

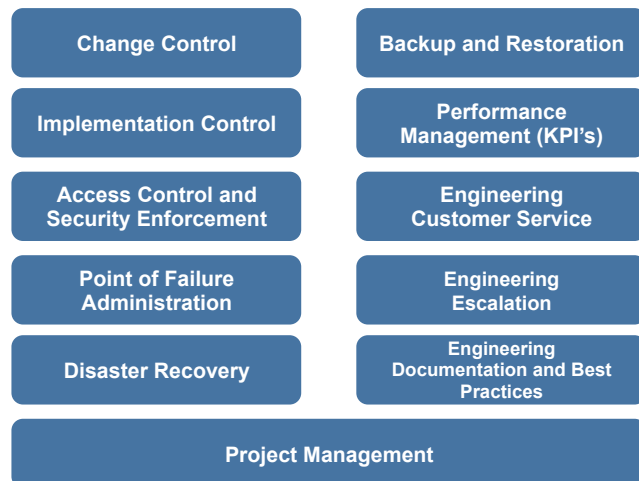
The ultimate objective of our framework is to close the gaps inherently created during the execution of multiple tasks in a VoIP Service Provider environment and that in conjunction with the workload and the organic growth in the organization, the teams establish practices that inhibit the proper identification and management of the operating and technological risks, pushing the operator into a spiral of inefficiency that will eventually impact the quality and availability of their services as well as the ability to meet financial goals.

Our model requires direct access to the daily operation within the organization in order to learn, understand and categorize the work groups, hierarchical structure, responsibilities and tasks executed on a daily basis to locate them individually as factors within the equation of each policy to be implemented, to then design, along with all the stakeholders, the processes and procedures that will conform such policies, always based upon best practices and upon a pragmatic version of a security standard.

The ASLO Risk Management, Information and Communications Security Framework

There are several Risk Management and Quality standards available for the IT industry in general. Our objective is to bring your organization to a place where it seriously makes sense to consider the implementation of a security or quality assurance standard ensuring that this endeavor is not destined to fail.

ASLO will implement a schema of policies and procedures to help your company comply with the requisites of order, collaboration and performance measurement in the following areas:



Our framework ensures a set of reliable key performance indicators for the operational groups responsible for managing the business side of the technology, which results on:

- ✧ A tangible improvement in the service availability
- ✧ Awareness and correct expectations related to the cost and real consequences of downtime
- ✧ Certainty in the operation of systems in production.
- ✧ Reliable administration of changes.
- ✧ Correct estimation of resources (time, personnel, materials)
- ✧ Readiness – immediate disposition to act before, during and after a potentially service affecting issue.
- ✧ Compliance with the most important IT security requirements.
- ✧ Vertical and horizontal transparency in your organization.
- ✧ Ownership on every member of the organization.