Purpose
IT service providers are frequently exposed to significant threats to their safe and reliable operation and provision of services for their customers. These threats come in a wide variety of forms and, when combined with vulnerabilities in the systems, processes and people of the IT provider, can result in major disruptions. Risk management seeks to address these potential risks to the organization and its services by establishing a formal, standardized process of identifying risks, assessing their potential impact and devising strategies to respond to them.

NC State University's Office of Information Technology (OIT) provides IT services that are critical to the business and academic functioning of the university. The OIT leadership team and staff have investigated current risk management best practices in the IT industry and higher education. This document formalizes OIT’s risk management strategy and details the processes, procedures and tools that OIT will use to manage risks to the IT services it provides to the campus community.

Risk Assessment Process Overview
While every organization will by necessity create a particular risk management process that is unique to their particular requirements, all programs within the organization utilize the same standard approach to assessing risks. The standard approach to risk assessment developed by OIT consists of the following steps:

1. Identify and quantify risks to critical assets
   Critical assets are those systems, processes, or people any given service relies upon for normal, sustained operation. Risk is defined as the potential that a threat will take advantage of a vulnerability identified in a critical asset, thus impacting the continued operation of the associated service. In order to identify risks, then, it is necessary to first identify the critical assets and any possible vulnerabilities to specific threats that exist, and then to determine the potential impact to the service that would result. Finally, a risk factor can be calculated for the risk that allows each risk to be compared against other risks using the same standard calculation. The risk factor is calculated by quantifying the likelihood of the identified risk occurring, quantifying the expected impact and multiplying them together (*Risk = Likelihood x Expected Impact*).

   Outputs from this step:
   - Critical assets identified
   - Threats and vulnerabilities identified
   - Likelihoods and impacts identified and quantified
   - Risk factors calculated

<table>
<thead>
<tr>
<th>Likelihood Scale</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very Low</td>
<td>Unlikely to occur within the next year</td>
</tr>
<tr>
<td>Low</td>
<td>Likely to occur about once a year</td>
</tr>
<tr>
<td>Medium</td>
<td>Likely to occur about once every six months</td>
</tr>
<tr>
<td>High</td>
<td>Likely to occur about once a month</td>
</tr>
<tr>
<td>Very High</td>
<td>Occurs about once a week</td>
</tr>
</tbody>
</table>
### Impact Scale

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minor</td>
<td>Very limited interruption to the service; no adverse effect on service perceptions; requires very limited staff time to resolve</td>
</tr>
<tr>
<td>Moderate</td>
<td>Moderate interruption to the service; limited adverse effect on service perceptions; requires possibly heavy staff activity (limited to service team) to resolve</td>
</tr>
<tr>
<td>Major</td>
<td>Extended interruption to the service; major adverse effect on service perceptions; results in measurable reduction in work efficiency for customers; requires possibly heavy staff activity (across multiple teams) to resolve; may result in limited negative publicity</td>
</tr>
<tr>
<td>Critical</td>
<td>Extremely extended interruption to the service; major adverse effect on service perceptions; results in significant reduction in work efficiency for customers; requires extremely heavy staff activity (across the division) to resolve; results in significant negative publicity</td>
</tr>
</tbody>
</table>

2. **Identify and quantify possible response to these risks**

Once the risks have been identified, the next step is to identify possible responses to the risks. Possible responses to risk involve accepting the risk (doing nothing), transferring the risk (by passing risk along to others, i.e. insurance), avoiding/limiting the risk altogether (in most cases extremely difficult if not impossible), or attempting to mitigate or reduce the risk by implementing a risk reduction plan. For each response, the resource cost of implementation is calculated as is the likely reduction in impact or likelihood of occurrence due to the implemented response. As was done in the above step, by quantifying these values and then multiplying them together, a risk response effectiveness factor is calculated (*Risk Response Effectiveness = Resource Cost \times Likely Risk Reduction*). This can then be used to compare possible responses against each other.

Outputs from this step:
- Possible risk responses identified
- Resource cost and risk reduction identified and quantified
- Risk response effectiveness calculated

### Resource Cost Scale

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Work can be performed by the current staff; would not require any additional hardware and/or software purchases</td>
</tr>
<tr>
<td>Medium</td>
<td>Work may require additional staff or the repurposing of current staff priorities; would require moderate investment in additional hardware and/or software</td>
</tr>
<tr>
<td>High</td>
<td>Work would require additional staff (full-time or contracted); would require significant investment in additional hardware and/or software</td>
</tr>
</tbody>
</table>
3. **Select appropriate responses for implementation**
With all risks and possible responses to those risks adequately identified and quantified, management is now able to make appropriate risk management decisions. With risks normalized across the entire organization via the use of the risk factor, discerning which risks are most urgent and require immediate responses and which do not is greatly simplified. In the same way, by comparing the risk response effectiveness of all risks across the organization, management is quickly able to identify which responses should be implemented to provide the most benefit for the resources invested and which to avoid due to too high a cost or a very low likely benefit.

Outputs from this step:
- List of risk responses to be implemented

4. **Track progress and effectiveness of responses**
Once specific risk responses have been identified for implementation, they are tracked and monitored to ensure that they are progressing on their established timetables. Additionally, the effectiveness of the response is assessed once the implementation has been completed to verify whether the resource cost and the total risk reduction were achieved as intended.

Outputs from this step:
- On-going reports on progress of risk response implementations
- Report on effectiveness of risk response implementation when completed

5. **Repeat the process on a regular basis**
Risk assessment is not a one-time process. The IT risk environment is constantly changing, and new risks are appearing all the time. Thus the full risk assessment process needs to be repeated on a regular basis to ensure that these new risks are being addressed by the same formal, standardized process applied to older risks.
The OIT Risk Assessment Process

A. On an at least yearly basis, OIT service owners, with input from their service team, are responsible for conducting a risk assessment of their service. This will include identifying risks, including assigning a likelihood and impact value, as well as identifying possible risk responses, including assigning a resource cost and risk reduction value. They will utilize OIT’s Risk Management application to gather this information.

B. While it is only required to perform a risk assessment on a yearly basis, it is recommended that OIT service owners do individual risk assessments when those risks are identified. This will not only reduce the workload necessary during the yearly assessment, but also will allow for potentially quicker management response to urgent risks.

C. Each director will regularly review the risk reports associated with services for which they are responsible (i.e. the service owner works in their unit). This information will assist the director in making resource allocation decisions as well as make them aware of possible urgent risk situations.

D. At least annually, the directors and CIO will meet to review the risk environment of OIT. This will involve assessing any current risk response efforts as well as reviewing the overall risk reports in the Risk Management application, in case any new urgent risks demanding action have arisen since their last review.

E. The Risk Management Process Owner is responsible for maintaining the Risk Management application as well as making continuing refinements of the overall process or associated documents and tools. This person or group is also responsible for tracking and monitoring the identified risk responses to ensure that they are progressing on their established timetables and for producing a yearly public report on the risk environment of OIT. Lastly, they also are available to assist individual service teams or the directors if they require it.

The following guiding principles were used to develop the above process:

Keep it simple
As evidenced by the above description of the process, risk assessment can seem to many people like a fairly complicated process with multiple steps and unfamiliar terminology and concepts. It can be very enticing to design a highly complex risk assessment process that is intended to capture every minor detail in an effort to produce the most accurate and detailed information; however, if the organization is not ready or able to handle a process at that high level of complexity, then all that design work is wasted. As a result, it was agreed that OIT’s risk management implementation would require only some basic training for staff, coupled with sufficient documentation online.

Service-oriented
As part of OIT’s ongoing efforts toward achieving a more service-oriented organization, it was agreed that risk assessments would be conducted within the context of specific OIT services. This means that the activities of identifying critical assets to the service, identifying threats, vulnerabilities and impacts to the service, and identifying possible risk responses as well as the resource costs and expected risk reductions would all be conducted at the service level by the service owner and other service team members. As these individuals are the most likely to fully understand the particulars of their service and its associated risks, having them conduct these assessments makes sense. This is a contributing factor in keeping the process as simple as possible as well as informing the last guiding principle.

Low-overhead
With so many staff involved in one way or another with risk assessment, it becomes imperative to implement a process that requires the commitment of as few resources as possible. OIT staff members never have a shortage of work, so adding a possibly very time-consuming risk assessment process on top of their workload is simply not sustainable. This is true across all units and all levels within OIT. Keeping the process as simple as possible and involving staff at the service level are likely to reduce the workload on any single individual or group of individuals. Additionally, a commitment to minimizing the workload led to the decision to use a Risk Management application that simplifies the gathering of the risk information as well as performing the calculations of the risk factors and risk response effectiveness values. This application also is able to display these values in a manner that easily allows management to compare risks and responses against each other to more effectively and efficiently make decisions on them.

Approval
Approval of this process by the OIT Directors and the CIO/Vice Chancellor for Information Technology is required. Review of this document and the overall risk management strategy will be conducted at least annually.