Objective: To determine if the department/unit has developed and documented a comprehensive business continuity plan as it relates to dependency on technology resources and mission accomplishment.

Risk Level/Potential Impact: High; In the event information technology resources are unavailable, what documented plans are in place to ensure that critical business operations resume during the outage.

Criteria: Institutional policies and procedures; Best business practices.

Frequently Observed Weaknesses/Deficiencies:
- Failure to have documented downtime procedures and business continuity plans.
- Inadequate or nonfunctional downtime procedures and business continuity plans.
- Failure to periodically review and update plans.
- Failure to communicate plans to responsible individuals, as well as to other employees of the business unit.
- Only one employee knowledgeable of and/or in possession of downtime procedures and business continuity plans and execution of them.
- Failure to appoint a backup person for execution of plans.
- Inappropriate storage location/site for plan (Maintaining plans in same area and/or building that may be affected).
- Lack of alternative work space arrangements established in the event current space is unusable.
- Data are stored locally and if the current space is inaccessible, data are unavailable.

Helpful Tools:
- Information Technology Services – [https://paws.gru.edu/pub/its](https://paws.gru.edu/pub/its)
- Compliance and Enterprise Risk Management (CERM) – [http://www.gru.edu/compliance/](http://www.gru.edu/compliance/)
- Critical Event Preparedness and Response (CEPaR) – [http://www.gru.edu/cepar/](http://www.gru.edu/cepar/)

Helpful Tools Continued:
- FEMA – [https://www.fema.gov/continuity-operations](https://www.fema.gov/continuity-operations)

GRU Contact Office and Information Resource(s):
- Information Technology Services (ITS) – (706) 721-7500
- Compliance and Enterprise Risk Management (CERM) – (706) 721-0900
- Critical Event Preparedness and Response (CEPaR) – (706) 667-4207
- Public Safety – (706) 721-2914

Best Business Practices:
1. Develop and document comprehensive downtime procedures and business continuity plans.
2. Report, manage and address infrastructure risk on a continuing basis.
3. Identify maximum acceptable outage times for critical business processes and operations.
4. Identify the process for converting operations from your current facility to alternate processing facilities if necessary.
5. Ensure plans incorporate building plans, network/communication diagrams and other documents warranted by the unique function(s) of the department/unit.
6. Ensure plans include any special software that the department/unit may utilize.
7. Ensure employees of the department/unit are familiar with downtime procedures/business continuity plans and acceptable outage/down times.
8. Management should periodically communicate/refresh employees on plans.
9. Ensure a copy of the business continuity plans are stored off-site and/or in an appropriate second location outside of the area/building that may be affected.
10. Encourage employees to promptly report business risks that they may discover.
<table>
<thead>
<tr>
<th>Self-Assessment of Internal Controls for Business Continuity Planning</th>
<th>Yes</th>
<th>No</th>
<th>N/A</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do employees know what to do if their computers or IT systems are not available to use?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are source or primary data stored on ITS supported storage infrastructure?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Does the department have plans for the following scenarios?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>● ITSS resources are down. The department is still functioning.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>● Building or department processes are down, but ITSS resources are available at other locations.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>● Both are down.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>● Neither are down, but staffing is unavailable (i.e. influenza epidemic)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Has the department identified tolerance levels for above scenarios?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>● 0-24 hours</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>● 24-72 hours</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>● 72 hours or more</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Has the department identified critical periods within the year where IT resources are required? (i.e. Banner, PeopleSoft HRMS, PeopleSoft Financials, TimeNet, etc.)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>