Salesforce Sandbox Refresh Checklist

1. Pre-Refresh (Preparation)

Before you hit the "Refresh" button in Production, you need to "freeze" the state of your sandbox to prevent data loss.

- **Audit Outbound Change Sets:** Ensure all developed features have been deployed to Production or backed up.
- **Backup Metadata:** Use VS Code/SFDX or a backup tool to pull the current metadata of the sandbox.
- **Identify Local-Only Data:** If you have manual test data in the sandbox that doesn't exist in Prod, export it via Data Loader.
- **Check Apex/Flow Versions:** Document any active versions that differ from Production.
- **Communication:** Notify all stakeholders of the "Downtime Window" where the sandbox will be unavailable.

---

2. The Refresh Execution

- **Initiate Refresh:** Navigate to `Setup > Sandboxes` and click **Refresh** next to the target sandbox.
- **Select Sandbox Template:** (For Partial/Full Sandboxes) Ensure you are using the correct data template to pull the right objects.
- **Activation:** Once the status is "Ready for Activation," click **Activate**.

> ***Note:*** *Activation deletes the old version of the sandbox permanently.*

---

3. Post-Refresh (Configuration)

Once the sandbox is live, it's essentially a clone of Production. You must now "de-activate" production-level settings to avoid accidental emails or API calls.

Category	Activity	Responsibility
Email	Set **Email Deliverability** to "System Email Only" or "All Emails" (if testing).	Admin
Users	Update email addresses (Salesforce appends `.invalid` to user emails post-refresh).	Admin
Integrations	Update API endpoints (Point them to "Staging" or "Dev" servers, not Prod).	Developer
Connected Apps	Re-authenticate any connected apps (e.g., DocuSign, Outreach, MuleSoft).	Admin/Dev
SSO	Update Single Sign-On settings if your sandbox uses a specific URL.	Admin
Scheduled Jobs	Re-schedule any Apex jobs or Dashboard refreshes that didn't carry over.	Admin

---

4. Data Masking & Security

- **Data Masking:** If you are using a Full Sandbox with sensitive PII (Personally Identifiable Information), run your Data Masking scripts immediately.
- **Masking Emails:** Ensure customer email addresses are scrambled to prevent accidental "test" emails hitting real clients.
- **Update Named Credentials:** Ensure any stored credentials for external services are updated to the sandbox equivalents.

---

5. Validation & Sign-off

- **Smoke Test:** Perform a basic walkthrough of core business processes (Lead to Cash, etc.).
- **Integration Check:** Verify that the "handshake" between Salesforce and your external systems is successful.
- **Final Handover:** Notify the development/QA team that the environment is ready for use.

> ***Pro-Tip:*** *Create a* ***Post-Copy Apex Class****. Salesforce allows you to specify a script that runs automatically after a refresh to automate things like updating custom settings or obfuscating data.*