The purpose of an Information Technology Standard is to specify requirements for compliance with Old Dominion University Information Technology policies, other University policies, as well as applicable laws and regulations. Standards may include business principles, best practices, technical standards, migration and implementation strategies, that direct the design, deployment and management of information technology.

Information Technology Standard: Risk Assessment Standard
Reference Number: 08.1.0
Date of Current Revision or Creation: May 29, 2013

A. PURPOSE

The purpose of this standard is to define the risk assessment and treatment requirements used to implement information technology security controls.

B. DEFINITIONS

Data Owner is the individual responsible for the practice decisions of data.

Information Security Office is the unit within the Information Technology Services responsible for overseeing efforts to protect ODU’s computing and information assets and to assist in compliance efforts with information-related laws, regulations, and policies.

Risk Treatments involve identifying the range of options for treating unacceptable risk, assessing those options, preparing risk treatment plans and implementing them.

Risks are those factors that could affect the security, availability, and integrity of the University’s key information assets and systems.

Sensitive System is a classification given to any IT system in which the loss to confidentiality, integrity, and/or availability of the system or data could have a material adverse effect on the University interests or the privacy to which individuals are entitled.

System Design Change is defined as any combination of changes to individual system components, or major modifications to software, hardware, or database components that
effectively change the way the system operates or responds to the user. Changes include an operating system change, type of database used, changes to underlying processes such as the use of new scripting language or web development platform, a complete hardware lifecycle change, or a change to the authentication system being used.

**System Risk Assessment** is the overall process of system risk analysis and risk evaluation, and identification of risk treatments. It is also the name of the report required as documentation.

**System Owner** is the manager responsible for operation and maintenance of a University IT system, and is responsible for conducting a risk assessment and for initiating risk treatment whenever inadequate controls are identified. Documentation of the System Risk Assessment or annual determination of system status is the responsibility of the System owner.

C. **STANDARDS STATEMENT**

**Responsibilities**
The Information Security Office is a unit within Information Technology Services which assists departments in understanding system risk assessments, and provides standard forms and directions, reviews all system risk assessments and retains the documents, reviews industry standards and activities of relevant organizations in order to improve the risk assessment process.

The System Owner is responsible for documenting and maintaining the system risk assessment information for systems owned and is authorized to perform all tasks necessary to perform this function.

The Data Owner is responsible for classifying the IT system as sensitive if any type of data handled by the system has a sensitivity of high on any of the criteria of confidentiality, integrity, or availability and defines the protection requirements for the data based on the sensitivity of the data, any legal or regulatory requirements, and business needs.

**System Risk Assessments**
The overall process of system risk analysis and risk evaluation, and identification of risk treatments, is formally documented in the System Risk Assessment provided to System Owners by the Information Security Office.

**New systems**
All new an IT system, as a part of the project management process and before a system is placed in production, will conduct a system inventory in order to determine the data and system classifications. For systems classified as sensitive, a System Risk Assessment must be completed.

**All systems**
System Owners, in collaboration with the Data Owners, must conduct and document System Risk Assessment of IT systems they own or manage as noted below:
1) A System Risk Assessment is required before a system is placed in production to provide services for the University (as noted above.)

2) A System Risk Assessment is required whenever a system design change occurs that may alter the risks associated the classification, environment, or operation and may impact the confidentiality, integrity or availability of a system.

3) Annually, the System Owner must determine if the current System Risk Assessment is valid. If a system design change has occurred that alters the risks to the system, a new System Risk Assessment is required. The outcome of the annual determination is provided to the Information Security Office upon conclusion.

**System Risk Assessment Documentation**

System Owners, in collaboration with the Data Owners, must complete or update the System Risk Assessment, in the form provided by the Information Security Office that includes, at a minimum, identification of all vulnerabilities discovered during the assessment, and a summary, including major findings and risk mitigation recommendations, if any.

All information collected or used as a part of the System Risk Assessment must be formally documented and securely maintained. New or updated System Risk Assessments are provided to the Information Security Officer upon completion.

**Risk Treatment**

Risk treatments should be undertaken to mitigate identified high or unacceptable risks, using appropriate administrative, technical and physical security controls.

In the event any risk assessment identifies inadequate controls or a lack of compliance with controls, a risk treatment will be undertaken, reported to upper management, and tracked until compliance is achieved or mitigating controls have been established and implemented. Risk treatments should take account of the legal-regulatory and private certificatory requirements, the organizational objectives, operational requirements and constraints; and the costs associated with implementation and operation relative to risks being reduced.

Risk treatment decisions must be must be formally documented and securely maintained. Risk treatment decisions are provided to the Information Security Officer upon completion.

**External Parties**

External parties, including partners, vendors and contractors, are responsible for managing the risks to their information assets that are accessed, processed, communicated with in accordance with the contract and any guidelines provided by the Information Security Office.

**Assistance**
This Information Security Office is available to assist System Owners in understanding the process and completing the System Inventory and System Risk Assessments.

D. PROCEDURES, GUIDELINES & OTHER RELATED INFORMATION

Federal and State Law

University IT Policies

ITS Standards and Guidelines

- 01.2.0  IT Roles and Responsibilities
- 06.3.0  Project Management Standard
- 06.4.0  IT System Inventory Standard

Detailed procedures are provided on the System Risk Assessment web page.

HISTORY

<table>
<thead>
<tr>
<th>Date</th>
<th>Responsible Party</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>October 2008</td>
<td>CIO/ITAC</td>
<td>Created</td>
</tr>
<tr>
<td>October 2009</td>
<td>CIO/ITAC</td>
<td>Reaffirmed</td>
</tr>
<tr>
<td>October 2010</td>
<td>CIO/ITAC</td>
<td>Reaffirmed</td>
</tr>
<tr>
<td>October 2011</td>
<td>CIO/ITAC</td>
<td>Reaffirmed</td>
</tr>
<tr>
<td>September 2012</td>
<td>CIO/ITAC</td>
<td>Revised</td>
</tr>
<tr>
<td>December 2012</td>
<td>IT Policy Office</td>
<td>Numbering revised</td>
</tr>
<tr>
<td>May 2013</td>
<td>IT Policy Office</td>
<td>Review process modified</td>
</tr>
<tr>
<td>June 2013</td>
<td>CIO/ITAC</td>
<td></td>
</tr>
</tbody>
</table>