Phase 2: Requirement Analysis

Prevent User Deletion if Assigned to an Incident

Project Title	Prevent User Deletion if Assigned to an Incident
Team ID	LTVIP2026TMIDS84378
Prepared For	SmartInternz / Mentor Review
Platform	ServiceNow PDI (Personal Developer Instance)
Module	ITSM (Incident Management)
Document Version	1.0
Date	14 Feb 2026

Team Details

Team Leader	Valluri Reethi
Team Member	Pothula Lalitha Sri Pani
Team Member	Ramena Mohana Satya Vamsi Kowsik
Team Member	Rudraraju Jogi Subrahmanyam Raju

1. Introduction

This document captures the Requirement Analysis phase for the ServiceNow project **“Prevent User Deletion if Assigned to an Incident”**. The objective is to identify and document the functional and non-functional requirements, system scope, constraints, and acceptance criteria for implementing a safeguard in the **sys_user** table.

2. Problem Statement

In IT Service Management, incidents are assigned to users (agents). If a user record is deleted while they are assigned to one or more incidents, it may break incident ownership, reduce traceability, and impact workflow continuity. In real-world enterprise systems, accidental user deletion can lead to data integrity issues and operational disruptions.

3. Stakeholders

- ServiceNow Administrators
- IT Support / Service Desk Team
- Incident Managers
- Auditors / Compliance Team
- End Users (Indirectly affected)

4. Scope

In Scope

- Create two test users (User 1 and User 2).
- Assign at least one role to User 1 so that incident assignment is possible.
- Create a new incident and assign it to User 1.
- Develop a Business Rule on sys_user table that prevents deletion when incidents exist.
- Validate deletion is blocked for assigned users and allowed for unassigned users.

Out of Scope

- Preventing user deactivation (Active=false) — only deletion is restricted.
- Preventing deletion if assigned to other task tables (Change, Problem, Request).
- User provisioning workflows and integrations.
- Custom UI pages, portals, or dashboards.

5. Assumptions & Constraints

Assumptions

- The project is implemented on a ServiceNow Personal Developer Instance (PDI).
- The admin user has permission to create users, incidents, and business rules.
- Incident table is available and ITSM plugin is active.
- Incidents are assigned using the field **assigned_to** which references sys_user.

Constraints

- The Business Rule should run only on **Delete** operation.
- The solution must not require external integrations or paid plugins.
- Implementation should be simple and aligned with SmartInternz guided project steps.
- The rule must be server-side to enforce deletion restriction reliably.

6. Functional Requirements

ID	Requirement
FR-01	System shall allow creation of test users in sys_user table.
FR-02	System shall allow assigning at least one role to a user (User 1).
FR-03	System shall allow creating an incident in incident table.
FR-04	System shall allow assigning the incident to User 1 using Assigned to field.
FR-05	System shall execute a Business Rule before deleting a user record.
FR-06	System shall check if any incident record exists where assigned_to = current user.
FR-07	System shall block deletion when incidents exist for that user.
FR-08	System shall show an error message when deletion is blocked.
FR-09	System shall allow deletion for a user with no incident assignments (User 2).

7. Non-Functional Requirements

ID	Type	Requirement
NFR-01	Performance	Business Rule should check existence efficiently using setLimit(1).
NFR-02	Security	Only admin can delete users; rule should apply even for admin.
NFR-03	Reliability	Deletion must be blocked consistently every time when condition matches.
NFR-04	Usability	Error message should clearly explain why deletion is blocked.
NFR-05	Maintainability	Rule name and script should be readable and easy to modify.
NFR-06	Auditability	Incident ownership must remain intact for reporting and compliance.

8. Business Rule Requirements

Table	sys_user
Name	Prevent User Deletion
When	Before
Action	Delete
Active	true
Script Logic	Check incident table for assigned_to=current.sys_id. If found, abort deletion.

9. Acceptance Criteria

- If a user is assigned to at least one incident, deletion must be blocked.
- System must display the message: “This user cannot be deleted because they are assigned to one or more incidents.”
- If a user has no incident assignments, deletion must be successful.
- The Business Rule must be visible under System Definition → Business Rules.
- The incident must show Assigned to = User 1, State = In Progress, and Active = true.

10. Risks & Mitigation

Risk	Impact	Mitigation
User has no role	Incident cannot be assigned	Assign at least one ITIL/incident role to User 1.
Rule not configured for Delete	User deletion will still happen	Ensure Delete checkbox is enabled and When=Before.
Script error	Deletion may fail for all users	Test with User 2 and validate logs.
Multiple incidents	Performance issue	Use setLimit(1) to check existence only.

11. Conclusion

The requirement analysis confirms the need for a server-side validation mechanism that prevents deletion of users who are currently assigned to incidents. The documented requirements will guide the design and implementation phases to ensure data integrity, operational continuity, and compliance within the ServiceNow ITSM environment.