Standard Operating Procedure for Centralized CloudTrail

**To create a CloudTrail trail and logs in your organization account, follow the below steps:**

1. Log in to your AWS Management Console with your organization's master account credentials.
2. Open the AWS CloudTrail console.
3. In the navigation pane, choose Trails, and then click on the Create Trail button.
4. Enter a trail name and select the "Yes" radio button if you want CloudTrail to create a new S3 bucket automatically or “No if you want to specify an existing S3 bucket to store your logs in.
5. Configure the trail settings. You can choose to enable log file encryption and log file validation to increase security.
6. Select the option to log data events and management events. Data events record resource operations such as configuration changes to S3 buckets and CloudFront distributions, while management events record AWS service management operations such as API calls.
7. Set up the log file delivery options to specify which S3 bucket to deliver the log files to. You can choose the default option to deliver to the specified S3 bucket, or select CloudWatch Logs to deliver log files to CloudWatch Logs as well.
8. Add tags (optional) to help identify your trail. Tags enable you to categorize your trail and view it easily in your list of trails.
9. Review the configured trail settings and click on the Create button to create the trail and start logging.

Once created, the CloudTrail trail will start logging and sending the events to the specified S3 bucket or CloudWatch Logs depending on your setup.

It is important to note that **CloudTrail can only capture events for services in the regions that it is enabled for**, so ensure that your trail is enabled in all the applicable regions where you want to collect logs.