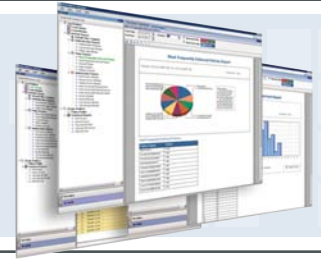


Identisphere™ ID-Audit™ and Meeting FISMA Compliance



The Federal Information Security Management Act of 2002 (FISMA) is a federal law enacted in 2002. The Act has brought information security to the attention of the Federal Government and has increased awareness regarding the protection of information and securing the networks in which it resides. FISMA imposes a mandatory set of processes that must be followed for all information systems used or operated by a US Government federal agency or by a contractor or other organization on behalf of a US Government agency. These processes must follow a combination of Federal Information Processing standards (FIPS) documents, the special publications SP-800 series issued by NIST, and other legislation pertinent to federal information systems.

Applied Identity's Solutions in Relation to NIST 800-53A

Federal agencies must meet the minimum security requirements defined in FIPS 200 through the use of the security controls in NIST Special Publication 800-53 revision 1, which contains the management, operational, and technical safeguards or countermeasures prescribed for an information system. NIST SP 800-53A – the latest iteration of the publication - provides guidance on the assessment methods, policies, procedures and continuous monitoring where applicable to individual controls.

Identity-Driven Access Management

Applied Identity is a leading provider of enterprise-class, identity aware network solutions that allows organizations to:

- Audit user access and resource usage based on user identity
- Unify multiple disparate identity stores to create a single authoritative source
- Define new or redefine existing access policies based on user identity rather than IP address
- Enforce user access policies at the network layer
- Leverage existing identity stores such as Microsoft Active Directory, SUNOne, Novell eDirectory, and other LDAP and non-LDAP compliant identity repositories

Applied Identity is the only vendor to provide a complete policy lifecycle management solution that enables global policy creation and network-level enforcement based on user identity.

ID-Audit

Applied Identity's ID-Audit solution consolidates and makes sense of all the information generated by the ID-Enforce Gateways deployed within the network. ID-Audit uses the audit data to model a user or groups behavior & resource usage, which in turn is used to help define access policy, as well as redefining existing policy implied by IP-based security controls already embedded within the network. This approach provides a much more manageable and granular centralized policy for network level enforcement than traditional IP-based security controls such as firewalls, VLAN's and ACL's.

ID-Audit can create real-time views of user access to critical resources, as well as historical reports that can be filtered to provide succinct detail for policy creation and both internal and external audit requirements.

Mapping the ID-Audit Feature Set to NIST 800-53A

The feature set of Applied Identity's ID-Audit solution has been mapped to the following controls and control enhancements within the Access Control (AC) section of the NIST SP 800-53A

publication. Additional NIST SP 800-53A mappings for the Access Control (AC) section are addressed by Applied Identity's ID-Enforce solution in a separate document.

Note: The 20 Controls outlined in the Audit and Accounting section (AU-1 through AU-11) have additional control enhancements that provide greater clarification and functionality requirements and are listed below in the following format AU-3(1).1, AU-4(1).1, AU-4(2).1. etc.

Controls and Control Enhancements in the following sections have been omitted as they are either a) written policy or internal procedures b) Non-applicable functionality c) Non supported functionality; AU-1 and AU-6

800-53A CNTL NO.	800-53A CONTROL NAME	Applied Identity Support	Applied Identity Function
AU-1	Audit and Accountability Policy and Procedures		
AU-1	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.	NA	This is a manpower-driven internal policy and procedures exercise.
AU-2	Auditable Events		
AU-2	The information system generates audit records for the following events: [Assignment: organization-defined auditable events].	Supported	ID-Audit has the ability to consolidate predefined system level and system wide audit events.
AU-2(1).1	The information system provides the capability to compile audit records from multiple components throughout the system into a system wide (logical or physical), time-correlated audit trail.	Supported	ID-Audit compiles audit log information from multiple ID-Enforce gateways to provide a centralized time-correlated audit trail
AU-2(2).1	The information system provides the capability to manage the selection of events to be audited by individual components of the system.	Supported	ID-Audit provides the ability to audit user authentication successes and failures, authorization successes and failures. The system provides the ability to filter these events out-of-the-box.
AU-2(3).1	The organization periodically reviews and updates the list of organization-defined auditable events.	Supported	ID-Audit provides the ability to generate metrics on the effectiveness of a given organizational policy. Reports generated include "Most Frequently Enforced Policies", "Least Frequently Enforced Policies" and "Unused Policies"
AU-3	Content of Audit Records		
AU-3	The information system produces audit records that contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.	Supported	ID-Audit logs events related to user authentication, authorization, bandwidth consumption and policy enforcement and which ID-Enforce gateway(s) these events originated from.
AU-3(1).1	The information system provides the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject.	Supported	ID-Audit events include information about user, source IP, destination IP, the originating ID-Enforce IP, authentication domain, service accessed, event outcome (success/failure), event severity and access policy violations.
AU-3(2).1	The information system provides the capability to centrally manage the content of audit records generated by individual components throughout the system.	Supported	ID-Audit provides a single, scalable repository to process and store audit logs received from multiple ID-Enforce devices.

800-53A CNTL NO.	800-53A CONTROL NAME	Applied Identity Support	Applied Identity Function
AU-4	Audit Storage Capacity		
AU-4	The organization allocates sufficient audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.	Supported; (archive feature supported in future release)	Applied Identity will provide general guidelines on the storage capacity needed based on the organization's requirements. ID-Audit will provide the ability to either purge historical data or archive off to long-term storage.
AU-5	Response and Audit Processing Failures		
AU-5	The information system alerts appropriate organizational officials in the event of an audit processing failure and takes the following additional actions: [Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)].	Supported; (Alert feature supported in future release)	The ability to generate real-time alerts based on audit event failures is on our product roadmap. ACTIONS: ID-Audit supports HA functionality so that in the event of failure of the primary ID-Audit server, the originator of the event can fall-over to the secondary ID-Audit server.
AU-5(1).1	The information system provides a warning when allocated audit record storage volume reaches [Assignment: organization-defined percentage of maximum audit record storage capacity].	Supported; (Alert feature supported in future release)	The ability to generate real-time alerts based on audit event failures is on our product roadmap. Currently, an error log is generated when system storage capacity is exceeded.
AU-5(2).1	The information system provides a real-time alert when the following audit failure events occur: [Assignment: organization-defined audit failure events requiring real-time alerts].	Indirect Support	The ability to generate real-time alerts based on audit event failures is on our product roadmap.
AU-6	Audit Monitoring, Audit, and Analysis		
AU-6	The organization regularly reviews/ analyzes information system audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.	NA	This is a manpower-driven internal policy and procedures exercise.
AU-6(1).1	The organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.	Supported	ID-Audit provides real-time and historical log analysis and report generation capabilities. ID-Audit reports on authorized and unauthorized user access to critical assets in the enterprise and provides mechanism to develop policies based on such accesses.
AU-6(2).1	The organization employs automated mechanisms to alert security personnel of the following inappropriate or unusual activities with security implications: [Assignment: organization-defined list of inappropriate or unusual activities that are to result in alerts].	Alert feature supported in future release)	The ability to generate real-time alerts based on auditable events is in our product roadmap.
AU-7	Audit Reduction and Report Generation		
AU-7	The information system provides an audit reduction and report generation capability.	Supported; (archive feature supported in future release)	ID-Audit will provide a GUI-based capability to either archive or purge log data at periodic intervals.
AU-7(1).1	The information system provides the capability to automatically process audit records for events of interest based upon selectable, event criteria.	Supported	ID-Audit provides simple and complex filters based on regular expressions for filtering auditable events.

800-53A CNTL NO.	800-53A CONTROL NAME	Applied Identity Support	Applied Identity Function
AU-8	Time Stamps		
AU-8	The information system provides time stamps for use in audit record generation.	Supported (timestamp feature supported in future release for ID-Audit & ID-Unify)	ID-Enforce generates log data with timestamps and ID-Audit has the ability to generate reports between any specified date and time. UTC and NTP is supported on the gateway and will be supported on ID-Unify and ID-Audit in future releases.
AU-8(1).1	The organization synchronizes internal information system clocks [Assignment: organization-defined frequency].	Supported	All auditable events are generated with UTC timestamps.
AU-9	Protection of Audit Data		
AU-9	The information system protects audit information and audit tools from unauthorized access, modification, and deletion.	Indirect (role-based access feature supported in future releases)	ID-Audit database and UI will be password protected to prevent unauthorized access. More granular role-based access controls to ID-Audit functionality, reporting and management will be supported in future releases.
AU-9(1).1	The information system produces audit records on hardware-enforced, write-once media.	Indirect Support	Audit records from ID-Enforce can be written to a SYSLOG residing on write once media dependent on hardware requirements.
AU-10	Non-Repudiation		
AC-10	The information system provides the capability to determine whether a given individual took a particular action.	Supported	ID-Mark provides the ability to tag IP packets from client to gateway for non-repudiation. ID-Audit provides reports on a user's access to a specific resource.
AU-11	Audit Record Retention		
AU-11	The organization retains audit records for [Assignment: organization-defined time period] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.	Indirect Support	ID-Audit will provide the capability to archive historical log data to long-term storage such as a NAS device.

