Using IASM To Support Sarbanes-Oxley Compliance

Introduction

The Sarbanes-Oxley Act of 2002 (SOX) was signed into law in July 2002, in part as a reaction to the widely reported Worldcom and Enron scandals – which were caused by failures of the internal financial controls at those companies – and applies to all publicly held companies in the US. The main effect of SOX is to require affected companies to provide compelling evidence for the existence, operation, and effectiveness of the internal financial controls to which corporate officers and independent auditors must attest. In most companies, substantial portions of the financial controls are implemented using Information Technology (IT). This document describes how the Promia Intelligent Agent Security Manager (IASM) can be used to collect and analyze audit data from IT-based internal financial controls and produce reports documenting the continuous operation and effectiveness of those controls.

Overview of Sarbanes-Oxley

The Sarbanes-Oxley Act of 2002 – i.e., U.S. Public Law 107-204 – is often abbreviated as either "SOX" or "SarbOx". It is designed to hold corporate officers (specifically the CEO and CFO) of publicly held companies fully accountable for the correctness and accuracy of the yearly financial reports submitted to the SEC. The law introduces specific obligations on both the corporate officers of a company and on the independent auditors of that company's financial reports.

This document is primarily concerned with the obligations imposed on corporate officers, which include:

- Preparing, reviewing, and signing a periodic financial report to the SEC that does not contain any materially untrue statements or material omissions that could be considered misleading; *[§302, §401]*
- Fairly and materially presenting the financial condition and the internal audit results within the financial statements and related information contained in the report; *[§302]*
- Establishing internal financial controls, then evaluating and documenting the scope, adequacy, and effectiveness of those internal controls within the ninety days prior to publication of the report; *[§302, §404]*
- Listing all identified deficiencies in the internal controls and information on any fraud that involves employees who are involved with internal activities in the report; *[§302]*
- Identifying any significant changes in internal controls or related factors that could have a negative impact on the internal controls in the report; *[§302]*
- Immediately reporting any information on material changes in their financial condition or operations; *[§409]*
- Make no attempt to alter, destroy, mutilate, conceal, or falsify records, documents or tangible objects with the intent to obstruct, impede or influence a legal investigation or face fines and/or up to 20 years in prison; *[§802]*
- Make no attempt to avoid these requirements by reincorporating their activities or transferring their activities outside of the United States; *[§302]*

The remainder of this document explains how the IASM can be used as part of the IT-based internal controls to which the CEO and CFO must attest under SOX.

Using IASM To Support Sarbanes-Oxley Compliance

Overview of IASM

The Intelligent Agent Security Manager (IASM) is a high-speed, security-hardened appliance that collects, consolidates, and analyzes log data from network and security devices, as well as operating systems and applications, to detect and manage operational and security incidents. It is designed to also pull data from vulnerability management systems as well as databases and syslog servers. As well, it is capable of rapidly reconfiguring itself to receive and process data from new devices, systems, and applications. Log records are first analyzed, pre-filtered, and normalized by intelligent agent for each sensor on the monitored network. The records are then sent to the IASM appliance where the data is then correlated and analyzed further by one or more analytic engines to determine cyber attack profiles in real time.

The IASM includes the Asset Viewer (AV) graphical user interface, which uses flexible and powerful 3-dimensional, user-definable, graphical components to provide a consolidated visualization of all assets on the monitored network. This visualization includes versions and patch levels of node operating systems, device and application status, ports in use, and other related information. The visualization also allows an operator to navigate between subnets of the monitored network, thus exposing the contextual relationship between those subnets. It also displays both operational and security incidents detected by the IASM appliance in a rapidly comprehensible view suitable to the needs of enterprise network operations center personnel. These visualization models have been operationally validated in a globally distributed enterprise. The visual elements can also be annotated with English descriptions to help operations personnel interpret their networks' electronic terrain.

Also included in the IASM family of products is the Network Security Event Sensor (NSES) appliance, which functions as both an integral component of the IASM asset management capabilities and as a stand-alone intrusion and asset detection appliance. The NSES appliance provides: asset identification and mapping, passive asset fingerprinting, IP traffic anomaly detection (which is able to detect Zero-day network attacks), and attack signature sensing based on the Snort engine. The NSES also includes a collection of analytic services including false positive reduction, message aggregation, and IP address white- and black-listing. It also incorporates a "fishbowl" capability that records 1-60 second "snapshots" of IP traffic both before and after a security event for later review by remote analysts. This feature allows rapid propagation of summary event records while retaining contextual traffic information at the sensor level in case forensic review by highly skilled incident analysis personnel is later required.

Figure 1, below, shows the operational concept for how the IASM, NSES, and Asset Viewer fit together with a monitored network.

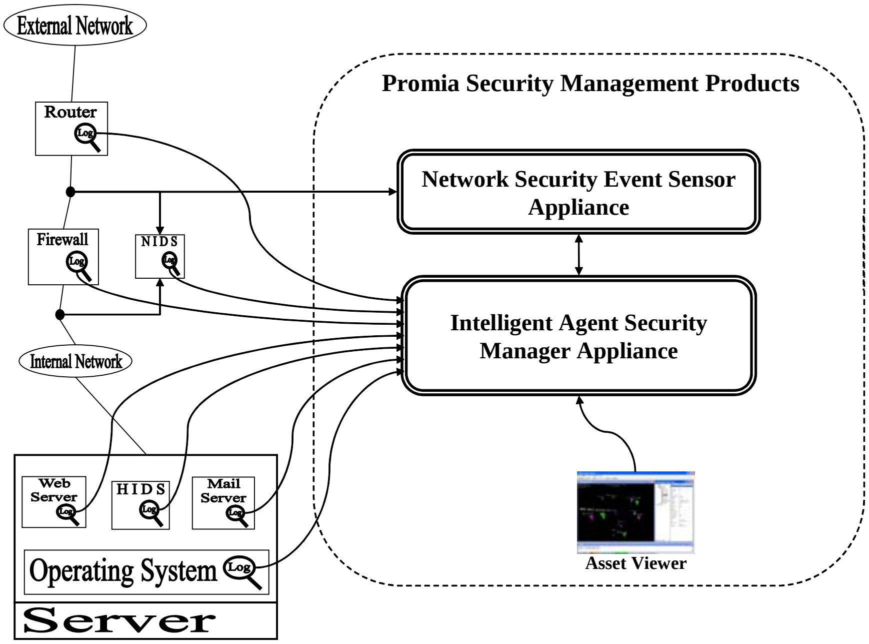

Figure 1 – Promia Security Management Products Operational Concept

In summary, the IASM family of products provides the following set of functions for possible use as part of the IT controls needed to comply with Sarbanes-Oxley requirements:

- Automatic detection (by the NSES) and visualization (by the AV) of hardware, operating system, and software application assets on the monitored network;
- Network intrusion detection sensors (on the NSES) that use both signature- and anomaly-based algorithms to detect known and previously unseen network intrusion attempts;
- Collection and consolidation of operational and security events – from both the NSES and third-party products – into a unified, high-integrity, security information management (SIM) repository where they are later available for a SOX compliance audit;
- Real-time analysis of events – as they are collected from sensors on the monitored network – by one or more analytic engines to monitor and detect security, operations, and SOX non-compliance incidents as they occur;
- Real-time visualization of emerging incidents, backed up by the ability to drill down through the security, operations, and SOX non-compliance incidents into the events that indicate and support the incident;
- Tools for managing the lifecycle of detected security, operations, and SOX non-compliance incidents: including remediation actions taken to correct detected problems;
- Tools for defining and generating summary and detail reports about security, operations, and SOX non-compliance incidents and actions taken to address the incidents, which can be used for continuous SOX compliance monitoring, as well as compliance audits;

Using IASM To Support Sarbanes-Oxley Compliance

Using IASM to Implement Sarbanes-Oxley Technical Controls

Most Sarbanes-Oxley regulations and guidance documents cite the *Control Objectives for Information and related Technology* (COBIT®) – produced by the IT Governance Institute and currently at release 4.0 – as the most appropriate foundation on which to build a Sarbanes-Oxley IT compliance strategy. COBIT 4.0 identifies 34 IT processes that encompass 247 detailed control objectives – all oriented towards integrating IT into a comprehensive system of internal controls. The table below identifies the each of detailed control objectives for which the IASM could be a useful implementation or support tool and describes how the IASM could provide support.

CNTL ID.	CONTROL OBJECTIVE NAME	IASM Support for the Control Objective
	Plan and Organize	
PO1	**Define a Strategic IT Plan**	
PO1.3	Assessment of Current Performance	The IASM can support this detailed objective by both identifying existing IT resources and providing summary reports about the usage and users of those resources based on network traffic indicators.
PO2	**Define the Information Architecture**	
PO2.1	Enterprise Information Architecture Model	When SOX compliance is a business concern, log records that are analyzed to verify compliance and detect non-compliance must be included in the EIAM. The IASM repository design embodies a Data Dictionary, Syntax Rules, and Classification schemes for log records and audit incidents detected in log records. The Repository implementation enforces defined confidentiality, integrity, and availability policies over the log and audit incident data.
PO2.2	Enterprise Data Dictionary & Data Syntax Rules	
PO2.3	Data Classification Scheme	
PO2.4	Integrity Management	
PO3	**Determine Technological Direction**	
PO3.1	Technological Direction Planning	The IASM is an existing technology that should be considered as a tool to meet SOX compliance and security management requirements.
PO3.3	Monitoring of Future Trends & Regulations	Promia actively monitors and alerts customers to threat and technology trends, as well as emerging regulatory compliance issues, thus helping organizations with this control objective.
PO3.4	Technology Standards	Promia personnel are active and respected participants in the regulatory compliance, software assurance, and security technologies communities at the Object Management Group and the company is committed to implementing applicable specifications that come out of those communities. Working through these OMG communities allows an organization to both meet these control objectives and influence the IASM.
PO3.5	IT Architecture Board	
PO4	**Define the IT Processes, Organization and Relationships**	
PO4.6	Roles and Responsibilities	Use of the IASM in an organization may affect the specific roles and duties identified with an organization.
PO4.8	Responsibility for Risk, Security & Compliance	
PO4.9	Data and System Ownership	The IASM is one of the tools available for managing Data and System Ownership issues.
PO4.11	Segregation of Duties	The IASM enforces low-level, appropriately segregated, roles. It also provides mechanisms by which the use and segregation policies of higher-level roles can be effectively monitored in near-real-time.
PO4.12	IT Staffing	The use of the IASM can have an impact of the number of staff required for regulatory compliance and security auditing

CNTL ID.	CONTROL OBJECTIVE NAME	IASM Support for the Control Objective
PO4.13	Key IT Personnel	and the definition of key personnel in those areas.
PO6	**Communicate Management Aims and Direction**	
PO6.2	Enterprise IT Risk & Internal Control Framework	The IASM may be used as a crucial component of the internal control framework, especially as it relates to the "timely identification of irregularities, limitation of losses, and timely recovery of business assets."
PO9	**Assess and Manage IT Risks**	
PO9.3	Event Identification	As part of its incident response features, the IASM provides a database that includes fields for describing "a potential impact on the goals or operations of the enterprise, including business, regulatory, legal, technology, trading partner, human resources and operational aspects." This database would be an effective repository for information collected to meet this control objective.
PO9.4	Risk Assessment	The IASM asset detection features can be used as part of the Risk Assessment process.
PO9.5	Risk Response	Other fields in the IASM incident response database capture both summary and detailed descriptions of how to respond to incidents, which are displayed when an IASM incident issue is selected in the IASM Operator interface.
PO9.6	Maintenance & Monitoring of a Risk Action Plan	The IASM features will influence and support the Risk Action Plan.
Acquire and Implement		
AI1	**Identify Automated Solutions**	
AI1.2	Risk Analysis Report	For organizations that choose to consider current assets and threat activity during the Risk Analysis, the IASM asset and incident detection features can be used as input to the analysis.
AI2	**Acquire and Maintain Application Software**	
AI2.1	High-level Design	As part of the NIAP common Criteria evaluation, Promia prepared documents detailing the IASM High-level and detailed designs. Under appropriate NDA's, this information could be shared with IASM customers.
AI2.2	Detailed Design	
AI2.3	Application Control and Auditability	As a result of designing the IASM repository, Promia has processes and technology that IASM customers can leverage to meet this control objective.
AI3	**Acquire & Maintain Technology Infrastructure**	
AI3.2	Infrastructure Resource Protection and Availability	The IASM is designed to be an integral and effective component of Infrastructure Resource Protection and Availability.
AI3.3	Infrastructure Maintenance	The IASM provides several tools for monitoring risks and vulnerabilities in an existing infrastructure.
AI4	**Enable Operation and Use**	
AI4.4	Knowledge Transfer to Operations and Support Staff	Promia provides initial and ongoing IASM training and operations documentation that can be used to implement this control objective.
AI7	**Install and Accredit Solutions and Changes**	
AI7.1	Training	Promia provides initial and ongoing IASM training and operations documentation that can be used to implement this control objective.

CNTL ID.	CONTROL OBJECTIVE NAME	IASM Support for the Control Objective
AI7.2	Test Plan	Promia has experience with successfully developing and executing functional- and security- testing programs for the IASM under both the lab-oriented NIAP (Common Criteria) and the operational system oriented US DoD DITSCAP processes.
AI7.4	Test Environment	
AI7.6	Testing of Changes	
AI7.7	Final Acceptance Test	
AI7.12	Post-implementation Review	The IASM can be used to provide continuous monitoring, analysis, and reporting of any aspects of the operational system for which relevant logs are produced.
Deliver and Support		
DS1	**Define and Manage Service Levels**	
DS1.5	Monitoring and Reporting of Service Level Achievements	The IASM can be used to provide continuous monitoring, analysis, and reporting of any aspects of the operational system for which relevant logs are produced – including service level achievement.
DS2	**Manage Third-party Services**	
DS2.3	Supplier Risk Management	Promia has a strong history of successfully meeting security compliance standards (i.e., DITSCAP and NIAP) and is committed to doing the same for any other regulatory compliance standards that are important to customers.
DS3	**Manage Performance and Capacity**	
DS3.2	Current Capacity and Performance	The IASM asset management and event log collection, analysis, and reporting capabilities can be effectively used to continuously monitor and assess the sufficiency of IT resources' performance and capacity.
DS3.5	Monitoring and Reporting	
DS4	**Ensure Continuous Service**	
DS4.1	IT Continuity Framework	The IASM asset management features provide a potentially useful tool for "monitoring and reporting on the availability of critical resources".
DS5	**Ensure Systems Security**	
DS5.5	Security Testing, Surveillance and Monitoring	The IASM is designed, implemented, and tested to meet rigorous standards of security hardening. Its primary function is to provide a "logging and monitoring function *that* enables the early detection of unusual or abnormal activities that may need to be addressed" with built-in access control capabilities.
DS5.6	Security Incident Definition	The IASM incident response database provides a tool in which to capture and enforce the information developed out of this control objective.
DS5.7	Protection of Security Technology	The IASM is designed, implemented, and tested to meet rigorous standards of security hardening.
DS5.10	Network Security	The IASM is designed to be an integral component of a network security infrastructure – with a focus on detecting complex intrusion attempts.
DS8	**Manage Service Desk and Incidents**	
DS8.2	Registration of Customer Queries	For customer service incidents that (potentially) involve the network – and especially security incidents on the network – the IASM provides asset monitoring and incident management tools that inform and integrate with the global service desk capabilities.
DS8.3	Incident Escalation	
DS8.4	Incident Closure	

Using IASM To Support Sarbanes-Oxley Compliance

CNTL ID.	CONTROL OBJECTIVE NAME	IASM Support for the Control Objective
DS9	**Manage the Configuration**	
DS9.3	Configuration Integrity Review	The IASM asset detection capabilities can be used to check the “as deployed” configuration of any IT components that are visible through a network interface.
DS10	**Manage Problems**	
DS10.1	Identification and Classification of Problems	Combining the Incident and Asset management features of the IASM provides an effective platform for managing many operational problems in the network infrastructure.
DS10.2	Problem Tracking and Resolution	
DS10.3	Problem Closure	
DS11	**Manage Data**	
DS11.6	Security Requirements for Data Management	When the Data Management requirements include the log and audit any or all of “the receipt, processing, physical storage and output of data and sensitive messages”, the IASM provides an effective tool for doing so.
DS13	**Manage Operations**	
DS13.3	IT Infrastructure Monitoring	Its design and operational evolution has resulted in the IASM providing a comprehensive set of features oriented towards implementing this control objective.
Monitor and Evaluate		
ME1	**Monitor and Evaluate IT Performance**	
ME1.1	Monitoring Approach	For any aspects of the monitoring approach and design that rely on electronic logs, the IASM provides a collection, consolidation, analysis, and reporting capability that can provide input to the comprehensive system
ME1.2	Definition and Collection of Monitoring Data	
ME1.3	Monitoring Method	
ME2	**Monitor and Evaluate Internal Control**	
ME2.1	Monitoring of Internal Control Framework	When information that is relevant to monitoring and evaluating the internal controls is derived from IT system logs, the IASM can be used to collect, consolidate, help analyze, and present that information for human review and action.
ME2.2	Supervisory Review	
ME2.5	Assurance of Internal Control	
ME2.6	Internal Control at Third Parties	
ME3	**Ensure Regulatory Compliance**	
ME3.2	Optimization of Response to Regulatory Requirements	When information that is relevant to monitoring and assuring regulatory compliance is derived from IT system logs, the IASM can be used to collect, consolidate, help analyze, and present that information for human review and action.
ME3.3	Evaluation of Compliance With Regulatory Requirements	
ME3.4	Positive Assurance of Compliance	
ME3.5	Integrated Reporting	Regulatory Compliance reports based on information maintained by the IASM can be developed and scheduled to be produced at the same time as other IASM reports.