SailPoint

SOLUTION BRIEF

How to Effectively Meet Tax Information Security Guidelines

Securely managing access to applications, systems and data files is a growing challenge. The amount of data stored in file servers and NAS devices, collaboration portals, mailboxes and cloud folders has increased exponentially over the past few years. Yet, with no easy means to track, control and protect data files, governments and public agencies face growing security, legal and regulatory risks.

SailPoint and IRS Publication 1075

All agency information systems used for receiving, processing, storing or transmitting Federal Tax Information (FTI) must be hardened in accordance with the requirements in IRS Publication 1075, "Tax Information Security Guidelines for Federal, State and Local Agencies: Safeguards for Protecting Federal Tax Returns and Return Information."

It is the responsibility of each agency to build in effective security controls into its own IT infrastructure that ensure FTI is protected at all points where it is received, processed, stored and transmitted.

The computer security framework was primarily developed using guidelines specified in NIST SP 800-30 Revision 1, Guide for Conducting Risk Assessments, and NIST SP 800- 53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations.

SailPoint helps governments and public agencies meet IRS Publication 1075 requirements by securing sensitive data and mitigating risks for regulatory non-compliance. SailPoint's comprehensive identity governance solution enables organizations to securely deliver appropriate user access to systems, applications and data files wherever they reside.

Achieving IRS Publication 1075 Compliance with SailPoint

SailPoint's comprehensive solution provides automated controls that are vital to achieving and maintaining compliance with IRS Publication 1075.

- **Automated Access Certifications:** Streamlines periodic review and approval of all workers' physical and logical access across the organization
- **Real-Time Policy Monitoring:** Allows for continuous detection of separation of duty (SoD) and other access policy violations such as suitability
- **Automated Processes:** Centralizes and monitors all access requests and approvals across the organization
- **Dashboards:** Enables top-down visibility into compliance processes, such as access reviews status and results, policy violations and user risk scoring
- **Business and Technical Reports:** Documents critical cyber assets, users and their access privileges, access review status and results, access policy and violations
- **Integrated Risk Modeling and Management:** Identifies key risk user factors and monitors the effectiveness of controls in reducing risk

Major Components of SailPoint's Comprehensive Identity Governance Solution:

Streamline Processes
Centralize identity data, roles, business policy and risk modeling to support compliance initiatives and user lifecycle management.

Improve Regulatory Compliance
Streamline compliance controls and improve audit performance through automated access certifications and policy enforcement.

Drive Efficiency
Provide self-service access request and lifecycle event management to simplify the process of creating, changing and revoking user access privileges.

Optimize Access
Support flexible options for implementing changes requested by the business during compliance and lifecycle management processes.

Make Data-Driven Decisions
Highlight business-relevant information in easy-to-understand dashboards, reports and advanced analytics.

Gain Visibility
Allow organizations to find and classify sensitive information in order to apply effective controls for managing and protecting the information.

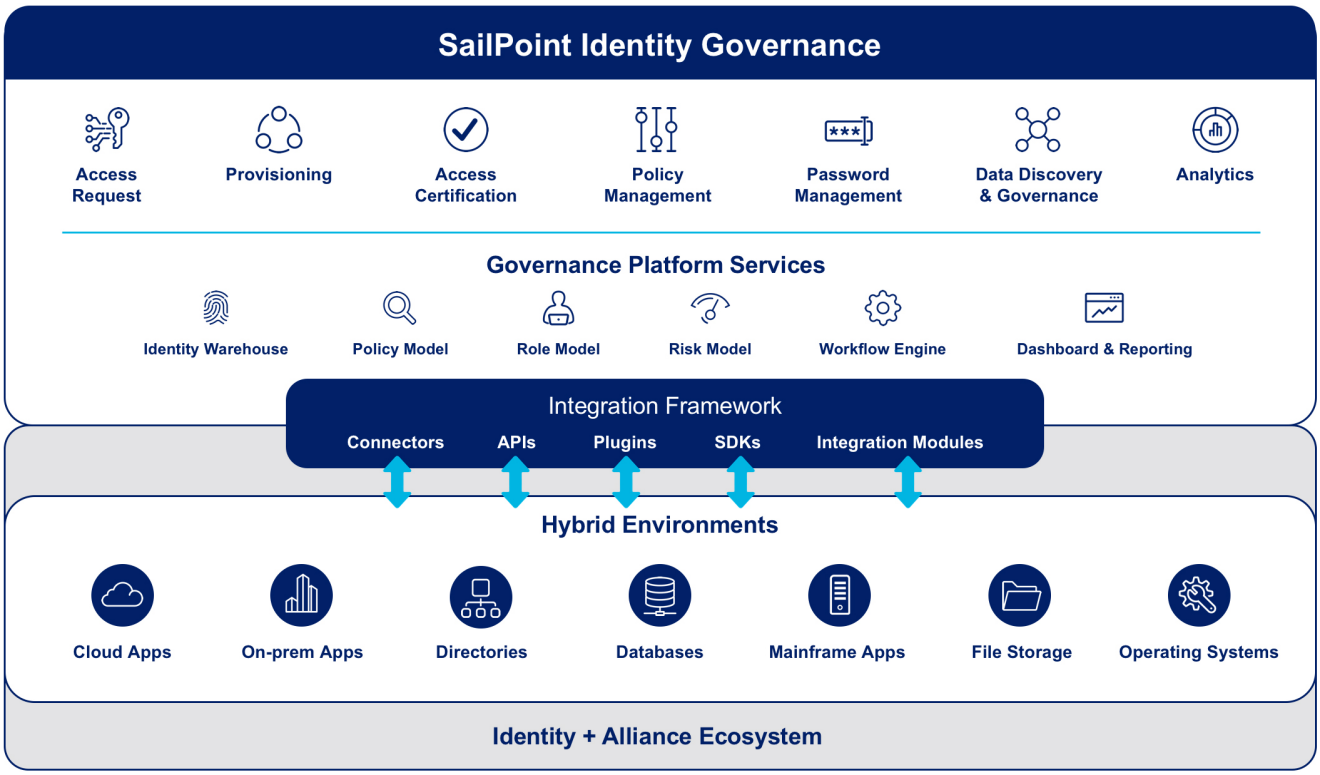
Manage Permissions
Automatically collect and analyze effective permissions across on-premises Windows file-servers, NAS devices, SharePoint and Exchange, as well as cloud-based portals including Office 365, Box, Dropbox, and Google Drive.

Track Data Activity
Allow organizations to find and classify sensitive information to apply effective controls for managing and protecting the information.

How Governments and Public Agencies Can Benefit from SailPoint

By augmenting identity data from structured systems with permission data from data file targets, your organization can more quickly identify risks, spot compliance issues and make the right decisions to strengthen controls. Specifically, SailPoint's solution benefits governments and public agencies in the following ways:

- Provides centralized visibility to wherever data resides in the enterprise – all applications, all data and all users
- Adds data file targets to preventive and detective controls, such as access certifications and SoD policy enforcement
- Automates provisioning of access to data repositories and revocation of inappropriate access
- Informs the identity management system with real-time activity data to improve risk mitigation and understand appropriate use



How SailPoint Specifically Addresses Key Requirements for the IRS Publication 1075 and NIST SP 800-53 Control Families

Control Family	Description	SailPoint Compliance
Access Control (AC) (AC-2), (AC-3), (AC-5), (AC-6), (AC-14), (AC-17), (AC-18), (AC-19), (AC-20), (AC-21), (AC-22)	Limit access to FTI to specific approved individuals, ensure remote access to systems is secured, and manage accounts so that unapproved individuals cannot gain unauthorized system access.	SailPoint provides out-of-the-box functionality to fully support the entire lifecycle management process, self-service access requests and workflows, the granting and assignment of group and role membership, and built-in business processes for creating, provisioning, updating and disabling system accounts. Any provisioning event, assignment, or access request is subject to evaluation. The role, policy and risk models enable an organization to enforce access control restrictions, separation of duties and enforce least privilege assignment of entitlements. The business-friendly interface enables users to conduct periodic reviews of accounts, applications and data, and notifies the appropriate personnel of need-to-know changes, terminated or transferred users.
Awareness & Training (AT) (AT-2), (AT-3), (AT-4)	Develop and provide security awareness training to all individuals accessing information systems and document all training activities.	The business-friendly interface facilitates periodic reviews of accounts, such as Learning Management Systems (LMS). Integration with LMS data allows agencies to ensure at a minimum that a user has completed the necessary training to be suitable for network or access to data.
Audit and Accountability (AU) (AU-1), (AU-2), (AU-3), (AU-4), (AU-5), (AU-6), (AU-7), (AU-8), (AU-9), (AU-11), (AU-12), (AU-16)	Develop and implement an audit and accountability policy to proactively detect and prevent unauthorized access to FTI, following specific federal guidelines.	SailPoint provides a business-friendly interface and out-of-the box reports and analytic tools to create, correlate, identify and report on identities, entitlements, system related events and activity. Each identity event is captured in the systems audit logs, identity snapshots and event history for each user. The solution also captures access, permissions, and the usage of data files by each unique user. Ad hoc and built-In reports can be generated and disseminated on scheduled basis to appropriate consumers.

Control Family	Description	SailPoint Compliance
Assessment and Authorization (CA)	Develop and implement a security assessment and authorization policy, identify an agency official to approve system access, and authorize connections to other information systems – regularly assess and continuously monitor security controls.	SailPoint has been certified and granted authority to operate in the most stringent financial, federal public sector, department of defense and intelligence communities.
Configuration Management (CM)	Configure IT products that receive, process, store and transmit FTI using Office of Safeguards–approved compliance requirements, documenting the baseline configuration, change control procedures and system inventory.	The solution can be implemented in highly secure manner to ensure secure data-at-rest and data-in-motion requirements as required and evaluated by National Information Assurance Program (NIAP) Common Criteria.
Contingency Plan (CP)	Develop and implement contingency planning controls to ensure FTI and user information is protected, stored, backed up and available in the event of a disaster.	SailPoint supports an agencies Disaster Recovery and High Availability requirements.
Identification and Authentication (IA) (IA-1), (IA-2), (IA-4), (IA-5), (IA-8)	Uniquely identify and authenticate each user and device, using multi-factor authentication for all remote network access and cryptographic modules.	SailPoint uniquely identifies each user and correlates all related enterprise accounts. A 360-degree view of an identities' attributes, roles, accounts, entitlements, risk, violations and history is maintained in the Identity Warehouse. Each application configured can have its own individually complex password policy. From a single interface, users can change one, several or all their accounts by either entering their own desired password or using a built-in password generation utility. SailPoint supports username and password, strong authentication (PKI) and multi-factor authentication (MFA), and can be integrated with web access management solutions and secure token services.

Control Family	Description	SailPoint Compliance
Incident Response (IR)	Monitor, handle and report all incidents affecting physical and information system security – provide response testing and training for all users.	SailPoint's solution integrates with security information and event management (SIEM) software products and services to provide identity context to events and activities for forensic analysis.
Maintenance (MA)	Develop and implement a system maintenance policy to ensure information systems stay in good working order.	SailPoint's object model can be integrated with developer tools to manage, deploy and maintain system artifacts across multiple environments to increase productivity and availability.
Media Protection Policy and Procedures (MP)	Physically control and securely store information system media, restricting use of media that receives, processes, stores or transmits FTI using physical and automated controls.	SailPoint's solution provides deep insight to permissions, ownership, data access and usage, and content (such as PII, classification markings, patterns, and strings) to ensure data files are secured against unauthorized use. Remediation policies can be activated to enforce least-privilege access to data files wherever they reside.
Physical and Environmental Protection (PE) (PE-2), (PE-3), (PE-18)	Prevent unauthorized access to information systems using multiple physical barriers and check points for entry.	SailPoint's solution can be integrated with visitor control systems, physical badging and enforcement systems to grant access authorizations to the facilities and information systems where FTI is stored.
Planning (PL)	Develop and implement a System Security Plan (SSP) and Safeguard Security Report (SSR) establishing information systems, controls, operational environment and rules of behavior.	The solution is role-based for least privileged access to system functionality and data.
Personnel Security (PS)	Identify and screen personnel with access to secure systems, including third party personnel and prohibit access once personnel have been transferred to other roles or terminated.	SailPoint delivers a 360-degree view of a user's access and entitlements. Upon termination, transfer or failure to comply with organizational policies, all access can immediately be terminated or suspended.

Control Family	Description	SailPoint Compliance
Risk Assessment (RA)	Assess risks and scan for vulnerabilities, issues resulting from unauthorized access, use, disclosure, disruption, modification or destruction of the information system.	The SailPoint solution assesses the risk an individual presents the agency based on the number of application accounts, roles, entitlements and privileges assigned. Additionally, the risk model can identify risky applications based on the number of entitlements and privileged users. A key factor in the calculation of a user or applications risk is the last time it was certified for access. SailPoint ensures that periodic certifications are completed in a timely manner. The business-friendly access certification process and interface allows scheduled certification campaigns to be completed with increased efficiency and accuracy in a timely manner.
System and Services Acquisition (SA)	Acquire, document and configure systems and services to meet security regulations, ensuring all components are actively supported by service and systems providers.	SailPoint's governance solution has been certified by the NIAP Common Criteria and has been certified and granted authority to operate in the most stringent financial, federal public sector, Department of Defense and intelligence communities. SailPoint provides access to product documentation, technical guides, community forums, training, software and patches to its customers and partners via a dedicated portal.
System and Communications Protection (SC)	Protect the confidentiality and integrity of transmitted information, implementing a secure managed interface for each component.	SailPoint can be deployed in a highly secure environment using FIPS-approved encryption to ensure data security. The application boundary is protected by strong authentication principles and role-based system capabilities to enforce least privilege access and ensure unauthorized access to applications and data.

Control Family	Description	SailPoint Compliance
System and Information Integrity (SI)	Ensure the information system and the data in the system is protected against malware, spam and errors system flaws with continuous monitoring.	SailPoint's auditing and logging capabilities can provide indicators of potential attacks of the identity system, unauthorized access and activity. SailPoint takes security seriously. Upon discovery of a system flaw or security vulnerability, the issue will immediately be evaluated and prioritized, and remediation will be made available according to impact to its customers.
Program Management (PM)	Appoint a senior information security officer to develop, implement and maintain an information security program.	The solution's role-based interface and included business process model easily allow security officer enablement, notification, authorization and sign-off of approvals, certifications and reports.

If you need help with securing information in accordance to IRS Publication 1075, contact us for a free initial consultation at sales@sailpoint.com or call 1-888-472-4578.

SAILPOINT: THE POWER OF IDENTITY™

sailpoint.com

SailPoint, the leader in enterprise identity management, brings the Power of Identity to customers around the world. SailPoint's open identity platform gives organizations the power to enter new markets, scale their workforces, embrace new technologies, innovate faster and compete on a global basis. As both an industry pioneer and market leader in identity governance, SailPoint delivers security, operational efficiency and compliance to enterprises with complex IT environments. SailPoint's customers are among the world's largest companies in a wide range of industries, including: 6 of the top 15 banks, 4 of the top 6 healthcare insurance and managed care providers, 8 of the top 15 property and casualty insurance providers, 5 of the top 15 pharmaceutical companies, and six of the largest 15 federal agencies.

SB1197-1802