions.
	P.ACCACT	O.AUDITS realizes the P.ACCACT policy by mandating that the TOE record audit records of TOE data accesses and use of TOE functions.
O.INTEGR	T.COMINT	O.INTEGR mitigates the T.COMINT threat by mandating integrity protection mechanisms for TOE data.
	T.LOSSOF	O.INTEGR mitigates the T.LOSSOF threat by mandating integrity

Objective	Threats Mitigated By the Objective	Rationale
		protection mechanisms for TOE data.
	P.INTGTY	O.INTEGR realizes the P.INTGTY policy by mandating integrity protection mechanisms for data that is collected and produced by the TOE.

8.1.2 Rationale for TOE Environment Security Objectives

Table 8-2 – Rationale for TOE Environment Security Objectives

Objective	Threats Mitigated By the Objective	Rationale
O.INSTAL	A.NOEVIL	O.INSTAL imposes an operational constraint that is consistent with the A.NOEVIL assumption that authorized administrators of the TOE will follow and abide by the instructions provided in the TOE documentation.
	A.NETSEP	O.INSTAL imposes an operational constraint that ensures that the A.NETSEP assumption is faithfully implemented in the operational environments where the TOE is used.
	T.IMPCON	O.INSTAL mitigates the T.IMPCON threat by mandating that authorized administrators configure the TOE properly - thus establishing an "appropriate" configuration.
	P.MANAGE	O.INSTAL realizes the P.MANAGE policy by mandating that those responsible for security will manage the TOE in accordance with all provided documentation and maintain the security policy.
O.PHYCAL	A.PROTCT	O.PHYCAL imposes an operational constraint that is consistent with the A.PROTCT assumption of physical protection for the TOE.
	A.LOCATE	The O.PHYCAL TOE environment objective wording implies that the TOE will be located within controlled access facilities to prevent unauthorized physical access.
	A.NOEVIL	O.PHYCAL imposes an operational constraint that is consistent with the A.NOEVIL assumption that authorized administrators of the TOE are not careless, willfully negligent, or hostile.
	A.NOTRST	O.PHYCAL imposes an operational

Objective	Threats Mitigated By the Objective	Rationale
		constraint that is consistent with the A.NOTRST assumption that only authorized users can physically access the TOE hardware.
	P.PROTCT	O.PHYCAL supports the P.PROTCT policy by mandating that only authorized users can physically access the TOE hardware.
O.CREDEN	A.NOEVIL	O.CREDEN imposes an operational constraint that is consistent with the A.NOEVIL assumption that authorized administrators of the TOE will follow and abide by the instructions provided in the TOE documentation.
	A.NOTRST	O.CREDEN supports the A.NOTRST assumption by mandating that authorized users protect their authentication data, thus preventing unauthorized users from trivially gaining access to the TOE.
	T.PRIVIL	O.CREDEN mitigates the T.PRIVIL threat by mandating that authorized users protect their credentials to prevent an unauthorized user from being able to masquerade as an authorized user.
	T.IMPCON	O.CREDEN mitigates the T.IMPCON threat by mandating that authorized users protect their credentials to prevent an unauthorized user from being able to masquerade as an authorized user.
	P.MANAGE	O.CREDEN realizes the P.MANAGE policy by mandating that authorized users - including administrators - protect their credentials to prevent an unauthorized user from being able to masquerade as an authorized user.
	P.ACCESS	O.CREDEN realizes the P.ACCESS policy by requiring authorized users to protect their authentication data, thus preventing unauthorized users from trivially gaining access to the TOE by masquerading as an authorized user.
	P.ACCACT	O.CREDEN realizes the P.ACCACT policy by requiring authorized users to protect their authentication data, thus preventing unauthorized users from masquerading as an authorized user.
	P.PROTCT	O.CREDEN realizes the P.PROTCT policy by requiring authorized users to

Objective	Threats Mitigated By the Objective	Rationale
		protect their authentication data, thus preventing unauthorized users from trivially gaining access to the TOE by masquerading as an authorized user.
O.PERSON	A.DYNMIC	O.PERSON obligates the TOE Environment to fulfill the A.DYNMIC assumption of competent active management.
	A.MANAGE	O.PERSON obligates the TOE Environment to fulfill the A.MANAGE assumption that all authorized administrators are qualified and trained to manage the TOE.
	P.MANAGE	O.PERSON realizes the P.MANAGE policy by mandating that authorized administrators are carefully chosen and trained for their responsibilities.
O.INTROP	P.USESTD	O.INTROP realizes the P.USESTD policy by mandating that the TOE interoperate with the IT System: implicitly requiring use of the same network & security technologies.
	A.EVENTS	O.INTROP imposes an operational constraint that is consistent with the A.EVENTS assumption that the TOE and devices on the external network use the same security technologies to communicate.
	A.DYNMIC	O.INTROP imposes an operational constraint that is consistent with the A.DYNMIC assumption that the TOE will be able to effect its management actions.
	A.ASCOPE	O.INTROP imposes an operational constraint that is consistent with the A.ASCOPE assumption that the TOE will be used only to protect networks that do not exceed the TOE's monitoring capacity.
	A.COMMS	O.INTROP imposes an operational constraint that is consistent with the A.COMMS assumption that there is an adequate networking infrastructure to support intra- and extra-TOE communications.
O.SENSRS	P.DETECT	O.SENSRS obligates the TOE Environment to actually contain specific software that collects and sends the events required to meet the P.DETECT policy.

Objective	Threats Mitigated By the Objective	Rationale
	P.USESTD	O.SENSRS obligates the TOE Environment to actually contain specific software that interoperates with the TOE and therefore must meet the P.USESTD policy.
	T.INFLUX	O.SENSRS obligates the TOE Environment to actually contain specific software with features (i.e., buffering) that mitigate T.INFLUX.
	T.MISUSE	Mitigating T.MISUSE first requires the observation of events that might indicate such misuse. O.SENSRS obligates the TOE Environment to actually contain specific software that collects and sends such events to the TOE.
	T.INADVE	Mitigating T.INADVE first requires the observation of events that might indicate such inadvertent activity and access. O.SENSRS obligates the TOE Environment to actually contain specific software that collects and sends such events to the TOE.
	T.MISACT	Mitigating T.MISACT first requires the observation of events that might indicate such malicious activity. O.SENSRS obligates the TOE Environment to actually contain specific software that collects and sends such events to the TOE.
	A.EVENTS	O.SENSRS obligates the TOE Environment to actually contain specific software that collects and sends the events referenced in A.EVENTS to the TOE.
	A.ASCOPE	O.SENSRS obligates the TOE Environment to actually contain specific software that is able to conform to A.ASCOPE.
O.ANALYZ	P.DETECT	O.ANALYZ obligates the TOE Environment to actually contain specific software that detects security incidents, as required by the P.DETECT policy.
	P.USESTD	O.ANALYZ obligates the TOE Environment to actually contain specific software that interoperates with the TOE and therefore must meet the P.USESTD policy.
	T.MISUSE	Mitigating T.MISUSE requires

Objective	Threats Mitigated By the Objective	Rationale
		detection of misuse by analyzing events collected from the IT System. O.ANALYZ obligates the TOE Environment to actually contain specific software that does such analysis and detection and sends the TOE detected security incidents.
	T.INADVE	Mitigating T.INADVE requires detection of inadvertent activity and access by analyzing events collected from the IT System. O.ANALYZ obligates the TOE Environment to actually contain specific software that does such analysis and detection and sends the TOE detected security incidents.
	T.MISACT	Mitigating T.MISACT requires detection of malicious activity by analyzing events collected from the IT System. O.ANALYZ obligates the TOE Environment to actually contain specific software that does such analysis and detection and sends the TOE detected security incidents.

Table 8-3 – Summary Correlation of Security Objectives With Assumptions, Threats, and Policies

Assumptions, Threats, and Policies	O.PROTCT	O.EVENTS	O.INCDNT	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.COMACC	O.COMCON	O.COMINT	O.OFLOWS	O.AUDITS	O.INTEGR	O.INSTAL	O.PHYCAL	O.CREDEN	O.PERSON	O.INTROP	O.SENSRS	O.ANALYZ
A.DYNMIC																	X	X		
A.EVENTS																		X	X	
A.ASCOPE																		X	X	
A.COMMS																		X		
A.NETSEP														X						
A.PROTCT															X					
A.LOCATE															X					
A.MANAGE																	X			
A.NOEVIL														X	X	X				
A.NOTRST															X	X				
T.COMINT	X					X	X	X		X			X							
T.COMDIS	X					X	X	X	X											
T.LOSSOF	X					X	X	X		X			X							
T.NOHALT		X				X	X	X												
T.PRIVIL	X					X	X	X								X				
T.IMPCON	X				X	X	X							X		X				
T.INFLUX											X								X	
T.FACCNT												X								
T.MISUSE		X	X									X							X	X
T.INADVE		X	X									X							X	X
T.MISACT		X	X									X							X	X
P.DETECT		X	X									X							X	X
P.RESPND				X																
P.MANAGE	X				X	X	X							X		X	X			
P.ACCESS	X					X	X	X								X				
P.ACCACT							X					X				X				
P.INTGTY	X									X			X							
P.PROTCT	X					X	X	X	X		X				X	X				
P.USESTD								X										X	X	X

8.2 Rationale for TOE Security Requirements

Table 8-4 – Rationale for TOE Security Requirements

Objective	Security Function Requirements Addressing the Objective	Rationale
O.PROTCT	FAU_GEN.1, FAU_SAR.1, FAU_SAR.2, FPT_STM.1	FAU_GEN.1, FAU_SAR 1, FAU_SAR.2, and FPT_STM.1 require that the TOE be able to generate and make available to TOE administrators time-stamped audit records of a specified set of security-relevant events related to the TOE operations so that, if other self-protection mechanisms fail, the TOE administrators can determine how the failure occurred and assess the extent of the damage.
	FAU_STG.2, FAU_STG.4, IDS_STG_(EXP).1	FAU_STG.2, FAU_STG.4 and IDS_STG_(EXP).1 require the TOE to protect SIM repository that holds both the TOE security audit data and collected event and incident data from deletion as well as guarantee the data availability in the event of storage exhaustion, failure or attack.
	FIA_AFL.1, FIA_UAU.1, FIA_UID.1	FIA_AFL.1, FIA_UAU.1, and FIA_UID.1 require the TOE to prevent unauthenticated (and therefore, unauthorized) users from having access to any TOE functions or data.
	FIA_SOS.2	FIA_SOS.2 requires the TOE to provide a mechanism by which to generate user authentication secrets that are "strong enough" for a given installation of the TOE.
	FMT_MOF.1, FMT_MTD.1, FMT_SMF.1	FMT_MOF.1 and FMT_MTD.1 require the TOE to protect its TSF functions and data from access by non-privileged users.
	FTP_ITC.1	FTP_ITC.1 requires the TOE to refuse to open a communication channel with an external entity that is not using the security function that allows the TOE to identify, authenticate, and protect sensitive information exchanged with that entity.
	FPT_RVM.1, FPT_SEP.1	FPT_RVM.1 and FPT_SEP.1 require the TOE to provide mechanisms that ensure the effective enforcement of access to and isolation of TOE Security Functions.
O.EVENTS	FAU_GEN.1	FAU_GEN.1 requires that TOE components, including Sensors, have the ability to generate records of defined security-relevant events.
	FPT_STM.1	FPT_STM.1 requires the TOE to have a source of reliable timestamps, which are a critical component of the information that must be associated with each event collected and stored by the TOE.
	IDS_SDC_(EXP).1	IDS_SDC_(EXP).1 requires the TOE to accept and store event data, which may have indications of inappropriate activity resulting from misuse of, access to, or malicious activity on monitored system assets, from devices on the monitored network and defines the minimum information that must be collected for each kind of event.

Objective	Security Function Requirements Addressing the Objective	Rationale
O.INCDNT	FPT_STM.1	FPT_STM.1 requires the TOE to have a source of reliable timestamps, which are a critical component of the information that must be associated with each incident collected and stored by the TOE.
	IDS_SDC_(EXP).1	IDS_SDC_(EXP).1 requires the TOE to accept, and store in the SIM repository, information about probable incidents.
O.RESPON	IDS_RCT_(EXP).1	IDS_RCT_(EXP).1 requires the TOE to display applicable response policies for each detected probable incident.
O.EADMIN	FAU_SAR 1, FAU_SAR.3	FAU_SAR.1 and FAU_SAR.3 require the TOE to provide the ability to review and manage information in the SIM repository that is related to the TOE operations.
	FAU_STG.4	FAU_STG.4 requires the TOE to provide the ability to manage the lifecycle of information in the SIM repository that is related to the TOE operations
	FIA_AFL.1	FIA_AFL.1 requires the TOE to provide the Administrator role with the ability to limit authenticator guessing attacks on authorized users' accounts.
	FIA_SOS.2	FIA_SOS.2 requires the TOE to provide the Administrator role with the ability to set the quality of the password authenticators that will be generated and used for user authentication.
	FMT_MOF.1, FMT_MTD.1 FMT_SMF.1	FMT_MOF.1 and FMT_MTD.1 require the TOE to restrict the authority to modify the behavior of TOE functions (which have been defined in FMT_SMF.1) and values of TSF data to the Administrator role.
	FPT_RVM.1, FPT_SEP.1	FPT_RVM.1 and FPT_SEP.1 require the TOE to provide mechanisms that ensure the effective enforcement of access to and isolation of administrative functions.
	IDS_RDR_(EXP).1	IDS_RDR_(EXP).1 requires the TOE to provide the ability to review and manage information in the SIM repository.
	IDS_STG_(EXP).1, IDS_STG_(EXP).2	IDS_STG_(EXP).1 and IDS_STG_(EXP).2 require the TOE to provide the ability to manage the lifecycle of information in the SIM repository that is related to the monitored system.
O.ACCESS	FAU_SAR 1, FAU_SAR.2, IDS_RDR_(EXP).1	FAU_SAR.1, FAU_SAR.2, and IDS_RDR_(EXP).1 establish the disclosure access control policy for the collections of security- and intrusion-relevant events managed by the TOE.
	FAU_STG.2, FAU_STG.4, IDS_STG_(EXP).1	FAU_STG.2, FAU_STG.4, and IDS_STG_(EXP).1 establish the integrity access control policy for the collections of security- and intrusion-relevant events managed by the TOE.
	FIA_AFL.1, FIA_UAU.1, FIA_UID.1	FIA_AFL.1, FIA_UAU.1, and FIA_UID.1 require the TOE to prevent unauthenticated (and therefore, unauthorized) users from having access to any TOE functions or data.
	FIA_ATD.1, FMT_SMR.1	FIA_ATD.1 and FMT_SMR.1 require the TOE to maintain specific access control information for use in making access control decisions.
	FMT_MOF.1, FMT_MTD.1	FMT_MOF.1 and FMT_MTD.1 establish the disclosure and integrity access control policies for TSF functions and data.

Objective	Security Function Requirements Addressing the Objective	Rationale
	FPT_RVM.1, FPT_SEP.1	FPT_RVM.1 and FPT_SEP.1 require the TOE to provide mechanisms that ensure the correct computation and effective enforcement of access control policies.
O.IDAUTH	FIA_AFL.1	FIA_AFL.1 requires the TOE to provide a mechanism for limiting authenticator guessing attacks on authorized users' accounts.
	FIA_ATD.1, FMT_SMR.1	FIA_ATD.1 and FMT_SMR.1 require the TOE to associate specified security attributes, including authentication data, with authorized users of the TOE.
	FIA_SOS.2	FIA_SOS.2 requires the TOE to provide a mechanism by which to generate user authentication secrets that are "strong enough" for a given installation of the TOE.
	FIA_UAU.1, FIA_UID.1	FIA_UAU.1 and FIA_UID.1 require the TOE to identify and authenticate a user before allowing that user to access any TOE functions or data.
	FPT_RVM.1, FPT_SEP.1	FPT_RVM.1 and FPT_SEP.1 require the TOE to provide mechanisms that ensure the correct computation and effective enforcement of identification and authentication decisions.
O.COMACC	FTP_ITC.1	FTP_ITC.1 requires the TOE to provide a security function that protects sensitive information in transit between the TOE and an identified and authenticated external entity.
	FPT_RVM.1	FPT_RVM.1 requires the TOE to ensure that the FTP_ITC.1 identification and authentication security function(s) are always successfully invoked before communicating with external entities.
	FPT_SEP.1	FPT_SEP.1 requires the TOE to prevent the FTP_ITC.1 identification and authentication security function(s) from being affected by the actions of any external entities.
O.COMCON	FTP_ITC.1	FTP_ITC.1 requires the TOE to provide a security function that protects sensitive information in transit between the TOE and an identified and authenticated external entity from disclosure.
	FPT_RVM.1	FPT_RVM.1 requires the TOE to ensure that the FTP_ITC.1 confidentiality protection security function(s) are always successfully invoked when communicating with external entities.
	FPT_SEP.1	FPT_SEP.1 requires the TOE to prevent the FTP_ITC.1 confidentiality protection security function(s) from being affected by the actions of any external entities.
O.COMINT	FTP_ITC.1	FTP_ITC.1 requires the TOE to provide a security function that protects sensitive information in transit between the TOE and an identified and authenticated external entity from undetected modification or loss.
	FPT_RVM.1	FPT_RVM.1 requires the TOE to ensure that the FTP_ITC.1 integrity protection security function(s) are always successfully invoked when communicating with external

Objective	Security Function Requirements Addressing the Objective	Rationale
		entities.
	FPT_SEP.1	FPT_SEP.1 requires the TOE to prevent the FTP_ITC.1 integrity protection security function(s) from being affected by the actions of any external entities.
O.OFLOWS	FAU_STG.2	FAU_STG.2 requires the TOE to protect the collection of security-relevant events related to the TOE operations from deletion as well as guarantee the availability of those events if the storage media for that collection becomes full, fails, or is attacked.
	FAU_STG.4	FAU_STG.4 requires the TOE to prevent the loss of the collection of security-relevant events related to the TOE operations if the storage media for that collection becomes full.
	IDS_STG_(EXP).1	IDS_STG_(EXP).1 requires the TOE to to protect the collection of intrusion-relevant events related to the IT System from any modification and unauthorized deletion, as well as guarantee the availability of those events if the storage media for that collection becomes full, fails, or is attacked.
	IDS_STG_(EXP).2	IDS_STG_(EXP).2 requires the TOE to prevent the loss of the collection of intrusion-relevant events related to the IT System if the storage media for that collection becomes full.
O.AUDITS	FAU_GEN.1	FAU_GEN.1 requires that the TOE be able to generate audit records of a specified set of security-relevant events related to the TOE operations.
	FAU_SAR.1, FAU_SAR.2, FAU_SAR.3	FAU_SAR.1, FAU_SAR.2, and FAU_SAR.3 requires the TOE to provided appropriately controlled mechanisms for reviewing the collection of security-relevant events related to the TOE operations.
	FPT_RVM.1, FPT_SEP.1	FPT_RVM.1 and FPT_SEP.1 require the TOE to provide mechanisms that ensure the correct and effective operation of the audit functions.
	FPT_STM.1	FPT_STM.1 requires the TOE to have a source of reliable timestamps for use in the audit records.
O.INTEGR	FAU_STG.2, FAU_STG.4, IDS_STG_(EXP).1	FAU_STG.2, FAU_STG.4, and IDS_STG_(EXP).1 establish the integrity access control policy for the collections of security- and intrusion-relevant events managed by the TOE.
	FMT_MTD.1	FMT_MTD.1 requires the TOE to ensure that only authorized administrators of the System can query or add audit and System data.
	FPT_RVM.1, FPT_SEP.1	FPT_RVM.1 and FPT_SEP.1 require the TOE to provide mechanisms that ensure the correct computation and effective enforcement of integrity access control policies.
O.ANALYZ	IDS_ANL_(EXP).1	IDS_ANL_(EXP).1 requires the TOE environment to contain at least one external entity that provides an analytic capability with specific characteristics.

Table 8-5 – Summary Correlation of Security Objectives With Security Function Requirements

Security Function Requirements	O.PROTCT	O.EVENTS	O.INCDNT	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.COMACC	O.COMCON	O.COMINT	O.OFLOWS	O.AUDITS	O.INTEGR	O.ANALYZ
FAU_GEN.1	X	X										X		
FAU_SAR 1	X				X	X						X		
FAU_SAR.2	X					X						X		
FAU_SAR.3					X							X		
FAU_STG.2	X					X					X		X	
FAU_STG.4	X				X	X					X		X	
FIA_AFL.1	X				X	X	X							
FIA_ATD.1						X	X							
FIA_SOS.2	X				X		X							
FIA_UAU.1	X					X	X							
FIA_UID.1	X					X	X							
FMT_MOF.1	X				X	X								
FMT_MTD.1	X				X	X							X	
FMT_SMF.1	X				X									
FMT_SMR.1						X	X							
FPT_RVM.1	X				X	X	X	X	X	X		X	X	
FPT_SEP.1	X				X	X	X	X	X	X		X	X	
FPT_STM.1	X	X	X									X		
FTP_ITC.1	X							X	X	X				
IDS_SDC_(EXP).1		X	X											
IDS_RCT_(EXP).1				X										
IDS_RDR_(EXP).1					X	X								
IDS_STG_(EXP).1	X				X	X					X		X	
IDS_STG_(EXP).2					X						X			
IDS_ANL_(EXP).1														X

8.3 Rationale for Strength of Security Functions

The rationale for TOE Strength of Function described in this section satisfies the SOF-Basic claim. The reasoning for SOF-Basic claim is that the TOE strength of function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential. The SOF-basic strength level is also sufficient to meet the objectives of the TOE given the security environment described in the ST.

This Security Target includes a probabilistic or permutation analysis of the password mechanism as required by AVA_SOF.1. This is provided below along with an analysis showing that the design basis for specific security function requirements (SFRs) – FIA_UAU.2.1 (Identification and Authentication) and FIA_SOS.2.1 (TSF Generation of secrets) – satisfies both the AVA_SOF.1 security assurance requirement claim of SOF-Basic and the SFRs' statements. The only probabilistic function on which the strength of the authentication mechanisms depends is the password entered for login into the User Console. The User Console valid range of values for a password is constrained by the rules summarized in Section 6.6.3: as required in FIA_SOS.2.1. Briefly, these rules require a password of at least 8 non-repeated characters, which starts and ends with an alphanumeric character and must have at least one special character in one of the other positions. The alphabetic characters are case sensitive. For purposes of the analysis below, the other password rules are simplistically and conservatively interpreted to reduce the password space by prohibiting substrings of 2 or more purely numeric characters and 2 or more purely alphabetic characters (where the following character substitutions are considered during the purely alphabetic substring analysis (0=O, 1=L, 3=E, 5=S, 8=B, !=L, @=A, $=S, &=A). This substring approach handles the rules for: use of the login-id (which must be comprised of the alphanumeric characters, "-" and "_"); use of words in any language (since any non-English language would have to be transliterated into some sequence of ASCII alphabetic characters); sequences of letters or numbers; keyboard patterns; and the use of certain special characters in place of alphabetic characters.

The TOE recognizes 52 alphabetic characters (a-z, A-Z), 10 numeric characters (0 to 9), and 32 special characters (~, `, !, @, #, $, %, ^, &, *, (,), _, +, -, =, [,], {, }, \, |, ;, : ", ', ,, ., <, >, ?, /). According to the password generation rules in Section 6.6.3 the shortest allowable password is 8 characters, has no repeating characters, starts and ends with an alphanumeric character, and has at least one special character in one of the other positions. Applying this rule, with no additional constraints, results in a maximum password generation space of 62*93*92*91*90*89*88*56 = 1,905,491,750,722,560 possible passwords.

The full set of rules, however, requires that this space be reduced by excluding prohibited substrings from consideration. As noted above, this analysis has been simplified by prohibiting any purely alphabetic or purely numeric substring. Since this is actually more restrictive than the specific rules, it ensures that the analysis is conservative and that the actually acceptable password strength is relatively greater due to an even larger space within which a search would have to be conducted.

The excluded substrings are computed in the following way. For each *Size* of substring (2 characters through 8 characters), the total number of possible prohibited strings is computed using the following formula:

P * ((L! / (L-*Size*)!) + (N! / (N-*Size*)!))

where the letter “L” represents the standard alphabetic characters (52) plus the 9 alphabetic-equivalent characters identified above, the letter “N” represents the 10 numeric characters, and the letter “P” represents the number of places within an 8-character string at which substrings of length *Size* could start (computed as 8-(*Size*-1)). The numbers of excluded substrings for each different substring size are computed and then summed and subtracted from the maximum password generation space to derive the baseline password generation space. The baseline password generation space computation is as follows:

Substring Size	Computation	Value
2	7 * ((61! / 59!) + (10! / 8!))	26,250
3	6 * ((61! / 58!) + (10! / 7!))	1,299,960
4	5 * ((61! / 57!) + (10! / 6!))	62,647,800
5	4 * ((61! / 56!) + (10! / 5!))	2,855,711,520
6	3 * ((61! / 55!) + (10! / 4!))	119,935,257,120
7	2 * ((61! / 54!) + (10! / 3!))	4,397,610,672,000
8	(61! / 53!) + (10! / 2!)	118,735,457,299,200
	Totals	123,255,922,913,850

Maximum Password Space = 1,905,491,750,722,560 - 123,255,922,913,850
Baseline Password Space = 1,782,235,827,808,710

To mount a brute-force attack on the baseline password space, an attacker would, on average, have to try half of the passwords in the space (891,117,913,904,355) before discovering a valid password. Assuming that a failed login attempt takes 10 seconds, and since the TOE locks the authentication mechanism for 360 seconds (6 mins) after 3 failed authentication attempts, the average cost of a failed login attempt is ((3*10)+360)/3 = 130 seconds. Thus, on average, it will take 3,670,916,952 years ((891,117,913,904,355 tries * 130 s/try) / 31,557,600 s/yr) for a brute-force attack on a generated IASM TOE password to succeed.

According to the Common Evaluation Methodology Table B3 (page 365), the elapsed time *is not practical*. The result presents a HIGH strength of function, which surpasses SOF-Basic.

8.4 Rationale for Assurance Requirements

EAL3 was chosen to comply with the DoDI8500.2 guidance for the use of Low to Medium Robustness products. The EAL3 Assurance Requirements have been augmented with ALC_FLR.2 and ALC_LCD.1 in order to satisfy a perceived market expectation that vendors of security products should employ more consistent software security engineering practices that include a systematic process for accepting reports of security flaws and then developing and distributing repairs for those flaws.

8.5 Requirement Dependency Rationale

The IASM Security Target does satisfy all the requirement dependencies of the Common Criteria. Table 14 lists each requirement from the IASM SFRs in Section 5.1 with a dependency and indicates whether the dependent requirement was included. As the table indicates, all dependencies among the requirements from the CC Part 2 catalog have been met.

Table 8-6 – Requirement Dependencies

Functional Component	Depends On	Included
FAU_GEN.1	FPT_STM.1	Yes
FAU_SAR.1	FAU_GEN.1	Yes
FAU_SAR.2	FAU_SAR.1	Yes
FAU_SAR.3	FAU_SAR.1	Yes
FAU_STG.2	FAU_GEN.1	Yes
FAU_STG.4	FAU_STG.2*	Yes
FIA_AFL.1	FIA_UAU.1	Yes
FIA_ATD.1	None	
FIA_SOS.2	None	
FIA_UAU.1	FIA_UID.1	Yes
FIA_UID.1	None	
FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	Yes
FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	Yes
FMT_SMF.1	None	
FMT_SMR.1	FIA_UID.1	Yes
FPT_RVM.1	None	
FPT_SEP.1	None	
FPT_STM.1	None	
FTP_ITC.1	None	

* CC v2.2 actually identifies the dependency as FAU_STG.1, but FAU_STG.2 is hierarchical to FAU_STG.1 and therefore effectively satisfies the dependency.

8.6 Explicitly Stated Requirement Dependency Rationale

This ST also includes explicitly stated IDS requirements from [IDSSYPP]. The family of IDS requirements was created to specifically address the data collected and analyzed by an IDS. The audit family of the CC (FAU) was used as a model for creating these requirements. The purpose of this family of requirements is to address the unique nature of IDS data and provide for requirements about collecting, reviewing and managing the data. The stated IDS requirements have no dependencies since they embody all of the necessary security functions.

9 REFERENCES

[CC] *Common Criteria for Information Technology Security Evaluation, ISO/IEC 15408 Version 2.2*, International Standardization Organization, January 2004

[IDSSYPP] *Intrusion Detection System System Protection Profile, Version 1.5*, National Security Agency, March 2005

[IATF] *Information Assurance Technical Framework, Version 3.0*, National Security Agency, September 2000

10 ACRONYMS

The following abbreviations from the Common Criteria are used in this Security Target:

AES	Advanced Encryption Standard
ATM	Asynchronous Transfer Method
CC	Common Criteria for Information Technology Security Evaluation
DES	Data Encryption Standard
DoD	Department of Defense
DMZ	Demilitarized zone
EAL	Evaluation Assurance Level
ESP	Encapsulating Security Payload
FIPS PUB	Federal Information Processing Standard Publication
FTP	File Transfer Protocol
GIG	Global Information Grid
HTTP	Hypertext Transfer Protocol
I&A	Identification and Authentication
IATF	Information Assurance Technical Framework
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IPSEC ESP	Internet Protocol Security Encapsulating Security Payload
IP	Internet Protocol
IT	Information Technology
MRE	Medium Robustness Environment
NBIAT&S	Network Boundary Information Assurance Technologies and Solutions Support
NIAP	National Information Assurance Partnership

NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSES	(IASM) Network Security Event Sensor
NTP	Network Time Protocol
PKI	Public Key Infrastructure
PP	Protection Profile
RNG	Random Number Generator
SFP	Security Function Policy
SMTP	Simple Mail Transfer Protocol
SOF	Strength of Function
SSL	Secure Sockets Layer
SSLIOP	SSL Inter-ORB Protocol
ST	Security Target
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TOE	Target of Evaluation
TSE	TOE Security Environment
TSF	TOE Security Function
TSP	TOE Security Policy
UDP	User Datagram Protocol
URL	Uniform Research Locator
VPN	Virtual Private Network

11 RATIONALE FOR USE OF PREVIOUSLY EVALUATED IA PRODUCTS IN THE PROMIA IASM TOE

PD 0117, PP Conformance Using and Underlying Evaluated Product, establishes the guidelines under which a previously evaluated IA product (PEP) can be used as a component of a larger TOE evaluation. The Promia Intelligent Agent Security Manager (IASM) uses 2 previously evaluated products: Windows XP Professional and SuSE Linux 9.1. This Chapter provides analyses of the SuSE Linux Enterprise Server Version 9 ST and the Windows XP Professional ST with respect to each of the clauses of PD 011 in order to demonstrate that the IASM TOE reliance on these two products is appropriate and consistent with PD-0117.

11.1 Rationale for the Use of SuSE LINUX 9.1 in the IASM TOE

11.1.1 Required PEP Assurance Level

SuSE Linux 9.1 was evaluated at EAL4, augmented with ALC_FLR.3. The IASM TOE ST claims EAL3+: specifically, augmentation with ALC_FLR.2 and ALC_LCD.1. The EAL4 augmented level of SuSE Linux 9.1 is greater than the EAL3 augmented level claimed for the IASM TOE. Likewise, the ALC_FLR.3 SAR that augments SuSE Linux 9.1 is hierarchical to ALC_FLR.2 SAR that augments the IASM TOE, thus meeting this constraint.

11.1.2 IASM TOE Must Leverage Some SuSE LINUX 9.1 SFRs

11.1.3 SuSE LINUX 9.1 SFRs Must Not Conflict with IASM TOE SFRs

SuSE Linux Enterprise Server (SLES) 9.1 is the operating system used on all of the hardware components that comprise the actual IASM TOE appliance. Table 11-1, below, explains both how the IASM TOE leverages certain Security Function Requirements (SFRs) (highlighted in gray in the table) from the SLES 9.1 Security Target [EAL4-SLES-ST] and why the SFRs that are not leveraged by the IASM TOE do not conflict or interfere with the ability of the IASM TOE to meet its own SFRs.

Table 11-1 – IASM Use of SUSE Linux Enterprise Server 9.1 (SLES) Security Features

SFR name	SLES	IASM	Relationship of SLES SFR to IASM SFR
FAU_GEN.1	X	X	The IASM does not rely on the SLES FAU_GEN.1 SFR. While both STs include this requirement, the sets of specific objects and events to which the requirement applies are entirely disjoint.
FAU_GEN.2	X		The IASM does not rely on the SLES FAU_GEN.2 SFR. In addition to the IASM ST not including the SFR, the IASM maintains its own user identity database and would therefore not be able to use the SLES information.
FAU_SAR.1	X	X	The IASM does not rely on the SLES FAU_SAR.1, FAU_SAR.2, or FAU_SAR.3 SFRs. While both STs include these requirements, the sets of specific objects to which the SFRs apply, and the SFR enforcement
FAU_SAR.2	X	X	

FAU_SAR.3	**X**	**X**	mechanisms, are entirely disjoint.
FAU_SEL.1	**X**		The IASM does not rely on the SLES FAU_SEL.1 SFR.
FAU_STG.1	**X**		The IASM does not rely on the SLES FAU_STG.1 SFR. While the IASM ST implicitly includes the FAU_STG.1 SFR words by using FAU_STG.2, the sets of specific objects to which the SFRs apply and the SFR enforcement mechanisms, are entirely disjoint.
FAU_STG.2		**X**	
FAU_STG.3	**X**		The IASM does not rely on the SLES FAU_STG.3 SFR.
FAU_STG.4	**X**	**X**	The IASM does not rely on the SLES FAU_STG.4 SFR because it independently implements the capability for the objects to which the IASM ST instance of the SFR applies. The IASM TOE could be affected by the SLES instance of the SFR if IASM component actions cause the SLES TOE to invoke the function(s) implementing the SFR.
FCS_CKM.1	**X**		The IASM does not rely on the SLES FCS_CKM.1 SFR because it makes no specific claims about key generation.
FCS_CKM.2	**X**		The IASM does not rely on the SLES FCS_CKM.2 SFR because it makes no specific claims about key distribution.
FCS_COP.1	**X**		The IASM does not rely on the SLES FCS_COP.1 SFR because the IASM TOE implementation, itself, incorporates all cryptographic capabilities required for FTP_ITC.
FDP_ACC.1	**X**		The IASM does rely on the SLES FDP_ACC.1 and FDP_ACF.1 SFRs as an additional mechanism for enforcing the IASM FPT_SEP.1 SFR by providing selective separation between SLES processes in which IASM software subsystems are executing.
FDP_ACF.1	**X**		
FDP_RIP.2	**X**		The IASM does rely on the SLES FDP_RIP.2 SFR to provide necessary support for the SLES FPT_SEP.1 SFR.
FDP_UCT.2	**X**		The IASM does not rely on the SLES FDP_UCT.2 and FDP_UIT.1 SFRs because the IASM ST doesn't explicitly include these SFRs and any such capabilities are internal to the IASM implementation.
FDP_UIT.1	**X**		
FIA_ATD.1	**X**	**X**	The IASM does not rely on the SLES FIA_ATD.1 SFR because the IASM uses an authentication mechanism and database other than the SLES one.
FIA_SOS.1	**X**		The IASM does not rely on the SLES FIA_SOS.1 SFR because the IASM uses a password verification mechanism other than the SLES one and requires password generation, which SLES doesn't.
FIA_SOS.2		**X**	
FIA_UAU.2	**X**		The IASM does not rely on the SLES FIA_UAU.2, FIA_UAU.7 FIA_UID.2, and FIA_USB.1 SFRs because it includes an independent IASM user I&A implementation with its own user security information model.
FIA_UAU.7	**X**		
FIA_UID.2	**X**		
FIA_USB.1	**X**		

FMT_MSA.1	X		The IASM does rely on the SLES FDP_ MSA.1 SFR to provide necessary support for the IASM FPT_SEP.1 SFR.
FMT_MSA.2	X		The IASM does not rely on the SLES FMT_MSA.2 SFR.
FMT_MSA.3	X		The IASM does rely on the SLES FDP_MSA.3 SFR to provide necessary support for the IASM FPT_SEP.1 SFR.
FMT_MTD.1	X	X	The IASM does not rely on the SLES FMT_MTD.1 SFR because the specific refinements in each ST refer to different objects and events.
FMT_REV.1	X		The IASM does not rely on the SLES FMT_REV.1 SFR.
FMT_SMF.1	X	X	The IASM does not rely on the SLES FMT_SMF.1 SFR because the specified information and functions are different.
FMT_SMR.1	X	X	The IASM does not rely on the SLES FMT_SMR.1 SFR because the specified roles are interpreted in different contexts.
FPT_AMT.1	X		The IASM does rely on the SLES FDP_AMT.1 SFR to provide necessary support for the IASM FPT_RVM.1 SFR.
FPT_RVM.1	X	X	The IASM does rely on the SLES FPT_RVM.1 SFR as described in section 6.2.2.
FPT_SEP.1	X	X	The IASM does rely on the SLES FPT_SEP.1 SFR as described in section 6.2.3.
FPT_STM.1	X	X	The IASM does rely on the SLES FPT_STM.1 SFR as described in section 6.2.4.
FTP_ITC.1	X	X	The IASM does not rely on the SLES FTP_ITC.1 SFR because it uses an independent implementation of the same mechanism.

11.1.4 IASM TOE Use of SuSE LINUX 9.1 Evaluated Interfaces

As described in detail in the IASM High-Level Design document, the primary SLES interfaces used by the IASM TOE are the ones for process management and network communications. As explained in the Table 11-1 entry for FTP_ITC.1, the IASM TOE doesn't use the SLES implementation of SSLv3 and therefore only uses the basic SLES network socket interfaces, rather than the secure socket interfaces.

11.1.5 IASM TOE Use of Evaluated Version of SuSE LINUX 9.1

One of the hardware platforms identified in the [EAL4-SLES-ST] is the IBM eServer model 325, which is a single-CPU system based on the AMD Opteron processor. As described in section 2.1.1, each hardware component of the IASM Appliance uses a Tyan dual-CPU Opteron-based system. While not exactly the same as the hardware specified in [EAL4-SLES-ST], the IASM hardware does comply with the requirements stated for the hardware environment section in

[EAL4-SLES-ST] section 5.3. As also described in section 2.1.1, the IASM SLES 9.1 baseline uses a subset of the evaluated SLES 9.1 packages in order to provide an even more restricted operational environment. The specific packages included in the IASM baseline are specified in the IASM CM Configuration List.

11.1.6 Approach to Ensuring that IASM TOE Tests Confirm Correct Use of SuSE LINUX 9.1 Interfaces

It is ultimately the responsibility of the CCTL to satisfy this clause of PD-0117 based on the description of how the IASM TOE leverages the SLES 9.1 SFR (as provided in Table 11-1 above) and the mapping of the IASM SFRs that leverage SLES 9.1 SFRs onto IASM Security Functional Tests.

11.1.7 IASM TOE Guidance for Proper Configuration of SuSE LINUX 9.1 to Support IASM TOE Security Requirements and Functions

The IASM TOE uses the SLES 9.1 OS as a statically configured, integrated element of the IASM Appliance components. As such, the description of how SLES 9.1 is configured for the IASM Appliance is contained in the section of the IASM CM documentation that describes the IASM TOE build process.

11.1.8 IASM TOE ST Must Identify the Applicable SuSE LINUX 9.1 ST

[EAL4-SLES-ST]	*SUSE Linux Enterprise Server v9 Security Target for CAPP Compliance, Version 3.10*, IBM Corp and atsec GmbH, 17 January 2005

11.2 Rationale for the Use of Windows XP Professional in the IASM TOE

11.2.1 Required PEP Assurance Level

Windows XP Professional was evaluated at EAL4, augmented with ALC_FLR.3. The IASM TOE ST claims EAL3+: specifically, augmentation with ALC_FLR.2 and ALC_LCD.1. The EAL4 augmented level of Windows XP Professional is greater than the EAL3 augmented level claimed for the IASM TOE. Likewise, the ALC_FLR.3 SAR that augments Windows XP Professional is hierarchical to ALC_FLR.2 SAR that augments the IASM TOE, thus meeting this constraint.

11.2.2 IASM TOE Leverage of Windows XP Professional SFRs

11.2.3 Windows XP Professional SFRs Must Not Conflict with IASM TOE SFRs

Windows XP Professional is the operating system used on the IASM TOE User Console. Table 11-2, below, explains both how the IASM TOE leverages certain Security Function Requirements (SFRs) (highlighted in gray in the table) from the Windows XP Professional Security Target [EAL4-WXP-ST] and why the SFRs that are not leveraged by the IASM TOE do not conflict or interfere with the ability of the IASM TOE to meet its own SFRs.

Table 11-2 – IASM Use of Windows XP Professional (WXP) Security Features

SFR name	WinXP	IASM	Relationship of WinXP SFR to IASM SFR(s)
FAU_GEN.1	X	X	The IASM does not rely on the WXP FAU_GEN.1 SFR. While both STs include this requirement, the sets of specific objects and events to which the requirement applies are entirely disjoint.
FAU_GEN.2	X		The IASM does not rely on the WXP FAU_GEN.2 SFR. In addition to the IASM ST not including the SFR, the IASM maintains its own user identity database and would therefore not be able to use the WXP information.
FAU_SAR.1	X	X	The IASM does not rely on the WXP FAU_SAR.* SFRs. While both STs include these requirements, the sets of specific objects to which the SFRs apply, and the SFR enforcement mechanisms, are entirely disjoint.
FAU_SAR.2	X	X	
FAU_SAR.3	X	X	
FAU_STG.1	X		The IASM does not rely on the WXP FAU_STG.1 SFR. While the IASM ST implicitly includes the FAU_STG.1 SFR words by using FAU_STG.2, the sets of specific objects to which the SFRs apply and the SFR enforcement mechanisms, are entirely disjoint.
FAU_STG.2		X	
FAU_STG.3	X		The IASM does not rely on the WXP FAU_STG.3 SFR, mainly because it does not include an equivalent claim.
FAU_STG.4	X	X	The IASM does not rely on the WXP FAU_STG.4 SFR because it independently implements the capability for the objects to which the

			IASM ST instance of the SFR applies. The IASM TOE could be affected by the WXP instance of the SFR if user actions cause the WXP TOE to invoke the function(s) that implement the SFR.
FCS_COP.1	X		The IASM does not rely on the WXP FCS_COP.1 SFR because the IASM TOE implementation, itself, incorporates all cryptographic capabilities required for FTP_ITC.
FCS_CKM.1	X		The IASM does not rely on the WXP FCS_CKM SFRs because key management is assumed as a largely manual activity within the IASM TOE envirionment.
FCS_CKM.2	X		
FCS_CKM.4	X		
FCS_CKM_EX.1	X		
FCS_CKM_EX.2	X		
FDP_ACC.2	X		The IASM does not rely on the WXP FDP_ACC.2 SFR.
FDP_ACF.1	X		The IASM does not rely on the WXP FDP_ACF.1 SFR.
FDP_IFC.1	X		The IASM does not rely on the WXP FDP_IFC.1, FDP_IFF.1, and FDP_ITT.1 SFRs because all potentially relevant communications are not with another WXP TOE.
FDP_IFF.1	X		
FDP_ITT.1	X		
FDP_RIP.2	X		The IASM does rely on the WXP FDP_RIP.2 and FDP_RIP.2 (Notel_EX) SFRs as supporting aspects of meeting the WXP FPT_SEP.1 SFR on which the IASM relies.
FDP_RIP.2 (Notel_EX)	X		
FDP_UCT.1	X		The IASM does not rely on the WXP FDP_UCT.1 and FDP_UIT.1 SFRs because they only apply to Web User objects, which is too limited for the IASM purposes.
FDP_UIT.1	X		
FIA_AFL.1	X	X	The IASM does not rely on the WXP FIA_AFL.1 SFR because the IASM uses an authentication mechanism other than the WXP one.
FIA_ATD.1	X	X	The IASM does not rely on the WXP FIA_ATD.1 SFR because the IASM uses an authentication mechanism and database other than the WXP one.
FIA_SOS.1	X		The IASM does not rely on the WXP FIA_SOS.1 SFR because the IASM uses a password verification mechanism other than the WXP one and requires password generation, which WXP doesn't.
FIA_SOS.2		X	
FIA_UAU.1	X		The IASM does rely on the WXP FIA_UAU.1, FIA_UAU.6, FIA_UAU.7, and FIA_UID.1 SFRs as a secondary basis for meeting the IASM ST FPT_RVM SFR: as described in section 6.2.2.
FIA_UAU.6	X		
FIA_UAU.7	X		

FIA_UID.1	X		
FIA_USB.1_EX	X		The IASM does not rely on the WXP FIA_ USB.1_EX SFR because the IASM uses an identification mechanism and database other than the WXP one.
FMT_MOF.1	X	X	The IASM does not rely on the WXP FMT_MOF.1 SFR because the specific refinements in each ST refer to different objects and events.
FMT_MSA.1	X		The IASM does not rely on the WXP FMT_MSA.1 SFR because each ST refers to different objects and security attributes.
FMT_MSA_EX.2	X		The IASM does not rely on the WXP FMT_MSA_EX.2 SFR because the IASM uses an authentication mechanism other than the WXP one.
FMT_MSA.3	X		The IASM does not rely on the WXP FMT_MSA.3 SFR.
FMT_MTD.1	X	X	The IASM does not rely on the WXP FMT_MTD.1 SFR because the specific refinements in each ST refer to different objects and events.
FMT_MTD.2	X		The IASM does rely on the WXP FMT_MTD.2 SFR as a secondary basis for meeting the IASM ST FPT_RVM SFR: as described in section 6.2.2. As delivered, the IASM uses the default evaluated settings for OS login at the User Console, but those settings can be changed to suit site policy.
FMT_REV.1	X		The IASM does not rely on the WXP FMT_REV.1 SFR.
FMT_SAE.1	X		The IASM does not rely on the WXP FMT_SAE.1 SFR.
FMT_SMF.1	X		The IASM does not rely on the WXP FMT_SMR.1 SFR because each ST refers to different security functions.
FMT_SMR.1	X	X	The IASM does not rely on the WXP FMT_SMR.1 and FMT_SMR.3 SFRs because the specific refinements in each ST refer to different objects and events.
FMT_SMR.3	X		
TRANSFER_PROT_EX.1	X		The IASM does not rely on the TRANSFER_PROT_EX.1, TRANSFER_PROT_EX.3, FPT_RPL_EX.1 and FPT_TRC_EX.1 SFRs because all potentially relevant communications are not with another WXP TOE.
TRANSFER_PROT_EX.3	X		
FPT_RPL_EX.1	X		
FPT_TRC_EX.1	X		
FPT_RVM.1	X	X	The IASM does rely on the WXP FPT_RVM.1 SFR as described in section 6.2.2.
FPT_SEP.1	X	X	The IASM does rely on the WXP FPT_SEP.1 SFR as described in section 6.2.3.

FPT_STM.1	X	X	The IASM does rely on the WXP FPT_STM.1 SFR as described in section 6.2.4.
FRU_RSA.1	X		The IASM does not rely on the WXP FRU_RSA.1 SFR.
FTA_LSA_EX.1	X		The IASM does not rely on the WXP FTA_LSA_EX.1 and FTA_MCS_EX.1 SFRs because the IASM TOE does not make use of WXP domains.
FTA_MCS_EX.1	X		
FTA_SSL.1	X		The IASM does not rely on the WXP FTA_SSL.1 and FTA_SSL.2 SFRs to meet any of its own SFRs; however, a specific site could use the WXP capabilities to support IASM TOE Environment Objectives.
FTA_SSL.2	X		
FTA_TAB.1	X		The IASM does not rely on the WXP FTA_TAB.1 SFR.
FTA_TSE.1	X		The IASM does not rely on the WXP FTA_TSE.1 SFR.
FTP_TRP.1	X		The IASM does rely on the WXP FTP_TRP.1 SFR as an implicit part of the argument that the WXP FPT_RVM.1 and FPT_SEP.1 SFRs support the IASM FPT_RVM.1 and FPT_SEP.1 SFRs.

11.2.4 IASM TOE Use of Windows XP Professional Evaluated Interfaces

As described in detail in the IASM High-Level Design document, the primary Windows XP Professional interfaces used by the IASM TOE are the ones for process and window management and network communications.

11.2.5 IASM TOE Use of Evaluated Version of Windows XP Professional

The Dell PowerEdge 1750 server used in the IASM TOE is a predecessor product to the Dell Optiplex GX270, which is one of the hardware platforms identified in the [EAL4-WXP-ST]. The Windows XP Professional OS is statically configured in exactly the configuration specified in [EAL4-WXP-ST].

11.2.6 Approach to Ensuring that IASM TOE Tests Confirm Correct Use of Windows XP Professional Interfaces

It is ultimately the responsibility of the CCTL to satisfy this clause of PD-0117 based on the description of how the IASM TOE leverages the Windows XP Professional SFR (as provided in Table 11-2 above) and the mapping of the IASM SFRs that leverage Windows XP Professional SFRs onto IASM Security Functional Tests.

11.2.7 IASM TOE Guidance for Proper Configuration of Windows XP Professional to Support IASM TOE Security Requirements and Functions

The IASM TOE uses the Windows XP Professional OS as a statically configured, integrated element of the IASM User Console component that is configured exactly as described in the

CCEVS Validation Report and [EAL4-WXP-ST] and then patched as described in the IASM VLA document.

11.2.8 IASM TOE ST Must Identify the Applicable Windows XP Professional ST

[EAL4-WXP-ST]	*Windows XP Professional Security Target, Version 2.0,* Microsoft Corp, 18 October 2002