2.1 INTRODUCTION

Risk management is a systematic approach to maximize the prospects of ongoing success by identifying, analyzing, evaluating and treating threats. (ISO/IEC Guide 73 (2002)

Risk management of the Colleges of Technology (CTs) is designed to understand, prioritize and develop action plans for avoiding potential risks and their consequences that may affect the efficiency of running the college operations.

2.2 POLICY

The colleges of technology recognize that risk in its many forms can affect governance and management, reputation, health and safety, environment and community. They must therefore be committed to identify, manage and minimize risks that may affect the day-to-day college operations.

2.3 SCOPE

Staff in the college has a role to play in the identification and analysis of risk through the risk management processes which are incorporated within the operational and activity plans of centers and departments. The college is responsible to do the following;

- Setting out a risk management policy to support the objectives such as:
  a) avoid or minimize loss,
  b) identify opportunities and threats, and
  c) manage risks.
- Training the staff to provide a rational basis in deciding what to do with regard to any identified risks.

2.4 PROCEDURES

Step (1) Risk Identification

Step (2) Risk Analysis

Step (3) Risk Evaluation

Step (4) Risk Treatment
Step (5) Risk Monitoring

Note: For details of the procedures, see the Annexure.

2.5 Risk Management Committee
This committee is responsible for ensuring that risk management is applied to all college activities.

A. Membership
Chairman: Dean
Members: The ADAA, ADSA and ADAF
Heads of Centers and Heads of Departments (HoDs and HoCs)
College Risk Officer (CRO)

B. Roles and Responsibilities
Chairman
1. Oversees the functioning of the CRO.
2. Reviews the identified risks along with the corresponding contingency plans submitted by CRO.
3. Approves the contingency plan for identified risks.
4. Ensures proper implementation of the risk management system in the college.

HoCs and HoDs
1. Promote risk awareness among staff through discussions and training.
2. Ensure that procedures are followed in identifying, assessing, and managing risks according to policy.
3. Inform the CRO which risk requires immediate attention.
4. Submit risk register to CRO.

CRO
1. Oversees the risk management activities of the centers and departments.
2. Reviews the risk register submitted by centers and departments.
3. Evaluates and prioritizes treatment of risks.
4. Prepares contingency plans for identified high risk cases.
5. Reports to the Chairman of the Committee the identified risks along with the corresponding contingency plans and the actions taken by the units concerned.
2.6 RELATED DOCUMENTS

1. Bylaws of Colleges of Technology
2. Quality Assurance Manual (QAM)
3. Quality Sub-Manuals (QSMs)

Approval:

Effective Date: 
Approved By: 
First Review Date:
Annexure

Risk Management Process

Risk management is the process of anticipating and analyzing risks and coming up with effective and efficient ways of managing and eliminating them. Managing risks is a continuous activity, which assists in making decisions to improve current work practices.

In establishing the context, risk management process requires an examination of the external and organizational aspects of the college. It also studies the environment for risk identification, analysis and treatment options. The context determines the scope for each level of the assessment.

There are different steps involved in this process, which are illustrated in Figure 1 below.

**Step (1) Risk Identification:** Define the types of risks that may occur, how they could happen, and which stakeholders (students, staff, community) will be affected. The table below defines the types of risks with examples.

<table>
<thead>
<tr>
<th>Types of Risks</th>
<th>Definition</th>
<th>Examples</th>
</tr>
</thead>
</table>
| Strategic      | An unexpected event which may affect the effectiveness of the management process towards meeting the college objectives. | • Planning and implementation of college strategic and operational plan  
• Major decisions taken by management |
| Operational    | Risk resulting from inadequate or failed internal systems and processes, resources, or from external events. | • Recruitment problem  
• Failure in accounting controls  
• Failure in IT systems, e.g. registration  
• Breakdown of equipment  
• Inadequate document retention or record keeping  
• Poor management  
• Lack of supervision, accountability and control |
| Financial      | The risk of having inadequate budget to meet financial obligations. | • Budget allocation  
• Links between planning and resource allocation |
| Compliance     | Risk arising from centers and departments not following policies and procedures. | • Non-adherence to new policies such as health and safety policy, parking policy and maintenance policy |
| Reputation     | Risk arising from negative opinion of others which affects the institution’s image and its ability to continue or establish new relationships or services. | • Leakage of information |
Step (2) Risk Analysis: The likelihood of the risk happening and the consequences or impact of that event occurring.

Step (3) Risk Evaluation: Describe and quantify the likelihood and consequences that risks may cause. The risks are ranked and prioritized to help in deciding the extent and nature of treatment required. The table below describes the degrees of consequences and likelihood of risks.

### Table 2. Severity

<table>
<thead>
<tr>
<th>Level</th>
<th>Descriptor</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Very High</td>
<td>Loss would lead to questioning the viability of the college and system.</td>
</tr>
<tr>
<td>4</td>
<td>High</td>
<td>Loss will disrupt the functioning of the college.</td>
</tr>
<tr>
<td>3</td>
<td>Average</td>
<td>Loss would disrupt operations or threaten the viability of an operational process.</td>
</tr>
<tr>
<td>2</td>
<td>Low</td>
<td>Minor loss.</td>
</tr>
<tr>
<td>1</td>
<td>Very Low</td>
<td>Loss is within acceptable or reasonable range associated with day-to-day activities.</td>
</tr>
</tbody>
</table>

### Table 3. Occurrence

<table>
<thead>
<tr>
<th>Level</th>
<th>Descriptor</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Very High</td>
<td>Loss is likely to occur on a day-to-day basis.</td>
</tr>
<tr>
<td>B</td>
<td>High</td>
<td>Loss is likely to occur at regular intervals.</td>
</tr>
<tr>
<td>C</td>
<td>Average</td>
<td>Loss is likely to occur within the upcoming year.</td>
</tr>
<tr>
<td>D</td>
<td>Low</td>
<td>Occurrence of loss in the future.</td>
</tr>
<tr>
<td>E</td>
<td>Very Low</td>
<td>Occurrence of loss in the near future is possible, but unlikely.</td>
</tr>
</tbody>
</table>
**Step (4) Risk Treatment:** Develop and implement a plan with specific solutions to address the identified risks.

**Table 4. Risk Register**

<table>
<thead>
<tr>
<th>Event/ Situation</th>
<th>Possible loss due to Event/Situation</th>
<th>Risk base on Severity Occurrence</th>
<th>Recommended Solution</th>
<th>Resources Needed</th>
<th>Possible handling options</th>
<th>How risk options can be monitored</th>
<th>Staff Responsible</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computers breakdown due to electric failure</td>
<td>In-progress practical sessions need to be postponed</td>
<td>4 B</td>
<td>Provide generator or Powerful Uninterrupted Power Supply (UPS)</td>
<td>Generator or powerful UPS</td>
<td>Ensure the availability of resources</td>
<td>Technicians of centers and departments</td>
<td></td>
</tr>
<tr>
<td>Lack of classrooms due to increase of enrollees</td>
<td>Timetable schedules not followed.</td>
<td>3 C</td>
<td>*Extend the number of teaching hours * Increase number of buildings</td>
<td>Forecasting of student enrollees</td>
<td>HoCs and HoDs</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Step (5) Risk Monitoring:** Monitor the activities and processes to determine the accuracy of assumptions and the effectiveness of the measures taken to treat the risk (see Table 4 above).