1. Sales Admin Test Scenarios

Focus: Sales team configuration, user access, and sales-specific permissions

Scenario 1.1: Sales Rep Profile Validation

* Objective: Verify Sales Rep profile has correct object permissions
* Steps:
  1. Locate "Sales Rep" profile in the spreadsheet
  2. Confirm it has "Sales\_Rep\_Object\_Read\_Access" and "Sales\_Rep\_Object\_Edit\_Create\_Access"
  3. Verify it does NOT have "Executive\_Object\_Modify\_All\_Access"
* Expected: Sales Rep can create/edit leads/opportunities but can't modify all records

Scenario 1.2: Role Hierarchy Testing

* Objective: Ensure DCFC Staff role inherits proper permissions
* Steps:
  1. Find "DCFC Staff" role
  2. Verify it's associated with "Sales Rep" profile
  3. Test that a DCFC Staff user can't access Executive permissions
* Expected: Role hierarchy prevents permission escalation

Scenario 1.3: Lead Conversion Permissions

* Objective: Validate lead conversion workflow for sales team
* Steps:
  1. Check if "System\_Permission\_View\_and\_Edit\_Converted\_Leads" is assigned to Sales Rep profile
  2. Test converting a lead as a Sales Rep user
  3. Verify access to converted lead data
* Expected: Sales Reps can view/edit their converted leads

2. System Administrator Test Scenarios

Focus: Deployment integrity, security model, and system-wide configuration

Scenario 2.1: Full Deployment Validation

* Objective: Verify end-to-end deployment of all components
* Steps:
  1. Filter spreadsheet to all "Yes" in Deployable columns
  2. Generate deployment package
  3. Deploy to sandbox environment
  4. Validate all components deploy without errors
* Expected: 100% successful deployment with no dependency failures

Scenario 2.2: Permission Conflict Detection

* Objective: Identify conflicting permission assignments
* Steps:
  1. Check "Executive" profile has "Executive\_Object\_Modify\_All\_Access"
  2. Verify same profile doesn't have restrictive "Sales\_Rep\_Object\_Read\_Access"
  3. Test permission precedence in Salesforce
* Expected: Modify All permissions override read-only permissions correctly

Scenario 2.3: Security Model Audit

* Objective: Validate least-privilege access model
* Steps:
  1. Review all permission sets assigned to profiles
  2. Confirm "System\_Permission\_API\_Enabled" is only assigned to necessary profiles
  3. Verify "System\_Permission\_Transfer\_Records" is restricted to executives
* Expected: No excessive permissions granted to lower-level profiles

### 3. Sales Representative Test Scenarios

Focus: Day-to-day functionality and access limitations

#### Scenario 3.1: Object Access Validation

* Objective: Confirm CRUD access for sales objects
* Steps:
  1. Login as Sales Rep user
  2. Attempt to:
     + Create new Lead
     + Edit Opportunity
     + Delete Contact (should fail)
     + View Account (should succeed)
* Expected: Can create/edit sales objects but can't delete records

#### Scenario 3.2: Lightning Experience Navigation

* Objective: Verify UI functionality for sales users
* Steps:
  1. Confirm "System\_Permission\_Lightning\_Experience\_User" is assigned
  2. Login and navigate:
     + Leads tab
     + Opportunities dashboard
     + Reports (should be limited)
* Expected: Full Lightning access but restricted to sales-related features

#### Scenario 3.3: API Access Limitations

* Objective: Test API capabilities for sales users
* Steps:
  1. Verify "System\_Permission\_API\_Enabled" is assigned to Sales Rep profile
  2. Attempt to:
     + Connect via Data Loader
     + Export own Leads
     + Export all Accounts (should fail)
* Expected: Can access own data via API but can't bulk export all records

### Cross-Role Integration Scenarios

#### Scenario 4.1: Lead Ownership Transfer

* Objective: Test record transfer between roles
* Steps:
  + Sales Rep creates Lead
  + Sales Admin attempts to transfer Lead to Executive
  + Executive modifies Lead data
* Expected:
  + Sales Rep: Can initiate transfer
  + Sales Admin: Can reassign ownership
  + Executive: Can modify transferred lead

#### Scenario 4.2: Permission Inheritance Test

* Objective: Validate permission propagation
* Steps:
  1. System Admin adds new permission to "Sales\_Rep\_Object\_Read\_Access"
  2. Sales Rep logs in and tests new access
  3. Sales Admin verifies in permission matrix
* Expected: New permission immediately available to all Sales Reps

#### Scenario 4.3: Deployment Impact Analysis

* Objective: Test deployment effects across roles
* Steps:
  + System Admin deploys updated "Executive\_Object\_Modify\_All\_Access"
  + Executive attempts to modify all records
  + Sales Rep attempts same operation (should fail)
  + Sales Admin verifies permission reports
* Expected:
  + Executive: Gains modify all access
  + Sales Rep: No change in permissions
  + Reports show accurate permission assignments