**Operational Challenges:**

* Can we change region access after LZ is deployed?
* What is the implementation challenges he faced earlier while deploying LZ.
* Implementing guardrails while LZ creation with best practices / after creation.
* Existing or New account confirmation?
* Mandatory Requirements before going through LZ deployment.
* What is the initial approach of creating LZ deployment in existing account (like pre-requirements to get installed/created) – No use of existing one.
* Can we rollback the operation of LZ deployment while implementing it due to any misconfiguration, if yes how much time will it take to reflect changes?
* Cloud formation for further use of resources deployment or terraform script as DR also involved? Recommendation

**Notes:**

* Email id addresses for each account/OU.

Should we go ahead with a single email address?

Need 4 Valid email addresses for below scenario:

1. **management account** - The account you are setting up AWS Control Tower in
2. **log archive** - Where security and compliance logs like AWS Config, AWS CloudTrail are stored!
3. **audit** (or security tooling) - Where services like AWS Security Hub, Guard Duty and similar might be managed from
4. **sandbox** account - for your sandbox account, created via the account factory!

**@ Need email access to get verification confirmations from aws for multiple actions.**

Need Domain mail address since this is GMA future ready scenario.

Root Security OU Log Archive (account)

(Cloud trail and cloud config)

Security/Audit account.

(Guard Duty, Security Hub etc.)

Sandbox OU Sandbox account.

Workload OU Dev (Trianz)

Test (Trianz)

UAT (Trianz and GMA users)

Prod (Trianz and GMA, public secured)