Board of Visitors
Audit, Integrity and Compliance Committee
12:00 p.m.
September 14, 2023
VCU School of Business
301 W. Main Street, Third Floor, Room B3187

Minutes

COMMITTEE MEMBERS PRESENT Mr.
Peter Farrell, *Chair*
Ms. Ellen Fitzsimmons, *Vice Chair* Dr.
Dale Jones
Mr. Edward McCoy
Mr. Keith Parker
Mr. P2 Sandhu
The Honorable Todd Haymore, *Rector*

COMMITTEE MEMBERS ABSENT
Mr. H. Benson Dendy, III

OTHERS PRESENT
Ms. Karen Helderman, *Executive Director for Audit and Compliance Services*
Dr. Michael Rao, *President*
Mr. Jacob A. Belue, *Associate University Counsel*
Staff from VCU

CALL TO ORDER

Mr. Peter Farrell, Chair, called the meeting to order at 12:11 p.m.

APPROVAL OF MINUTES

Mr. Peter Farrell asked for a motion to approve the minutes of the May 11, 2023 meeting of the Audit, Integrity and Compliance Committee, as published. After motion duly made and seconded, the minutes of the May 11, 2023 Audit, Integrity, and Compliance Committee meeting were approved. A copy of the minutes can be found on the VCU website at the following webpage http://www.president.vcu.edu/board/minutes.html

Report from the Executive Director of Audit and Compliance Services

Karen Helderman shared the results of several audit reports. The first was a status report on the implementation of corrective actions in response to previous audit findings. There were three findings in the report, all dating back to January 2020, and each requested a due date extension to early summer 2024. Mr. Farrell noted that there seems to be a pattern with follow ups not meeting the target date. He also stated that the board needs to be notified at each meeting whether or not target dates will be met. The second was a report on Parking Bill and Reserves which recommended the university develop a parking, citations and enforcement policy to ensure compliance with the Virginia Debt Collection Act. There were then two reports on Global Education and the Graduate School and these had no board level recommendations. The final audit report was an evaluation of the Athletics Name, Image and Likeness compliance program and there were no board level findings. In addition, VCU's Chief Ethics and Compliance Officer, Suzanne Milton, presented an annual Integrity and Compliance Services report. The report noted a 24% increase in the number of reported concerns since last year, which is an indicator that individuals are feeling more comfortable speaking up. VCU's substantiation rate of these concerns, at 58%, is trending higher than our industry benchmark of 41%. This indicates that when our employees speak up, more often than not their concern is valid. 7% of the individuals reporting concerns at VCU express a fear of retaliation down from 11% in fiscal year 2022.

Information Technology Update

Alex Henson, Chief Technology Officer updated the committee on VCU's major enterprise IT risks and mitigations underway or planned to address these risks.

A copy of the presentation is attached hereto as **Attachment A** and is made a part hereof.

CLOSED SESSION

On motion made and seconded, the Audit, Integrity, and Compliance Committee of the Virginia Commonwealth University Board of Visitors convened into closed session under Section 2.2-3711 (A)(7) of the Virginia Freedom of Information Act for consultation with legal counsel pertaining to specific legal matters requiring legal advice by counsel and actual or probable litigation, where such consultation of briefing in open meeting would adversely affect the negotiating or litigating posture of the university, namely a survey of and status report on the university's positions in potential and current litigation in state and federal courts and other legal matters relating to pending investigations; and under Section 2.2-3711 (A)(19) for discussion of specific cybersecurity vulnerabilities and briefing by staff concerning actions taken to respond to such matters, specifically pertaining to human subjects research data and related IT processes.

RECONVENED SESSION

Following the closed session, the public was invited to return to the meeting. Mr. Farrell, Chair, called the meeting to order. On motion duly made and seconded the following resolution of certification was approved by a roll call vote:

Resolution of Certification

BE IT RESOLVED, that the Audit, Integrity, and Compliance Committee of the Board of Visitors of Virginia Commonwealth University certifies that, to the best of each member's knowledge, (i) only public business matters lawfully exempted from open meeting requirements under this chapter were discussed in the closed meeting to which this certification resolution applies, and (ii) only such public business matters as were identified in the motion by which the closed session was convened were heard, discussed or considered by the Committee of the Board.

Vote	Ayes	Nays
Mr. Peter Farrell, Chair	X	
Ms. Ellen Fitzsimmons, Vice Chair	X	
Dr. Dale Jones	X	
Mr. Edward McCoy	X	
Mr. Keith Parker	X	
Mr. P2 Sandhu	X	
Mr. Todd Haymore, Rector	X	

All members responding affirmatively, the motion was adopted.

ADJOURNMENT

There being no further business, Mr. Farrell, Chair, adjourned the meeting at 1:53 p.m.

ATTACHMENT A

Board of Visitors
Audit, Integrity and Compliance Committee

September 14, 2023

ACTION ITEMS

APPROVAL OF MINUTES

- Audit, Integrity and Compliance Committee Meeting held on May 11, 2023

- Motion to approve the Minutes

FOR INFORMATION

Committee Dashboard Measures

- 🟢 Data Governance Program
- 🟡 Data Security
- 🟡 ERM Mitigation Plans
- 🟢 Planned Audits
- 🟢 Planned Special Projects
- 🟢 Ethics and Compliance Program Oversight

ACS Departmental Update

- ## Staffing and Credentials

    - ✓ Well Qualified

- ## Department Expenses

    - ✓ Department expenses higher than prior year due to 5% pay increase but still within authorized budget

- ## Audit Survey Results

    - ✓ Overall rating of 3.62/4.0; consistent with rating of 3.61 in FY22

Status of FY23 Follow-up Report

Board Level Finding	First Revised Date	Current Due Date
Enforce Central Works Pro Fire Alarm Server Security Baseline Compliance *(Jan 2020)*	Jan 2023	June 2024

Management Level Findings	First Revised Date	Current Due Date
Facilitate Establishment of Policy to Govern Non-Research Institutes and Centers *(Jan 2020)*	May 2023	May 2024
Develop Operations Center Disaster Recovery Plan *(Jan 2020)*	Jan 2023	June 2024

Parking Billing and Reserves

Audit Scope:

- Accurate calculation of parking rates

- Timely deactivation of parking privileges upon separation from the university

- Collections of fines for parking violations

- Method of determination and monitoring of reserves

Conclusion:

Parking collected sufficient revenues to sustain operations as an auxiliary enterprise and maintain required reserves, however, parking did not have a policy and related procedures for collecting unpaid fines and penalties compliant with the Virginia Debt Collection Act

One Board Level Finding

- Develop a Parking, Citations, and Enforcement Policy

Audit Scope:

Reviewed selected controls and compliance areas

- reconciliations
- purchases
- Pcards
- fixed asset management

No Board level findings

Athletics-Name, Image and Likeness

Audit Scope:

We focused on an evaluation of Athletics' compliance program specific to NIL activities, based on the elements of an effective compliance program:
- Oversight
- Policies
- Training
- Communication
- Monitoring
- Enforcement
- Corrective Action

Conclusion:

Athletics had effective compliance processes in place that would ensure due diligence in compliance with name, image and likeness regulations

No Board level findings

Academic and Executive Administrator Contracts

Audit Scope:

Our review encompassed fiscal years 2022 and 2023, focusing on current practices of developing and issuing employment contracts for academic and executive administrator contracts.

Conclusion:

Current academic and executive administrator contracts reflect compensation appropriately approved and adjusted for changes in roles and responsibilities

No Board level findings

Integrity and Compliance
Annual Report

FISCAL YEAR 2023

Annual Report Highlights

Three-Year Workplan Areas of Focus

|		
Program Structure	**Culture**	**Policies**
Investigations and Accountability	**Training and Communications**	**Risk Assessment and Monitoring**

# Program Structure and Resources

Compliance Steering Committee meets quarterly:

- **Focused on compliance program documentation (one-pagers), improvements in training/communication, monitoring/auditing and risk assessment**

- **Forum for information sharing, collaboration and issue-spotting (compliance gaps)**

- **Larger Compliance Advisory Committee meets twice annually, usually including a government relations briefing**

Culture and Data Analysis

Report volumes are trending up to pre-pandemic levels; retaliation allegations, anonymous reports trending down
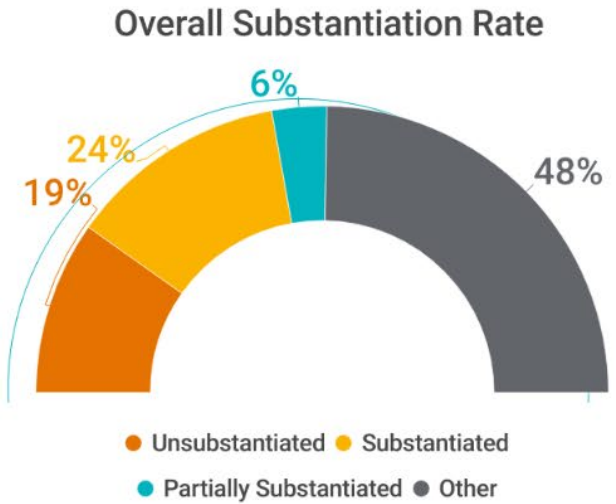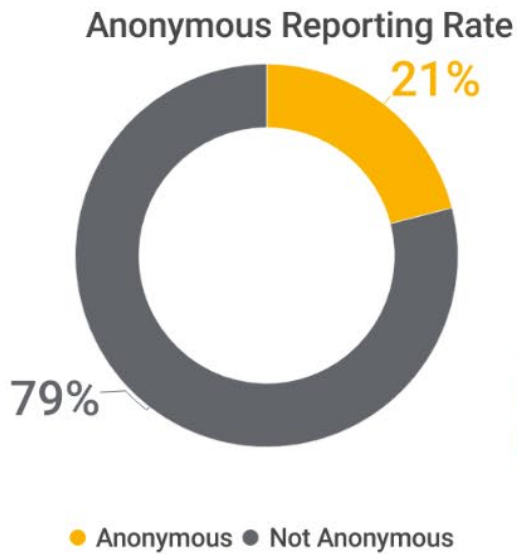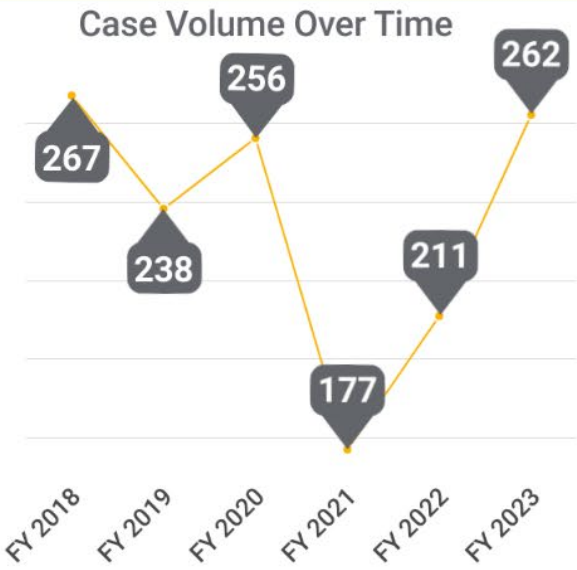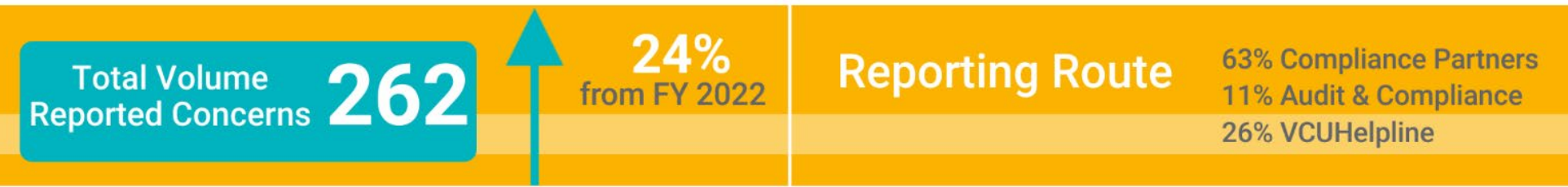
Culture and Data Analysis

Adjusted substantiation rate (excluding cases not investigated) rises to 58%, favorable to benchmarks and SPLY. Anonymous rate remains better than internal benchmark and significantly better than external rate.

	Cases per 100 Employees	Anonymous Reporting Rate	Substantiation Rate	Concerns of Retaliation	Most Common Issue Type
NAVEX Benchmark	1.47	56%	41%	0.96%	HR, Diversity, and Workplace Respect
VCU Internal Benchmark	1.95	23%	45%	7%	Ethics Violation
Current Fiscal Year	2.45	21%	30% raw / 58% adj'd	7%	Ethics Violation

Culture: New Integrity Survey FY 2024

➢ **Due to organizational changes in Institutional Research and Decision Support (IRDS) and Institutional Equity, Effectiveness and Success (IEES), VCU's Culture and Climate Survey was not fielded in FY 2023, so the planned Integrity Index was not delivered.**
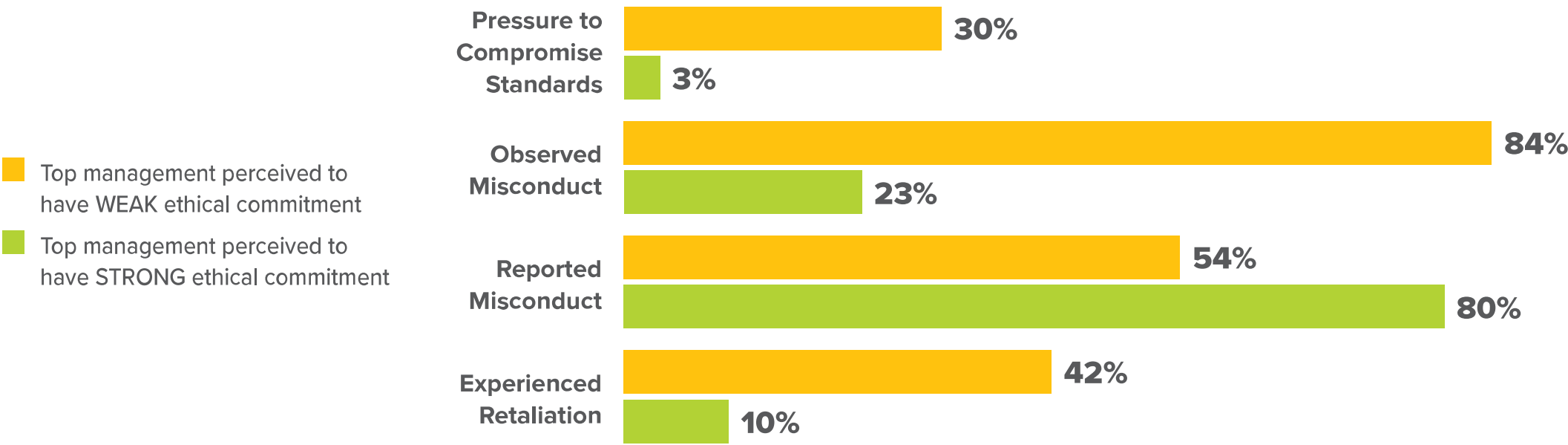
➢ **Instead, the Integrity and Compliance Office (ICO) is contracting for a third-party hosted integrity survey to be fielded in FY 2024 to provide baseline and benchmarked data on the culture of integrity at VCU.**

➢ **ICO will report this data to departments and partner with them to understand their results and make progress in sustaining a culture of integrity and openness.**

Measuring Culture

When leaders demonstrate a commitment to ethics, workplace integrity improves significantly.*

Legend:
- 🟧 Top management perceived to have WEAK ethical commitment
- 🟩 Top management perceived to have STRONG ethical commitment

Category	WEAK	STRONG
Pressure to Compromise Standards	30%	3%
Observed Misconduct	84%	23%
Reported Misconduct	54%	80%
Experienced Retaliation	42%	10%

*Ethics and Compliance Initiative (ECI), July, 2023 Fellows Meeting, taken from 2023 Global Business Ethics Survey, (forthcoming, fall 2023).

Policy Program Update

161
TOTAL POLICIES

13
New or Substantially Revised

20
Minor Revisions Made

37
Past Due or Under Review

7
Retired

Out of Date Policies Over Time

FY 2017	FY 2018	FY 2019	FY 2020	FY 2021	FY 2022	FY 2023
53%	34%	37%	40%	34%	28%	23%
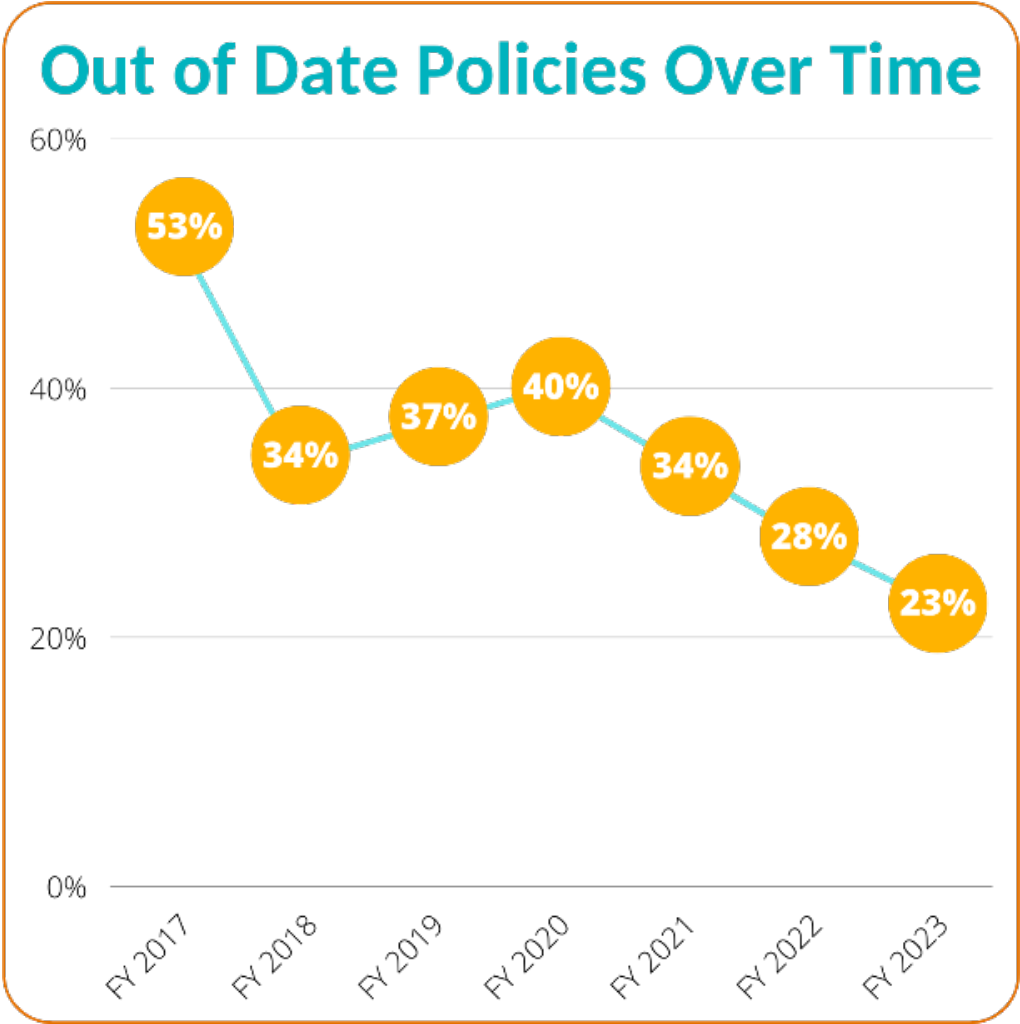
Investigations and Accountability

Sanctions

Sanction	Count
Verbal Counseling	23
Training Required	21
Written Counseling	11
Written Warning I	11
Resignation	6
Termination	4
Group I Written Notice	4

48 Average Days to Close

28 Open Cases Remaining

	Average Days to Close
NAVEX Benchmark	44
VCU 3-Year Benchmark	86
FY 2023	48
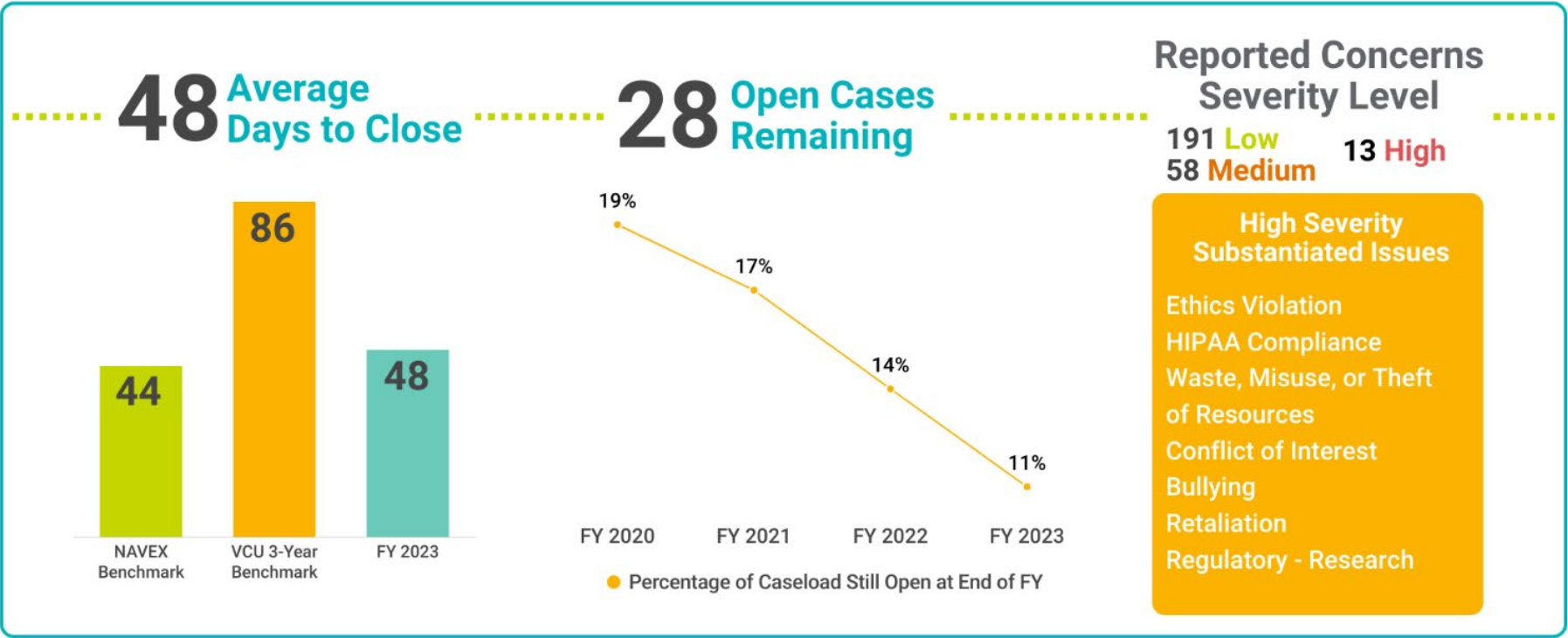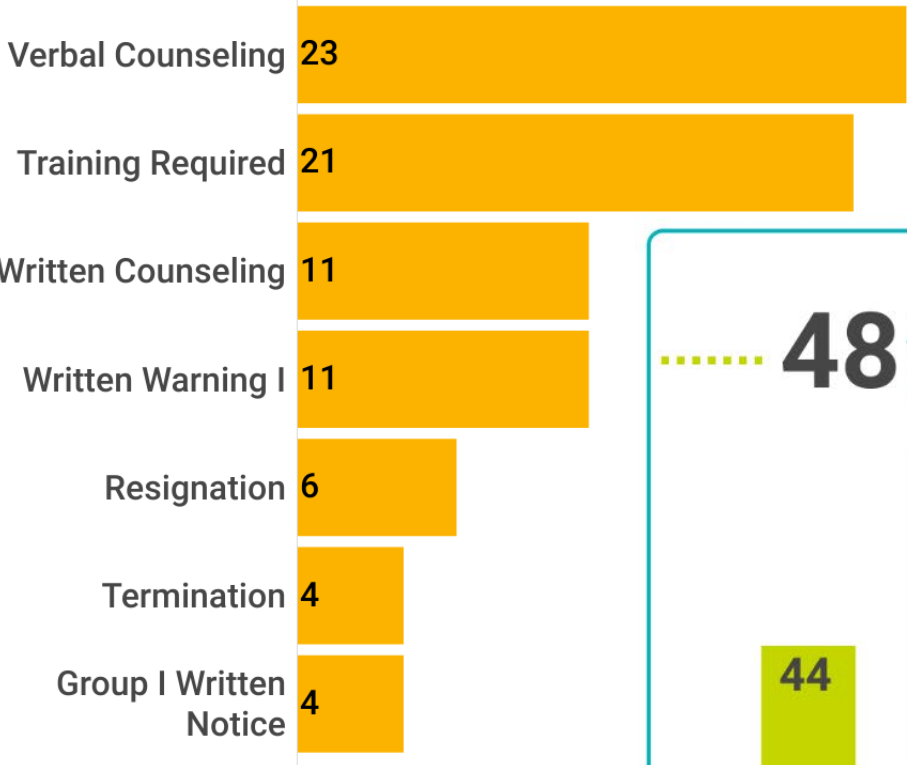
Percentage of Caseload Still Open at End of FY

- FY 2020: 19%
- FY 2021: 17%
- FY 2022: 14%
- FY 2023: 11%

Reported Concerns Severity Level

191 Low
58 Medium
13 High

High Severity Substantiated Issues

Ethics Violation
HIPAA Compliance
Waste, Misuse, or Theft of Resources
Conflict of Interest
Bullying
Retaliation
Regulatory - Research

Training and Communications

- Launched two university-wide required trainings (to catch up from pandemic delay)

- Increased employee engagement by adding interactive scenarios (Fig. 1), videos featuring students (Fig. 2), faculty, staff and our CECO to the FY 2023 training

- Created/facilitated new workshop for leadership on Psychological Safety; recently debuted a team version, for managers and employees

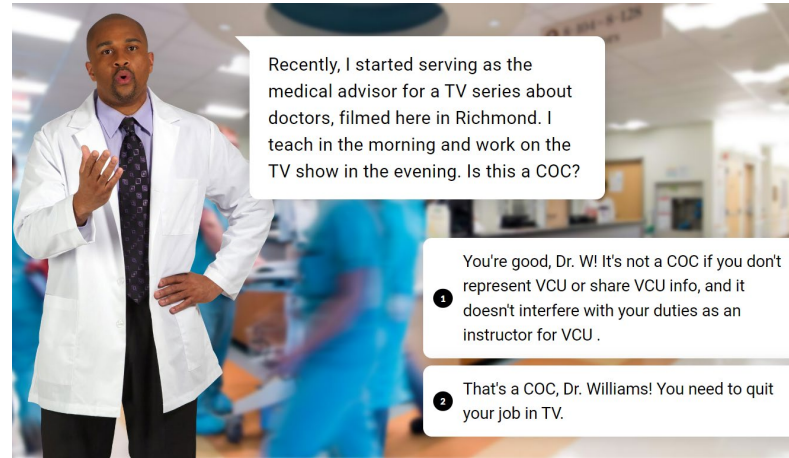- Continued monthly blog, featuring E&C trends and case studies

Fig. 1

Fig. 2

8,351
Employees who completed the Ethics and Compliance Annual Training for FY23

2
Email blasts
8,653
recipients ea.
65.71%
avg. open rate

1
New workshop created
5
conducted
2
upcoming

12
Compliance Case Studies posted to ICO blog
2653
page views

Risk Assessment and Monitoring

COI&C

Action: Completed new COI&C policy, completed pilot test in four schools, new system rolling out now university-wide
Results: Standardizes expectations, closes compliance gaps, reduces administrative burden

Research Infrastructure

Action: Handle research matters in close collaboration with OVPRI, support "speak-up, listen-up" cultural learning and development in OVPRI and with partners
Results: Renewed focus on Research Infrastructure, must support compliance and culture of transparency and accountability

Speak-up Culture & Leadership

Action: Created, continuing facilitation of Psychological Safety workshop for leaders and teams
Results: Reduced allegations and substantiation of retaliation but continued trend of significant number of substantiated cases involving more senior leaders

ERM

Action: Participating in ERM Steering Committee; engaging both CAC and CSC in documenting, integrating risk identification, mitigation and escalation processes
Results: Provides opportunity to integrate risk assessments, ensures emerging risks are captured and addressed

IT Risk Management Update

Board of Visitors Meeting
Audit, Integrity and Compliance Committee
Alex Henson, Chief Information Officer
September 14, 2023

Enterprise Risk Classified Out of Tolerance

IT System Availability and Data Security

Extended systems or connectivity outage

**Theft or improper exposure of data**

Sub-Risks and Drivers

Unplanned outage of Ellucian Banner ERP System (Finance, HR, Student)

- Run on-premise in one data center with limited fail-over capability
- Vulnerable to power and weather conditions
- Time to restore in the event of disaster increased impact/severity associated with risk
- ***Risk drastically reduced through Ellucian Cloud migration***

Data exposure or theft through Ransomware, Malware, or other attack vector focused on end-users

- Decentralized device management
- Controls like Multi-factor authentication (MFA) and the Virtual Private Network (VPN) did not cover the whole enterprise
- ***Risk reduced by implementing SASE/Zscaler zero-trust architecture and leveraging centralized endpoint management***

Risk Tolerance
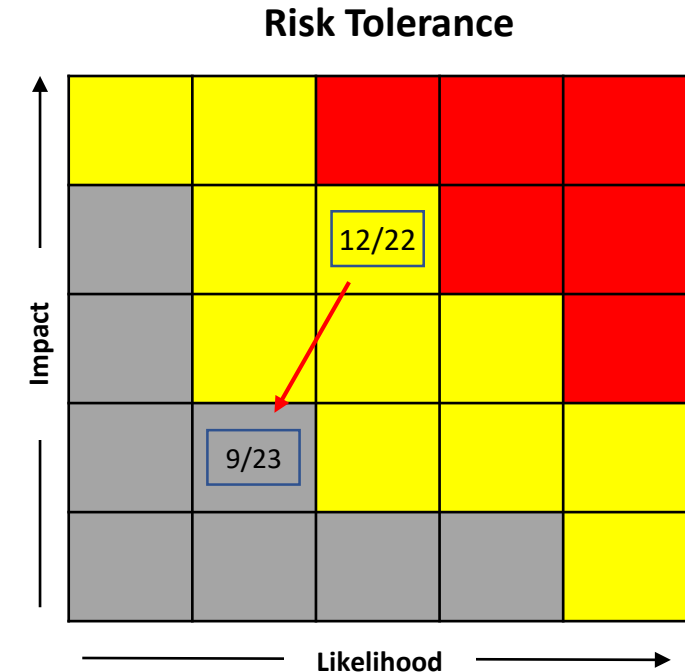
Risk Mitigation: IT Infrastructure

Develop and maintain a modern, robust, and "always-on" IT infrastructure to maximize uptime and minimize vulnerabilities and operational impact due to external factors.

Cloud Strategy and Service Migrations
- Banner migration to Ellucian Cloud
- Cloud migration of other vendor managed applications
- Cloud-first strategy and roadmap development
- Leverage Infrastructure as a Service (IaaS) where advantageous

Technology Operations Center
- TOC Construction in progress for go-live of new data center in early 2024
- Redundant power and generator
- Robust back-up and recovery leveraging in-house and cloud resources

Network Upgrades & Expansion
- Continued development of redundant fiber paths
- Use of multiple commodity internet providers
- Implementation of Application Centric Infrastructure (ACI) to automate and optimize the data network progressing

IT Infrastructure Management
- Day to day maintenance, upgrades, support of systems/services
- Rigorous change management procedures/processes
- Leverage new technologies

Risk Mitigation: Data Security

Develop and maintain a secure IT environment with supporting policies and processes that drive compliance to security and privacy laws and protect VCU data

Implement New Security Architecture

- Phase 1 of Secure Access Server Edge (SASE) deployment complete with zScaler fully implemented
- Upgrading VPN and ultimately replacing with cloud-based service

Expand Multi Factor Authentication

- Use of DUO multifactor authentication now mandatory for students
- DUO authentication required for all applications with any level of sensitive data

Renewed Focus on Secure Data Use for Research

- Implementing new Horizon system for researchers accessing clinical data
- Strengthening Honest Broker program for researchers to use data protected by HIPAA
- Enhanced support for PIs

IT Governance and Data Governance

- Revamped IT Governance program to ensure all IT purchases have thorough security review and data classification review
- Continued refinement of data governance policies and procedures and investment in technologies that automate data governance

Emerging Risks & Challenges

Increasing reliance on Third-Parties
- Reliant on contractual provisions, security assessments, and audit reports
- Proliferation of cloud-based services requires increased scrutiny and governance

Increased sophistication of global ransomware organizations and other threat actors
- "Long game" targeted social engineering has become profitable
- Credential stuffing and other threats have increased
- Education and training even more critical

Increasing Compliance Requirements
- New GLBA and Department of Education requirements – particularly around Financial Aid and other Controlled Unclassified Information (CUI)
- Latest version of PCI-DSS (Payment Card Industry – Data Security Standards) is more stringent

Questions?

CLOSED SESSION