Information Security Advisory Council (ISAC)

September 17, 2009
Agenda

• Old Business
  » Approval of Minutes
  » Approval of Program Framework
  » Draft Charter
  » Data Steward Role

• New Business
  » Risk Assessment

• Next Meeting
Agenda

• Old Business
  » Approval of Minutes
  » Approval of Program Framework
  » Draft Charter
  » Data Steward Role

• New Business
  » Risk Assessment

• Next Meeting
Agenda

• Old Business
  » Approval of Minutes
  » Approval of Program Framework
  » Draft Charter
  » Data Steward Role

• New Business
  » Risk Assessment

• Next Meeting
Draft Charter

The Information Security Advisory Council will provide guidance and oversight of the Information Security program with an emphasis on risk assessment, risk prioritization, strategy and policy issues.
Data Steward Role

• Recap
  » Retrain Data Stewards
    • More clarity on their responsibilities
    • Loyola Protected Data
      – Not stored, if possible
      – If needs to be stored, it should be stored on a network device (file server, application server)
      – Discuss recommended changes to the policy
  » Enterprise level scanner
    • Budget request has been made
  » Timing
    • Semi-annual vs. Annual
    • Each department uses own schedule
Agenda

• Old Business
  » Approval of Minutes
  » Approval of Program Framework
  » Draft Charter
  » Data Steward Role

• New Business
  » Risk Assessment

• Next Meeting
Risk Assessment

• What is a Risk Assessment?
  » Identifies threats
  » Evaluates the likelihood that the threat will be exploited
  » Estimates the potential impact (losses) of an occurrence
  » Qualitative vs. Quantitative

• Why do a Risk Assessment?
  » Define what needs to be done
  » Determine the priority of the projects and tasks
  » Identify and justify the resources required
Risk Assessment

• Approach
  » Identify and prioritize information security risks using a two phase approach
    • Phase I – High level risk assessment using ISO 27001/27002 Standards as a basis
    • Phase II – Broader, deeper risk assessment including interviews with staff and faculty data owners
  » UISO would conduct initial gap analysis, report findings, and make risk recommendations
  » ISAC will review and modify recommendations as appropriate, rank the priorities, and make recommendations for the final project proposal to go to the ITESC

• Scope
  » Phase I of the Risk Assessment process would compare the controls in the ISO 27002 standard to Loyola’s existing ITS environment
    • Existing systems not managed by ITS would be out of scope (Phase II)
  » An evaluation would be made of the applicability of each control to the environment
    • Not all controls will be 100% applicable
  » Controls requiring in-depth evaluation may be out of scope (Phase II)

• Phase II
  » Once Phase I has been completed, ISAC can consider approach to Phase II
Information Technology Standards

• Standards
   » ISO 27000
      • Information Security standards published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).
   » ITIL
      • Information Technology Infrastructure Library (ITIL) – standards for managing IT infrastructure, development and operations, including Information Security.
   » COBIT
      • Control Objectives for Information and related Technology (COBIT) - framework for IT controls and governance
   » FISMA/NIST
      • Federal Information Security Management Act of 2002 / National Institute of Standards and Technology – FISMA dictates what government organizations must do to secure their systems, while NIST provides the underlying standards and security requirements
ISO 27002 Standard

• UISO has adopted the ISO 27002 security standard
  » Strategic
  » Security-centric
  » International standard for an international university
ISO 27002 Domains

ISO 27002 Controls

- Compliance
- Information Security Policy
- Security Organization
- Asset Management
- Human Resources Security
- Physical & Environmental Security
- Acquisition, Development & Maintenance
- Risk Assessment
- Communications & Operations Management
- Access Control
- Incident Management
- Business Continuity Management
## Risk Assessment Example

<table>
<thead>
<tr>
<th>Clause #</th>
<th>Clause Title</th>
<th>Category #</th>
<th>Category Title</th>
<th>Control #</th>
<th>Control Title</th>
<th>Control Description Long</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Security Policy</td>
<td>5.1</td>
<td>Information Security Policy</td>
<td>5.1.1</td>
<td>Information Security Policy Document</td>
<td>An information security policy document should be approved by management, and published and communicated to all employees and relevant external parties.</td>
</tr>
<tr>
<td>6</td>
<td>Organization of information security</td>
<td>6.1</td>
<td>Internal Organization</td>
<td>6.1.5</td>
<td>Confidentiality agreements</td>
<td>Requirements for confidentiality or non-disclosure agreements reflecting the organization’s needs for the protection of information should be identified and regularly reviewed.</td>
</tr>
<tr>
<td>7</td>
<td>Asset management</td>
<td>7.1</td>
<td>Responsibility for assets</td>
<td>7.1.3</td>
<td>Acceptable use of assets</td>
<td>Rules for the acceptable use of information and assets associated with information processing facilities should be identified, documented, and implemented.</td>
</tr>
<tr>
<td>7</td>
<td>Asset management</td>
<td>7.2</td>
<td>Information Classification</td>
<td>7.2.1</td>
<td>Classification guidelines</td>
<td>Information should be classified in terms of its value, legal requirements, sensitivity, and criticality to the organization.</td>
</tr>
<tr>
<td>8</td>
<td>Human resources security</td>
<td>8.2</td>
<td>During employment</td>
<td>8.2.2</td>
<td>Information security awareness, education, and training</td>
<td>All employees of the organization and, where relevant, contractors and third party users should receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.</td>
</tr>
</tbody>
</table>
## Risk Assessment Example

<table>
<thead>
<tr>
<th>Clause</th>
<th>Clause Title</th>
<th>Category #</th>
<th>Category Title</th>
<th>Control #</th>
<th>Control Title</th>
<th>Control Description Long</th>
<th>Applicability</th>
<th>Risk/Control Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Security Policy</td>
<td>5.1</td>
<td>Information Security Policy</td>
<td>5.1.1</td>
<td>Information Security Policy Document</td>
<td>An information security policy document should be approved by management, and published and communicated to all employees and relevant external parties.</td>
<td>Applicable</td>
<td>The policy should be amended to include the implementation guidance, including a definition of security, a statement of management intent and support, a framework (risk management) for implementing controls, and roles and responsibilities.</td>
</tr>
<tr>
<td>6</td>
<td>Organization of information security</td>
<td>6.1</td>
<td>Internal Organization</td>
<td>6.1.5</td>
<td>Confidentiality agreements</td>
<td>Requirements for confidentiality or non-disclosure agreements reflecting the organization’s needs for the protection of information should be identified and regularly reviewed.</td>
<td>Applicable</td>
<td>A policy stipulating requirements for the use of confidentiality and non-disclosure agreements does not currently exist and should be created.</td>
</tr>
<tr>
<td>7</td>
<td>Asset management</td>
<td>7.1</td>
<td>Responsibility for assets</td>
<td>7.1.3</td>
<td>Acceptable use of assets</td>
<td>Rules for the acceptable use of information and assets associated with information processing facilities should be identified, documented, and implemented.</td>
<td>Applicable</td>
<td>The University has an existing Acceptable Use Policy that meets the suggested guidelines.</td>
</tr>
<tr>
<td>7</td>
<td>Asset management</td>
<td>7.2</td>
<td>Information Classification</td>
<td>7.2.1</td>
<td>Classification guidelines</td>
<td>Information should be classified in terms of its value, legal requirements, sensitivity, and criticality to the organization.</td>
<td>Applicable</td>
<td>The University has existing Information Classification policies that meet the guidelines. These policies should be revised to reflect new standards.</td>
</tr>
<tr>
<td>8</td>
<td>Human resources security</td>
<td>8.2</td>
<td>During employment</td>
<td>8.2.2</td>
<td>Information security awareness, education, and training</td>
<td>All employees of the organization and, where relevant, contractors and third party users should receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.</td>
<td>Applicable</td>
<td>The University should create a formal Information Security Awareness, Education and Training program.</td>
</tr>
</tbody>
</table>
## Risk Assessment Example

<table>
<thead>
<tr>
<th>Clause #</th>
<th>Clause Title</th>
<th>Category #</th>
<th>Category Title</th>
<th>Control #</th>
<th>Control Title</th>
<th>Control Description Long</th>
<th>Applicability</th>
<th>Risk/Control Description</th>
<th>Risk Probability</th>
<th>Risk Impact</th>
<th>Risk Score</th>
<th>Risk Rank</th>
<th>Remediation Effort / Project Sizing</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Security Policy</td>
<td>5.1</td>
<td>Information Security Policy</td>
<td>5.1.1</td>
<td>Information Security Policy Document</td>
<td>An information security policy document should be approved by management, and published and communicated to all employees and relevant external parties.</td>
<td>Applicable</td>
<td>The policy should be amended to include the implementation guidance, including a definition of security, a statement of management intent and support, a framework (risk management) for implementing controls, and roles and responsibilities.</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>Medium</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Organization of information security</td>
<td>6.1</td>
<td>Internal Organization</td>
<td>6.1.5</td>
<td>Confidentiality agreements</td>
<td>Requirements for confidentiality or non-disclosure agreements reflecting the organization’s needs for the protection of information should be identified and regularly reviewed.</td>
<td>Applicable</td>
<td>A policy stipulating requirements for the use of confidentiality and non-disclosure agreements does not currently exist and should be created.</td>
<td>2</td>
<td>3</td>
<td>5</td>
<td>Medium</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Asset management</td>
<td>7.1</td>
<td>Responsibility for assets</td>
<td>7.1.3</td>
<td>Acceptable use of assets</td>
<td>Rules for the acceptable use of information and assets associated with information processing facilities should be identified, documented, and implemented.</td>
<td>Applicable</td>
<td>The University has an existing Acceptable Use Policy that meets the suggested guidelines.</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Asset management</td>
<td>7.2</td>
<td>Information Classification</td>
<td>7.2.1</td>
<td>Classification guidelines</td>
<td>Information should be classified in terms of its value, legal requirements, sensitivity, and criticality to the organization.</td>
<td>Applicable</td>
<td>The University has existing Information Classification policies that meet the guidelines. These policies should be revised to reflect new standards.</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>Small</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Human resources security</td>
<td>8.2</td>
<td>During employment</td>
<td>8.2.2</td>
<td>Information security awareness, education, and training</td>
<td>All employees of the organization and, where relevant, contractors and third party users should receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.</td>
<td>Applicable</td>
<td>The University should create a formal Information Security Awareness, Education and Training program.</td>
<td>3</td>
<td>4</td>
<td>7</td>
<td>Large</td>
<td></td>
</tr>
</tbody>
</table>
**Risk Assessment Examples**

### Risk Matrix

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Unlikely</th>
<th>Low</th>
<th>Medium</th>
<th>High</th>
<th>Occurs Regularly</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Very Low</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>2</td>
<td>Low</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>3</td>
<td>Medium</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
</tr>
<tr>
<td>4</td>
<td>High</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
</tr>
<tr>
<td>5</td>
<td>Very High</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
</tr>
</tbody>
</table>

### Project Sizing Matrix

<table>
<thead>
<tr>
<th>T-Shirt Sizing</th>
<th>Size</th>
<th>Relative Terms</th>
<th>Method 1 Hours</th>
<th>Method 1 Hours</th>
<th>Method 2 Est. Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>X-Small</td>
<td>&lt; 5 Days</td>
<td>Up to 1 week</td>
<td>11</td>
<td>40</td>
<td>11-40</td>
</tr>
<tr>
<td>Small</td>
<td>5-30 Days</td>
<td>Up to 6 weeks</td>
<td>41</td>
<td>240</td>
<td>41-250</td>
</tr>
<tr>
<td>Medium</td>
<td>31-60 Days</td>
<td>Up to 12 weeks</td>
<td>241</td>
<td>480</td>
<td>251-500</td>
</tr>
<tr>
<td>Large</td>
<td>61-120 Days</td>
<td>Up to 24 weeks</td>
<td>481</td>
<td>960</td>
<td>501-1000</td>
</tr>
<tr>
<td>X-Large</td>
<td>&gt;120 Days</td>
<td>Over 24 weeks</td>
<td>961</td>
<td>~</td>
<td>1000+</td>
</tr>
</tbody>
</table>
Risk Assessment – Prioritization Example

Risk Assessment - Prioritization

- Quick Hits
- Strategic
- Low Hanging Fruit
- Low Priority

Risk Mitigation vs. Effort Graph
Proposed Timeline

- **Aug**: ISAC Formation
- **Sep**: Program Approval
- **Oct**: Phase I Risk Assessment
- **Nov**: Risk Prioritization
- **Dec**: ITESC Approval
- **Jan**: Project Planning/Scoping
- **Feb**
- **Mar**
- **Apr**
Logistics

• Next meeting will be end of October
  » Location TBD
# ISAC Members

**Chair:** Leilani Lauger, *University Information Security Office*

<table>
<thead>
<tr>
<th>Department/Area</th>
<th>Primary</th>
<th>Alternate</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Academic Affairs</em></td>
<td>John Connolly</td>
<td>Francesca Pirovano</td>
</tr>
<tr>
<td><em>Advancement</em></td>
<td>Ron Iwanski</td>
<td></td>
</tr>
<tr>
<td><em>Finance</em></td>
<td>Cory O’Brien</td>
<td></td>
</tr>
<tr>
<td><em>Financial Assistance</em></td>
<td>Tad Verdun</td>
<td>Eric Weems</td>
</tr>
<tr>
<td><em>Human Resources</em></td>
<td>Carol Mc Cormack</td>
<td>Mike Capulong</td>
</tr>
<tr>
<td><em>ITS - Infrastructure</em></td>
<td>Dave Wieczorek</td>
<td>Jeff Apa</td>
</tr>
<tr>
<td><em>ITS - Applications</em></td>
<td>Cheryl Heckel</td>
<td>Charlotte Pullen</td>
</tr>
<tr>
<td><em>Registration &amp; Records</em></td>
<td>Diane Hullinger</td>
<td>Eric Pittenger</td>
</tr>
<tr>
<td><em>Risk Management</em></td>
<td>Stephen Ham</td>
<td>Sue Bodin</td>
</tr>
<tr>
<td><em>Student/Judicial Affairs</em></td>
<td>Jeremy Inabinet</td>
<td>Tim Love</td>
</tr>
<tr>
<td><em>Ex-Officio</em></td>
<td>Jim Sibenaller</td>
<td></td>
</tr>
</tbody>
</table>