BAKER TILLY AND ACUA WEBINAR

IT risk assessment – a practical holistic approach

bakertilly
now, for tomorrow.

ACUA
ASSOCIATION OF COLLEGE & UNIVERSITY AUDITORS
Advancing Auditing in Higher Education

The information provided here is of a general nature and is not intended to address the specific circumstances of any individual or entity. In specific circumstances, the services of a professional should be sought. Tax information, if any, contained in this communication was not intended or written to be used by any person for the purpose of avoiding penalties, nor should such information be construed as an opinion upon which any person may rely. The intended recipients of this communication and any attachments are not subject to any limitation on the disclosure of the tax treatment or tax structure of any transaction or matter that is the subject of this communication and any attachments. Baker Tilly Virchow Krause, LLP trading as Baker Tilly is a member of the global network of Baker Tilly International Ltd., the members of which are separate and independent legal entities. © 2019 Baker Tilly Virchow Krause, LLP

bakertilly
now, for tomorrow.

INTRODUCTIONS

Today's webinar moderator

Amy Hughes
ACUA Distance Learning Director
Director of Internal Audit
Michigan Technological University

ACUA
ASSOCIATION OF COLLEGE & UNIVERSITY AUDITORS
Advancing Auditing in Higher Education

INTRODUCTIONS

GoToWebinar guide

- Everyone is muted to avoid background noise.
- Asking questions: Ask questions by clicking on the Questions panel on the right side of your screen, type your question and submit to all organizers.
- If disconnected: If audio is disconnected, click on the Audio panel on the right side of your screen, or refer back to your e-mail for the dial-in number.
- Support #: If you have any technical problems, call GoToWebinar support at 1 888 646 0014.
- Today’s webinar will be recorded.

INTRODUCTIONS

Today's speakers

Du'Neika Easley
Assistant VP of Internal Audit
University of Richmond
deasley@richmond.edu

Mike Cullen
Senior Manager
Baker Tilly
mike.cullen@bakertilly.com

Jimmy Edmundson
Manager
Baker Tilly
jimmy.edmundson@bakertilly.com

Haley Widdowson
Senior Consultant
Baker Tilly
haley.widdowson@bakertilly.com

LEARNING OBJECTIVES

After today’s webinar, you will be able to:

- Understand the current information technology landscape and key trends in higher education
- Identify key risk areas impacting the confidentiality, integrity, and availability of institutional information/data and systems
- Apply methods for conducting IT risk assessments and evaluating the effectiveness of IT risk management activities

bakertilly
now, for tomorrow.

Purposes

IT audit

- Internal Audit driven and focused
- Create IT audit universe
- Identify IT audit projects

IT management

- IT management driven and focused
- Identify blind spots for regulatory and control gaps
- Determine resource allocations
- Guide project decisions

IT risk management

- Enterprise IT risk driven and focused
- IA and IT partner together
- Best of both worlds

POLLING QUESTION #1

What do you believe is the top IT risk facing your institution?

A. Data or system loss

B. Criminal hackers attacking

C. Trusted insiders acting against the institution

D. Do not know or other

bakertilly
now, for tomorrow.

Common challenges, trends

- ✓ Distributed IT
- ✓ Academic, research, administrative computing
- ✓ Data classification and flows
- ✓ Cybersecurity
- ✓ Myriad regulatory requirements
- ✓ Unique business processes
- ✓ Distributed IT purchasing power
- ✓ Cloud vs. on-premises
- ✓ Awareness

```
15:53  .
15:53  ..
2015   bin -> usr/bin
09:31  boot
15:50  dev
09:32  etc
p 15:52  home
ep 2015  lib -> usr/lib
ep 2015  lib64 -> usr/lib
ul 10:01  lost+found
Aug 22:45  mnt
Sep 2015  opt
Sep 15:52  private -> /home/en
Sep 08:15  proc
Aug 15:37  root
Sep 15:50  run
. Sep 2015  sbin -> usr/bin
1. Sep 2015  srv
1. Sep 15:51  sys
12. Sep 15:45  tmp
23. Aug 15:39  usr
Jul 10:25  var
21. Sep 15:5
```

now, for tomorrow.

POLLING QUESTION #2

Does your institution have an established IT risk assessment program?

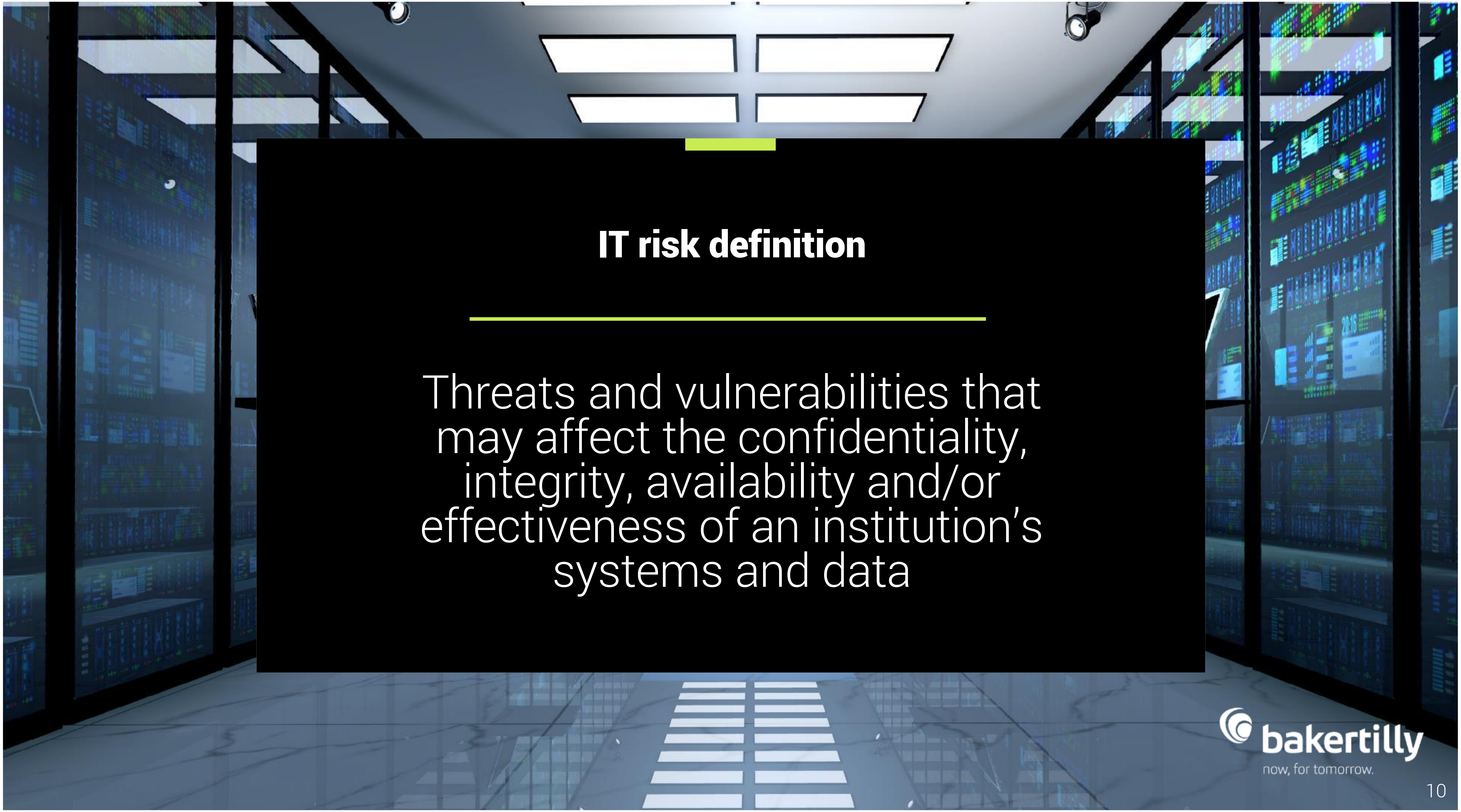
A. Yes

B. No, but starting soon

C. No

D. Do not know or other

bakertilly
now, for tomorrow.



IT risk definition

Threats and vulnerabilities that may affect the confidentiality, integrity, availability and/or effectiveness of an institution’s systems and data

IT risk areas

- Academic computing
- Application development
- Cloud/vendor systems
- Computer operations
- Data management
- Device management
- End-user support
- Funding
- Information security and privacy
- Infrastructure – network
- Infrastructure – servers/storage
- IT governance
- New enterprise systems
- People resources
- Physical/environmental controls
- Project management
- Research computing
- System availability
- Technology choice
- Vendor management

POLLING QUESTION #3

Who leads or owns the IT risk assessment program at your institution?

bakertilly
now, for tomorrow.

A. CIO and central IT

B. Internal Audit

C. Enterprise risk management

D. Do not know or other

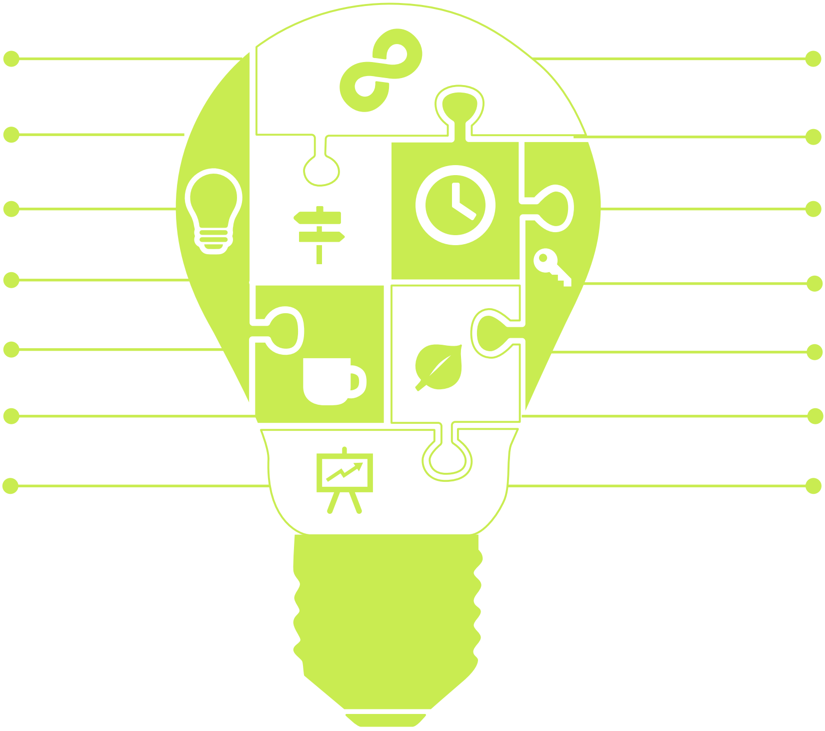
Approach for institution-wide IT risk assessment

1. Project planning
2. Information gathering
3. Analysis
4. Reporting
5. IT audit schedule development

Information gathering

- ✓ Identify stakeholders
- ✓ Determine gathering methods (e.g., survey, interview)
- ✓ Determine timing

Stakeholders



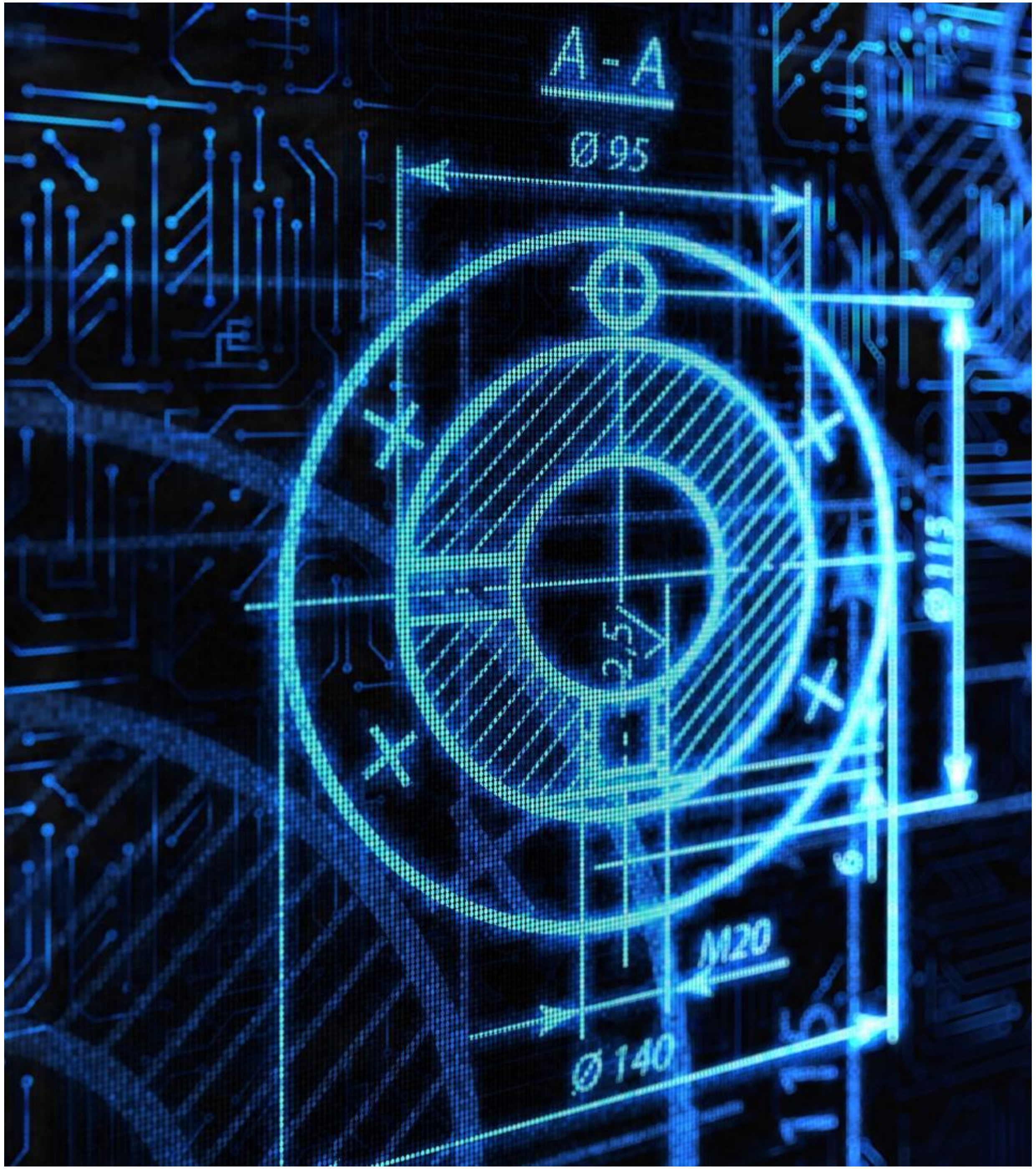
- Central IT function
- Distributed academic IT functions
- Chief business officer
- Provost(s) / Deans
- General counsel
- Compliance
- Board
- Research
- Residential life (housing, dining)
- Campus safety
- Athletics
- Library
- Facilities
- Institutional research

Analysis

- ✓ Synthesize IT risks
- ✓ Determine inherent risk
- ✓ Identify risk management activities
- ✓ Determine residual risk

IT risk register example

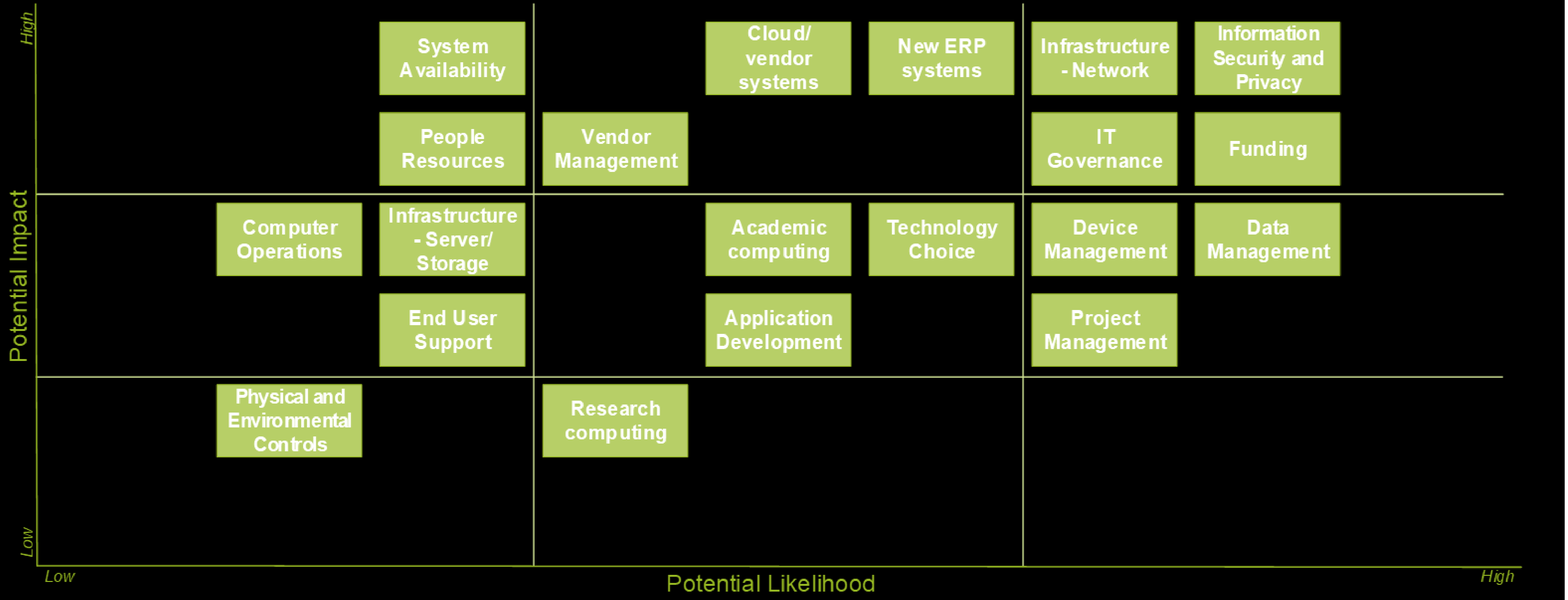
IT risk area	IT risk statement	Current state	IT risk mgmt. activities
Information Security and Privacy The policies, practices, and tools implemented on the University's systems and data to maintain confidentiality of information.	Users activities, of any kind (e.g., accidental, malicious), do not follow university policies or legal/regulatory requirements regarding the use of systems and data resulting in a security incident.	– Training is strongly encouraged but optional for faculty – CISO is updating policies and procedures – Compliance requirements are increasing for higher education institutions	– Security Awareness Training is mandatory for staff – Data Security Policy references responsibilities due to requirements, including FERPA – CISO sends out a monthly security topic email



Reporting

- ✓ Develop heat map
- ✓ Document risk register
- ✓ Identify control gaps and recommendations (optional)

Heat map



System Availability

Cloud/ vendor systems

New ERP systems

Infrastructure - Network

Information Security and Privacy

People Resources

Vendor Management

IT Governance

Funding

Computer Operations

Infrastructure - Server/ Storage

Academic computing

Technology Choice

Device Management

Data Management

End User Support

Application Development

Project Management

Physical and Environmental Controls

Research computing

IT audit plan

- ✓ Identify assurance and advisory projects aligned with top risks
- ✓ Align schedule with IT plans/projects
- ✓ Map out timing of audit projects (e.g., multi-year audit calendar)

Note: Always allow for changes to the IT audit plan on at least an annual basis, as IT is a dynamic area where risks are continually changing.

Example IT projects

Audit

- Incident response (FY20)
- Network security (FY20)
- IT governance (FY21)
- Mobile device management (FY22)

Advisory

- IT funding (FY20)
- Data management (FY21)
- System implementation (FY21)
- Vendor management (FY22)

POLLING QUESTION #4

After viewing this webinar, when will your institution undertake a new or refreshed IT risk assessment?

A. In the next 12 months

B. In the next 13 to 24 months

C. Never

D. Do not know or other

bakertilly
now, for tomorrow.

THANK YOU

Additional resources

- EDUCAUSE IT Risk Register
- ISACA COBIT 5 for Risk
- NIST Cybersecurity Framework
- NIST Special Publications 800 series

bakertilly
now, for tomorrow.

THANK YOU

Connect with us

Amy Hughes
ACUA Distance Learning Director
Director of Internal Audit
Michigan Technological University

ACUA
ASSOCIATION OF COLLEGE & UNIVERSITY AUDITORS
Advancing Auditing in Higher Education

ACUA
WEBINARS

Join us for our upcoming webinar.