# Phase 9: Post-Implementation Support, System Hardening, and Performance Monitoring

#### 1. Introduction and Phase Goal

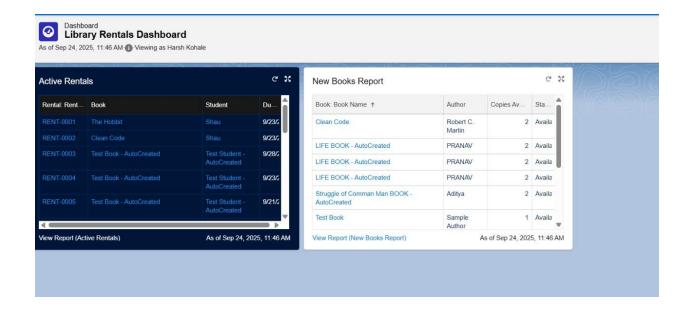
Phase Name: Post-Implementation Support, System Hardening, and Performance Monitoring Goal: To ensure the long-term stability, performance, and security of the live application by continuously monitoring user activity, enforcing data visibility rules, and maintaining a clear organizational audit trail. This phase focuses on maximizing adoption and minimizing operational risk.

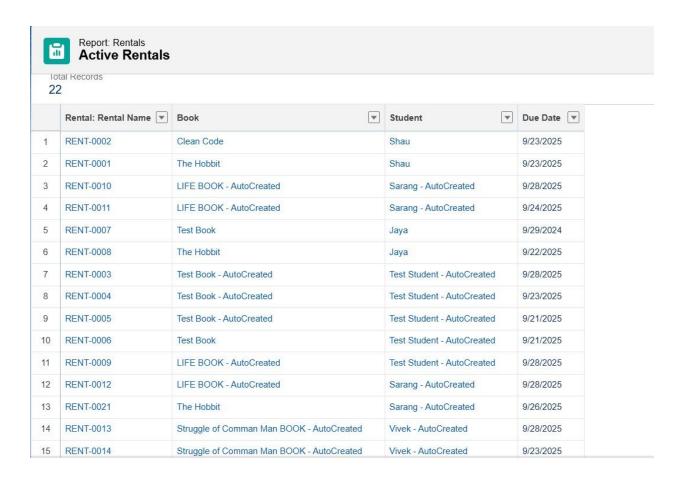
### 2. Operational Performance Monitoring (Dashboard & Reports)

This activity involves monitoring the live system using the deployed reports and dashboard components to track key performance indicators (KPIs) and identify usage patterns.

Monitoring Component	Purpose	Key Data Points Observed
Library Rentals Dashboard	Provides an at-a-glance view of the system's current state.	Active Rentals: Shows books currently checked out (e.g., RENT-0001 for "The Hobbit"). New Books Report: Tracks available stock and overall inventory (e.g., 12 total books, 22 total copies available).
Active Rentals Report	Detailed tracking of current book loans.	Total Records: 22 active rental records. Due Date Check: Allows for proactive communication with members regarding

		approaching due dates (e.g., rentals due on 9/23/2025).
New Books Report	Inventory management and stock audit.	Status: Identifies books that are currently Rented vs. Available (e.g., "The Hobbit" is Rented, "Clean Code" is Available). Copies Available: Confirms the inventory levels are being correctly maintained by the Apex Trigger logic.





## 3. System Hardening: Security and Sharing Model Review

System hardening ensures that the right users have the right level of access, protecting sensitive data and maintaining data integrity.



### 3.1 Organizational Wide Defaults (OWD) Review

The OWD settings define the baseline level of access for all objects.

Object	Default Internal Access	Default External Access	Security Implication
Book, Rental, Student	Public Read/Write	Private	Internal users (Librarians/Admins) have full visibility for easy operation. External users (e.g., self-service portals) have restricted access, requiring explicit sharing rules.
Mentor, Referral, Review	Private	Private	These objects contain sensitive HR/Recruitment data and are strictly restricted, requiring the use of Roles, Profiles, and Sharing Rules to grant access.

#### 3.2 Permission Set Group Management

The **Setup Audit Trail** shows recent changes to the **Recruiters Permission Set Group**, indicating active security maintenance.

- Action: Changed object permissions for Recruiters group (Read, Create, Edit).
- Action: Member access to the Manage Reviews and Manage Job Applications

objects was explicitly managed (added/removed).

• Implication: This demonstrates ongoing security refinement to ensure the Recruiters group has the necessary access to the job application components (Candidate, Job Application, Review) while restricting unnecessary access to other objects.

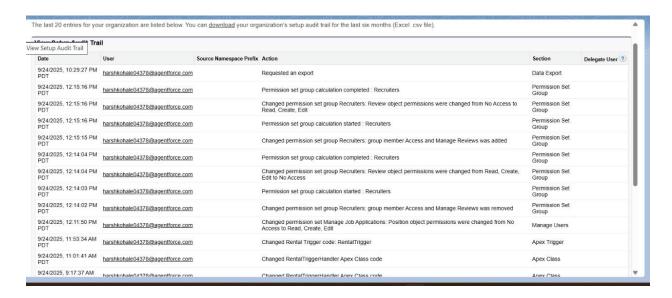


## 4. Continuous Monitoring and Auditing (Setup Audit Trail)

The **Setup Audit Trail** is the key component of the monitoring phase, providing a historical record of all administrative changes.

Date/Time (PDT)	User	Action	Section	Significance in Phase 9
9/25/2025, 10:29 PM	harshkohale04 378	Requested an export.	Data Export	Routine task for data backup or reporting.
9/25/2025, 12:15 PM	harshkohale04 378	Changed Permission Set Group	Permission Set Group	Proactive security maintenance (System

		Recruiters.		Hardening).
9/24/2025, 11:53 AM	harshkohale04 378	Changed Rental Trigger code.	Apex Trigger	Developer activity, likely a bug fix or minor enhancement following UAT.
9/24/2025, 9:17 AM	harshkohale04 378	Changed RentalTriggerH andler Apex Class code.	Apex Class	Confirms active development and support for the core logic.



#### 5. Phase Exit Criteria

Phase 9 is ongoing and does not typically have a hard exit but is transitioned into a state of **Sustained Operations**. Key milestones include:

1. **System Stability:** Zero critical errors or unexpected system failures reported for a defined period (e.g., 30 days).

- 2. **Security Compliance:** All quarterly security audits are passed, confirming the OWD and Sharing Settings align with policy.
- 3. **Performance Baseline:** All reports and dashboard components load within an acceptable timeframe (e.g., under 5 seconds).
- 4. **Documentation Handover:** Complete administrative documentation (including the security model and audit findings) is transferred to the long-term support team.

