Purpose and Summary
This standard supports ISO-200 Information Security Risk Management and Security Planning Policy and applies to all Information Resources owned or operated by or on behalf of the University.

This standard establishes the minimum Information Security Office (ISO) requirements for reporting information security risk management activities. The information security risk management process ensures that, for each University Information Resource, critical information security roles are assigned, information security risk is assessed and analyzed, risk treatment decisions and security plans are documented, and sufficient information is communicated to the ISO to develop, test, review, and maintain a comprehensive, University-wide information security plan.

Definitions
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Owner</td>
<td>The individual(s) or Unit with operational authority for specified University Information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. This individual or Unit is responsible for making risk tolerance decisions related to the owned University Information on behalf of the University and is responsible for any loss associated with a realized information security risk scenario.</td>
</tr>
<tr>
<td>Information Resources</td>
<td>University Information and related resources, such as equipment, devices, software, and other information technology.</td>
</tr>
<tr>
<td>Information Resource Owner</td>
<td>Collective term used to refer to Information Owners and Information System Owners.</td>
</tr>
<tr>
<td>Information System</td>
<td>A major application or general support system for storing, possessing, or transmitting University Information. An Information System may contain multiple subsystems. Subsystems typically fall under the same management authority as the parent Information System. Additionally, an Information System and its constituent subsystems generally have the same function or mission objective, essentially the same operating characteristics, the same security needs, and reside in the same general operating environment.</td>
</tr>
<tr>
<td>Information System Owner</td>
<td>The individual(s) or Unit responsible for the overall procurement, development, integration, modification, and operation and maintenance of an Information System. This individual or Unit is responsible for making risk tolerance decisions related to the owned Information Systems on behalf of the University and is responsible for the loss, limited by the bounds of the Information System, associated with a realized information security risk scenario.</td>
</tr>
<tr>
<td>Information Security Risk Manager</td>
<td>An individual designated by the supervisor of a Unit (e.g., a Vice President, Dean, Director, Department Head, or Head of a center or other office) to be responsible for managing an organization's information security risks and minimizing the adverse impact of losses on the achievement of organizational objectives.</td>
</tr>
<tr>
<td>ISO</td>
<td>The University's Information Security Office, responsible for coordinating the development and dissemination of information security policies, standards, and guidelines for the University.</td>
</tr>
<tr>
<td>IT Security Manager</td>
<td>An individual designated by the supervisor of a Unit (e.g., a Vice President, Dean, Director, Department Head, or Head of a center or other office) to serve as the primary contact between</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>----------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>the respective Unit and the ISO for all matters relating to information security.</td>
<td></td>
</tr>
<tr>
<td>Unit</td>
<td>A college, department, school, program, research center, business service center, or other operating Unit of the University.</td>
</tr>
</tbody>
</table>

**Statements of Standard**

A. **Information security risk management activities must include the following activities:**

1. **Data Collection** – Narrowly define the information security risk management project, document the business context of the assessment, and identify the people that will participate. The following shall be submitted to the ISO:
   a) Scope of the information security risk management project, including:
      i. Business Criticality
      ii. Data Sensitivity
      iii. Assessment Type (either Information System or Business Process)
      iv. Responsible Department
      v. Business Purpose or Use
      vi. Description of Components
      vii. Information Resources
   b) Identify the stakeholders and their information security roles, including:
      i. Information Resource Owner
      ii. Information Security Risk Manager
      iii. Information Technology Security Manager
   c) Ranked business impacts and a characterization of the result if a threat that is realized, including:
      i. Unintended Disclosure
      ii. Unauthorized Modification
      iii. Loss of Access

2. **Risk Assessment** – Answer, at minimum, all required questions in the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) based assessment (NIST CSF), which has been adapted and published by the University ISO with modified questions applicable to the University environment. These questions are available through the information security risk management portal. The results of the assessment must be submitted to the ISO.

3. **Risk Analysis** – Create a risk register that aggregates the potential vulnerabilities and risks identified during risk assessment, filters out false-positives, and maps identified vulnerabilities and risks to threats and business impacts. The risk register shall be submitted to the ISO and each risk statement must include the following attributes:
   a) Risk Statement, phrased using a “<business impact> from <threat> due to <vulnerability>” sentence structure
   b) Date that the risk statement was written
   c) Likelihood of the risk statement occurring
   d) Impact of the risk statement occurring
e) Risk Rating representing the combination of likelihood and impact

4. Security Planning – Create and document risk treatment decisions. The security plan shall be submitted to the ISO and must include the following attributes:
   a) Risk treatment decision for each risk statement in the risk register that includes at least one (1) of the following options:
      i. Accept
      ii. Avoid
      iii. Transfer
      iv. Mitigate
   b) Approval of the security plan by at least one (1) of the Information Resource Owners
   c) Date of approval for the security plan

Responsibility

Information Resource Owners responsible for satisfying the requirements of this standard are divided into two types of owners:

- Information Owners -- The individual(s) or Unit with operational authority for specified University Information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. This individual or Unit is responsible for making risk tolerance decisions related to the owned University Information on behalf of the University and is responsible for any loss associated with a realized information security risk scenario.

- Information System Owners -- The individual(s) or Unit responsible for the overall procurement, development, integration, modification, and operation and maintenance of an Information System. This individual or Unit is responsible for making risk tolerance decisions related to the owned Information Systems on behalf of the University and is responsible for the loss, limited by the bounds of the Information System, associated with a realized information security risk scenario.

Related Documentation/Resources

- Information Security Risk Management Instructions
- Exception Process/Procedure