BOARD *of* GOVERNORS
State University System of Florida

Audit and Compliance Committee

Joe Maleszewski, Inspector General and Director of Compliance
January 25, 2018

www.flbog.edu

STATE UNIVERSITY SYSTEM of FLORIDA
Board of Governors

Office of the Chancellor
325 West Gaines Street, Suite 1614
Tallahassee, FL 32399
Phone 850.245.0466
Fax 850.245.9685
www.flbog.edu

September 1, 2017

MEMORANDUM

To: Chairs, University Boards of Trustees
          University Presidents

From: Thomas G. Kuntz, Chair

Subject: 2017 SUS ERM Practices Survey - Due September 15, 2017

An important part of governance for higher education is having processes in place to ensure that administrators and boards of trustees identify, assess, manage, and control risks. According to the Society of Corporate Compliance and Ethics, universities are the most regulated industry. This is due to the broad portfolio of risks that universities must manage.

Enterprise Risk Management (ERM), as used by governing boards and senior administrators, combines traditional risk management, strategic planning, and internal controls. The goal of ERM is to move away from viewing risk in silos, separate and distinct from the university's overall mission. Instead, ERM encourages a more holistic view of risk by considering risks across the university. By adopting this approach, leadership can focus more broadly on the risks most likely to impede the university's achievement of its mission.

The board of trustees has overall responsibility for ensuring that risks are managed. In practice, the board of trustees delegates the operation of the risk management framework to the management team, who are responsible for its implementation. Everyone in the organization plays a role in ensuring successful ERM, but the primary responsibility for identifying and managing risks lies with management. Done well, ERM identifies potential events that may adversely affect the university and appropriately manages risks within the range of risk tolerance acceptable to each board.

14 *A Wake-up Call: Enterprise Risk*
ge and university governing boards
An effective institutional or ERM
ard, will increase the likelihood that
uent university, will achieve its

nsibility, the Board of Governors
oss the State University System. I
eturn the attached *2017 SUS ERM*
mber 15, 2017, to our Inspector
below.

nforming the Board of Governors
tor General will summarize and
and Compliance Committee

e do not hesitate to contact the Board
eneral@flbog.edu or 850-245-0466.

ee Chair

rector of Compliance

Florida A&M University | Florida Atlantic University | Florida Gulf Coast University | Florida International University
Florida Polytechnic University | Florida State University | New College of Florida | University of Central Florida
University of Florida | University of North Florida | University of South Florida | University of West Florida

"Higher education is the most regulated industry"

Adam Turteltaub, Vice President, Society for Corporate Compliance and Ethics Professionals, 2014 Higher Education Compliance Conference

"Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes."

GOVERNANCE, CONTROL, AND RISK MANAGMENT

Governance	• Strategic and operational decision-making • Overseeing and communicating risk management and control information • Promoting organizational ethics and values • Ensuring effective organizational performance management and accountability • Coordinating with the board, external and internal auditors, other assurance providers, and management
Control	Any action taken by management, the board, and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved. Management plans, organizes, and directs the performance of sufficient actions to provide reasonable assurance that objectives and goals will be achieved.
Risk Management	A process to identify, assess, manage, and control potential events or situations to provide reasonable assurance regarding the achievement of the organization's objectives.

2120 – Risk Management

The internal audit activity <u>must</u> evaluate the effectiveness and contribute to the improvement of risk management processes.

2120.C3 – When assisting management in establishing or improving risk management processes, internal auditors must refrain from assuming any management responsibility by actually managing risks.

TRADITIONAL RISK MANAGEMENT V. ERM

Traditional Risk Management	Enterprise Risk Management
Segmented	Enterprise-wide
Department-driven risk approach	Board-driven risk approach
Little or no knowledge of overall organizational risks	Broad perspective on overall organizational risk
Focused on preventing loss within the business unit (tactical)	Focused on enhancing value, capitalizing on opportunities, and managing all risks across the entire organization (strategic)
Scope: physical and financial assets	Scope: entire asset portfolio
Siloed risk mitigation	Enterprise-wide risk mitigation

ERM PROGRAM CHARACTERISTICS

- Enterprise-wide Approach
- Executive-level Sponsorship
- Defined Accountability
- Intentional
- Systematic and Structured
- Defined Risk Appetite
- Establishment and Communication of Risk Management Process Goals and Activities
- Monitored Treatment Plans

Essential Elements of Enterprise Risk Management (ERM)

Align ERM process to goals and objectives → Identify Risks → Assess Risks → Select Risk Response → Monitor Risks → Communicate and Report on Risks

SUS RISK MANAGEMENT SURVEY RESULTS

Percent	Information
100%	Traditional risk management
100%	Communicate risks to senior management
50%	Enterprise-level risk inventory
100%	Board-level committee responsible for risk management
50%	Management-level risk committee
25%	ERM governing document
75%	Board of Trustees communicates Risk Appetite

University	Best Practices
FIU	• Enterprise Risk Management Framework (23-pages) • Executive ERM sponsor
UWF	• Risk and Compliance Council (with Charter) • Annual risk heat matrix
USF	• Triennial enterprise-wide risk assessment (2011) • Risk mitigation follow-up in years 2 and 3

Mental Health Counseling

Campus Safety

Cloud Computing

PBF Data and Metrics

Facilities Infrastructure

Sliding Enrollments

Cost and Access

Delivering Value

Campus Climate

Cybersecurity/Cyberterrorism

Academic Freedom & Free Speech

Achieving and Maintaining Diversity

Speed of Growth

Regulation Compliance

Legislation/Regulation Complexity

Cost of Faculty/Staff Recruitment

Meeting University's Mission

Corrective Action Plan Timeline

DATE	ACTION
March 28, 2017	Final Report Issued
March 30-31, 2017	Investigative findings presentation, BOG meeting
April 18, 2017	CAP requested (Due: May 26, 2017)
May 9, 2017	FGCU BOT meeting; Received FGCU CAP
June 13, 2017	FGCU BOT meeting
June 21, 2017	CAP update presentation, BOG meeting
June 29, 2017	FGCU BOT conference call
October 10, 2017	FGCU BOT meeting
December 8, 2017	FGCU BOT meeting
January 25, 2018	CAP update presentation, BOG meeting
June 2018	Anticipated final BOG update

Corrective Actions Status Summary

Complete (13)

Expected Completion Spring 2018 (1)

Pending Completion (1)

Corrective Actions Status Summary

Complete (87%)	Pending Completion (7%)	Expected Completion Spring 2018 (6%)
• Vice Chair Election • Autonomous AACC • Separate BOT and AACC Chair • Sunshine Law training • SACS Consult • Legal Opinion - Advisory Committee Meeting Minutes • Supervisory Training • OIEC Coordination • **Enhanced New Trustee Orientation with Acknowledgement Form**	• Strategic Plan Approval by Board of Governors	• Ethics Training for Board of Trustees

SUS Compliance Program Status Checklist Summary - Baseline

Univ.	University-Wide Compliance Program	Program Plan	BOT Committee	Chief Compliance Officer	External 5-Year Program Review
FAMU	🟢 🟢 N/B N/B	N/B N/B 🟢 ✔ N/B	🟢 🟢 N/B N/B	🟢 🟢 🟢 N/B N/B	–
FAU	🟢 ✔ 🟢 ✔	🟢 🟢 🟢 ✔ 🟢	🟢 🟢 🟢 🟢	✔ ✔ 🟢 ✔ 🟢	–
FGCU	🟡 🟡 🟢 🟡	🟡 🟢 🟢 ✔ N/B	🟢 N/B 🟢 ✔	✔ 🟢 🟢 ✔ ✔	–
FIU	✔ ✔ 🟢 ✔	🟢 🟢 ✔ ✔ 🟢	✔ 🟢 ✔ ✔	🟢 ✔ 🟢 ✔ ✔	–
FL Poly	🟡 🟡 🟡 🟢	🟡 🟡 🟡 🟡 🟡	🟡 🟡 🟡 🟡	🟡 🟡 🟡 🟡 🟡	–
FSU	🟡 N/B 🟡 🟡	N/B 🟡 N/B 🟢 N/B	N/B N/B N/B N/B	N/B N/B N/B N/B N/B	–
NCF	🟡 N/B ✔ 🟡	🟡 🟡 🟡 🟡 N/B	🟢 🟢 N/B N/B	🟡 🟡 🟡 🟡 🟡	–
UCF	✔ ✔ ✔ ✔	🟢 🟢 ✔ ✔ ✔	✔ ✔ ✔ ✔	✔ ✔ ✔ ✔ ✔	–
UF	🟢 🟢 🟢 🟢	🟢 🟡 🟢 ✔ 🟢	🟢 🟢 🟢 🟢	🟢 🟢 🟢 🟢 🟢	–
UNF	🟢 ✔ 🟢 ✔	🟢 🟢 N/B 🟢 N/B	✔ ✔ ✔ 🟢	✔ ✔ 🟢 ✔ 🟢	–
USF	✔ ✔ ✔ ✔	🟢 🟢 🟢 ✔ ✔	✔ 🟢 ✔ ✔	✔ ✔ 🟢 ✔ ✔	–
UWF	🟢 🟢 ✔ ✔	🟢 🟢 🟢 🟢 🟢	✔ ✔ ✔ 🟢	🟢 🟡 ✔ 🟢 🟢	–

SUS Compliance Program Status Checklist Summary - Year 1

Univ.	University-Wide Compliance Program	Program Plan	BOT Committee	Chief Compliance Officer	External 5-Year Program Review
FAMU	● ● ● ✓	● ● ✓ ✓ ●	✓ ✓ ✓ ✓	✓ ✓ ✓ ✓ ✓	N/B
FAU	● ✓ ✓ ✓	● ● ✓ ✓ ✓	✓ ✓ ✓ ✓	✓ ✓ ● ✓ ●	N/B
FGCU	✓ ✓ ✓ ●	✓ ✓ ✓ ●	✓ ✓ ✓ ✓	✓ ✓ ✓ ✓	N/B
FIU	✓ ✓ ✓ ✓	✓ ✓ ✓ ✓ ✓	✓ ✓ ✓ ✓	✓ ✓ ✓ ✓ ✓	N/B
FL Poly	● ● ● ✓	● ● ● ● ✓	✓ ✓ ✓ ✓	✓ ✓ ✓ ✓ ✓	N/B
FSU	● N/B ● ●	N/B N/B ● ● ●	● ● N/B N/B	● ● N/B N/B N/B	N/B
NCF	● ● ✓ ●	● ● ✓ ✓ N/B	✓ ✓ ✓ ✓	✓ ✓ ✓ ✓ ✓	N/B
UCF	✓ ✓ ✓ ✓	✓ ✓ ✓ ✓	✓ ✓ ✓ ✓	✓ ✓ ✓ ✓	N/B
UF	✓ ✓ ✓ ✓	✓ ✓ ● ✓ ✓	✓ ✓ ✓ ✓	✓ ✓ ✓ ✓	N/B
UNF	✓ ✓ ✓ ✓	✓ ✓ ✓ ✓	✓ ✓ ✓ ✓	✓ ✓ ✓ ✓	N/B
USF	✓ ✓ ✓ ✓	✓ ✓ ✓ ✓	✓ ✓ ✓ ✓	✓ ✓ ✓ ✓	N/B
UWF	● ✓ ✓ ✓	● ● ● ✓ ●	✓ ✓ ✓ ●	● ● ✓ ● ●	N/B

Summary: All 18 Regulatory Elements

Less than Half:
FSU, UWF

Implemented:
FIU, UCF, UNF, USF
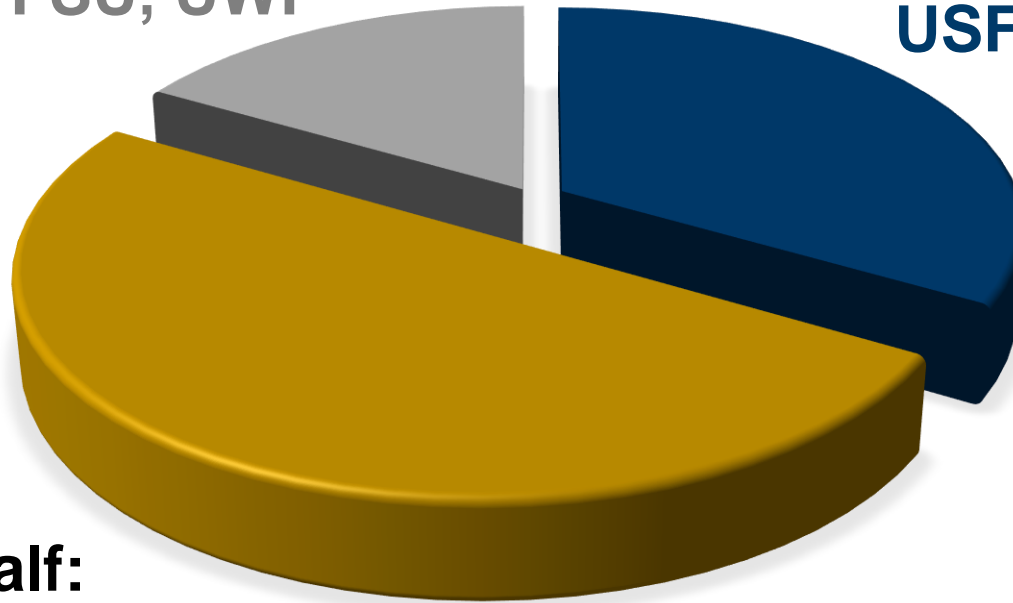
At Least Half:
FAMU, FAU, FGCU, FL Poly, NCF, UF

A1 – University-wide Compliance Program implemented consistent with Code of Ethics for Public Officers and Employees (Part III, Chapter 112, F.S.) and the Federal Sentencing Guidelines Manual, Chapter 8, Part B

On Target:
FAMU, FAU, FL Poly, FSU, NCF, UWF
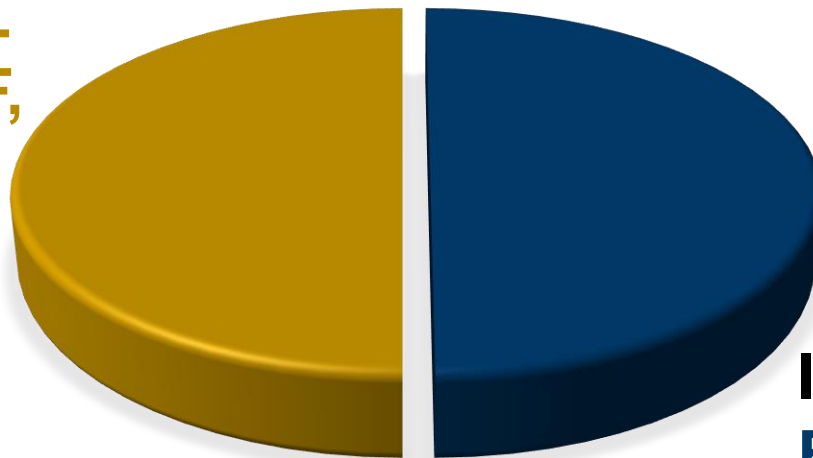
Implemented:
FGCU, FIU, UCF, UF, UNF, USF

A2 - CCO reports to the BOT at least annually on Program effectiveness

On Target:
FAMU, FL Poly, FSU, NCF
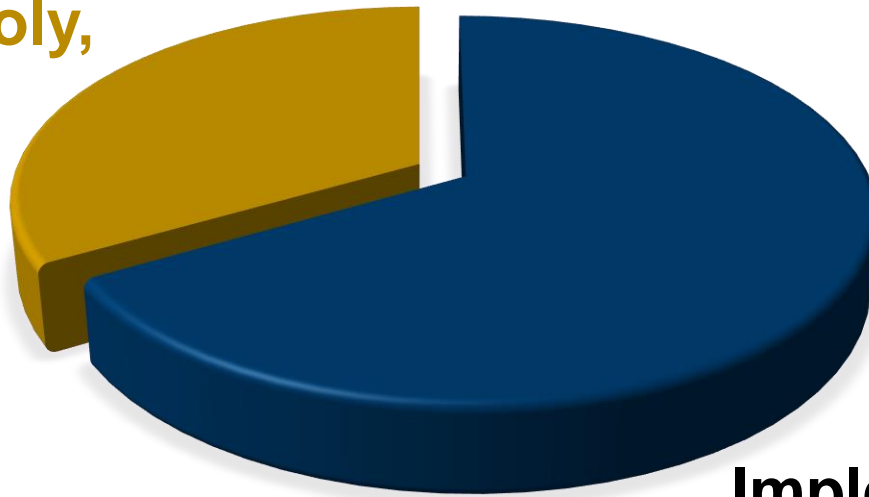
Implemented:
FAU, FGCU, FIU, UCF, UF, UNF, USF, UWF

A3 – External Program design and effectiveness review every 5-years

- **At the 5-year mark, programs will likely have reached a certain level of maturity**
- **All programs on target for November 2021 deadline**
- **FIU expects to conduct theirs this calendar year**

A4 – Process established for detecting and preventing non-compliance, unethical behavior, or criminal conduct

On Target:
FAMU, FL Poly, FSU
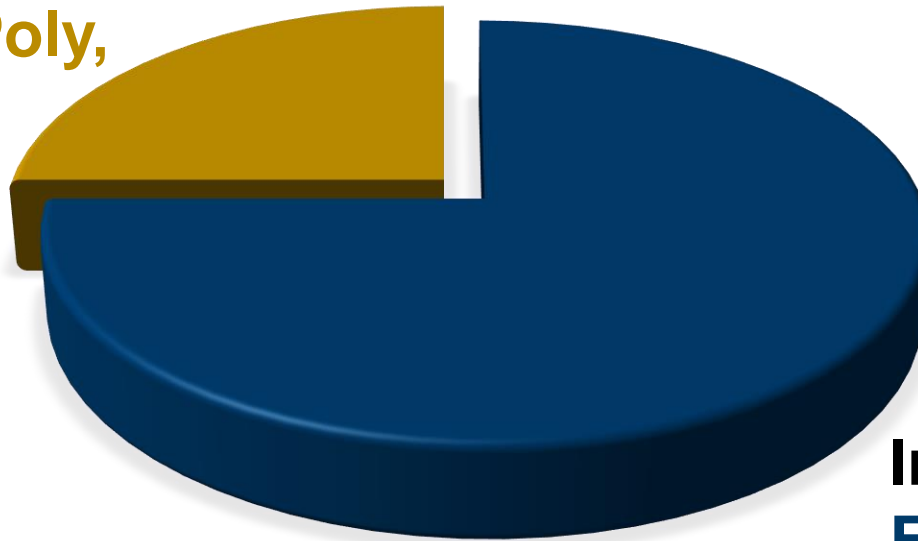
Implemented:
FAU, FGCU, FIU, NCF, UCF, UF, UNF, USF, UWF

A5 – Due diligence steps for not including individuals who have engaged in conduct not consistent with an effective Program

On Target:
FGCU, FSU, NCF
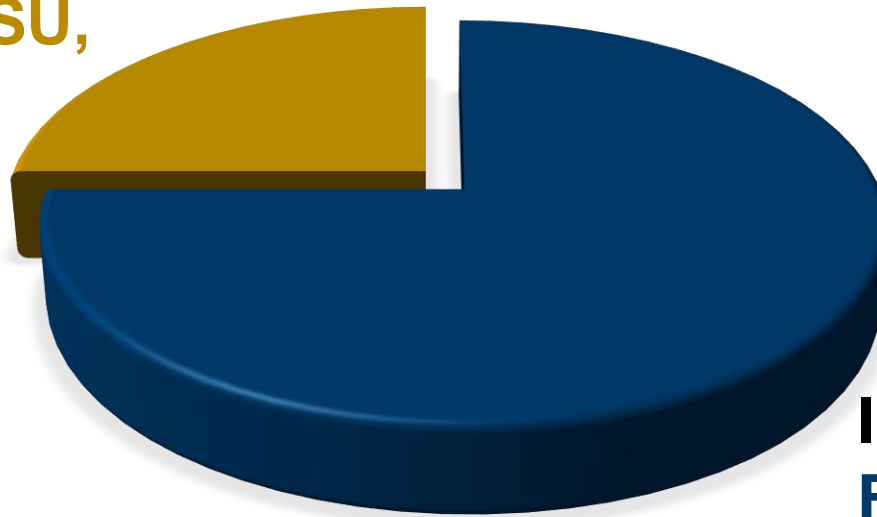
Implemented:
FAMU, FAU, FIU, FL Poly, UCF, UF, UNF, USF, UWF

B1 – Compliance and Ethics Program Plan approved by BOT

B2 – Plan provides for compliance training for university employees and BOT members

On Target:
FAMU, FAU, FL Poly, FSU, NCF, UWF
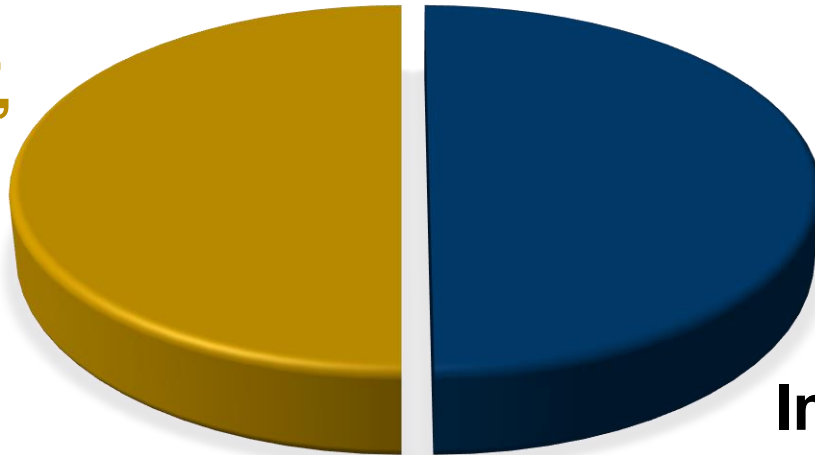
Implemented:
FGCU, FIU, UCF, UF, UNF, USF

B3 – Designated compliance officers (e.g., Title IX, Athletics, Research, etc.) as either direct reports or dotted-line reports

On Target:
FL Poly, FSU, UF, UWF
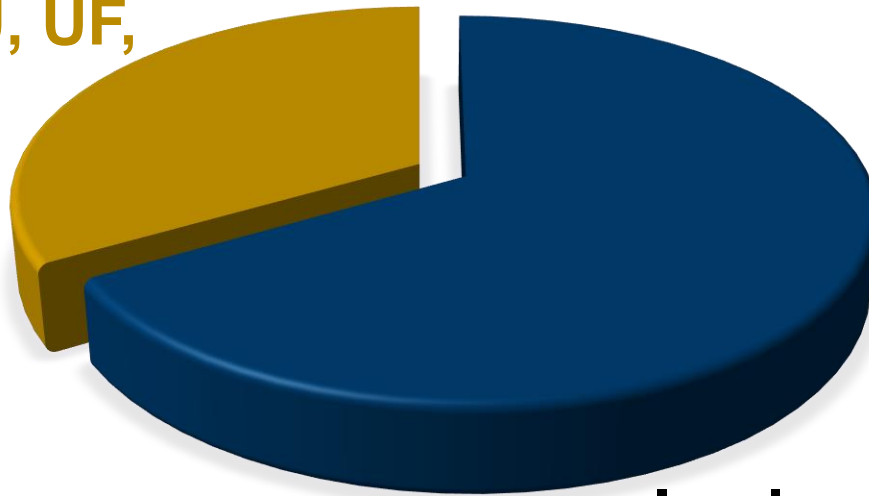
Implemented:
FAMU, FAU, FGCU, FIU, NCF, UCF, UNF, USF

B4 – Reporting mechanism (e.g., Hotline) for potential/actual violations and provides protection for reporting individuals from retaliation

On Target:
FL Poly, FSU
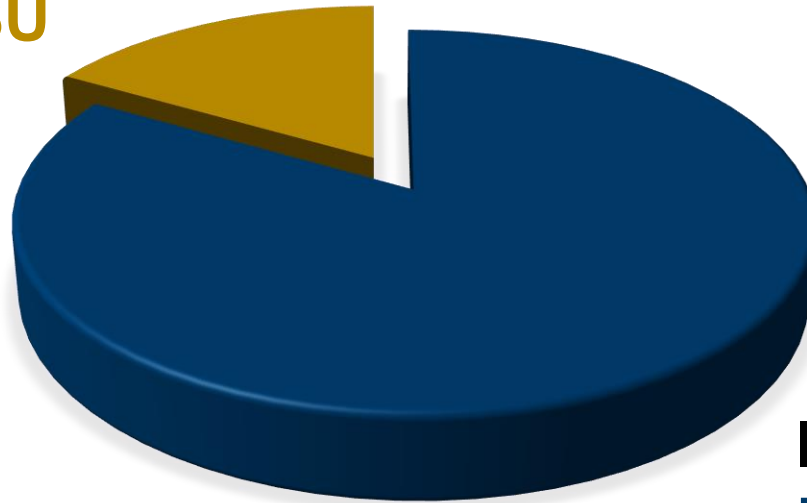
Implemented:
FAMU, FAU, FGCU, FIU, NCF, UCF, UF, UNF, USF, UWF

B5 – Promoting and enforcing the Program through incentives and disciplinary measures

On Target:
FAMU, FGCU, FSU, NCF, UWF
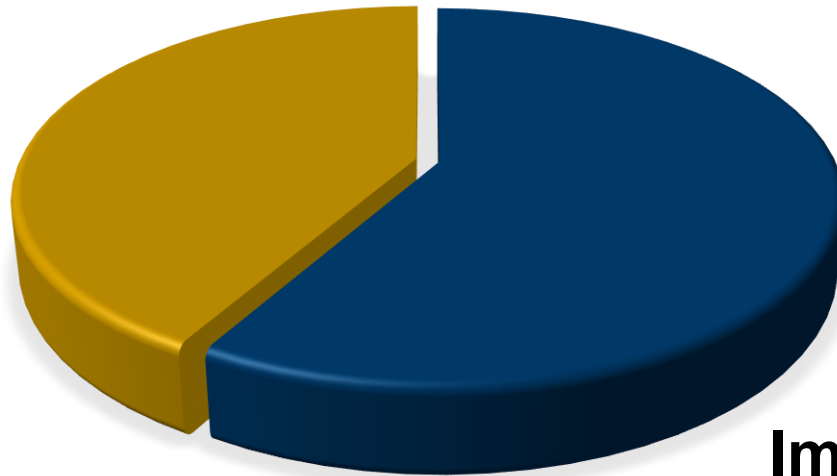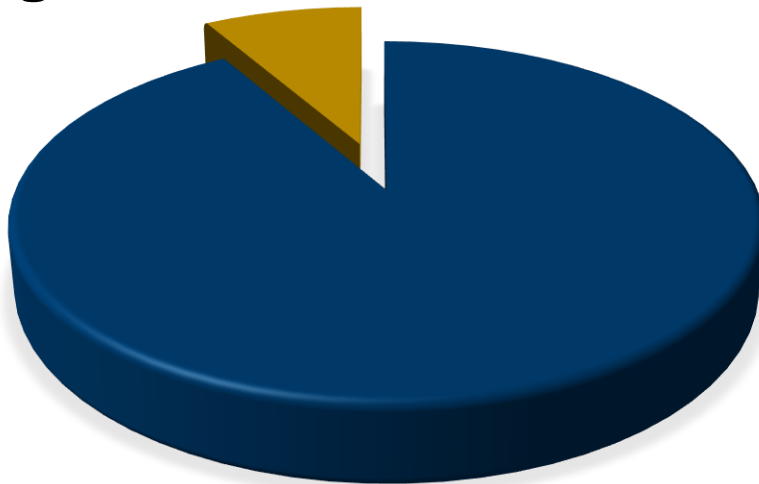

Implemented:
FAU, FIU, FL Poly, UCF, UF, UNF, USF

C1 – BOT Committee provides oversight to Compliance and Ethics Program

C2 – BOT Audit and Compliance Committee Charter

C3 – Routine CCO meetings with BOT Committee – nature and frequency of meetings (e.g., semi-annually, quarterly, monthly, etc.)

On Target: FSU

Implemented:
FAMU, FAU, FGCU, FIU, FL Poly, NCF, UCF, UF, UNF, USF, UWF

C4 – Routine CCO meetings with President or other regularly held direct reports or leadership meetings – nature and frequency (e.g., semi-annually, quarterly, monthly, etc.)

On Target:
FSU, UWF
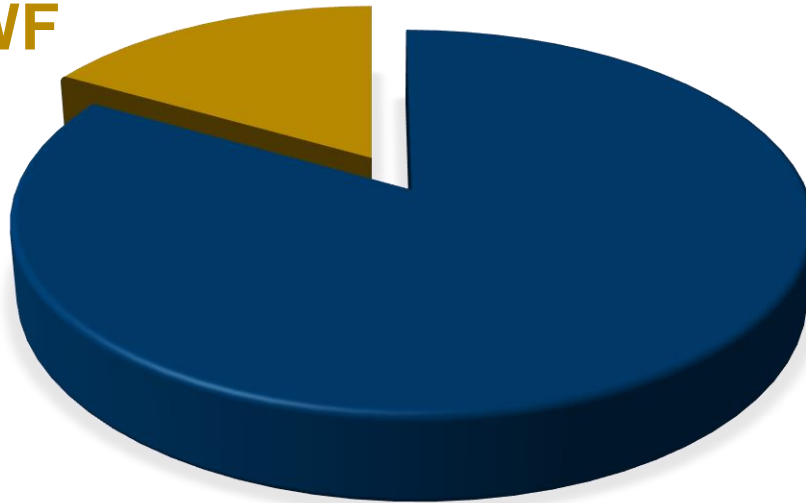
Implemented:
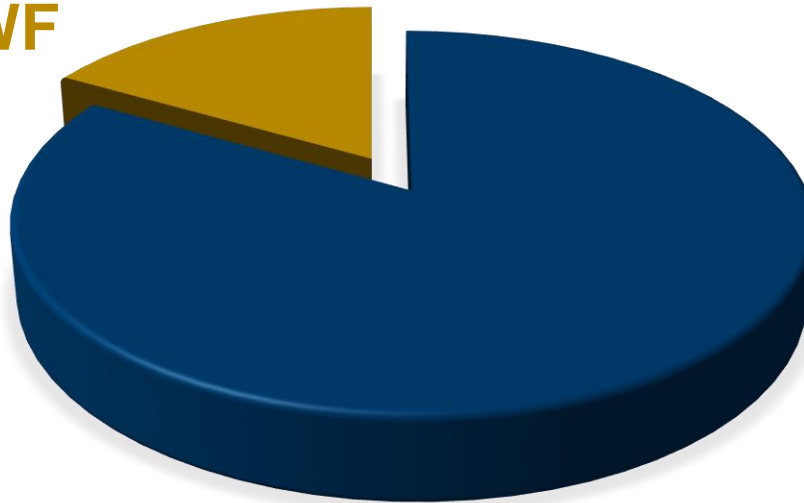**FAMU, FAU, FGCU, FIU, FL Poly, NCF, UCF, UF, UNF, USF**

D1 – Appointed Chief Compliance Officer

D2 – CCO reports functionally to Board and administratively to President

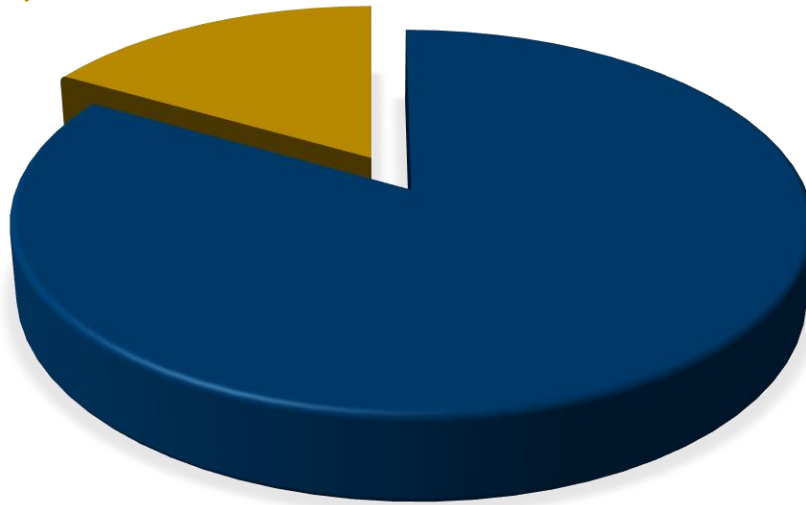**D4 – CCO independence, objectivity, and access**

On Target:
FSU, UWF

Implemented:
FAMU, FAU, FGCU, FIU, FL Poly, NCF, UCF, UF, UNF, USF

D3 – Compliance Office Charter

On Target:
FAU, FSU

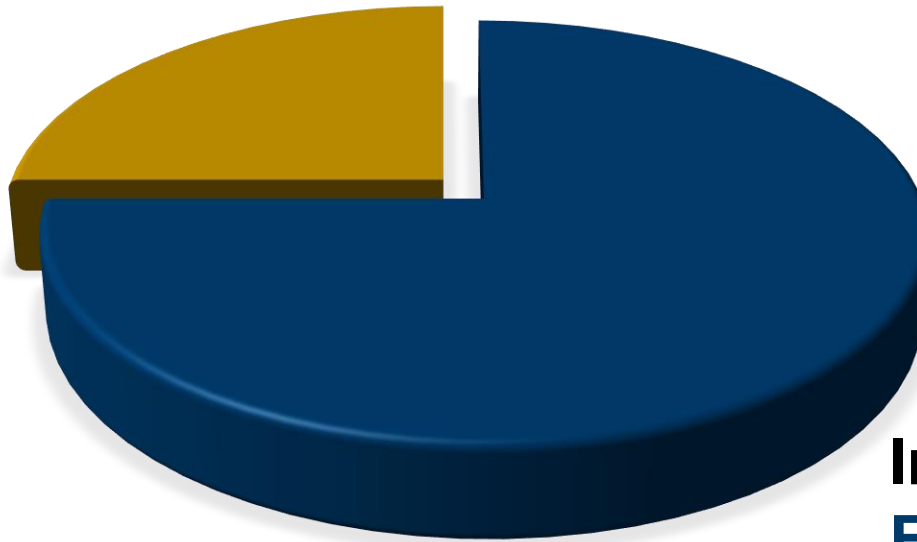**Implemented:**
FAMU, FGCU, FIU, FL Poly, NCF, UCF, UF, UNF, USF, UWF

D5 - CCO authority and resources (staffing and budget)

On Target:
FAU, FSU, UWF

Implemented:
FAMU, FGCU, FIU, FL Poly, NCF, UCF, UF, UNF, USF