Risk Assessment Methodology Recommendations
For Identity and Access Management (IAM)
IAM Focus Group

In an attempt to identify and manage risks to the University before problems arise, the University has embarked on a process known as enterprise risk management (ERM). The University is currently assessing risk in several categories, including strategic, financial, compliance-related, and operational. “Our goal is to create a risk-aware culture, permitting the University to identify and make plans to avoid material impact on finances and operations while encouraging the acceptance of manageable risks. Effective risk management is a proactive endeavor that helps to ensure that the University has an approach to risk that is well-defined, consistently applied and continually improved.” (Penn State Live 11/15/07)

Information technology (IT) risks throughout the University must also be assessed and managed. As our reliance on IT has increased exponentially over the years, so has our level of unknown and unmanaged risk of those systems. Currently, there is no formal, systematic process that is required by policy to assess and manage the risk of any new or existing system that is on-line at the University. However, we must take steps to identify and manage the vulnerabilities and threats to our systems that could potentially wreak havoc on our operations, reputation, and legal obligations. This can be accomplished with a thorough risk management process.

According to NIST 800-30 Risk Management Guide for IT Systems, in order to be effective, IT risk management should be totally integrated into all of the phases of the system development life cycle (SDLC). This includes: (1) system concept (2) development or acquisition of new systems, (3) implementation, (4) operation/maintenance, and (5) final disposal. Risk assessments identify the threats and vulnerabilities to a system and evaluate the administrative, physical, and technical safeguards. The potential combination of a threat to act upon a vulnerability is then measured by its probability of occurrence and the impact that it would have on an organization. The measure of the impact of a realized risk is then used to manage the risk appropriately. It is beyond the scope of this document to address the risk assessment process of an entire system and its supporting infrastructure. The purpose of this document is to address only how we might address one piece of an IT risk assessment and management process; that is, the risks associated with identity and access management (IAM) of the system. This is in support of the IAM initiative formed to address the need for a cohesive and comprehensive IAM strategy for the University.

Throughout all of the phases of the SDLC, system access requirements should be considered. For example:

- Who will need access to the system and for what purpose?
- Will it need to interface with any other systems?
- How will the system be accessed? Does the system require only local network access or should it be accessible over the internet?
• What type of data will the system process? How does that data fit into our formal data classification scheme (in process) and the associated level of assurance that is required for the asserted identity of the user?
• What are the authentication and access protocols that the system is compatible with? What are the inherent risks of those protocols? How does the system authentication capabilities fit into the (yet to be determined) University IAM infrastructure?
• Will future enhancements or revisions to the system continue to be compatible with access requirements?
• How can access to the system be properly eliminated when the system is being prepared for end-of-life?

**Data Classifications**
Soon, a formal data classification scheme will be announced at the University. This data classification scheme can then be used to determine a minimum level of assurance needed for access authentication. The level of assurance describes the degree of certainty that the user has presented a valid credential, normally done during the electronic authentication (E-authentication) process. Various sensitivity levels of data would require different levels of assurance that the presented access credential is valid. For example, the following data categories have been drafted by the data classification group (this is for illustrative purposes only and is subject to change):

- **Public** – Information is intended for distribution to the general public, both internal and external to the University. Release of the data either intentional or inadvertent would have no or minimal damage to the institution in any dimension.
- **Internal/Controlled** – Information is generally intended for distribution within Penn State only, generally to defined large subsets of the user population. Release of the data has the potential to create moderate damage to the institution.
- **Restricted** - Data which the University has a legal, regulatory or contractual obligation to protect and for which access must be strictly and individually controlled and logged. The release of such data has the potential to create major damage to the institution.

**Impact Level of Unauthorized Access**
Each of the data classifications should be evaluated to determine the potential impact associated with unauthorized access to it. Types of impact to be associated with unauthorized access should include categories for impact to reputation, financial resources, operations, confidential information, personal safety, or legal compliance requirements. It is likely that impact levels within a data classification could vary, based on the specific type of data, but each classification would have minimum and maximum impact value within the classification.

Impact levels of unauthorized access to a specific data category:
• **No impact** – The result would have no negative impact on any aspect of the University’s functions, mission, or obligations.
• Low impact - The result would have little negative impact on the reputation, financial resources, operations, confidential information, personal safety, or legal compliance requirements of the University.
• Moderate impact - The result would have a significant negative impact on the reputation, financial resources, operations, confidential information, personal safety, or legal compliance requirements of the University.
• High impact - The result would have a very significant, severe, or catastrophic negative impact on the reputation, financial resources, operations, confidential information, personal safety, or legal compliance requirements of the University.

<table>
<thead>
<tr>
<th>Category</th>
<th>No Impact</th>
<th>Low Impact</th>
<th>Moderate Impact</th>
<th>High Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reputation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Financial Resources</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operations</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confidential Information</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Personal Safety</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Legal Compliance</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The final impact score to be used is the highest potential impact recorded for all of the categories. For instance, if unauthorized access to a particular resource had no impact on any of the categories except for operations, then the highest score (low, moderate, or high) for the operational impact would be used in the next step of mapping to the required assurance level.

**Map Required Assurance Level to Potential Impact**
Map the final (highest) impact score with the level of assurance required. This could be done as follows:

<table>
<thead>
<tr>
<th>Final Impact Value</th>
<th>Level of Assurance Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>0</td>
</tr>
<tr>
<td>Low</td>
<td>1</td>
</tr>
<tr>
<td>Moderate</td>
<td>2, 3</td>
</tr>
<tr>
<td>High</td>
<td>4</td>
</tr>
</tbody>
</table>

The levels of assurance to be used (*currently in draft by committee*):

• Level 0: No confidence in the asserted identity’s validity. A userid and password may be requested but there is no vetting or proofing required.
• Level 1: Little confidence in the asserted identity’s validity. A userid and password may be requested. Vetting/validation is done by email or callback.
• Level 2: Some confidence in the asserted identity’s validity. A userid and password may be requested. There is 3rd party validation and in-person proofing performed by a trusted party.
• Level 3: High confidence in the asserted identity’s validity. Requires two-factor authentication (userid and password + SecurID, etc.)
• Level 4: Very high confidence in the asserted identity’s validity. Requires strong cryptographic authentication such as public/private asymmetric key pairs.

E-Authentication
After mapping the impact scores to the required assurance level, an appropriate technology can be chosen for the E-authentication process. The NIST 800-63 Electronic Authentication Guideline provides guidance for each of the levels of assurance on the following components of the E-authentication process:
• Tokens-the cryptographic key or password used to prove identity
• Registration-the identify proofing process done by the registration authority (RA)
• Authentication protocol-the electronic sequence of messages between claimants and verifiers that enables the verifier to verify that the claimant has control of a valid token to establish his/her identify.

Conclusion
The University should institute a systematic risk management process throughout the SDLC of information systems that are critical to the University mission. Additionally, a risk assessment methodology should be used to manage the risk of an IAM strategy. The steps to assess IAM risk are as follows:
• Categorize the data, based on sensitivity of the data.
• Measure the negative impact of unauthorized access to a given category of data based on the type of impact, such as, reputational, financial, operations, confidentiality, personal safety, and legal compliance obligations.
• Map the potential impact score with the level of assurance required to protect the data.
• Use the level of assurance required to choose an appropriate technology for E-authentication as recommended by the NIST 800-63 document, or use a similar methodology to assess the risk of a specific E-authentication method.
Resources

Whitehouse document, M-04-04
http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf

NIST 800-30 Risk Management Guide for Information Technology Systems

NIST 800-63 Electronic Authentication Guideline

CMS Information Security Risk Assessment Methodology

Federal government's eAuthentication initiative http://www.cio.gov/eauthentication/