The IT team is composed of security professionals who perform audits of units and processes at UM-Ann Arbor, Michigan Medicine, UM-Flint, and UM-Dearborn. Audit objectives align with IT strategic risks. The team audits things like:

- Authentication and authorization
- Physical security
- Environmental Conditions
- Complex applications
- Cloud applications and third-parties
- Network security
- Sensitive data
- Inventory of hardware and software

### Top IT Audit Findings

<table>
<thead>
<tr>
<th>Findings</th>
<th>Recommendations to Improve Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Weak access control management</td>
<td>• Periodically review whether employees and other who have access to systems, data, and buildings still need it</td>
</tr>
<tr>
<td>• Inadequate oversight of cloud-based software and a lack of Data Protection Agreements</td>
<td></td>
</tr>
<tr>
<td>• Poor management of third-party risks</td>
<td>• Set up Sponsored Affiliates with end-dates and know why you are sponsoring, and review periodically</td>
</tr>
<tr>
<td>Inability to track sensitive data</td>
<td>• Access – onboarding and offboarding</td>
</tr>
<tr>
<td>Inadequate patch management and vulnerability management programs, and weak configuration management</td>
<td>• Obtain security assessment on any third-party system and vendors</td>
</tr>
<tr>
<td>• Lack of security awareness of front line staff</td>
<td>• Know where your sensitive data is and what applications access that data</td>
</tr>
<tr>
<td>• Lack of knowledge of newly developed data standards</td>
<td>• Perform on-going vulnerability management</td>
</tr>
<tr>
<td>Incomplete RECON treatment plans</td>
<td>• Maintain a culture of security awareness</td>
</tr>
<tr>
<td>Lack of hardware and software inventory</td>
<td>• Provide periodic security updates</td>
</tr>
</tbody>
</table>

### IT Audit Criteria

The IT team uses widely accepted criteria for their review and evaluation process. Foremost among these are:

- SPG 601.12, Institutional Data Resource Policy
- SPG 601.27, Information Security
- SPG 601.07, Responsible Use of Information Resources
- Data Security Standards
- CIS foundational controls
- NIST 800-181
- NIST 800-53
- Department policies
- MM policy and procedures

### Links to Useful Information

We all work together to protect your personal information and U-M’s data and systems. Here are a few links so you can learn more about IT security:

- General Information Technology Policies
- Security Unit Liaison Directory
- Sensitive Data Guide
- Phishing & Suspicious Email
- Protect Your Unit's IT
- Secure Your Devices

Contact the Audit Services IT team at: uauditsITauditors@umich.edu