YOUR ROLE IN IMPROVING ORGANIZATIONAL CULTURE

Benito Ybarra, CIA, CISA, CFE, CCEP
Chief Audit and Compliance Officer

Kristin Alexander, CIA, CFE, CCEP
Director, Compliance Division
29 Full-Time Employees

Division Mission:
To foster stewardship by preventing and detecting fraud, waste, and abuse and by providing assurance regarding the integrity and performance of programs managed by the Department and TxDOT business partners.
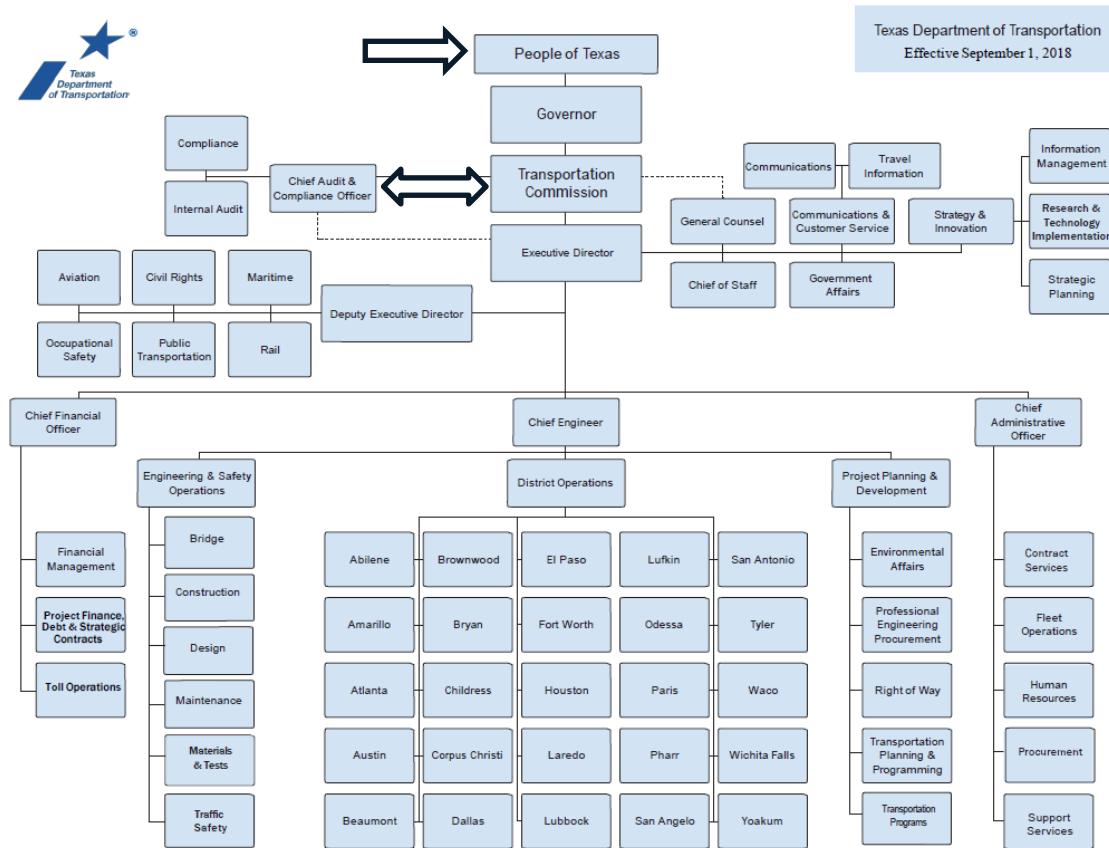
Craig Otto, CIA, CGAP, CRMA
Director, Internal Audit Division
39 Full-Time Employees

Division Mission:
To be leaders in providing assurance and problem-solving capability with professionalism, objectivity and integrity.

TxDOT Audit and Compliance - Introductions

Notable Takeaways

- Ultimate accountability to the People of Texas

- Chief Audit and Compliance Officer reports to full commission

- Organizational focus on service delivery, transparency and accountability

Ground Rules

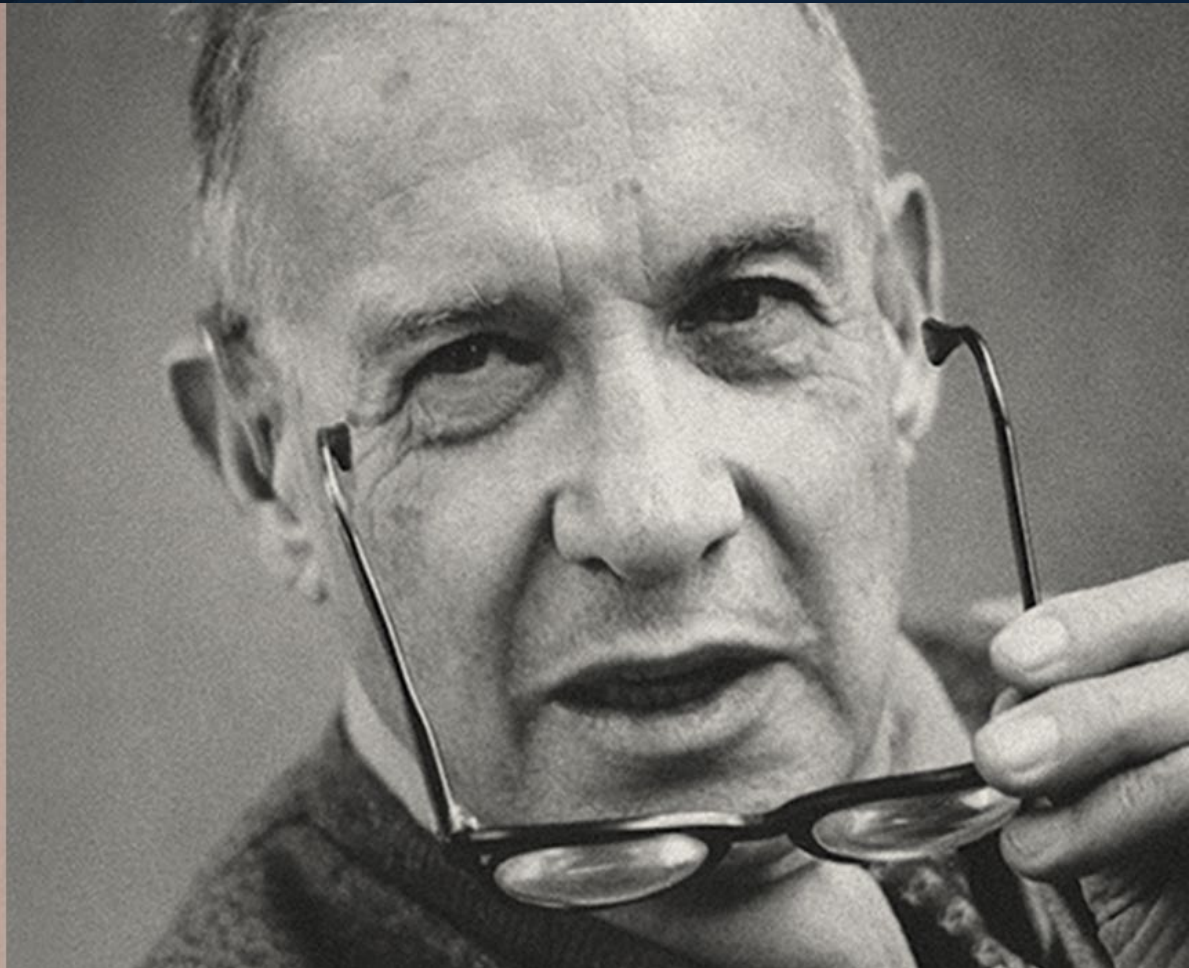Panelist Questions Throughout

Participation is Welcome

We are always right!

CULTURE EATS STRATEGY FOR BREAKFAST.

- Peter Drucker

How do you define organizational culture?

What are examples of organizational culture that impact employee actions?

What is Organizational Culture?

The ethical atmosphere created by the organization's leadership – **ACFE**

The level of commitment toward openness, honesty, integrity, and ethical behavior as embodied by the actions, directives, and behaviors of an organization's leaders – **AICPA**
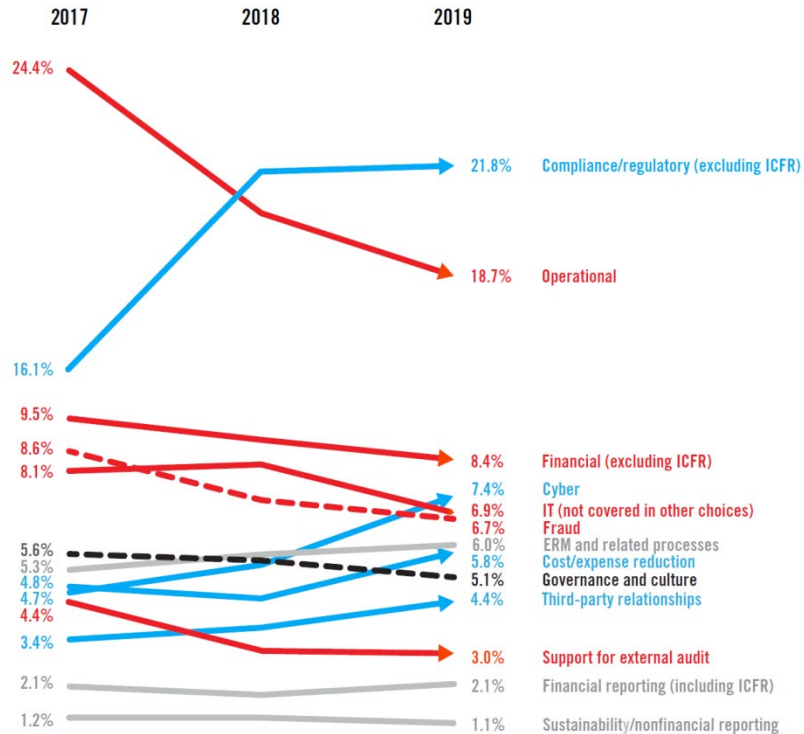
The company's commitment to integrity and ethical values, the importance of maintaining effective internal control, and the expectation that all employees will fulfill their internal control obligations – **COSO**

Culture encompasses the organization's values and how employees act out those values – **IIA Tone at the Top**

The way we do things around here

IIA Pulse of the Profession – Audit Plan Allocation (Public Sector)

Exhibit E: Audit Plan Allocation — Public Sector (2017 to 2019)

2017	2018	2019	
24.4%		21.8%	Compliance/regulatory (excluding ICFR)
		18.7%	Operational
16.1%			
9.5%		8.4%	Financial (excluding ICFR)
8.6%		7.4%	Cyber
8.1%		6.9%	IT (not covered in other choices)
		6.7%	Fraud
5.6%		6.0%	ERM and related processes
5.3%		5.8%	Cost/expense reduction
4.8%		5.1%	Governance and culture
4.7%		4.4%	Third-party relationships
4.4%			
3.4%		3.0%	Support for external audit
2.1%		2.1%	Financial reporting (including ICFR)
1.2%		1.1%	Sustainability/nonfinancial reporting

Observations

- Compliance/Regulatory and Operational comprise 41% of allocated time

- Largest coverage changes in Operational (downward) and Compliance/Regulatory (upward)

- Governance and Culture coverage steady at ~5%

Is 5% coverage sufficient?

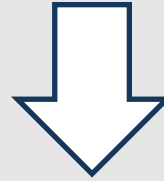Why is it important to understand and assess an organization's culture?

IIA Tone at the Top – Why Audit/Compliance Are Suited to Assess Culture

Interactions and candid conversations with employees at all levels

Internal controls experts

Understand and oversee compliance programs

Perspectives on which departments are difficult to work with

Perspectives on which departments experience recurring issues

Independence and objectivity

What do you see as challenges associated with auditing organizational culture?

Elements of Strong Ethics and Compliance Programs

2019 Definitive Corporate Compliance Benchmark Report
Navex Global

		MATURITY LEVEL				NUMBER OF EMPLOYEES		
		Reactive	Basic	Maturing	Advanced	Less than 1,000	1,000 – 6,000	6,001 or More
Code of Conduct	91%	83%	83%	97%	100%	90%	90%	96%
Policies and Procedures to Prohibit and Reduce Misconduct	87%	71%	78%	92%	97%	84%	83%	93%
Training Based on the Organization's Risks and Individual Roles	77%	40%	67%	87%	97%	72%	76%	85%
Non-Retaliation Policy	72%	56%	58%	78%	91%	66%	70%	82%
Case Management and Investigation Processes / Protocols	72%	46%	59%	82%	99%	63%	74%	85%
An Anonymous Internal Reporting Channel (e.g., Hotline)	71%	48%	59%	79%	91%	54%	80%	89%

Code of Conduct is number 1 – demonstrates strong tone at the top

"**Respect:** We treat others as we would like to be treated ourselves. Ruthlessness, callousness and arrogance don't belong here." ✓

"**Integrity:** We work with customers and prospects openly, honestly and sincerely. ✓ When we say we will do something, we will do it."
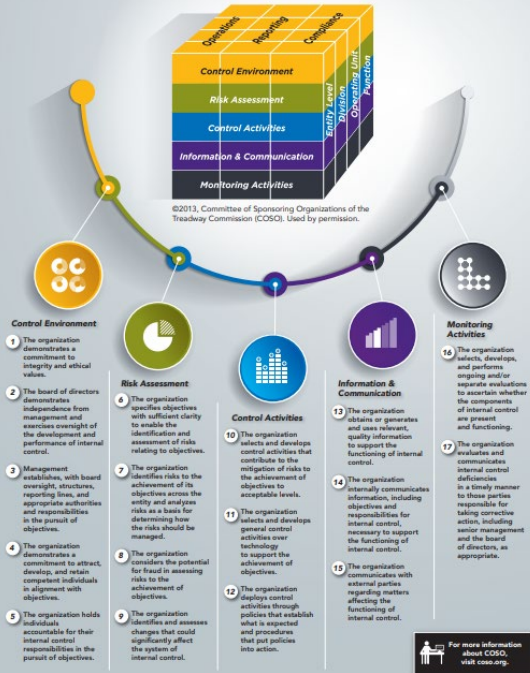
"**Excellence:** We are satisfied with nothing ✓ less than the very best. We will continue to raise the bar for everyone."

TxDOT Internal Audit Considerations

Committee of Sponsoring Organizations

COSO Internal Control — Integrated Framework Principles

Provides a framework that includes components of all organizations' internal controls principles

5 Primary Components
- Control Environment
- Risk Assessment
- Control Activities
- Information & Communication
- Monitoring Activities

17 Principles

TxDOT's Use of COSO Internal Control Integrated Framework (Internal Audit)

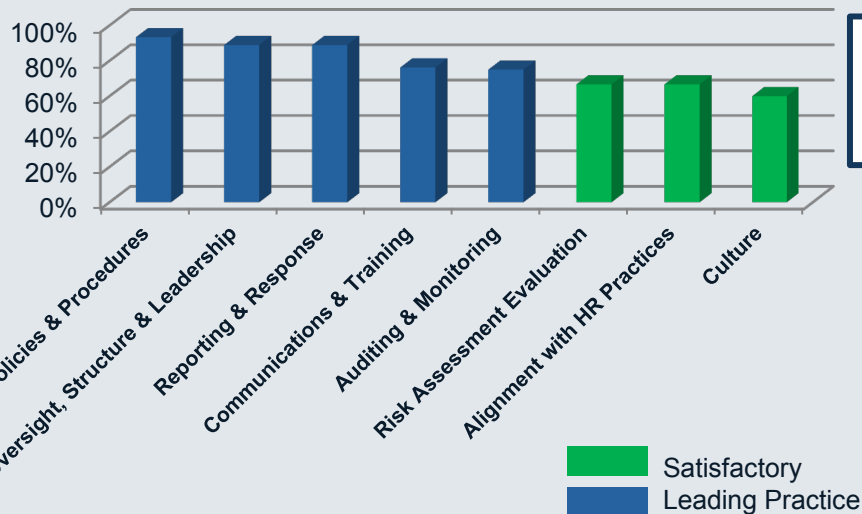| Audit Results Dashboard Name of Audit		Scope Areas Evaluated
Business Objectives (Reporting, Operational, Compliance)		R, O, C
ERM Component	Control Activities	Scope Area 1
Control Environment	Organizational Tone	
	Business Objective/Goal-Setting	
	Resource Capacity	
	Forecasting/Budget	
	Training and Development	
Risk Assessment	Risk Identification/Planning	
	Risk Assessment/Impact Analysis	
	Risk Response/Cost-Benefit Analysis	
	Business Continuity	
Control Activities	Policies/Procedure Development & Maintenance	
	Approvals/Authorizations	
	Supporting Evidence/Records Retention	
	Segregation of Duties/System Access	
	Safeguarding Assets/Security	
Information & Communication	Information Classification	
	Information Input	
	Information Processing	
	Information Output	
	Internal and External Reporting	
Monitoring	Exception Reporting Review	
	Reconciliations	
	Root-Cause Analysis	
	Evaluations/Inspections	
	Management Action Plans	
Scope Area Assessment		
Percentage of Completion		0%
Rating Assessment Grid		Exemplary / Satisfactory / Needs Improvement / Unsatisfactory

Highlights

- Rate audits and test areas according to ERM components

- Ratings range from Exemplary to Unsatisfactory

- Includes rating of *Organizational Tone*

TxDOT Compliance Considerations

Self Assessment of Compliance Program Effectiveness (Compliance)

Elements of an Effective Compliance Program

Based on US Sentencing Commission Guidelines

Categories (left to right):
- Standards, Policies & Procedures
- Oversight, Structure & Leadership
- Reporting & Response
- Communications & Training
- Auditing & Monitoring
- Risk Assessment Evaluation
- Alignment with HR Practices
- Culture

Legend:
- Satisfactory (green)
- Leading Practice (blue)

Culture

- Do employees believe that it is possible to behave ethically and achieve business objectives at the company? Is unethical behavior clearly seen as out of bounds?

- Do employees believe they can raise issues to management or the hotline number without fear of retaliation?

- Do employees believe that management will take appropriate action if misconduct is communicated to them?

- Do employees believe that others who violate company standards get promoted to positions of increased authority?

- Is the program viewed as a paper program or as a genuine commitment?

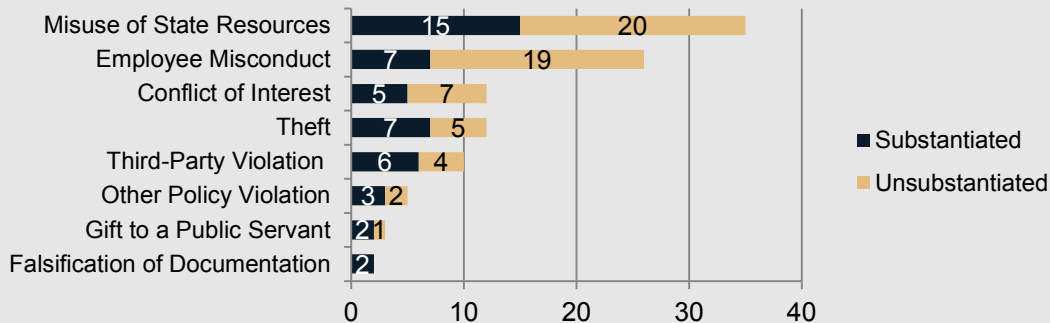# Analysis of Hotline Allegations and Investigation Results (Compliance)

Allegations:

- Received   301   283   4%
- Investigations initiated   117   98   18%
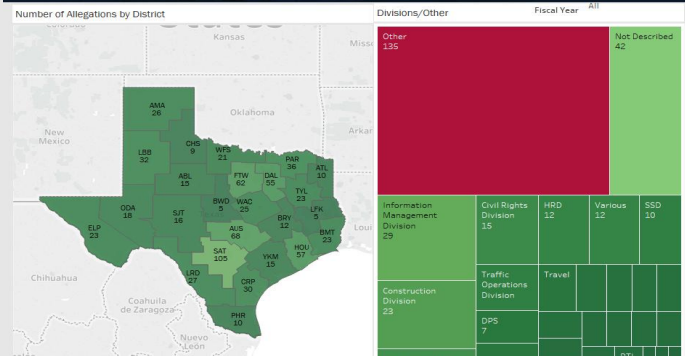
Closed Investigation Dispositions:

- Substantiated   47 (45%)   47 (45%)
- Unsubstantiated   58   57

Closed Investigation Locations:

- Districts   70   72
- Divisions   25   16
- Third-Party   10   16

Allegations by District and Division

Investigations by District and Division

Category	Substantiated	Unsubstantiated
Misuse of State Resources	15	20
Employee Misconduct	7	19
Conflict of Interest	5	7
Theft	7	5
Third-Party Violation	6	4
Other Policy Violation	3	2
Gift to a Public Servant	2	1
Falsification of Documentation	2	

■ Substantiated
■ Unsubstantiated
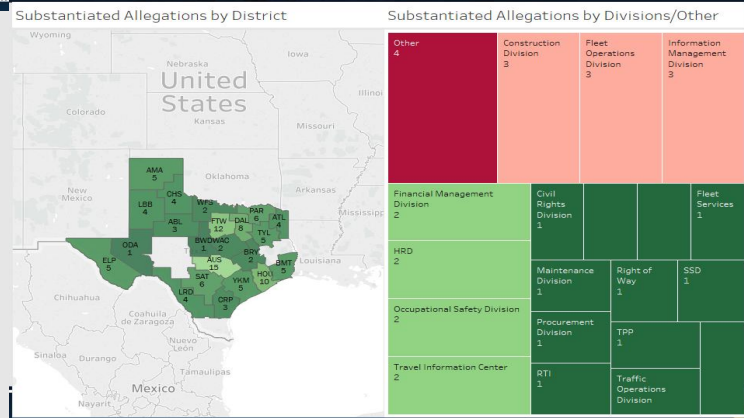
Control Self-Assessments and Reviews (Compliance)

Address below the line items with most effective risk mitigation strategies

Reassess existing risks & newly identified risks to create annual work plan

Risk Backlog

Risk Assessment

Continuous Compliance Program

Detection Program

Control Self-Assessments / Reviews

Evaluate risk areas with detection projects & continuous monitoring program

Dedicated Monitoring

Trainings

Perform CSAs/Reviews to identify improvement areas & monitoring opportunities, while also educating staff on regulations & fraud awareness

Quick Self-Assessment

Criteria	YES	NO
1. My organization has a way to report complaints outside of my management line (e.g. human resources, hotline, etc.).		
2. My executive team makes it clear that they want feedback from employees, customers and business partners.		
3. My management team welcomes feedback and uses it to make things better.		
4. Employees do not have to fear retaliation for reporting a complaint or issue.		
5. Employee culture/work life metrics are shared with executives and are used to address employee concerns.		

How can audit and compliance impact "NO" answers?

Thank you.

Now go impact your organization's culture!