1. Has your institution conducted an institution-wide IT risk assessment in the past 2 years?

<table>
<thead>
<tr>
<th>Response options</th>
<th>Count</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>19</td>
<td>33%</td>
</tr>
<tr>
<td>No</td>
<td>27</td>
<td>47%</td>
</tr>
<tr>
<td>In Progress</td>
<td>8</td>
<td>14%</td>
</tr>
<tr>
<td>Not Sure</td>
<td>3</td>
<td>5%</td>
</tr>
</tbody>
</table>

2. If your institution DID conduct an institution-wide IT risk assessment, did the results meet expectations?

<table>
<thead>
<tr>
<th>Response options</th>
<th>Count</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>9</td>
<td>25%</td>
</tr>
<tr>
<td>Somewhat</td>
<td>24</td>
<td>67%</td>
</tr>
<tr>
<td>No</td>
<td>3</td>
<td>8%</td>
</tr>
</tbody>
</table>

3. If your institution has NOT conducted an institution-wide IT risk assessment, why not?

<table>
<thead>
<tr>
<th>Response options</th>
<th>Count</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Institution ERM covers IT adequately</td>
<td>3</td>
<td>7%</td>
</tr>
<tr>
<td>Competing priorities</td>
<td>15</td>
<td>37%</td>
</tr>
<tr>
<td>Time commitment required</td>
<td>1</td>
<td>2%</td>
</tr>
<tr>
<td>Resources commitment required</td>
<td>17</td>
<td>41%</td>
</tr>
<tr>
<td>Other</td>
<td>5</td>
<td>12%</td>
</tr>
</tbody>
</table>
4. What IS or WAS the biggest obstacle for your institution when attempting to conduct an IT risk assessment?

Responses
Organization
$$$$$
Lack of clear process
Cost and timing
Expertise
Cost and timing
coordination
Resources
Preparing
Money and executives not thinking it was necessary
😊
Time and resources.
Apathy, I guess
Cooperation
Resources
Financial resources and selecting a M methodology
Buyin
Methodology to ensure we have caught all the appropriate risks
Resources to cover the large distributed campus.
Scope.
Resources
Compliance.
resources and support from directors
Scope
Time and expertise
n/a
Resource
Resources
Resources
Resources and skillset
Adequate breadth and broad IT management buy-in.
😊
Including all constituents
no framework
Commitment to respond to results
Identifying a good framework.
Politics
defining a simple process that delivered useful results
Lack of understanding
Fear of inadequate resources to respond
Determining which assessment approach will bring the right issues to light
Pace of change
5. Does your institution use any of these frameworks when managing IT risks?

<table>
<thead>
<tr>
<th>Framework</th>
<th>Count</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>ITIL</td>
<td>8</td>
<td>17%</td>
</tr>
<tr>
<td>ISO 27000</td>
<td>5</td>
<td>11%</td>
</tr>
<tr>
<td>NIST Cybersecurity</td>
<td>26</td>
<td>55%</td>
</tr>
<tr>
<td>COBIT</td>
<td>1</td>
<td>2%</td>
</tr>
<tr>
<td>Custom developed</td>
<td>3</td>
<td>6%</td>
</tr>
<tr>
<td>Other</td>
<td>4</td>
<td>9%</td>
</tr>
</tbody>
</table>

6. Does your institution have a definition of IT risk?

<table>
<thead>
<tr>
<th>Response</th>
<th>Count</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>8</td>
<td>19%</td>
</tr>
<tr>
<td>No</td>
<td>30</td>
<td>71%</td>
</tr>
<tr>
<td>Not sure</td>
<td>4</td>
<td>10%</td>
</tr>
</tbody>
</table>

7. What is more important when defining risk criteria for ratings?

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Count</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Potential impact of the risk</td>
<td>7</td>
<td>13%</td>
</tr>
<tr>
<td>Potential likelihood of the risk occurring</td>
<td>3</td>
<td>6%</td>
</tr>
<tr>
<td>Both are equally important</td>
<td>43</td>
<td>81%</td>
</tr>
</tbody>
</table>
8. As an IT professional, what is your biggest challenge protecting data?

Responses

- Identifying / Locating the data that needs to be protected.
- Finding out where it is
- Knowing where it is.
- Distributed departments
- Users
- User behavior
- Users
- Overview of which type of data exists
- Instructors using tools, often free ones, without our knowledge that have not been through our security review.
- Data silos
- Awareness
- Classification
- Endpoints
- Collaboration
- Ignorance on part of stewards
- Silos
- Excel
- Encryption consistency
- Not knowing where they all are
- Shadow IT
- Encryption and masking
- Sprawl
- Users
- Data classification
- Ease of use versus control/protection
- Correctly classifying data so we know how to best protect it.
- Educating the campus community
- Minimal control
- End user behaviors
- People - staff
- Not knowing where our inventory picture is like
- Shadow IT
- Managing ease of access vs. protecting
- Resources
- User indifference
9. As a Faculty member, what is your biggest challenge protecting data?

Responses

Don't know what options I have

Collaboration with external entities

Knowing where it is

Organizing it

Time consuming, poor solutions that I don't understand and that takes time from my actual work..

Easy to use tools

Why should I care?

Thinking about this question in the first place

Password management.

Known systems/tools to use for storage

Awareness and freedom to do research

Passwords

Why do I need to protect the data?

Ease of access

Knowing where to put it

Understanding what is sensitive

Tail wagging the dog

Lack of edict from provost

Email

Work-load

Protecting online test questions

Working around IT controls

Email

Not knowing what to protect

What's data protection?

Awareness

Regulatory and funding agency compliance

Deidentified data may be useless

Trusting IT guys

Passwords

Email

Lack of understanding categories of data
10. As a Staff member, what is your biggest challenge protecting data?

Responses
Faculty
User experience
Making it easy to do
No clear direction
Organizing unstructured data
Too hard
Access- who gets it, why, and how can it be used?
very different types of data, what goes where?
No idea what or how to do it
Time on task
Protecting Sensitive Information
Understanding my obligations as a non-IT person
Easy to use
Easy to change password
Lack of understanding data categories and what data to protect
too hard
Know how
faculty
Yes
Mixed data stores
Ir slows me down getting my job done.
Trying to balance security with service.
Ease of access to resources
Access
Understanding what data needs to be protected
Anywhere anytime any device access to data
Tools
Changing priorities
security expertise
Ease of use of technology
Post-it notes
Not having so many passwords
Understanding data risk
cumbersome
😊
too many hands in the pot
That's an IT problem.
Training
Knowing how to protect it
👩‍💻
11. What data point is the most important for developing an IT risk statement?

Response options

- Users share and store university data on personal tools, such as Gmail, Google Drive, and Dropbox
- Lack of awareness regarding tools to scrub data from devices, drives, and systems
- Email contains years worth of confidential data
- Employees sharing public and personal info via social media such as Facebook, Twitter, etc.
- Faculty suggested a central file system

Rank

1st
2nd
3rd
4th
5th
6th

Responses

22
22
22
22
22
22

12. How would you write the IT risk statement for the University community using and sharing data?

Responses

0

13. Which aspect of potential impact is most important to rating risk?

Response options

- Compliance = ability to comply with applicable laws, regulations, and/or contracts
- Reputation = ability to develop and maintain strong relationships with constituents
- Operations = ability to perform teaching, research, and administrative functions
- Finances = ability to meet financial obligations

Rank

1st
2nd
3rd
4th
5th

Responses

28
28
28
28
28

14. Which aspect of potential likelihood is most important to rating risk?

Response options

- Both inherent and residual likelihood
- The residual likelihood given the existence and application of processes
- The inherent likelihood of that risk occurring with no regard to processes

Rank

1st
2nd
3rd

Responses

23
23
23
15. How would you rank these risks based on their potential impact to your institution (highest to lowest)?

<table>
<thead>
<tr>
<th>Response options</th>
<th>Rank</th>
</tr>
</thead>
<tbody>
<tr>
<td>Educating community on cyber threats and protections</td>
<td>1st</td>
</tr>
<tr>
<td>Detecting, responding, and recovering from incidents</td>
<td>2nd</td>
</tr>
<tr>
<td>Managing devices to University standards and practices</td>
<td>3rd</td>
</tr>
<tr>
<td>Securing research data to meet external requirements</td>
<td>4th</td>
</tr>
</tbody>
</table>

16. How would you rank these risks based on their potential likelihood of occurring at your institution (highest to lowest)?

<table>
<thead>
<tr>
<th>Response options</th>
<th>Rank</th>
</tr>
</thead>
<tbody>
<tr>
<td>Educating community on cyber threats and protections</td>
<td>1st</td>
</tr>
<tr>
<td>Managing devices to University standards and practices</td>
<td>2nd</td>
</tr>
<tr>
<td>Detecting, responding, and recovering from incidents</td>
<td>3rd</td>
</tr>
<tr>
<td>Securing research data to meet external requirements</td>
<td>4th</td>
</tr>
</tbody>
</table>