The Governance Risk and Compliance Process Control Application is used to manage the internal/operational controls of a company. Controls are needed to:

1. Assure achievement of operational effectiveness
2. Detect and prevent frauds
3. Certify the company’s compliance with regulations, laws and policies.

SAP GRC Process Control offer those functionalities (and others for Access Control and Risk Management) through a set of Menus which contain specific activities:

<table>
<thead>
<tr>
<th>Menu</th>
<th>Main Functions</th>
<th>More Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>My Home</td>
<td>Provides the end user with Inbox Tasks and general features like creating issues and checking objects assigned.</td>
<td>My Home</td>
</tr>
<tr>
<td>Master Data</td>
<td>Where the Organizational and Process Hierarchies are maintained. You can manage Policies here also.</td>
<td>Master Data</td>
</tr>
<tr>
<td>Rule Setup</td>
<td>Dedicated to automation of controls.</td>
<td>Rule Setup</td>
</tr>
<tr>
<td>Assessments</td>
<td>Where the Surveys and Test Plans are maintained and Planner which schedules Tests and Assessments.</td>
<td>Assessments</td>
</tr>
<tr>
<td>Access Management</td>
<td>Section “GRC Role Assignments” provides assignment of users to roles, replacement of users and creation of delegations.</td>
<td>Access Management</td>
</tr>
<tr>
<td>Reports and Analytics</td>
<td>Where Management can check the Dashboards and ensure Compliance.</td>
<td>Reports and Analytics</td>
</tr>
</tbody>
</table>

**Overview**

**Organizational Hierarchy**

The first task on Process Control is to have the Organizational Structure well defined. This is done by creating the Organization Hierarchy Master Data:
Business Processes

After the organizations are created, the next step is to set up the Business Process structure. This will contain all the processes, subprocesses, and controls to be used in the organizations. Since the same subprocesses/controls are going to be used amongst different organizations, this business process hierarchy is normally referred to as the “central” business structure.

Subprocess and Control

Having both structures created, the subprocesses can be assigned to the organizations that follow those processes. When the subprocesses and controls from the central level are assigned to organizations, they create a new object which is referred to as "local":

- Image 1: Organizational Hierarchy screen (Master Data Menu Organizations Organizations).

- Image 2: Central Process Hierarchy (Master Data Menu Activities and Processes Business Processes).
Roles

After having Subprocesses and Controls tied to organizations, the people responsible for ensuring the effectiveness of those controls need to be assigned to their responsibilities. This can be done by either entering each organization and maintaining the roles at the roles tab, or mass assigning the users to the roles on the Access Management Menu.

- Image 3: Subprocess assignment (more details here).

- Image 4: Local Role assignment (more details here[link]).
Control Testing

Once the controls have users assigned, they can be tested. These tests can be manual or automated depending on the control "Test Automation" attribute.

Manual Test

To test the effectiveness of controls with Manual automation, we create Manual Tests Plans (details [link]) with the Manual Test Steps maintained and assign it to the control:

- Image 5: Mass Role assignment (more details here[link]).

The actual plan "Test Control Effectiveness" is then created through Planner (details [link]). Sometimes this is referred to as "MTOE" which stands for "Manual Test Of Effectiveness".

**Automated Control Monitoring**

For controls that can be automated (automation "Semi-Automatic" or "Automatic") the Continuous Control Monitoring (details [link]) (CCM) functionality is used. It is also called "Automated Controls". This automation of control testing requires a Data Source, Business Rule and the schedule of the jobs that will check for deficiencies in these controls:
Policies

Policies can be created and distributed to the end users through GRC. They can range from a simple acknowledgement to a survey or quiz that needs to be completed by the users. In the scope of the Policy one can have multiple entire organizations or only specific users, there can be even LDAP integration to distribute policies to user groups or distribution lists of Active Directory.
Compliance Dashboards and Sign-Off

During normal operation, the compliance is monitored through Dashboards. However, in determined timeframes depending on the Regulation, the Sign-Off process is started through the planner and locks the data for the past compliance period to avoid changes. This frozen data can then only be audited.

Image 10: Overall Compliance Status Dashboard showing compliance metrics for SOX regulation during the 2017 Timeframe on a test system.
- Image 11: Evaluation Status Dashboard showing the existing issues for SOX regulation on the 2017 Year Timeframe (Reports and Analytics Menu  Compliance  Evaluation Status Dashboard).

- Image 12: Sign-Off Monitor showing organizations that are subject to sign-off but are not yet signed (Assessments Menu  Assessment Planning  Sign-Off Monitor).

DISCLAIMER: Image/data in this WIKI is from SAP internal systems, sample data, or demo systems. Any resemblance to real data is purely coincidental.