The goal of Change Management is to ensure that standardized methods and procedures are used for efficient and prompt handling of all Changes, in order to minimize the impact of change-related problems upon the service quality.

**General Guidelines**

- Do not make changes during normal business hours (8:00am – 6:00pm M-F)
- Change implementer must be present the day after a change is implemented
- Notify customers 1-2 weeks in advance for high Risk changes

**Terminology & Roles**

Change Management is responsible for controlling change to all devices within the live production environment. It is not responsible for change within ongoing projects or test and development environments.

- **Change Requester**: Individual or department submitting a Request For Change (RFC). This individual can be either a customer or IT representative.
- **Change Review Board (CRB)**: Team responsible for reviewing all medium risk level RFCs. This team includes a “to be determined” cross-functional team of 4-5 members with process and technical expertise. The Change Manager is a member of this team.
- **Change Advisory Board (CAB)**: Team responsible for approving all Risk Level 5 RFCs. This team includes the UTS Deputy CIO and all Directors.
- **Emergency Change**: Requires immediate implementation to correct a disruption or outage of service.
- **Impact**: A measure of the effect of a Change on business processes or services. Impact is often based on how service levels will be affected. Impact can be measured by the number of people affected or the criticality of the system.
- **Risk**: A measure of the vulnerability of each service affected by the change.
- **Standard Change**: A pre-approved change that is low risk, relatively common and follows an established procedure, and is the accepted solution to a specific requirement or set of requirements.
- **Urgency**: A measure of how long it will be until a Change has a significant impact on the Business. Urgency reflects how quickly a change must be implemented, or the time available to reduce the impact of the change on the business.

**Assessment and Levels**

Each RFC is assigned a Risk Level. Risk levels, general description, required advanced notice, and approver are listed below:

<table>
<thead>
<tr>
<th>Risk Level</th>
<th>Description</th>
<th>Notice</th>
<th>Approver</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Level 1 &amp; 2</td>
<td>Pre-approved Standard Change.</td>
<td>n/a</td>
<td>Requester</td>
</tr>
<tr>
<td>Risk Level 3</td>
<td>Change is related to a single application or service and side-effects can be safely excluded</td>
<td>1+ week</td>
<td>CRB</td>
</tr>
<tr>
<td>Risk Level 4</td>
<td>Change affects several applications or services; or a large number of users</td>
<td>2+ weeks</td>
<td>CRB</td>
</tr>
<tr>
<td>Risk Level 5</td>
<td>Change affects a major part of the business-critical infrastructure</td>
<td>2+ weeks</td>
<td>CAB</td>
</tr>
</tbody>
</table>

When accessing the Change, consider the following factors to determine the Risk Level:

- Number of customers affected
- Duration and scope of the service disruption
- Availability of a solution or work around
- The criticality of the services being disrupted
- Awareness of the impact to the university
- Can the change be done during normal business hours?
- Possible impact if the change fails?
- Does the change involve a Router or Switch?
- Does the change involve ESD or the Data Warehouse?
- Can the change be easily rolled back?
Submission Process

The Change Requester follows the submission process depicted below when submitting a Request For Change (RFC).

1. Open Outlook 2007
2. Click "File"
3. Click "New"
4. Click "Choose Form"
5. Use the drop down and choose "Personal Forms Library"
6. Click "Change Request"
7. Click "Open"
8. Add information to subject line
9. Complete form
10. Click "Send"