NIST 800-53 Rev.5
PL (Planning) Control Family

Noah Barrall

Starfall Airlines System Categorization

Large Hub Airport	Receives 1 percent or more of the annual U.S. commercial enplanements
Employees	6500
Annual Boardings	5.8 million (Smallest major airport)

Confidentiality

High

Integrity

High

Availability

Moderate

Three Buckets

Important

- PL-2
  - System Security and Privacy Plans
- PL-4
  - Rules of Behavior
- PL-8
  - Security and Privacy Architectures
- PL-10
  - Baseline Selection
- PL-11
  - Baseline Tailoring

Secondary

- PL-1
  - Policy and Procedures
- PL-7
  - Concept of Operations
- PL-9
  - Central Management

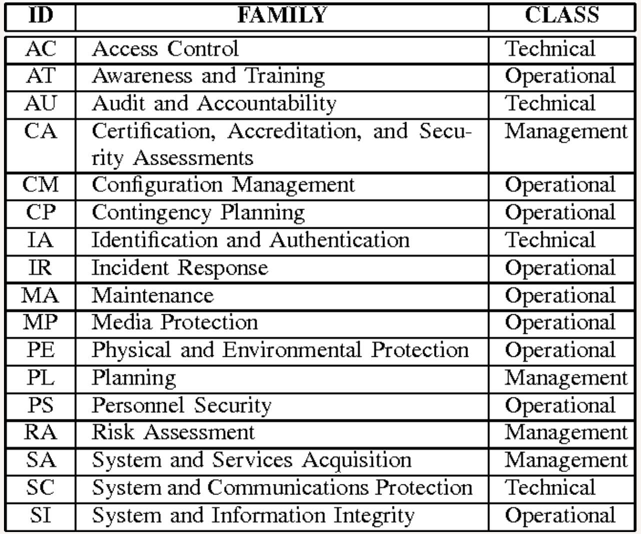
Not Important

- PL-3 (Withdrawn)
  - System Security Plan Update
  - Incorporated into PL-2
- PL-5 (Withdrawn)
  - Privacy Impact Assessment
  - Incorporated into RA-8
- PL-6 (Withdrawn)
  - Security-Related Activity Planning
  - Incorporated into PL-2

What is the Planning Control Family?

The PL family provides a comprehensive framework for:

- Addressing privacy and security concerns
- Ensuring organizations can effectively protect personal information
- Maintaining compliance with regulations
- Dealing with system architecture, system security plans, privacy security plans, and management processes



ID	FAMILY	CLASS
AC	Access Control	Technical
AT	Awareness and Training	Operational
AU	Audit and Accountability	Technical
CA	Certification, Accreditation, and Security Assessments	Management
CM	Configuration Management	Operational
CP	Contingency Planning	Operational
IA	Identification and Authentication	Technical
IR	Incident Response	Operational
MA	Maintenance	Operational
MP	Media Protection	Operational
PE	Physical and Environmental Protection	Operational
PL	Planning	Management
PS	Personnel Security	Operational
RA	Risk Assessment	Management
SA	System and Services Acquisition	Management
SC	System and Communications Protection	Technical
SI	System and Information Integrity	Operational

5 Scenarios

Scenario 1

Starfall Airlines experiences a cyberattack and many teams are not sure what to do. Due to the lack of urgency to find the threat, the attacker compromises passenger data, destroying Starfall's reputation ultimately causing massive financial losses.

PL-2 (System Security and Privacy Plans)

Implementation Effort

Moderate

Definition

- Develop security and privacy plans for the systems
- Update plans to address changes to system
- Protect plans from unauthorized disclosure and modification

Org Assignment

- Distribute copies of the plans and communicate subsequent changes to the plans to
  - Executive management
  - Information Security Team
  - Departments Heads
- Review the plans quarterly (four times a year)

Plans must:

- Be consistent with organizations architecture
- Identify roles and responsibilities
- Identify info types processed, stored, transmitted
- Provide security categorization
- Describe threats to system
- Provide overview of requirements for system

Scenario 2

John, the CFO at Starfall is informed that he has been involved in a data breach. John uses the same username and password across all platforms. Consequently an unauthorized user gains access to John’s account at Starfall where he holds highly confidential financial data and strategic business information.

PL-4 (Rules of Behavior)

Definition

- Developing clear and consistent policies and rules for individuals that have access to organizational systems and data
- Receive documented acknowledgement before granting access to system

Org Assignment

- Review and update the rules of behavior yearly
- Require individuals who have acknowledged a previous version of the rules to read and re-acknowledge one time a year when the rules are revised or updated

Implementation Effort

Low

Enhancement

- Social Media and External Site/Application Usage Restrictions
  - Use of social media sites
  - Posting organizational info on public sites
  - Use of organization provided credentials for creating accounts

Scenario 3

An attacker gains unauthorized access to a cloud storage container holding Social Security numbers due to inadequate access controls and encryption protocols (confidentiality & integrity issue).

PL-8 (Security and Privacy Architectures)

Definition

- Develop security and privacy architectures that:
  - Describe approach to CIA of organizational info
  - Describe approach for processing personally identifiable info
- Document information architecture for systems

Implementation Effort

Moderate

Org Assignment

- Review and update architectures twice a year to reflect changes in enterprise architecture

Enhancements

- Defense In Depth
- Supplier Diversity

Scenario 4

Starfalls inadequate selection of base controls and failure to adopt a set of security controls needed specifically to address the needs of the system leads to massive vulnerabilities in the systems. This leads to attackers gaining access and compromising financial data of passengers.

PL-10 (Baseline Selection)

Definition

- Selecting baseline of security controls to address security needs of a system
- Baseline is selected by:
  - Mandates and Regulations
  - Stakeholder Needs
  - Commons threats
- Selection will be designed to protect:
  - Information
  - Systems
  - Assets

Implementation Effort

Low

Scenario 5

The team at starfall fails to correctly tailor IA-2 enhancement 1, and only implements MFA to highly privileged accounts. A low level member of the security teams account is compromised and confidential data is stolen on Starfall’s upcoming security plans.

PL-11 (Baseline Tailoring)

Definition

- Identify essential controls
- Applying scoping considerations
- Selecting compensating controls
- Assign values to controls parameters
- Supplement control baseline with additional controls
- Provide info for control implementation

Organizational Benefit

- Customize to relevant systems and data
- Avoiding controls that don’t provide value
- Efficiency: Allows for more practicality

Implementation Effort

Moderate/
High

Thank you!