Board of Visitors
Audit, Compliance, and Risk Committee
March 3, 2022

March 2022

Audit, Compliance, and Risk Committee Meeting Agenda

- Remarks by Dr. Lateef, Committee Chair
- Overview of IT Audits: Co-sourcing with EY
- Process for refreshing/updating the risk-based audit plan
- Written Reports

Sean Jackson
Managing Director, Government and Public Sector; Education, EY

Ariel Johnson-Peredo, Senior Manager, EY

Overview of IT Audits: Co-sourcing with EY

UNIVERSITY of VIRGINIA | Office of Audit and Compliance
Audit Department

EY

IT Audits: Co-Sourcing with EY

The EY IT Audit Team will plan, design, and execute 8 IT audits for FY22:

1. KPMG 2019 Cyber Maturity Follow Up
2. Distributed IT Systems Management (DISM) – School of Nursing (SON)
3. Distributed IT Systems Management (DISM) – Batten School
4. Distributed IT Systems Management (DISM) – School of Medicine (SOM)
5. Distributed IT Systems Management (DISM) – School of Data Science
6. Research Data Security
7. Academic Records (not started)
8. Mandiant Ransomware Readiness Follow Up (not started)

Additional support activities will include:

- Support of the risk refresh for the FY23 audit plan
- Recommendations to enhance existing IT internal audit activities
- Project management and coordination with key UVA stakeholders and contacts

FY2022 IT Audits Timeline

JANUARY | FEBRUARY | MARCH | APRIL | MAY | JUNE

1. Cybermaturity Follow-Up
Estimated Completion: February 2022

Assess UVA's implementation of recommendations made in KPMG's 2019 Cyber Maturity assessment and Incident Response review (covers both Academic Division and UVA Health IT)

On Track

2. DISM School Nursing
Estimated Completion: February 2022

Assess the overall management of distributed informations system and adherence to to University policy controls within the related IT security frameworks (i.e ISO 27000 2013 series).

On Track

3. DISM - Batten School
Estimated Completion: February 2022

Assess the overall management of distributed informations system and adherence to University policy controls within the related IT security frameworks (i.e ISO 27000 2013 series).

On Track

4. DISM School of Medicine
Estimated Completion: March 2022

Assess the overall management of distributed informations system and adherence to University policy controls within the related IT security frameworks (i.e ISO 27000 2013 series).

On Track

5. DISM -School of Data Science
Estimated Completion: April 2022

Assess the overall management of distributed informations system and adherence to to University policy controls within the related IT security frameworks (i.e ISO 27000 2013 series).

On Track

6. Research Data Security
Estimated Completion: April 2022

Assess the overall protection of data at a specific set of schools, labs, instituites or academic divisions to determine if research specific data beyond CUI and other safeguarded environments is in adherence with University policy (i.e. ISO 27000 2013 series)

On Track

7. Academic Records
Estimated Completion: April 2022

To assess the Academic Records processes and controls to evaluate the university's ability to obtain, generate, and use relevant and quality information to support the functioning of internal control.

Not Started

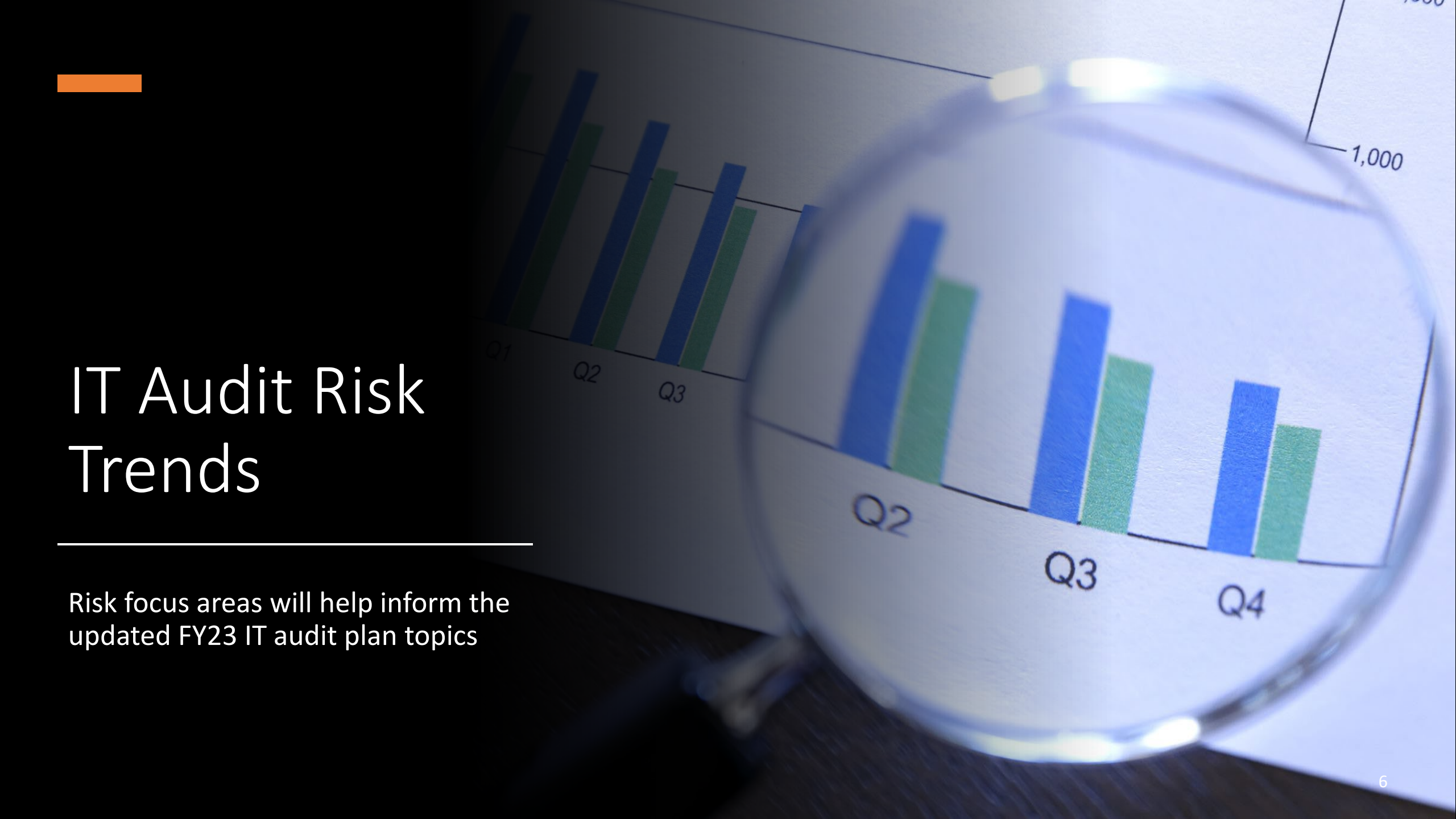
8. Ransomware Readiness
Estimated Completion: April 2022

Assess follow up of recommendations and remediation following the work completed by Mandiant.

Not Started

IT Audit Risk Trends

Risk focus areas will help inform the updated FY23 IT audit plan topics



Cybersecurity

UVA has two IT environments: UVA Health and the Academic divisions. While both environments proactively manage data, technology, and information risks, UVA's senior leaders and Board of Visitors should maintain awareness of cyber threats and UVA's preparedness as part of their oversight of risk management.

Cyber Focus Area	Description
Cyber Attacks Against Higher Education Institutions	Rise in complex security attacks – exponential increase in ransomware, phishing, privileged access credential abuse and endpoint security attacks (ex. Howard University Ransomware attack in September of 2021)
Maturity of Incident Response Program	Focus on simplification and automation of key cyber activities, improving the mean time to detect and respond to a cyber incident and assuring the security of trusted third parties
Cyber maturity frameworks such as CMMC (Cybersecurity Maturity Model Certification)	A regulatory push for minimum cyber standards with regulatory compliance continue to be the single biggest main driver for cyber spend by organizations. CMMC currently has five (5) levels and it is significant to highlight that it will have direct impacts to federally funded research, development centers, and university affiliated research centers. This will be significant for research that is currently conducted outside of more well-controlled environments such as CUI (Control Unclassified Information).
Increased Digital Adoption as a result of COVID-19	The increased digital response as a result of the pandemic has caused organizations to focus on cyber specific controls as a secondary step in the process only after they have adopting new technologies to increase the digital response to the new remote/hybrid way or working.

Data Integrity

Large organizations increasingly rely on increasingly complex system to support decisions and manage core processes.

Data Focus Area	Description
Data Governance	Digital dependency and the need for data driven decision making require data be carefully stewarded throughout its lifecycle.
Data Storage	Data storage monitoring and maintenance is important particularly in the following areas: 1. Data quality 2. Data volume 3. Complexity of transformation rules
Data Reconciliation	Data reconciliation and periodic review of the completeness and accuracy of the data is integral so that data can be relied upon for issue resolution management and root cause analysis.
Increased Digital Adoption as a result of COVID-19	The increased digital response as a result of the pandemic has caused organizations to focus on cyber specific controls as a secondary step in the process only after they have adopting new technologies to increase the digital response to the new remote/hybrid way or working.

Enterprise-Wide Systems Implementation Risk

Implementation of enterprise systems (e.g. Workday Financials) have certain inherent risks that can be assessed in follow-on IT audits

Systems Implementation Risk Areas	Risk Description
Data Conversion	Without adequate controls and procedures in place, historical and master data transferred to the new system may not be complete and/or accurate, and data from the old system may not be properly cleansed prior to conversion.
Cutover	Without adequate controls and procedures in place, the risk exists that appropriate cutover procedures are not developed which may lead to an inappropriate go live decision.
Security	Without adequate controls and procedures in place, the risk exists that security roles and separation of critical transactions and fraud risks may exist where employees may be able to process unauthorized and alter transactions. The security roles within the new module / applications should be clearly defined.
Hypercare	Without adequate controls and procedures in place, users may be granted access for extended timeframes or changes may not follow the appropriate change management process.
Interfaces	Without the adequate controls and procedures in place, data transferring between key source systems may not be complete and accurate. Additionally, the users with the ability to maintain and monitor key business process interfaces must be restricted to the appropriate personnel as to maintain the integrity of the data.

Carolyn Saint

Chief Audit Executive

Process for refreshing/updating the risk-based audit plan

Audit Plan Refresh Approach

FY2022-2024

Benchmark

Higher ed and healthcare risk topics and trends

- *Ivy Plus
- *ACUA
- *Gartner
- *Global audit firms

Stakeholder Meetings

Understand organizational projects and priorities

Validate or change audit topics or timing

Senior leadership

Review and advise on proposed FY23-FY24 audit plan

Audit Committee & BOV

Input on plan topics through ACR committee chair

Approve refreshed FY23-FY24 audit plan

February 2022-June 2022