UNIVERSITY OF VIRGINIA
BOARD OF VISITORS

Meeting of the Audit, Compliance, and Risk Committee

June 2, 2022

AUDIT, COMPLIANCE, AND RISK COMMITTEE

Thursday, June 2, 2022
1:30 – 2:15 p.m.
Board Room, The Rotunda

Committee Members:

Babur B. Lateef, M.D., Chair
Thomas A. DePasquale, Vice Chair
Robert M. Blue
Mark T. Bowles
L.D. Britt, M.D.
Barbara J. Fried
Louis S. Haddad
The Honorable L.F. Payne
Whittington W. Clement, Ex-officio
Adelaide Wilcox King, Faculty Consulting Member

AGENDA

UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY

BOARD MEETING: June 2, 2022

COMMITTEE: Audit, Compliance, and Risk

AGENDA ITEM: I. Remarks by the Committee Chair

ACTION REQUIRED: None

BACKGROUND: Dr. Babur Lateef, the Committee Chair, will open the meeting, welcome guests, and provide an overview of the agenda.

UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY

BOARD MEETING: June 2, 2022

COMMITTEE: Audit, Compliance, and Risk

AGENDA ITEM: II.A. Review and Approval of Two-Year, Risk-Based Internal Audit Plan Topics and Priorities

BACKGROUND: A refreshed internal audit plan is discussed with and approved annually by the Audit, Compliance, and Risk Committee. The audit plan is developed based on assessed risks to achievement of the University's objectives, stakeholder input, benchmarking with peers, macro-environmental factors, auditors' knowledge of UVA systems and processes, and resource availability. Timing of audits is influenced by institutional projects underway, unforeseeable events (see: pandemic), and available resources.

Within each audit topic selected, the audit will assess elements of the following:

UVA Health Division Two Year Audit Plan

FY2023 UVA Health Audit Topic	Scope
Joint Commission (JC) Readiness: Performance Improvement Chapter Updates – Gap Analysis	Quality program activities specific to the revised Performance Improvement Chapter in the JC Survey Manual. Identify gaps for action to support JC Survey readiness
Graduate Medical Education (GME) Program	Internal controls over the key processes for GME programs, such as accuracy of GME data reported

FY2023 UVA Health Audit Topic	Scope
	on Medicare Cost Reports, validation of rotation schedules, and time and effort reports
Charge Capture – Renal Services	Internal controls over capture of charges for renal services, including interface controls between clinical system and Epic hospital billing
Charge Capture – Interventional Radiology	Same as above-for Interventional Radiology
Coding Compliance: Implantable Cardiac Devices (ICD) Procedure with Separately Billed ECG	Review medical record documentation for cardiac pacemaker or ICD procedure to validate support for appending modifier 59 to the ECG
Physician Transactions (Purchased Services)	Compliance with contract terms and UVA policies, such as contract reviews/approvals
Case Management	Case management processes focused on inpatient throughput and preventing excess length of stay
UVACH: Controlled Substances Compliance	Compliance with controlled substances DEA regulations at one or more of the UVACH facilities
Capture of Complications and Comorbidities (CC) and Major Complications and Comorbidities (MCC)	Evaluate capture of CC/MCC, identify root causes of any gaps, and assess financial impact
Contract Management	Controls over contract development, approval, and management
Timekeeping/Payroll	Controls over timekeeping and payroll accuracy. Potential focus on high-risk areas such as premium pay, traveler payroll
UVACH: IRS 501(r) Compliance	Compliance with IRS 501(r) rules applicable to non-profit hospitals, such as community needs analyses and plans, financial assistance program elements, publication and required signage, etc.
Cloud-based and Software as a Service (SaaS) Vendor review (IT Audit)	Controls around the onboarding, setup, and establishment of key configurations for Cloud and SaaS based vendors
HIPAA Security Risk Assessment Follow-up (IT Audit)	Review results of periodic HIPAA security risk assessment and determine if any identified gaps were sufficiently addressed
Epic User Role Change Review (IT Audit)	Processes and controls followed when a user changes roles within the UVA Medical Center and determine how that user's access gets updated/changed or revoked accordingly
IT Disaster Recovery (IT Audit)	The design and operating effectiveness of the controls established for recovering data and systems during and after an event
FY2024 UVA Health Audit Topic	**Scope**
Financial Assistance/ Financial Counseling	Patient access processes for helping patients without insurance find resources to help them pay medical costs

FY2024 UVA Health Audit Topic	Scope
Insurance Verification/ Validation	Controls for validating patient insurance prior to providing services
Balance Billing (No Surprises Act)	Compliance with new regulatory requirement around specific services provided to patients with out-of-network coverage
Late Charges	Compliance with UVA Health late charge policy and any associated impact on timely billing
Opioid Stewardship Program	Assess maturity of the Opioid Stewardship program
Non-patient Receivables	Controls over collecting revenue for services provided to other organizations that are directly billed to that organization
Price Transparency	Compliance with this new regulatory requirement to publish standard fees and provide estimates
Provider Credentialing	Evaluate provider credentialing process for compliance with policy and timeliness
Practitioner Peer Review	Assess conformance of peer review process to policy
Event Reporting (Be Safe)	Processes and controls in place for event reporting, analysis, and response (adverse events, near misses and unsafe conditions)
Hospice Program	Processes in place for assuring compliance with the unique regulatory requirements surrounding hospice programs and hospice referrals
Information Blocking Rule	Compliance around this new HHS rule prohibiting any practice likely to interfere with, prevent, or discourage access, exchange, or use of electronic health information (EHI)
UVACH: Pharmacy 340B	Compliance with 340B regulatory requirements and best practices for maximizing realized savings
Data Loss Prevention (IT Audit)	The mechanisms and processes by which UVA Health protects sensitive or confidential data from being sent externally to an inappropriate party or in an unsecure manner
Data Warehouse Controls (IT Audit)	Design and effectiveness of controls over the access, change and operational controls for the UVA Health data warehouse
Ransomware Assessment Follow Up (IT Audit)	Determine if the recommendations of the two 2022 Mandiant Purple Team ransomware reports for both the Academic and Health System divisions have been implemented

UVA Academic Division Two Year Audit Plan

FY2023 UVA Academic Division Audit Topic	Scope
Research Data Security (In progress from prior year plan)	Security over IT systems and applications in selected labs
Safety and Security (In progress from prior year plan)	Follow up on implementation status of consultant's safety recommendations (in progress)
International Operations (In progress from prior year plan)	Phase 1: Develop inventory of international activities to determine eventual audit scope. Phase 2: Assess higher priority international activities identified in Phase 1.
Institutional Data (In progress from prior year plan)	Ensure data used in external reporting conveys quality information (complete, accurate, timely, available) for ratings and rankings. (COSO Principle 13)
Student Information System (SIS) Academic Records and IT Controls (In progress from prior year plan—previously titled Academic Records and Policies)	Evaluate design and effectiveness of controls over the Student Information System, with a focus on the accuracy and completeness of the source of record for maintaining degree progress data, grade submissions and changes, course substitutions and/or degree requirement exceptions.
CARES Compliance – Higher Education Emergency Relief Fund (HEERF I, II, III) – Part 2 (FY23)	Evaluate design and effectiveness of controls and processes related to HEERF funds data collection, use, accounting, and reporting.
Student Financial Aid: UVA Wise	Follow-up on APA findings at UVA Wise.
Research - Post Award Administration	Assess effectiveness of post-award controls for selected sponsored awards to ensure compliance with sponsor requirements, regulations, and University policy.
School-Level Audit (Pilot)	Develop and pilot an audit program to assess effectiveness of key unit/school level controls and processes.
Workday Financials Controls Validation	Assess the effectiveness of key financial and access controls post Workday Financials go-live.

FY2023 UVA Academic Division Audit Topic	Scope
Workday Benefits Administration	Follow-up on KPMG recommendations for the UVA Health Plan.
Cloud and SaaS Based Vendor Review (Salesforce Specific Focus)	Evaluate controls over the Salesforce Orgs across UVA to determine • Appropriate IT onboarding, vetting, and periodic access review has been completed and maintained • Salesforce instances have been appropriately configured for a specific unit, department, or school based on data security requirements.
Construction Projects • Hotel and Conference Center (In progress from prior year plan) • Physics Building Renovation (In progress from prior year plan)	Using an outside expert in construction project management accounting, perform procedures relevant to phases of specified construction projects.
University Police Department	Scope to be refined based on results of 2021 CALEA accreditation report.
Ransomware Assessment Follow Up (IT Audit)	Determine if the recommendations of the two 2022 Mandiant Purple Team ransomware reports for both the Academic and Health System divisions have been implemented.

FY2024 UVA Academic Division Audit Topic	Scope
Environmental, Social, and Governance (ESG) Reporting	Perform an inventory to gather data on current ESG reporting, metrics, and data analytics distributed across the University.
ESG Reporting: Sustainability	Assess controls ensuring sustainability reporting captures relevant information and maintains quality through the process, culminating in the preparation of reliable sustainability reports. Quality information is accessible, correct, current, protected, retained, sufficient, timely, valid, and verifiable per the COSO Framework. (COSO Principle 13)
Hazardous Waste Management	Ensure UVA manages hazardous waste safely and in accordance with laws and regulations.

FY2024 UVA Academic Division Audit Topic	Scope
Student Financial Services	Evaluate design and effectiveness of controls over the accuracy and timeliness of student billing and accounts receivable.
NCAA Compliance: Financial Aid for Student-Athletes	Assess UVA Athletics Department Compliance Office's oversight of student-athlete Financial Aid considering anticipated impacts of the NCAA Name, Image, and Likeness (NIL) policy.
School-Level Audit (3 Schools)	Assess effectiveness of key unit/school level controls and processes.
Payroll	Evaluate controls over Workday payroll user access, identification of employees working out of state/country, and untimely terminations resulting in overpayments.
Software Asset Management	Evaluate software asset management practices including policies, governance, inventory process, lifecycle management, and license compliance.
Identity and Access Management – Request Based Access	Assess the design and effectiveness of controls over request-based access for selected IT applications.
Data Privacy	Assess controls enabling compliance with UVA'S publicly posted Privacy Policy | The University of Virginia
Research Data Governance Follow Up	Follow up on recommendations from the research data governance assessment in 2020.
Post Implementation Review (Pre-Award Module)	Assess whether the implementation of the new Huron module achieved the scope and benefits promised.

ACTION REQUIRED: Approval by the Audit, Compliance, and Risk Committee and by the Board of Visitors

AUDIT DEPARTMENT FY2023-FY2024 AUDIT PLAN

RESOLVED, the Audit Department FY 2023-FY 2024 Audit Plan is approved as recommended by the Audit, Compliance, and Risk Committee.

UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY

BOARD MEETING: June 2, 2022

COMMITTEE: Audit, Compliance, and Risk

AGENDA ITEM: II.B. Auditor of Public Accounts FY2021-2022 Audit Entrance Meeting

ACTION REQUIRED: None

BACKGROUND: The Auditor of Public Accounts of the Commonwealth conducts an annual audit of the University and the Medical Center and reports findings to the Board of Visitors. Mr. Augie Maurelli, Associate Vice President for Financial Operations, will introduce Mr. David Rasnic, who will discuss with the committee the FY 2021-2022 audit.

David Rasnic is the Director of Higher Education Programs for the Virginia Auditor of Public Accounts. His current responsibilities include management of the office's Higher Education Programs Specialty Team and project management oversight for various agencies and institutions of the Commonwealth. He also coordinates required federal audits at the Commonwealth's institutions of higher education and NCAA Agreed Upon Procedures engagements. He is a graduate of Virginia Tech and is a CPA and CISA.

UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY

BOARD MEETING: June 2, 2022

COMMITTEE: Audit, Compliance, and Risk

AGENDA ITEM: II.C. Enterprise Risk Management (ERM) Program Report

BACKGROUND AND DISCUSSION: Mr. Maurelli will brief the committee on the work of the Academic Division's Enterprise Risk Management efforts, including the report by the Fiscal Sustainability Risk Working Group, charged with evaluating risks to the Academic Division's financial security and sustainability. The full report is available in the Appendix.

The Enterprise Risk Management program for the academic division has recently completed work, using a value-based approach, evaluating financial security and sustainability. While the University's sturdy balance sheet, strong governance, and diversified revenue mix contribute to the fiscal sustainability of the institution, the working group did evaluate and score 35 major financial risks. Five financial risks (capital expenditures and inflation; breach of sensitive financial data; governmental tax policy; regulations impacting athletics revenues; vendor payments) were closely reviewed. The Working Group found that the responsible business units had developed mitigation procedures that substantially reduce the likelihood of adverse impact on operations. As such, UVA's Academic Division is in a solid position with respect to almost all risks.

Of course, any ERM evaluation is a "snapshot in time" based on an appraisal of present circumstances in a fast-changing environment. We intend to engage in ongoing monitoring to ensure that risk assessments and mitigation strategies are continually updated to reflect changing circumstances.

The analysis and inputs on this effort will be additive as the next working group, launched in April 2022, addresses UVA's future state of work and all that entails from a human capital perspective. In addition, the Risk Management Network has broadened its access to better align and inform both UVA Wise and UVA Medical Center.

The following schedule of reports to the ACR Committee from the risk working groups is contemplated:

Risk Working Group	Report Schedule
Future of Work	Fall 2022
Safety and Security	Spring 2023

UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY

BOARD MEETING: June 2, 2022

COMMITTEE: Audit, Compliance, and Risk

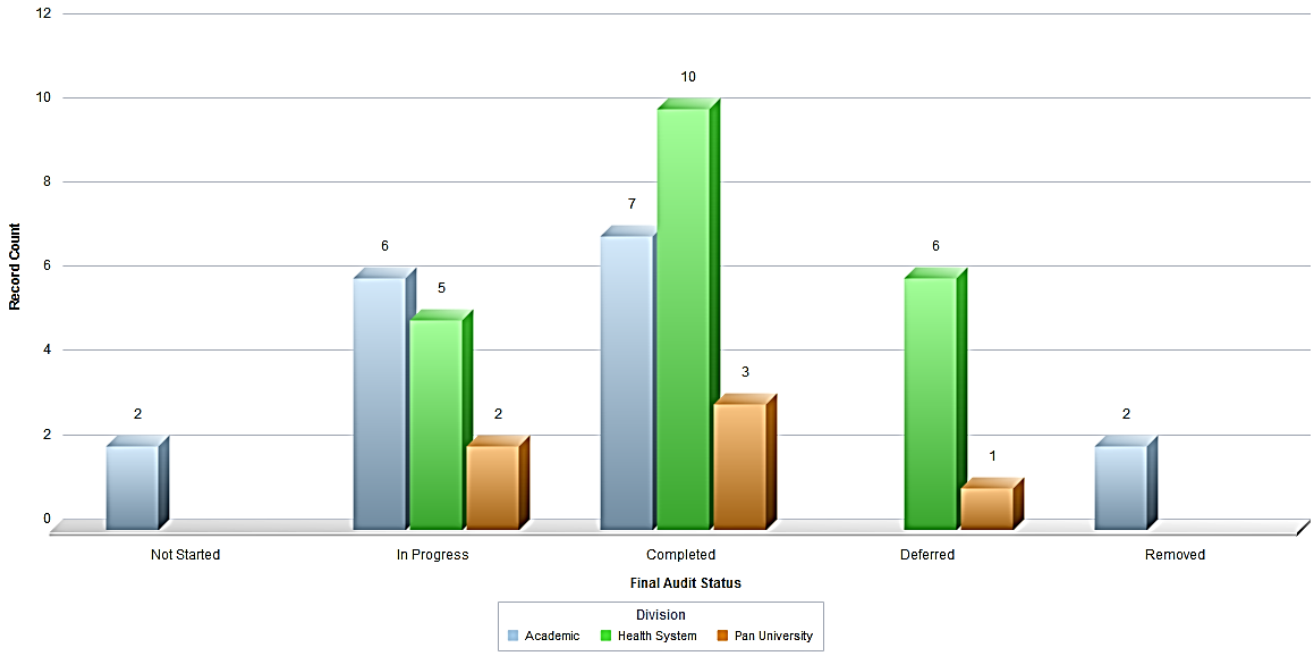
AGENDA ITEM: III.A. Audit Department Report (Written Report)

BACKGROUND: To facilitate the Committee's oversight of internal controls, risk management, and compliance, the written report summarizes UVA Audit's work performed during the period February 1, 2022- May 9, 2022:

1) Executive summary of audit activities
2) BOV approved audit plan status reports
3) Summary of audit findings for the period

1. UVA Audit: Activities for the Period[1]: Executive Summary

BOV Approved Audit Plan Status: as of May 9, 2022, 20 of 45 planned audits have been completed; 13 are in progress. We deferred seven audits to accommodate management's schedule/capacity and removed two to shift resources to other engagements. Final disposition of the FY2022 plan will be reported in September 2022.



[1] Board material due dates necessitate reporting only the data available to meet those deadlines (i.e. data is not a complete Fiscal Year quarter)

Third Quarter FY2022 Snapshot	Summary of Audit Activities
UVA Audit completed or is in progress on a range of assurance audits, investigations, and consultative activities during the quarter.	**14 Audit projects were completed since last report** (2/1/22-5/9-22) 1. Hospital Expansion Project Construction Closeout Audit Report 2. Undergraduate Student Advising Cost Analysis 3. Section 117 of the Higher Education Act Reporting Follow Up 4. CARES Compliance – Research (2020 OMB Supplement and Addendum, Memorandum 20-17)** 5. IT Audit: Cyber Maturity Assessment Follow Up Distributed IT Systems Management audits: 6. Batten School 7. School of Data Science 8. School of Nursing 9. School of Medicine 10. Point of Service Collections (UVA Health) 11. Monticello Community Surgery Center 12. Emergency Department Evaluation & Management Coding Compliance 13. Status Assignment 14. Controlled Substances Follow-up **13 audits and projects are in progress** 1. Research Data Security (IT Audit) 2. Student Health and Counseling** 3. NCAA Compliance (Integrated Assurance)** 4. Rebates and Credits Related to Sponsored Awards-Follow Up ** 5. CARES Compliance – Higher Education Emergency Relief Fund (HEERF I, II, III) – Part 2 (FY23) 6. Supplies Procurement (UVA Health) 7. Ambulatory Clinics Medication Charge Capture 8. Patient Choice Compliance 9. Safety & Security—Implementation of Consultant's Recommendations 10. International Operations Phase 1 11. Student Information System (SIS) Academic Records and IT Controls (formerly Academic Records and Policies) 12. Institutional Data 13. School of Medicine Special Project**

Third Quarter FY2022 Snapshot	Summary of Audit Activities
Consultative Activities and Support for Major University Projects	
	• Policy Review Committee • Identity and Access Management Steering Committee • Request Based Access Working Group • Role Based Access Steering Committee • Finance Strategic Transformation (FST) Executive Committee and Combined Steering/Advisory Committee • Workday Internal Controls Work Group • Kainos Smart Audit Working Group (Workday audit tool)

** Audit engaged by UVA Counsel; attorney client privileged

2. BOV Approved Audit Plan Status Report (Changes to Plan and Progress on Audits)

Because the plan is intentionally dynamic to maintain its relevance, a status report on the department's activities is provided at each Committee meeting.

	Division	Audit Topic
1	UVA Health	Case Management/ Utilization Management **(Deferred to FY2023 at management's request)**
2	UVA Health	Charge Capture – Radiation Oncology **(Completed)**
3	UVA Health	Financial Assistance and Financial Counseling **(Deferred to FY2024 at management's request)**
4	UVA Health	Point of Service Collections **(Completed)**
5	UVA Health	Emergency Department Evaluation & Management Levels **(Completed)**
6	UVA Health	Insurance Verification and Pre-Authorization **(Deferred to FY2024 at management's request)**
7	UVA Health	Status Assignment **(Completed)**
8	UVA Health	Controlled Substances Diversion Program **(Completed)**
9	UVA Health	Ambulatory Clinics Medication Charge Capture (**In progress**)
10	UVA Health	Monticello Community Surgery Center (MCSC) – (**Management requested addition - Completed**)
11	UVA Health	Distributed Information Systems Management (DISM) – School of Nursing **(Completed)**
12	UVA Health	Distributed IT System Management– School of Medicine **(Completed)**
13	UVA Health	Data Warehouse Controls **(Deferred to FY2024**)
14	UVA Health	Supplies Procurement **(In progress– pulled forward to replace a deferred audit)**

	Division	Audit Topic
15	UVA Health	Epic Provisioning and De-provisioning—clinical areas (**Deferred to FY2023**)
16	UVA Health	Patient Choice Compliance (**In progress - pulled forward to replace a deferred audit**)
1	Pan-University	Cyber Maturity Assessment Follow Up **(Completed)**
2	Pan-University	Safety and Security **(In progress)**
3	Pan-University	Research Data Security **(In progress)**
4	Pan-University	Ransomware Readiness (**Deferred to FY2023 at management request**)
5	Pan-University	Follow-up on External Active Directory Security Assessment (**In progress - replacement for deferral of Ransomware Readiness**)
1	Academic	Advancement Payment Processing **(Completed)**
2	Academic	Section 117 of the Higher Education Act Reporting **(Completed)**
3	Academic	Rebates and Credits Related to Sponsored Awards **(In progress)**
4	Academic	CARES Compliance - Research (2020 OMB Supplement and Addendum, Memorandum 20-17) **(Completed)**
5	Academic	CARES Compliance - Higher Education Emergency Relief Fund (HEERF I, II, III) **(Part 1 Completed; Part 2 (FY23) In progress)**
6	Academic	Cash Deficit Management Process **(Completed)**
7	Academic	NCAA Compliance (Integrated Assurance) **(In progress)**
8	Academic	Student Health & Counseling **(In progress)**
9	Academic	Undergraduate Student Advising **(Cost Analysis Completed)**
10	Academic	Study Enabling Technologies (**Removed; replaced by CARES Compliance HEERF expanded scope**)
11	Academic	Finance Strategic Transformation (FST) - Project Health Checks **(Removed from Plan)**
12	Academic	Construction Projects: • Hotel and Conference Center **(Begin planning in June 2022)** • Physics Building Renovation **(Begin planning in June 2022)** • Hospital Expansion Project Closeout **(Completed)** • Ivy Mountain Musculoskeletal Clinic Closeout **(Begin June 2022)**
13	Academic	International Operations - Phase 1: Inventory of Activities **(In progress)**
14	Academic	Academic Records and Policies **(In progress)**
15	Academic	Institutional Data **(Deferred to FY2023)**
16	Academic	Distributed IT Systems Management – School of Data Sciences **(Completed)**
17	Academic	Distributed IT Systems Management – Batten School **(Completed)**

* Audit engaged by UVA Counsel; attorney client privileged

3. Summary of Audit Findings for the Period March 1-May 9, 2022

The table below summarizes audit control findings by priority rating for audits performed since the last report to the Committee.

Project Name	Division	Priority Rating for Findings (see Ratings Scale for Definitions)					
		P1	P2	OP	W	DNM	PM
Hospital Expansion Project Closeout	Academic			2			
Distributed Information Security Management (DISM[2]) – Batten School	Academic Division				29	2	2
DISM – School of Data Science	Academic Division				32		3
DISM – School of Nursing	UVA Health				25	2	14
DISM – School of Medicine (5 units assessed)	UVA Health				116		20
Point of Service Collections	UVA Health		2		7		
Emergency Department (ED) Evaluation and Management (E/M) Levels	UVA Health		1	1			
Status Assignment	UVA Health			1	7		
Controlled Substances Compliance Follow-up	UVA Health		6		23		
Cyber Maturity Assessment Follow-up	Pan-University				26	1	4
OMB Flexibilities for Research*	Pan-University	2	1	1			
Total		2	10	5	265	5	43

* Audit conducted under Attorney-Client Privilege

[2] 50 IT controls based on UVA IT policies and ISO 27002-2013 are examined in each DISM audit

The following summarizes themes and findings from reports issued this period.

Audit	Summary of Findings
Hospital Expansion Construction Audit: Project Closeout	• The closeout audit did not identify any major billing errors or overcharges in the Construction Manager's (CM) Pay Applications. • Overall, the 13 contracts that comprised the Project grew from the original contract sum of $273,411,180 to the final contract sum of $315,934,973 through December 31, 2021 • The auditors analyzed the "Reason Codes" (RC's) assigned to the CCOP's to identify reasons for the $40 million budget growth in the Final Building Package. They recommend Facilities Management • ResX observed the RC definitions overlap and are not specific enough for post-project analysis of the cost of project changes (e.g., equipment cost escalation, user changes to equipment specifications, construction cost escalation, or design changes occurring after schematic design and project budget approval). • ResX recommends UVA Facilities Management Capital Construction and Renovations department reviews the CCOP RCs with the goal of improving the utility of these codes to illuminate the underlying cause of changes on future projects. • ResX agreed with HKA construction consultant's report and identified where recommendations aligned with previous ResX reports.
Distributed Information System Management (DISM) – Batten School 2 2 2 Does Not Meet (DNM) and 2 Partially Meets (PM) IT Control Findings	We evaluated controls based on UVA IT policies, which are grounded in ISO/IEC27002:2013 *Information Technology -- Security Techniques -- Code of Practice for Information Security Controls* (ISO). Of the 50 controls assessed, 29 of **met** the requirements of the relevant University policy; 2 **partially met** those requirements; and 2 controls tested **did not meet** UVA's policy requirements. Seventeen (17) controls did not apply at the Batten School unit level.
DISM – School of Data Science 3 3 Partially Meets (PM) IT Control Findings	We evaluated controls based on UVA IT policies, which are grounded in ISO/IEC27002:2013 *Information Technology -- Security Techniques -- Code of Practice for Information Security Controls* (ISO). Of the 50 controls assessed 32 **met** the requirements of the relevant University policy; 3 **partially** met those requirements. Fifteen (15) controls did not apply at the School of Data Science unit level.
DISM – School of Nursing 2 14	We evaluated controls based on UVA IT policies, which are grounded in ISO/IEC27002:2013 *Information Technology -- Security Techniques -- Code of Practice for Information Security*

Audit	Summary of Findings
2 Does Not Meet (DNM) and 14 Partially Meets (PM) IT Control Findings	*Controls* (ISO). The audit found 25 of the possible 50 controls assessed **met** the requirements of the relevant University policy; 14 **partially met** those requirements; and 2 controls tested **did not meet** UVA's policy requirements. Nine (9) controls did not apply at the School of Nursing unit level.
DISM – School of Medicine (5 units assessed) 20 20 Partially Meets (PM) IT Control Findings	We evaluated controls based on UVA IT policies, which are grounded in ISO/IEC27002:2013 *Information Technology -- Security Techniques -- Code of Practice for Information Security Controls* (ISO). The School of Medicine has disseminated the management of IT assets across various departments and **lacks a management structure for effective IT governance and oversight**. This lack of structure and management oversight impeded our ability to fully assess the School's IT environment. The controls we could not assess were in critical areas, such as defining accountability for information security responsibilities, segregation of IT duties, controlling access to systems and data, managing the development of new systems, and incident identification and response. As a result, we concluded the SOM faces an elevated level of risk for an IT control failure, such as a data or network breach, inappropriate access to systems, or loss of institutional data.
Point of Service Collections 2 1 2 Priority 2 (P2) Rated Findings and 1 Opportunity for Improvement (OP)	We assessed the policies, procedures and controls around identifying and collecting patient copays at the point of service. We found that **financial performance and cash flow could be strengthened** through improved collection of copays at the point of service. UVA Health has not established a formal policy or performance goals for this activity. UVA Health will develop and implement a formal policy and update the patient access training programs by September 30, 2022.
ED E/M Levels 1 1 Priority 2 (P2) Rated Finding	Gaps were identified in the UVA Health E/M Leveling Guidelines, which caused **difficulty validating** the E/M level assigned to **35** of the **150** cases. UVA Health will review and update the E/M Leveling Guidelines to meet the CMS expectations that facility guidelines be usable for compliance and audit purposes and result in coding decisions that can be verified by other hospital staff and outside resources. UVA Health will also review current specifications for E/M level assignment and update the point

Audit	Summary of Findings
	calculation criteria, to better conform the UVA Health Guidelines to the CMS principles.
Status Assignment 1 1 Performance Improvement opportunity	This audit assessed processes and controls supporting the appropriate level of care (patient status) to inpatients, which relates to several CMS billing regulations. For the cases reviewed, UVA Health demonstrated **strong adherence to the established procedures**. One opportunity for improvement of documentation was identified.
Cyber Maturity Assessment Follow-up 1 4 1 Does Not Meet (DNM) and 4 Partially Meets (PM) IT Control Findings	The audit followed up on the status of recommendations made by KPMG in its 2019 cyber security program maturity assessment and incident response review. The scope of the 2019 review, and our follow up procedures, encompassed University of Virginia's Academic and Health System IT infrastructures. We observed 28 of the 33 recommendations (~85%) have been **appropriately actioned**. The remaining 4 (~12%) recommendations flagged in the report as "**partially meets**" are in the process of being fully remediated, with a target completion by the end of the current calendar year. One item (~3%) was flagged as '**Does Not Meet**' and is targeted to be addressed by August of 2022.
Controlled Substances Follow-up 6 6 Priority 2 (P2) Findings	This audit was a follow-up to an audit conducted in late 2019, which noted a number of significant issues. We found that **75%** of the prior action plans **were sustained** and **25% were not**. The audit also identified **11 new areas** where controls could be strengthened. Pharmacy leadership plans to implement action plans addressing the findings by September 30, 2022.
OMB Flexibilities for Research*	Management is working on process improvements for issues identified during the audit (conducted under Attorney-Client Privilege).

Rating Scale		
P1	**Priority 1**	A Priority 1 item signifies a control and/or process deficiency of sufficiently high risk that it provides minimal or no assurance that institutional objectives will be achieved. Management must take immediate corrective action to mitigate Priority 1 deficiencies.
DNM	**Does Not Meet**	An IT control that is not in place or is ineffective to achieve the relevant IT controls framework (e.g., ISO-27002-2013) requirement

Rating Scale		
P2	**Priority 2**	A Priority 2 item signifies a control and/or process deficiency that hinders the effectiveness and efficiency of unit level operations, potentially impeding the attainment of institutional objectives. Management must take timely corrective action to mitigate Priority 2 deficiencies.
PM	**Partially Meets**	An IT control that meets some, but not all, of the relevant IT controls framework (e.g., ISO-27002-2013) requirement
OP	**Process Improvement**	A process improvement item signifies an opportunity to achieve additional control and/or process efficiencies.
W	**Working**	Control tested or process evaluated is working as designed

UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY

BOARD MEETING: June 2, 2022

COMMITTEE: Audit, Compliance, and Risk

AGENDA ITEM: III.B. Institutional Compliance and Medical Center Compliance Goals for FY2021-2022: Year-End Status Report

BACKGROUND AND DISCUSSION:

Institutional Compliance Goals
Fiscal Year 2021-2022
Year-End Status Report

1. **COVID-19**: Continued to support the University's efforts to successfully implement and monitor changes to processes in response to COVID-19, by overseeing reporting mechanisms through which the University received COVID-related compliance concerns, reviewing new policies and procedures, and participating in other related activities that have arisen. In addition, we leveraged the Compliance Network to share information about COVID compliance processes. We will continue to monitor court decisions related to the federal vaccine mandate for federal contractors, in order to determine applicability.

2. **Hotline Rationalization** – Enhanced reporting capabilities of the new compliance module, as well as developed a high-level institutional reporting tool for data in SafeGrounds to create standard reporting and monitor trends related to compliance concerns. Developed plans to market the new web intake form to receive compliance concerns and completed enhancements to the existing 800 number helpline to the University community. As soon as the web intake form was linked from the compliance website, the university community began to use it to report concerns for both the academic division and the medical center.

3. **Conflict of Interest Processes:** Coordinated a multi-department effort to update the processes related to conflicts of interest at the University in order to better understand how conflicts are documented and managed, as they relate to procurement, research, and the Statement of Economic Interests (SOEI) that are submitted to the state. Met with existing process owners to review the current procedures, updated the list of individuals required to complete the SOEI, and completed available training that we offer to the university community. We will continue to identify potential ways to streamline and improve existing processes.

Medical Center Compliance Goals
Fiscal Year 2021-2022
Year-End Status Report

1. **Compliance Program Effectiveness:** Completed the biennial organizational Compliance Program Effectiveness Evaluation to evaluate the UVA Health Compliance Program's effectiveness in identifying and preventing criminal conduct using federal regulatory criteria, indicators, and guidance of the U.S. Department of Justice Criminal Division Evaluation of Corporate Compliance Programs. The department completed a detailed effectiveness self-assessment, evaluating fulfillment of the OIG Compliance Guidance elements. A survey was distributed health system-wide, yielding a 14% response rate. All data was analyzed, questions responded to; action plans were developed and fulfilled. A high level of effectiveness was measured, and all participants and respondents gained a deeper understanding of the Compliance Program.

2. **Follow up on Compliance Risk Assessment**: Continued progress has been made on completion of the corrective action plans developed following completion of the prior fiscal year compliance risk assessment. Updates are routinely provided to the Compliance Steering Committee; of the items remaining, three are scheduled for completion by the end of FY22; one item has a scheduled completion data of late summer 2022. Another biennial Compliance Risk Assessment is scheduled for FY23.

3. **Organizational IT and Data Governance:** The health system data governance function has developed procedures, an intake process and workflow; roles and responsibilities in reviewing and responding to requests have been defined between HIT and Data Analytics. A steering/advisory leadership group has been designated to review variances in order to ensure appropriate access to and use of UVA Health data.

4. **Compliance Issues Database Transition:** The transition to UVA SafeGrounds on July 1, 2021, for compliance case management has been successful. Workflow capabilities allow for more effective collaboration amongst team members and cooperating departments. The addition of the customized web intake form to receive compliance reports has been communicated and is being used increasingly by the health system community. Overall, the system is versatile and allows for more effective management of reported compliance issues, workflow to refer cases to others as needed and offers web intake to facilitate the reporting of compliance concerns.

APPENDIX

Mission Statement

The University of Virginia is a public institution of higher learning guided by a founding vision of discovery, innovation, and development of the full potential of talented students from all walks of life. It serves the Commonwealth of Virginia, the nation, and the world by developing responsible citizen leaders and professionals; advancing, preserving, and disseminating knowledge; and providing world-class patient care.

We are defined by:

- Our enduring commitment to a vibrant and unique residential learning environment marked by the free and collegial exchange of ideas;
- Our unwavering support of a collaborative, diverse community bound together by distinctive foundational values of honor, integrity, trust, and respect;
- Our universal dedication to excellence and affordable access.

Our Values

This institution exists to serve others and does so through the expression of our core values.

Overview

UVA's Great and Good-2030 Plan is anchored around the University's Mission and Values. In observing how we approached solving challenges to strategic initiatives during COVID, the need for a new alignment of ERM around our institutional values became evident.

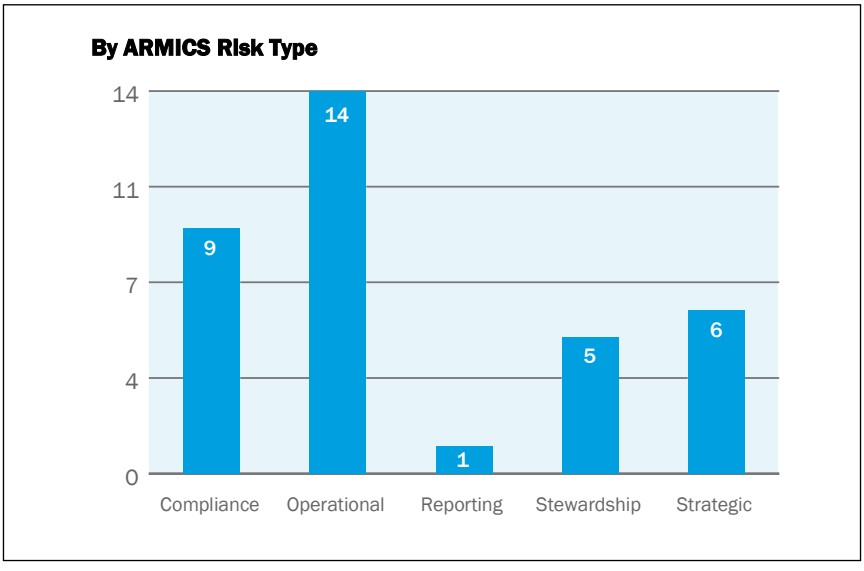
The University convened a Risk Management Network (RMN) in early 2021 to provide steering and oversight, including chartering of working groups, validation of working group membership and establishing risk scoring methodology. The RMN agreed that the first working group should investigate fiscal sustainability. The Fiscal Sustainability Working Group (FSWG) was launched in May of 2021 and charged with evaluating risks to the Academic Division's financial security and sustainability. The FSWG's analysis involved collaboration between the working group members and various risk owners throughout UVA to identify risks, tier them by magnitude, assess existing mitigation strategies, evaluate residual risks, and propose additional mitigation measures. A list of FSWG members is included in the attached appendix.

The FSWG identified several dozen enterprise-level risks that could potentially impact UVA's fiscal sustainability. However, in the case of each highly rated risk, the FSWG found that the responsible business units had developed mitigation procedures that substantially reduce the likelihood of adverse impact on operations. As such, UVA's Academic Division is in a solid position with respect to almost all risks. Of course, any ERM evaluation is a "snapshot in time" based on an appraisal of present circumstances. As such, UVA should engage in ongoing monitoring to ensure that its risk assessments and mitigation strategies are continually updated to reflect changing circumstances.

Methodology

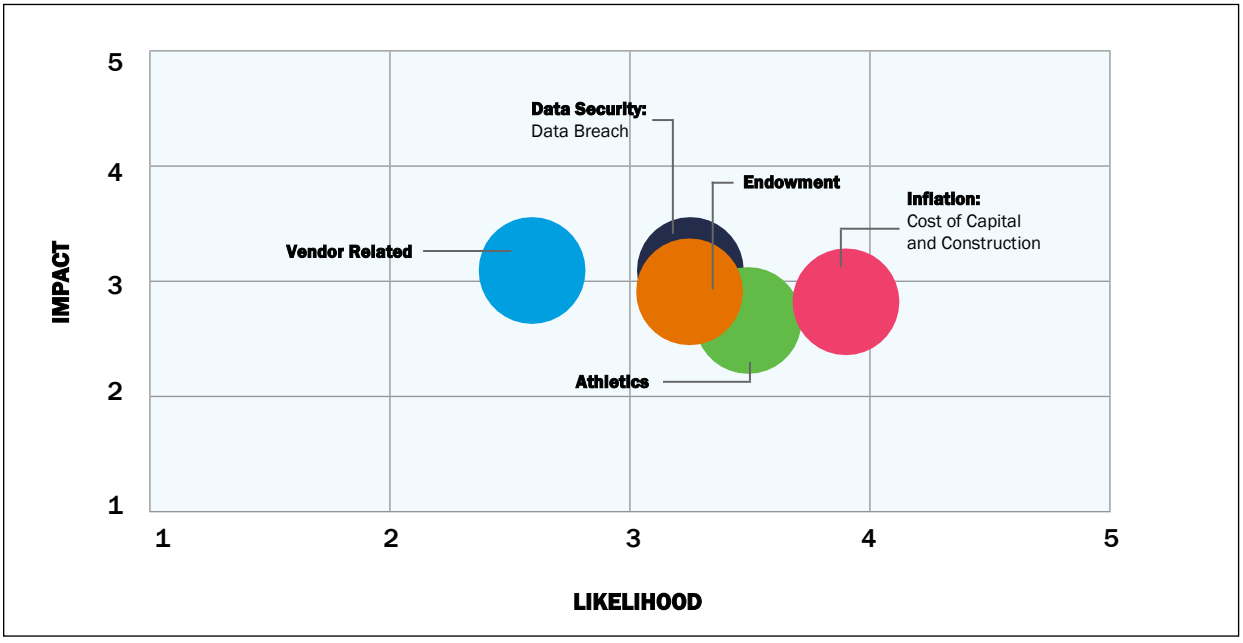
Instead of employing traditional approaches, UVA adopted a value based ERM approach with the intention of transforming ERM into a strategic management process that enhances long-term planning and business decision making. The FSWG also evaluated and quantified the types of risks consistent with the Commonwealth's Agency Risk Management and Internal Controls Standards (ARMICS) – compliance, operational, reporting, stewardship and strategic – and prioritized focus on those risks that pose the largest potential threat to successful completion the University's core missions.

To develop its register of financial risks, the FSWG built upon the previous UVA risk registers supplemented with additional risks appearing in the Enterprise Risk Management in Higher Education Practitioners Survey (Enterprise Risk Management in Higher Education | ERM - Enterprise Risk Management Initiative | NC State Poole College of Management (ncsu.edu)) and the Gartner ERM 2021 Risk Register (see Enterprise Risk Management Program Management Primer for 2021 (gartner.com). The FSWG submitted a draft risk register, comprising approximately thirty-five major risks, to the RMN for feedback and validation. The FSWG then blind-scored the risks on likelihood and financial impact.



The scoring process yielded five risks warranting full analysis by the FSWG, as well as two new enterprise-level risks that emerged from the scoring exercise and attendant discussions. One of those new risks – Athletics – was developed into a separate risk register. The Risk Management Network decided that the other new risk - Human Capital: Ability to Attract and Retain the Best Talent - should be the subject of a new, dedicated risk working group led by Chief Human Resources Officer, John Kosky and anchored around the work done by the "Future State of Work" committee.

	ARMICS CATEGORY	SCORE
Risk of escalating costs for buildings and other capital expenditures: inflation	Stewardship	10.7
Breach of sensitive data resulting in data compromise, fraud, financial loss, operational failure and reputational degradation	Operational	10.4
Adverse changes in government tax policy affecting endowment earnings or collegiate athletics	Strategic	10.3
Changes to Federal, NCAA and Conference regulations and requirements that have significant revenue and/or operational impacts on University Athletics	Operational	9.4
Inability to protect vendor identity, process accurate payments to vendors or financial beneficiaries and ensure against wire fraud for payment	Operational	9.1



The FSWG formed subsidiary teams for each risk warranting full analysis. These teams engaged with members of UVA leadership and internal and external subject matter experts to perform a thorough analysis of each risk and to develop corresponding subsidiary risk registers with more detailed analysis of risks, individual financial impact and current risk level assessment, and mitigation plans. The subsidiary risk registers are provided for reference in the attached appendix.

While the FSWG's initial risk report is complete, the group intends to remain active and to monitor and identify fiscal sustainability risks. To this end, the FSWG will reconvene at regular intervals, or as circumstances necessitate, to rescore current risks and to identify new risks to fiscal sustainability as they arise.

Major Fiscal Sustainability Risks

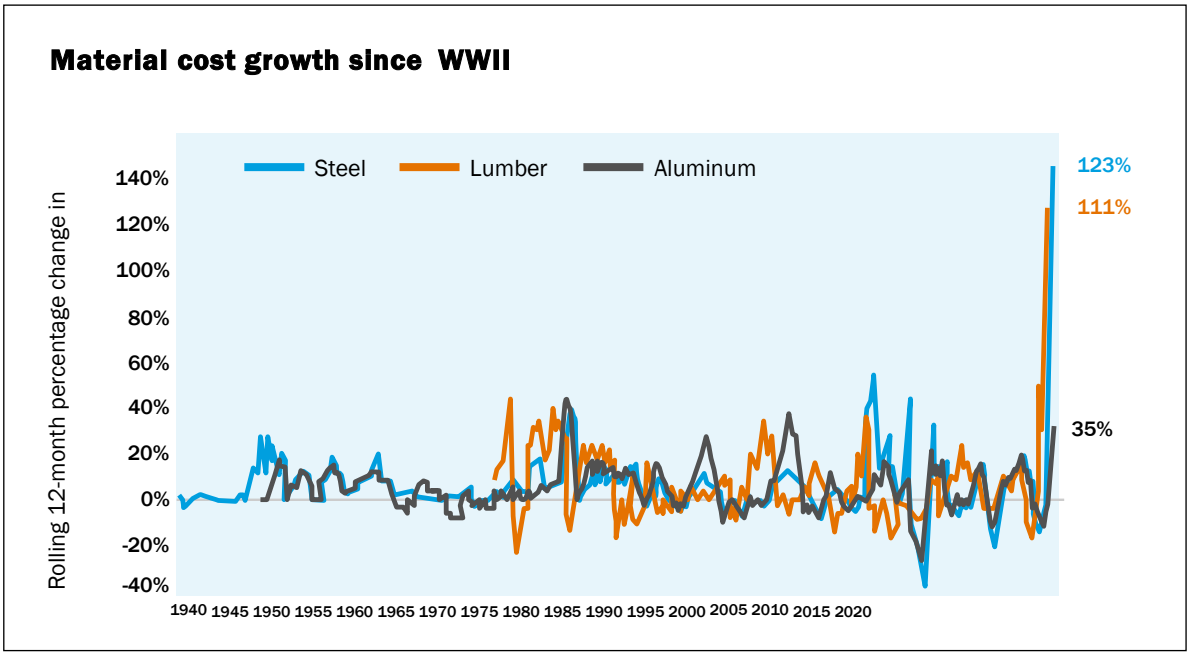
Inflation: Cost of Capital and Construction

The assessment on inflationary pressures, especially as they relate to large expenditures is timely and aligns with several industry surveys as a risk to monitor. Supply chain pressures combined with market liquidity have created what many experts feel is real risk regarding long term inflation, rather than the transitory categorization shared earlier by the United States Federal Reserve and its associated banks.

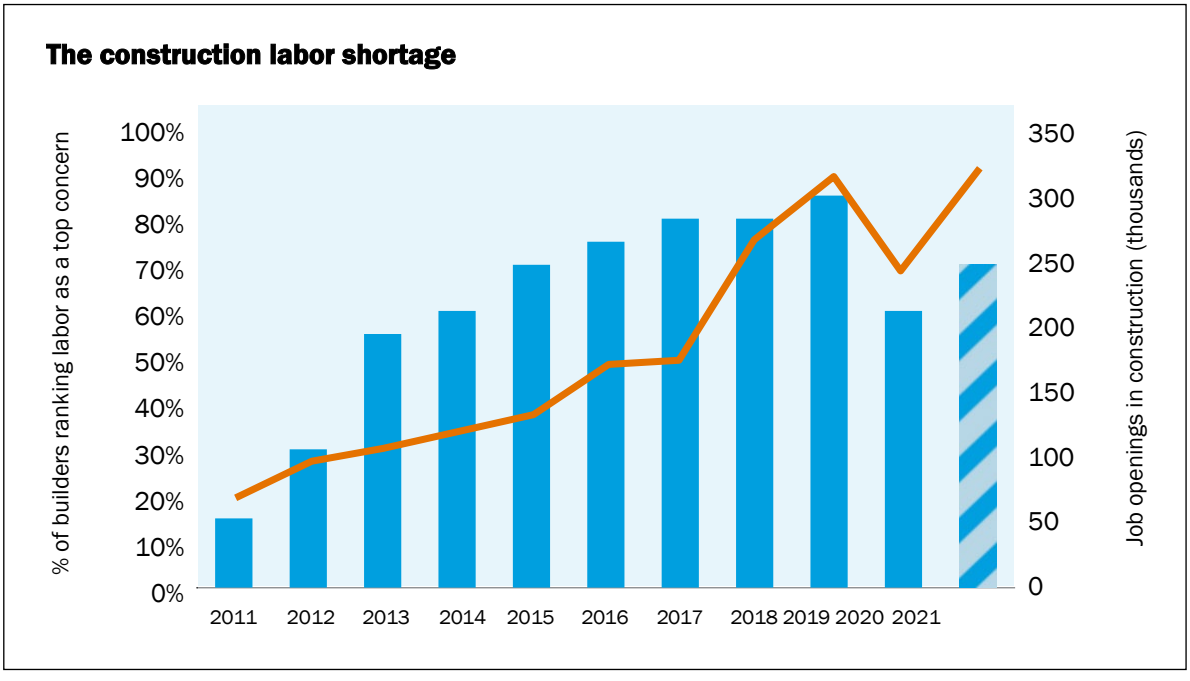
In early December, the 2021 annual unadjusted Consumer Price Index was at 6.7% in aggregate, outpacing United States Gross Domestic Product of 2.1%. The inflationary pressure was driven by 33.2% increase in the Energy sector, as well as commodities up 14.1% for the year. With those categories the main inputs for building materials combined with a tight labor market, it would be appropriate to evaluate and ensure mitigation strategies are contemplated for what is more than 10% of University spend. When considering the inflationary impact to the cost of utilities, technology, and other durable goods – the risk impact grows significantly and will need further monitoring into 2022.

Adequate facilities and capital expenditures are indispensable to achieving the 2030 plan. The FSWG explored risks to cost of capital from inflationary pressures and evaluated UVA's performance relative to its academic industry peers. It was calculated that a 10% increase in construction costs would translate into a $40 million annual impact on capital spending after factoring in competing priorities on the physical plant, compressed labor markets, supply chain and raw material impacts, and construction management costs. A Fall 2021 benchmarking study by HKA Global Inc. presented to the BOV concluded from a peer benchmarking survey and cost analysis that construction costs at UVa are generally in line with those at other institutions. However, the report identified twelve processes and procedures by which UVa executes its projects that could be improved and thereby have the potential to drive cost savings.

Cost pressure on capital projects is real and comes from a variety of sources including materials prices, labor shortages, supply chain disruption, and project sponsor desires that do not align with available financial resources. The University has several tools/strategies it uses to mitigate the risk of cost pressures. For example, 1) leveraging contingency that is a part of each capital project budget; 2) employing different procurement methods tailored to the particular project; 3) conducting value management with a goal to reduce costs; 4) rebidding subcontract packages with low responses to seek better pricing; and 5) specifying alternative materials when high cost materials are originally included in a design. The capital project team engaged with Organizational Excellence in 2020 and identified a number of process improvements. The HKA study also provided suggestions for process improvements that are currently being designed and implemented. While the risk from inflation and other cost pressures cannot be eliminated, the University has the tools needed to mitigate cost pressures.



Sources: JLL Research. U.S. Bureau of Labor Statistics



Sources: JLL Research. U.S. Bureau of Labor Statistics, NAHB

https://www.bdcnetwork.com/no-decline-construction-costs-sight

Data Security: Data Breach

Data Breaches in 2021 continued at a record pace. According to Identity Theft Resource Center (ITRC), the total number of data breaches through September 2021 was up 17%, with over 1,000 in the United States alone. Some popular names that fell victim to data breaches include Android, Facebook, LinkedIn, and a governmental utility pipeline to name just a few. Healthcare providers, governmental institutions and institutions of higher education continue to be prime targets. This past December 2021, a critical vulnerability called "log4j" was discovered that allows attackers to insert malicious code into a request to a website and gain control of the server. This most recent threat is a reminder of the daily onslaught of cyber activity targeting our critical systems.

The University collects and stores numerous types of legally protected and/or valuable information, such as student, financial and health data and export-controlled technology. The biggest threat to data security is the University's decentralized nature. The distributed nature of IT at the University leaves UVA susceptible to unauthorized access and ransomware attacks and also impedes its ability to comply with US government prohibitions against the purchase of certain foreign telecommunications components. In most cases, however, the University's established collection, retention and training procedures adequately mitigate the risk of improper disclosure.

Tax and Regulatory Changes Impacting Philanthropy and Endowment Return

Over 25% (approximately $500 million) of UVA's annual non-operating revenues are dependent on gift and investment income. Changes in regulatory policy towards collegiate athletics could have a substantial impact, as could changes in tax law related to executive compensation, foreign investments, charitable contributions, and endowment excise taxes. To ensure preservation of the endowment, the BOV recently modified the University's endowment spending policy to a minimum 3% distribution. In addition, University legal, compliance and financial administrators continue to monitor and evaluate tax and regulatory risks as they emerge.

Athletics

Athletics was deemed a free-standing financial risk due to the seismic changes that have occurred in the past year related to name-image-likeness licensing, the Alston US Supreme Court case permitting monetary compensation to collegiate athletes, and the NLRB memo implying that college athletes might be properly categorized as employees. Each of these changes is a step towards reclassification of collegiate athletics as an activity with more professional than amateur academic connotations. The treatment of athletics as a professional activity could have impacts on charitable giving, capital costs and operating budgets, and even unrelated business income tax.

Financial Operations: Vendor Payments

Cyber Security remains a critical risk for all businesses. The potential impact of fraud and/or security breaches on vendor payments can be significant from an enterprise risk management perspective. PWC recently surveyed 5,000 business that reported over $6 billion in losses due to fraud, and 40% of those instances were around vendor/customer record manipulation.

With over $1.1 billion a year flowing from UVA to over 6,700 suppliers, vendors, and non-employees, the risks of fraudulent payments, compromised systems, and inadequate controls require ongoing attention. Procurement and vendor payment processes were mapped with operational and systematic controls in place to ensure proper disbursement of over $10 million per week on average. Procurement risks are mitigated by a combination of a strong banking partner, migration to a cloud-based ERP system, separated Procurement and Accounts Payable processes, and cyber and crime insurance policies. In the age of digital banking UVA will need to dedicate ongoing attention to vendor payment risks, especially as implementation of the new Workday Finance ERP system approaches.

In the summer of 2021, Internal Audit with the support UVA Finance and Procurement and Supplier Diversity Services undertook a review of UVA's processes for determining and managing Mission Essential Vendors. As global supply chain disruptions continue as a result of Covid-19, this effort was helpful in solidifying a rubric for consistently identifying mission essential relationships. This effort also enhanced and formalized our procedures for managing and tracking those entities while ensuring they are included in the Continuity of Operations Plan (COOP).

Conclusions

The University's sturdy balance sheet, strong governance, and diversified revenue mix contribute to the fiscal sustainability of the institution. The University also benefited from strong endowment performance over the last two years, resulting in FY21 gains of $3.4b in net position and a consolidated endowment total of $12.5b as of December 31, 2021. While conducting educational activities in the current environment poses some inherent risks, the University's current mitigation strategies appear to align with institutional risk appetite and profile. The FSWG identified financial ERP deployment and the potential professionalization of collegiate athletics as future risks for consideration. Another emerging risk being contemplated is the emergence of environmental, social, and governance (ESG) regulatory requirements which include climate and sustainability requirements along with responsible investing and overall community and governance engagement.

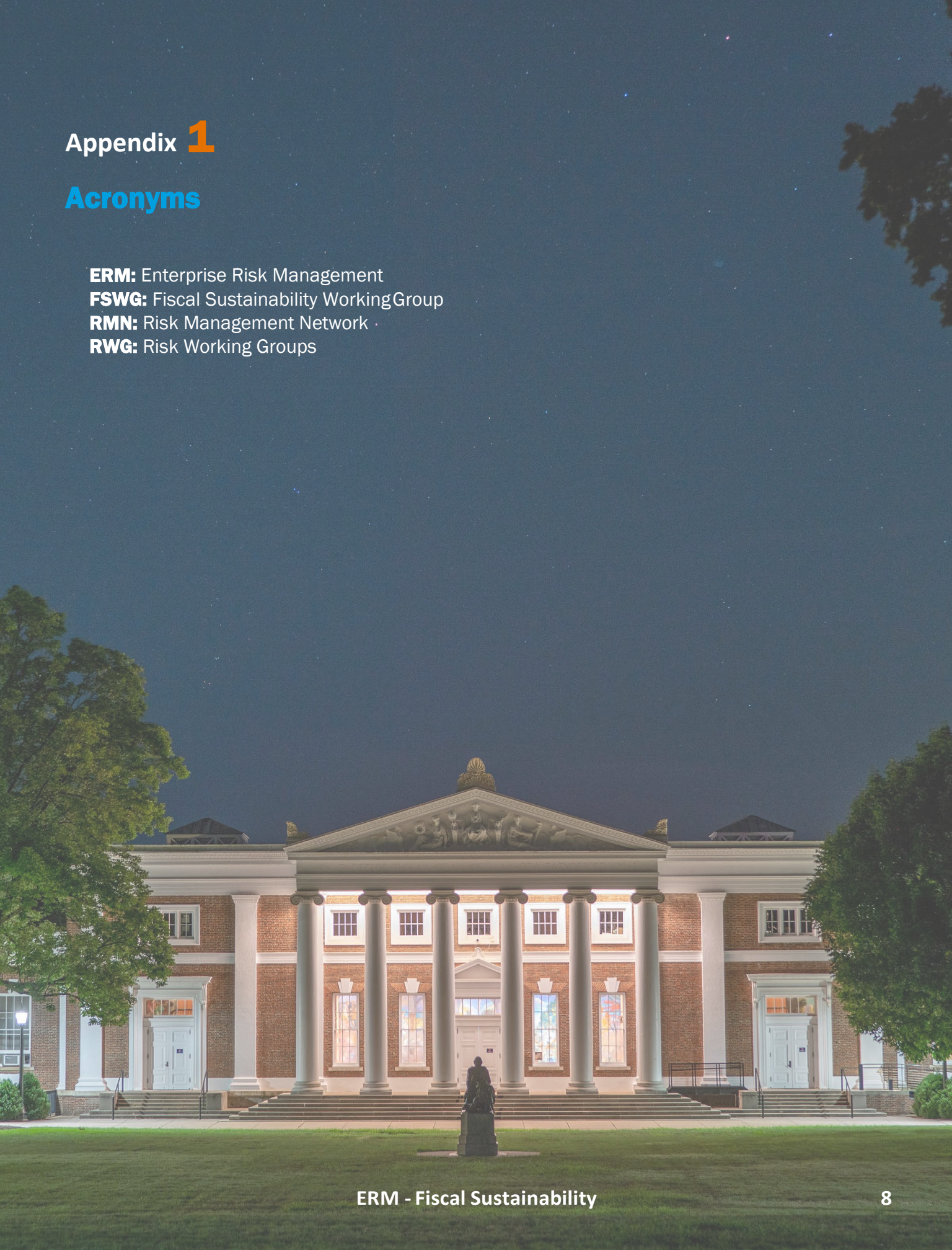
The importance of an ongoing review of overall risks is critical given the rapidly changing landscape as evidence by the changing regulatory environment and athletics rulings. A significant mitigation is the expertise of University administrators, supplemented as warranted with external consultants, who actively watch, evaluate, and consult with peers and others for emerging issues and best practices to address new and evolving risks.

The analysis and inputs on this effort will be additive as the next working group addresses UVA's future state of work and all that entails from a human capital perspective. In addition, the Risk Management Network will broaden its access to better align and inform both UVA Wise and UVA Medical Center.

Appendix 1

Acronyms

ERM: Enterprise Risk Management
FSWG: Fiscal Sustainability Working Group
RMN: Risk Management Network
RWG: Risk Working Groups



Appendix 2

Membership List and Governance Structure

PERT

James Ryan, University President
Ian Baucom, EVP and Provost
Jennifer "J.J." Wagner Davis, EVP and COO
Craig Kent, EVP for Health Affairs
John Jeffries, SVP for Advancement

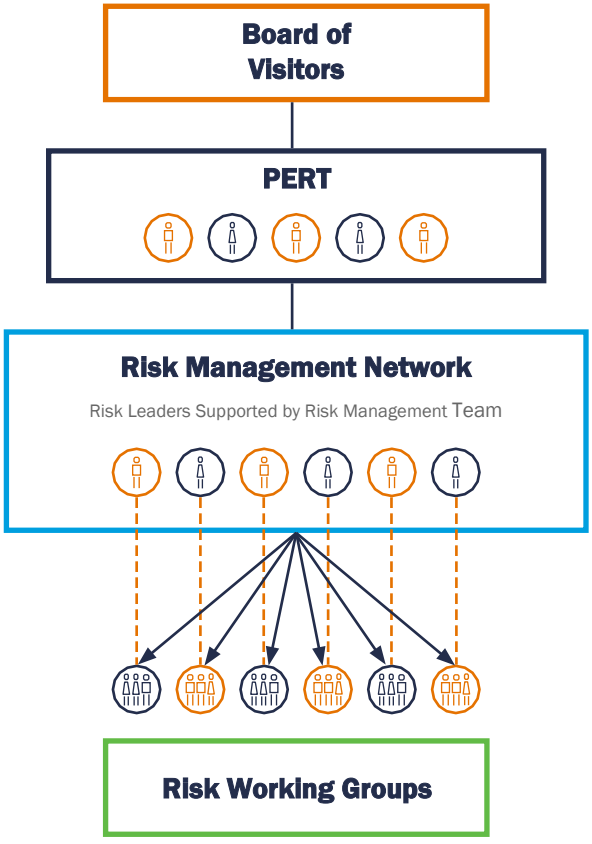
Risk Management Network / Risk Management Team

Melody S. Bianchetto, VP for Finance
Carolyn Devine Saint, Chief Audit Executive
Augie Maurelli, AVP for Financial Operations
William Define, Director of Financial Operations
Clara Tang, Senior Compliance Analyst

Fiscal Sustainability Risk Working Group Membership

Leads:	Melody Bianchetto, Vice President for Finance
	Adam Daniel, Vice Provost for Planning
	Ann Kromkowski, Sr. Assoc Dean for College of Engineering
Members:	Bill Ashby, Associate Vice President for Financial Strategy
	Julie Richardson, University Treasurer
	Eduardo Lorente, Associate Vice Provost for Budget & Financial Planning
	Mark Luellen, Vice President for Advancement
	Steve Kimata, Associate Vice President for Student Financial Services

Enterprise Risk Management Governance



Board of Visitors: The Board of Visitors Audit, Compliance & Risk Committee provides fiduciary oversight of UVA's ERM program and University risk management practices.

PERT: Comprised of the University President, Provost, COO, EVP of Health Affairs, and SVP for Advancement, PERT is responsible for ERM leadership and ultimately determines institutional risks for BOV discussions as well as oversees the work of the Risk Management Network.

Risk Management Network (RMN): Selected leaders from academic and administrative organizations with diverse perspectives will convene to discuss complicated and important prevention questions. The RMN, supported by the Risk Management Team, reviews and validates risk priorities and mitigation plans identified in Risk Working Groups. **The Risk Management Team (RMT)** includes the Vice President for Finance, Chief Audit Executive, AVP for Financial Operations and Director of Financial Operations.

Risk Working Groups (RWG): Selected functional risk owners and subject matter experts from academic and administrative organizations will identify, calibrate, develop and present values-based risk management/mitigation plans as well as work with the Risk Management Team to maintain risk registers and mitigation strategies.

Appendix 3

Subsidiary Risk Registers

Highly Rated Risks	Identified Sub Risk	Analysis of Risk	Mitigation Plan
Inflation: cost of Capital and Construction	**Managing alignment of scope, timeline, and resources with customer needs/ desires**	Development of a capital project from concept to planning to design and construction can be a long process. Customer desires often outstrip available resources. Quality, time, and money compete for priority. Program scope, building size, and available resources must be agreed to by all parties at the outset. Changes to any variables must be vetted and agreed to as well. HKA has recommended a project charter that establishes the parameters of a project that will help to avoid misunderstandings as a project moves through its development process.	University has a robust major capital process, including an annual process to add new projects, remove projects that are no longer a priority, and prioritize projects against establish criteria. During the design and construction of a project, the project's working group, made up of representatives from FM, Office of the Architect, and the project sponsor, meet regularly to monitor progress and make decisions as necessary with respect to the project's development, scope and budget. See https://svpo.virginia.edu/sites/operations.virginia.edu/files/processoverview.pdf for an overview of the process to manage major capital projects. Implement the HKA recommendation to create a project charter that establishes the parameters of a project, documents any scope and resource changes, and is acknowledged by the project sponsor and team. This will help to avoid misunderstandings and create a written record as a project moves through development
	Compressed Labor Market Increases Price and limit vendors for capital projects	UVA is in a relatively small market for skilled labor and construction management services. There are a limited number of firms and subcontractors to bid on projects. This is felt more acutely in the subcontractor market. The University has a large capital program that can strain these resources and cause labor shortages and/or higher prices.	• All construction projects have a 5% design contingency and 10% construction contingency, which can be utilized to address cost items • UVA rebids packages with low response and looks for opportunities to rescope packages for rebid • UVA performs value management on all construction projects greater than $3M
	Supply Chain and Inflation results in Raw Material Cost Impacts	Raw material costs such as steel and lumber have been incredibly volatile over the past several months and continue to be influenced by significant supply chain issues. The current environment suggests that contingency levels may or may not be adequate to cover the recent market volatility.	• All construction projects have a 5% design contingency and 10% construction contingency, which can be utilized to address cost items • UVA looks for alternative materials and specifications if certain materials have a higher cost than anticipated • HKA recommended a project risk register to promote open and transparent communication of factors that could compromise successful project delivery which the team is working on now. • Until the market stabilizes larger contingencies may be needed until pricing is secured which will impact overall project pricing.

	Benchmarking may no longer be a validation tool	Increased project scope, need for more technology and sustainability, combined with ever increasing competitive landscape for new students may render existing benchmarking tools obsolete, and as a result, not appropriately reflecting desired designs for the 100 year building and campus.	UVA periodically reaches out to other institutions to benchmark aspects of our costs. In FY20, Organizational Excellence assisted OAU, UVA Finance, and FM to review the end to end process, identify opportunities for improvement, and develop a roadmap for implementation. Additionally, in FY22, UVA engaged a third party, HKA, to review UVA's cost of construction, benchmark it against other Universities, and identify areas of improvement within the capital program. This was presented to the Board on 9.23.21.

Appendix 3

Highly Rated Risks	Identified Sub Risk	Analysis of Risk	Mitigation Plan
Data Security: Data Breach	**Student educational data breach (FERPA)**	The Family Policy Compliance Office of the U.S. Department of Education (FPCO) first works to bring noncompliant schools into voluntary FERPA compliance. If voluntary compliance is not achieved, the school would be in jeopardy of losing federal Title IV education dollars. To date, findings of non-compliance have not resulted in such action. There is no private cause of action (right to sue) under FERPA and, in 2002, the U.S. Supreme Court ruled in Gonzaga University v. John Doe that students and parents may not sue for damages to enforce FERPA.	UVA has compliance and training programs to ensure that all employees handling confidential student data are aware of their obligations under state and Federal law. The Chief Information Security Officer and team has completed a formal risk assessment of the student information system and regular scans are performed for vulnerabilities. With the FY2020 state audit, there was a management finding that other systems containing "non-public personal information" also required risk assessments; for example, UBI. The CISO and SFS plan to bring in a vendor to assist with these additional risk assessments.
	Student financial data breach (GLBA)	The Department of Education's Postsecondary Institution Cybersecurity Team ("Cybersecurity Team") may temporarily or permanently disable an institution's access to the DoE's information systems if it determines that the institution or servicer poses substantial risk to the security of student information. Additionally, if the Cybersecurity Team identifies serious internal control weaknesses, it may refer the institution to the DoE's Administrative Actions group for assessment of fine or other appropriate administrative action. The Gramm-Leach-Bliley Act applies to all penalties for noncompliance, including fines and imprisonment: • The institution can be subject to a civil penalty of up to $100,000 per violation. • Officers and directors of the institution will may be subject to civil penalties of up to $10,000 per violation. • The institution and its officers and directors will also be subject to fines in accordance with Title 18 of the United States Code or imprisonment for not more than five years, or both.	UVA has compliance and training programs to ensure that all employees handling confidential student data are aware of their obligations under state and Federal law. The Chief Information Security Officer and team has completed a formal risk assessment of the student information system and regular scans are performed for vulnerabilities. With the FY2020 state audit, there was a management finding that other systems containing "non-public personal information" also required risk assessments; for example, UBI. The CISO and SFS plan to bring in a vendor to assist with these additional risk assessments.
	Student financial data breach (CUI)	NIST could classify federal student financial aid data as "controlled unclassified information" (CUI). This designation would require additional capital expenditures and/or new compliance programs to meet heighted security requirements. If classified as CUI, data breaches of financial aid data could result in civil fines and/or criminal charges.	UVA would need to develop new compliance and training programs. In addition, per Virginia Evans (VP ITS), a change in Federal classification would require substantial expenditures to purchase new hardware and software solutions. Jason Belford felt that the risk could be substantially lowered by moving the Student System from Oracle to a cloud-based platform.

Appendix 3

Highly Rated Risks	Identified Sub Risk	Analysis of Risk	Mitigation Plan
Data Security: Data Breach	**Patient data breach (HIPAA)**	Each category of violation carries a separate HIPAA penalty. OCR considers a number of factors when determining penalties, such as the length of time a violation was allowed to persist, the number of people affected and the nature of the data exposed. An organization´s willingness to assist with an OCR investigation is also taken into account. The general factors that can affect the level of financial penalty also include prior history, the organization's financial condition and the level of harm caused by the violation. • Tier 1: Minimum fine of $100 per violation up to $50,000; • Tier 2: Minimum fine of $1,000 per violation up to $50,000; • Tier 3: Minimum fine of $10,000 per violation up to $50,000; • Tier 4: Minimum fine of $50,000 per violation.	The Academic Division's clinical units (Sheila Johnson Center; Psychology; Student Health; School of Medicine) have compliance and training programs to ensure that all employees handling HIPAA-protected data are aware of their obligations under state and Federal law.
	Donor data breach	A breach of donor data would cause reputational harm and bad publicity. Mark Luellen felt that the risk is low overall because most sensitive donor data is not retained and adequate data protection is followed, but that there is some risk associated with donor data provided to affiliated foundations.	Advancement does not retain donor payment card data or social security numbers. All vendors are required to be PCI/DSS compliant and provide appropriate PCI documentation. Advancement mitigates the risk from Foundation access to donor data by requiring Foundations to enter into an NDA.
	Export controls breach	Criminal penalties for export control law violations can include up to 20 years of imprisonment and up to $1 million in fines per violation, or both. Administrative monetary penalties can reach up to $300,000 per violation or twice the value of the transaction, whichever is greater.	UVA has compliance and training programs to ensure that all employees handling export-controlled data are aware of their obligations under Federal law.
	Research data breach or loss	Kelly Hochstetler feels that the lack of a centralized research data archive is the most significant research data risk. Without a central archive, the potential exists in the event data is lost or an audit of research data is required. Depending on the type of data lost, financial impacts could range from very modest to exceptionally severe, e.g. if protected or commercially valuable data was lost.	Mitigation would involve creation of a centralized data archive with appropriate security features, as well as compliance initiatives to ensure use by all faculty and research staff.

Appendix 3

Highly Rated Risks	Identified Sub Risk	Analysis of Risk	Mitigation Plan
Data Security: Data Breach	**Data breach via illegal procurement**	Procurement of electronic equipment also poses a risk in UVA's decentralized environment. The US government prohibits the purchase of computer information that includes components manufactured by Huawei and other companies with close affiliation to the Chinese communist party. UVA's purchase order threshold of $10k increases the likelihood that a department will inadvertently purchase banned electronic components. In the most dire scenario, use of the banned components could lead to a system security breach and loss of substantial amounts of protected and valuable data.	UVA partially mitigates this risk through staff education on the issue.
	Payment card network breach (PCI/DSS implications)	PCI/DSS fines are set by contract with the merchant banks and can range up to $500,000 per violation.	Point-to-point encryption (P2PE) substantially eliminates the risk of electronic mass theft of payment card information. Mitigation efforts therefore are focused on ensuring proper departmental practice for handling credit card information.
	Third-party attacks, such as ransomware, phishing, cloud breach or network breach	Jason Belford noted that the biggest risk for third-party breaches results from the decentralized nature of the University and the lack of consistent controls. Hackers pursue the path of least resistance which is usually to gain entry by compromising an individual's account through a phishing link or other means of obtaining internal network access. Of particular concern lately is the increased frequency of ransomware attacks alongside new, highly effective extortion strategies. These tactics put institutions at risk of reputational damage and operational losses from extended downtime and remediation costs.	InfoSec pursues multiple mitigation strategies: • (i) encryption (full-disk encryption coming soon); • (ii) insurance (covers most out-of-pocket costs but does not cover us for loss of research data and its implications); • (iii) increased employee training; • (iv) transitioning operations to cloud-based platforms; and • (v) employing tiered networks to restrict access via high-security VPN's.

Appendix 3

Highly Rated Risks	Identified Sub Risk	Analysis of Risk	Mitigation Plan
Tax and Regulatory Changes Impacting Philanthropy and Endowment Return	**Nonprofit status of college athletics modified, with impacts on charitable giving**	The U.S. Supreme Court's June 2021 NCAA v. Alston decision and the NLRB's October 2021 general counsel memo signal a clear intention to treat certain college athletic programs as professional activities for Federal labor law purposes. If Alston is expanded further to permit direct compensation to student athletes, a consensus could soon emerge that collegiate athletics should be treated as quasi-professional for-profit activities across the board, including for Federal tax purposes. There are two potential impacts on charitable giving: (i) *Alston* overturned the NCAA's prohibition on providing additional educational benefits to college athletes and the opinion invites further challenges to the NCAA's authority to limit athlete compensation. In a future without NCAA restrictions, it may be permissible for donors to support individual athletes directly rather than through contributions to the athletes' institutions. (ii) the treatment of college athletics as taxable activities could result in elimination of the charitable contribution deduction for athletics-related donations. Loss of the deduction would disincentivize certain donors from giving to impacted sports programs.	Mitigation of the compensation and labor law risks would center on fiscal strategies such as fundraising, revenue maximization and cost containment. For instance, UVA could develop capital campaigns to ensure adequate funding for Olympic sports and meet Title IX expenditure requirements.
	Resumption of Grassley initiative to require a minimum distribution (up to 5%) from nonprofit foundation endowments	KPMG noted that private 509(a)(9) foundations have been subject to a 5% payout requirement for years. The imposition of a similar requirement for 501(c)(3) nonprofits would require a potentially disruptive reconsideration of institutional budgets. John Winn agreed that the higher endowment payouts would have a substantial impact on long-term endowment returns, as less money would remain invested.	Mitigation would involve revising annual spending projections which would likely impact approaches to student tuition and fees, department funding structures, etc. The complexity of such impacts would require analysis beyond the scope of this risk review.

Appendix 3

Highly Rated Risks	Identified Sub Risk	Analysis of Risk	Mitigation Plan
Tax and Regulatory Changes Impacting Philanthropy and Endowment Return	**Endowment excise tax extended to include public institutions (currently imposed only on private institutions)**	KPMG felt that expansion of the endowment excise tax (1.4% of net investment income) to public institutions was the biggest potential financial exposure given the size of the UVA endowment. However, KPMG was not aware of any current discussions to extend the tax to public institutions. John Glier confirmed that the issue is not a priority for the Biden administration. John Winn noted that given the size of UVA's student body, only a fraction of UVA's endowment would currently be subject to the tax. Dan Clifton felt that Congress was unlikely to expand the endowment excise tax or the executive compensation excise under the present Democratic administration. Dan believes that these taxes would not be a priority even if the Republicans retake the House or Senate in the 2022 elections, as the focus on higher education was a peculiar priority for the Trump administration rather than the Republican party generally.	UVA should consider development of a comprehensive federal governmental relations strategy, which could include advocacy efforts to address potentially adverse tax changes.
	Executive compensation excise tax extended from the top 5 highest paid employees to the top 10; or the salary threshold for taxation could be lowered	Expansion of the executive compensation excise tax would increase UVIMCO's costs and thus lower net endowment return. KPMG is not aware of any current initiatives to expand the executive compensation excise tax. UVA currently pays about $1.1m in tax.	UVA should consider development of a comprehensive federal governmental relations strategy, which could include advocacy efforts to address potentially adverse tax changes.
	Foreign tax laws could be changed and adversely impact investment returns or strategies	KPMG felt that changes is foreign tax law could have a significant impact on endowment performance. John Winn explained that foreign tax rate increases or changes to "blocker corporation" rules would not have a major impact on UVIMCO for two reasons: (i) UVIMCO doesn't employ blocker corp strategies and (ii) UVIMCO's carry-forward UBTI losses are so substantial that out-of-pocket liability is unlikely in the near future.	UVIMCO's reliance on domestic investment approaches effectively mitigates the impact of this risk.

Appendix 3

Highly Rated Risks	Identified Sub Risk	Analysis of Risk	Mitigation Plan
Tax and Regulatory Changes Impacting Philanthropy and Endowment Return	**Adverse charitable contribution tax law changes impacting donors**	KPMG noted that tax policy is increasingly geared towards raising rates on high earners, and thus it's conceivable that Congress could set an income cap above which taxpayers could not claim a deduction for charitable contributions. That change would be an obvious disincentive to charitable giving. Dan Clifton thought that any tax changes in the 2021 stimulus bill would be neutral to beneficial for charitable giving. The most likely changes (as of 10/21/21) involve funding new government programs with increases in personal and corporate income tax rates, and potentially a decrease in the estate tax exemption. There is no current discussion of limiting charitable contributions. Generally speaking, higher personal and corporate rates positively incentivize charitable giving. John Glier from GG&A reiterated KPMG's sentiments about raising taxes on wealthy individuals, noting possible changes in the laws for carried interest and stepped-up basis. He's also seeing donors becoming more creative with philanthropy, especially in the area of "co-investment"; i.e. donors receiving an ownership percentage and/or revenue stream from the entities/facilities funded by their donations. The attendant risk is that UVA may lose its competitive edge vis-a-vis its peers if it adopts a conservative posture of only accepting traditional contributions.	Mark Luellen noted that UVA currently relies on substantial gifts from major donors who are not as sensitive to normal fluctuations in tax rates. UVA should monitor changes in tax law and adapt as needed.

Appendix 3

Highly Rated Risks	Identified Sub Risk	Analysis of Risk	Mitigation Plan
Athletics	**Changes to remuneration practices for collegiate athletes as a result of *NCAA v. Alston* and potential future changes to NCAA regulations**	A significant risk to athletics' financial stability is the potential professionalization of major-money collegiate sports by the Federal courts and regulatory bodies. For many years Congress has been ambivalent about treating college athletics as nonprofit amateur endeavors, especially in the context of sports like football and basketball that generate significant revenue from television royalties and other commercial sources. The U.S. Supreme Court's June 2021 *NCAA v. Alston* decision signaled an intention to liberalize the remuneration of collegiate athletes to permit educational benefit payments from schools by ruling that the NCAA lacked authority to impose restrictions on such payments. As schools compete for athletic talent, it is very likely that UVA will need to begin providing some form of educational benefits or other remuneration to basketball and football players, and perhaps athletes from other sports as well. The increased costs of athlete remuneration (and potentially) benefits, resultant Title IX equity issues, and the need to create a new HR infrastructure to support a hybrid student/employee model, would require substantial financial resources.	Mitigation of the compensation and labor law risks would center on fiscal strategies such as fundraising, revenue maximization and cost containment. For instance, UVA could develop capital campaigns to ensure adequate funding for Olympic sports and meet Title IX expenditure requirements.
	Changes to Federal labor law treatment of NCAA athletes	Following shortly after the U.S. Supreme Court's *Alston* decision, the NLRB's issued a general counsel memo in October 2021 stating that college athletes were considered employees for Federal labor law purposes. Because UVA is a public institution in a right-to-work state, the NLRB memo has no direct applicability at present. However, the memo further indicates a preference at the Federal level to treat collegiate athletes as both students and employees of their institutions.	Mitigation of the compensation and labor law risks would center on fiscal strategies such as fundraising, revenue maximization and cost containment. For instance, UVA could develop capital campaigns to ensure adequate funding for Olympic sports and meet Title IX expenditure requirements.

Appendix 3

Highly Rated Risks	Identified Sub Risk	Analysis of Risk	Mitigation Plan
Athletics	**Tax implications of recharacterization of college athletics as a for-profit endeavor**	If *Alston* is expanded, a consensus could emerge that major-money collegiate athletics should be treated as a quasi-professional for-profit activity for all purposes, including Federal taxation. This could have a variety of impacts, including: (i) UBIT: Revenue from certain sports could be deemed to be taxable "unrelated business income" rather than nontaxable mission-related income. (ii) Charitable giving: Absent NCAA restrictions on athlete compensation, it may be permissible for donors to support individual athletes directly rather than through contributions to their institutions; and (b) the charitable contribution deduction for athletics-related donations could be eliminated which would disincentivize certain donors from giving to impacted sports programs. (iii) Capital Costs: Athletic facilities for certain sports or of certain scale could be deemed ineligible for tax-exempt financing, raising costs of new construction and improvements.	Mitigation would entail making financial accommodations to address higher capital and tax costs and potentially lower charitable giving.
	Major natural or man-made disaster that renders JPJ and/or Scott stadium unusable, or results in cancellation of the entire football and/or basketball seasons	Athletics' revenue could be substantially impacted by either a natural disaster (hurricane, earthquake, tornado) or a man-made event (e.g. terrorist attack) that damages Scott Stadium and/or JPJ Arena, or precludes the conduct of a normal sports season. The COVID-19 pandemic was an illustration of this possibility.	Jim Booz noted that Athletics' response to natural disasters would be dependent on the nature of the disaster, but the primary driver for any response would be the safety and well-being of student athletes and Athletics' staff.
	Proliferation of name-image-likeness licensing by student athletes	As of July 1, 2021, NCAA rules permit student athletes to pursue name, image & likeness deals. While the arrangements would be directly between the athlete and the sponsoring entity, the possibility exists for NIL licensing to have a disruptive effect on team performance. The potential also exists for individual bad actors to arrange athlete sponsorship deals as a condition of attendance which would cause both compliance and reputational issues.	Jim Booz felt that NIL licensing was not presently a problem at UVA given the lack of stand-out major-money sports stars. The athletes most like to receive NIL payments at UVA are in baseball, swimming and volleyball where payment amounts tend to be rather modest. However, NIL could potentially become a problem if a top football or basketball recruit enrolled at UVA, and so the administration should continue to monitor this issue.

Appendix 3

Highly Rated Risks	Identified Sub Risk	Analysis of Risk	Mitigation Plan
Financial Operations: Vendor Payments	**Ghost vendor**	Fraud risk where an individual with access creates a fake vendor, gets a purchase order, and then submits invoices paid for services that are not performed	Vendor validation and approval when set up new vendors; periodically vendor validation for existing vendor to inactivate hibernating vendors.
	Vendor with COI not evaluated and disclosed	A university employee contracts out the same or similar services they already perform as an employee A university employee promotes their own business or family member's business, giving an advantage to that business over other suppliers	Annual COI disclosure process prompts the employee community to disclose relationships; and vendor registration system prompts vendors for relationship disclosure; in FY23, new reporting will audit/monitor employee and vendor records with the same address & Tax ID to further mitigate risk.
	Active valid vendor has their bank info inappropriately changed	1. Vendor entered incorrect bank info 2. Vendor failed to update its bank info 3. UVA employee change vendor bank info without approval - Note: Only applicable to Wire payments in FY22, as UVA employees will not be able to see or edit supplier bank accounts with ACH or PayMode 4. Bank system is compromised and vendor's bank info is changed 5. Imposter/Fraudster gains access to Supplier's ACH info by gaining username/password info	PaymentWorks was designed to prevent this fraud.
	Administrative error that UVA process over/under payment	1. Paymount Voucher Creation is incorrect amount 2. Match exceptions are not appropriately handled 3. Non PO Payment is made when should have been a PO	Workday will limit the volume of non-PO invoices allowed, reducing the overall impact of this risk. Department fiscal approvers will be asked to validate match exceptions in Workday prior to releasing payment.
	UVA employee processes same payment twice	1. Simultaneous entry on duplicate submission 2. Modification of an invoice during processing - amending Invoice # 3. Fraud / collusion	We are automating invoices with both cXML and OCR technology, limiting manual key entry and duplicates. Collusion is always a possibility, but can be monitored via advanced monitoring metrics we plan to introduce in FY23.
	UVA employee creates and processes fake payment	Fraud / collusion	We are investing in risk analytics/monitoring technology and advanced Workday reporting to catch this type of risk.

Appendix 3

Highly Rated Risks	Identified Sub Risk	Analysis of Risk	Mitigation Plan
Financial Operations: Vendor Payments	**Vendor over/under charged UVA and it is processed and paid without being noticed**	Vendor sends invoice multiple times, and changes the invoice number Vendor fails to send credit memo	This type of risk should get caught with match exception rules in place. Follow through on credit memos can be mitigated with periodic audits designed to pursue missing credits.
	Vendor charges UVA twice for the same product or services and gets processed and paid without being noticed	Match exceptions don't catch the error due to tolerance settings	The Workday match exceptions are fairly precise, but if the PO is set up as a high dollar balance/ blanket PO, double invoicing could get lost in the mix. Invoices > $10K will route to the department for fiscal approval to confirm receipt goods/ services.
	Vendor charged UVA for product or service not provided and gets processed and paid without being noticed	Department receives goods/services in full on the PO prior to goods/services been delivered. Vendor submits invoice and system automatically pays. Dept wants to dispute the invoice, but it's already paid.	Invoices > $10K will route to department for confirmation of receipt goods/services. Real risk is in the < $10K category.
	Vendor charges correctly and UVA process and pay correctly, but bank system is compromised resulting in payment issue	Cyber security fraud and/or social engineering fraud	PaymentWorks ensures $2M/incident in this type of fraud; UVA will insure an additional $3M/ incident on top of that and other insurance policies may be applicable depending on circumstances.
	Payment is late resulting in missing out payment incentives, or damaging relationships, or non-compliance to state requirement of 95% payment within terms	Invoices go on receiving hold due to lack of updated receiving, causing delays in payment	We are investing in invoice automation and improved reporting in order to prevent late payment. Historically, we have operated in the 98% prompt pay realm.


UNIVERSITY of VIRGINIA