

DISCUSSION TOPICS



1. Internal Controls
2. Avoiding Being the News Story
3. LEA Risk Self-Assessment Template
4. Utilizing the Results for Success

Why Is the Risk Self-Assessment Important?

It's a required internal control

Avoid monitoring and audit findings

Prevent fraud, waste, and abuse



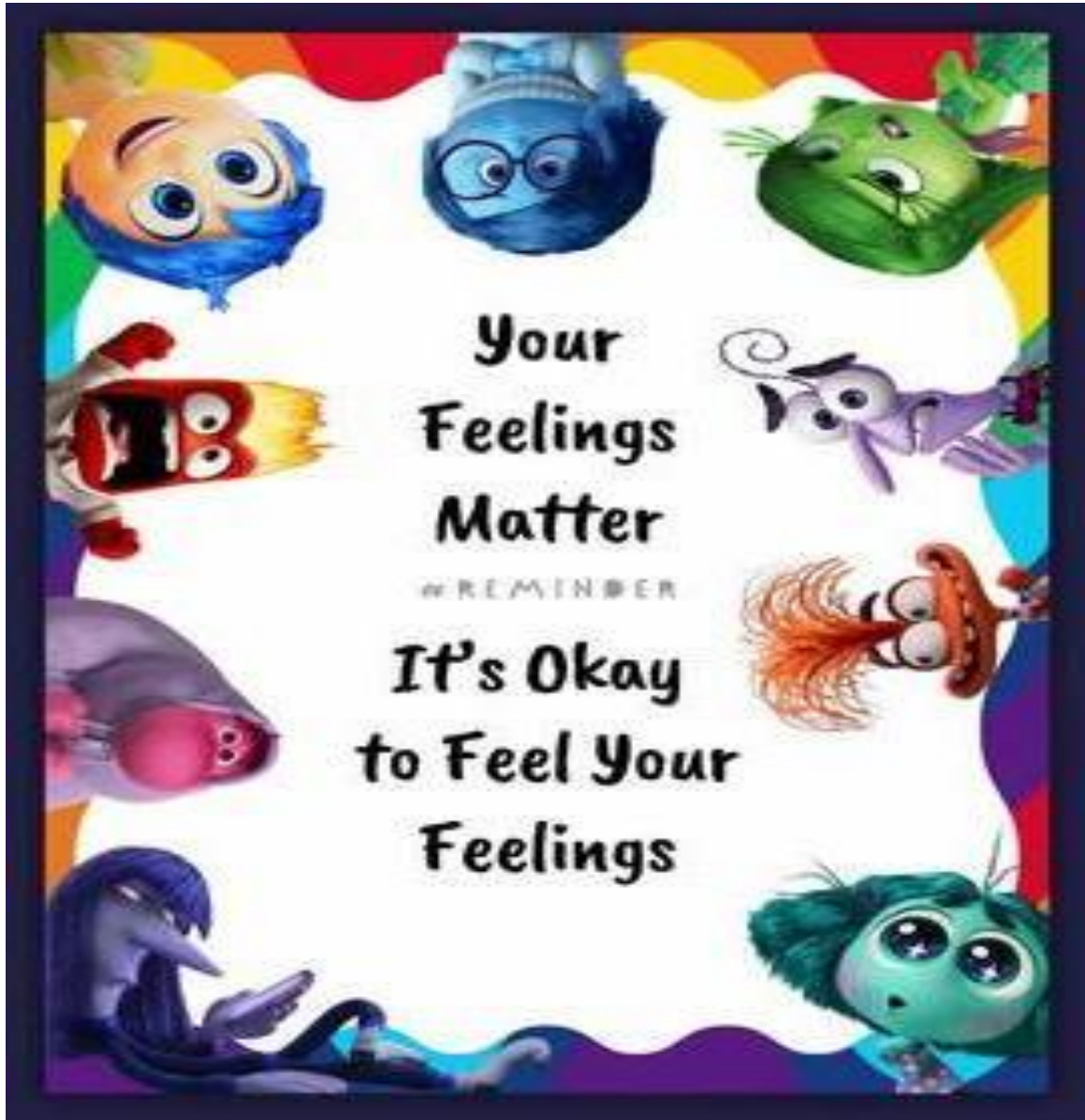
Fraud, Waste, and Abuse

- Former Orange County Education Official Sentenced to Nearly Six Years in Federal Prison for Embezzling More Than \$16.6 Million from School District
- “Contreras wrote checks in small dollar amounts written to “M S D,” with the letters spaced out, and, after receiving the proper signatures from others, would include fictitious names and increase the amounts of the checks and deposit the checks into his personal bank account via ATMs. To conceal his fraud, Contreras provided bank reconciliation packets to others at the school district with falsified bank statements and records.”
- Contreras embezzled approximately \$16,694,942 from the district

Fraud, Waste, and Abuse (cont.)



- Former New York City Department of Education CEO of School Support Services and Three Business Owners Sentenced to Prison for Corruption and Bribery
- “Goldstein abused his position as the DOE Chief Executive Officer of Office of School Support Services to accept nearly \$100,000 in bribes from co-defendants to knowingly serve unfit lunch choices for consumption to students and teachers.”
- Over a period of 14 months, contractors transferred money for Goldstein’s benefit, including payments to Goldstein’s divorce attorney and father.
- Contractors agreed to transfer ownership interest in their company to Goldstein, as well as to transfer \$66,670 to a bank account that Goldstein had opened and controlled.



Increased Accountability

Internal Controls Defined 200.1

- For recipients and subrecipients means processes designed and implemented by recipients and subrecipients to provide reasonable assurance regarding the achievement of objectives in the following categories:
 1. Effectiveness and efficiency of operations;
 2. Reliability of reporting for internal and external use; and
 3. Compliance with applicable laws and regulations.



Internal Control Objectives

1. Transactions are properly recorded and accounted for in order to:
 - a) Permit the preparation of reliable financial statements and federal reports;
 - b) Maintain accountability over assets; and
 - c) Demonstrate compliance with federal statutes, regulations, and the terms and conditions of the federal award;
2. Transactions are executed in compliance with:
 - a) Federal statutes, regulations, and the terms and conditions of the federal award that could have a direct and material effect on a federal program; and
 - b) Any other federal statutes and regulations that are identified in the Compliance Supplement; and
3. Funds, property, and other assets are safeguarded against loss from unauthorized use or disposition.

Internal Controls Requirements

200.303

- Establish, document, and maintain internal controls
 - Should **align** with “Green Book” or COSO Integrated Framework
- Comply with all requirements (including U.S. Constitution)
- Evaluate and monitor compliance
- Take prompt action to correct noncompliance
- Take **reasonable cybersecurity and other** measures to safeguard **information including** personally identifiable information (PII) and other types of information.
 - **This also includes** info the federal agency or pass-through designates as sensitive or info the recipient/subrecipient considers sensitive and is consistent with laws regarding privacy and responsibility over confidentiality

"Anxiety would have a
plan for that."

-fear

@counselorkim



Recent Findings: Failure to Have Documented Processes

Recent Internal Control Assessment Findings

Nevada (Consolidated Monitoring); West Virginia Governor's Office (GEER) -

- **Finding:** Lack of internal risk identification and assessment process, and a process for monitoring the operation of an organization's internal controls
 - **Required Action:** 60 days to create a process to identify and review internal controls of the agency

Oklahoma, Indiana (Consolidated Monitoring)

- **Finding:** Lacked (or no finalized) internal controls plan
 - **Required Action:** Within 60 business days of receiving report, OSDE must provide a plan that complies with GAO Green Book as outlined in 2 CFR 200.303

Recent Internal Control Assessment Findings (cont.)

1. Documentation of a regular process (e.g., quarterly, annually, biannually, etc.) for:
 - a) Identifying internal risks
 - a) The types of risk that will be evaluated and the indicators used
 - b) The process for establishing risk tolerances for different categories or types of risk
 - c) The process to complete the risk assessment (including responsible individuals)
 - d) The process to respond to identified risks
 - b) Maintaining and evaluating the performance and/or effectiveness of the agency's internal controls framework
 - a) A description of the process and its frequency, identify the staff responsible for performing such an evaluation, and include copies of any tools or checklists that will be used to accomplish the evaluations
- While the state cannot rely solely on external auditors to complete evaluations of internal controls, the process developed can be complementary in scope to the work performed by the external entities.

Expansive Mandatory Disclosures 200.113

- Applicant, recipients, and subrecipients must promptly disclose **whenever it has credible evidence of the commission of a violation of federal criminal law involving fraud, conflict of interest, bribery, or gratuity violations** under False Claims Act (Title 18 - Criminal and Title 31 – Civil)
- Must be made in writing to the Federal agency, **the agency's Office of Inspector General, and** the pass-through entity (if applicable)
- Also required to report to SAM and FAPIIS (as applicable)
 - Includes any activities or subawards in connection with the Federal award
- Failure to report can result in remedies for noncompliance (2 CFR 200.339)

More Required Financial Certifications

200.415

(a): States: **Removed certification for payment requests** (only for financial reports)

(b): **Subrecipients must certify to the pass-through entity whenever applying for funds, requesting payment, and submitting financial reports:**



"I certify to the best of my knowledge and belief that the information provided herein is true, complete, and accurate. I am aware that the provision of false, fictitious, or fraudulent information, or the omission of any material fact, may subject me to criminal, civil, or administrative consequences including, but not limited to violations of U.S. Code"

False Claims Act

“Any person who...”

“...knowingly presents, or causes to be presented, a false or fraudulent claim for payment or approval...”

“...is liable to the U.S. Government for a civil penalty of not less than \$5,000, plus 3 times the amount of damages the government sustains because of the act of that person.”

31 U.S.C. § 3729



New Whistleblower Protections 200.217



- An employee of a recipient or subrecipient must not be discharged, demoted, or otherwise discriminated against as a reprisal for disclosing information that the employee reasonably believes is:
 - Evidence of gross mismanagement,
 - Gross waste,
 - An abuse of authority,
 - A substantial and specific danger to public health or safety, or
 - A violation of law, rule, or regulation.
- The recipient and subrecipient must inform their employees in writing of employee whistleblower rights and protections under 41 U.S.C. 4712.



**So... how can
we prevent
being a news
story!???**

How Do I Know If We Have Problems?

We say: “Because We’ve Always Done It That Way!”

Magical Letters

“I signed off on it because Joe did”

Attempts to Circumvent Procedures or no procedures

Missing Property

Employees in the News!

Communication is Key

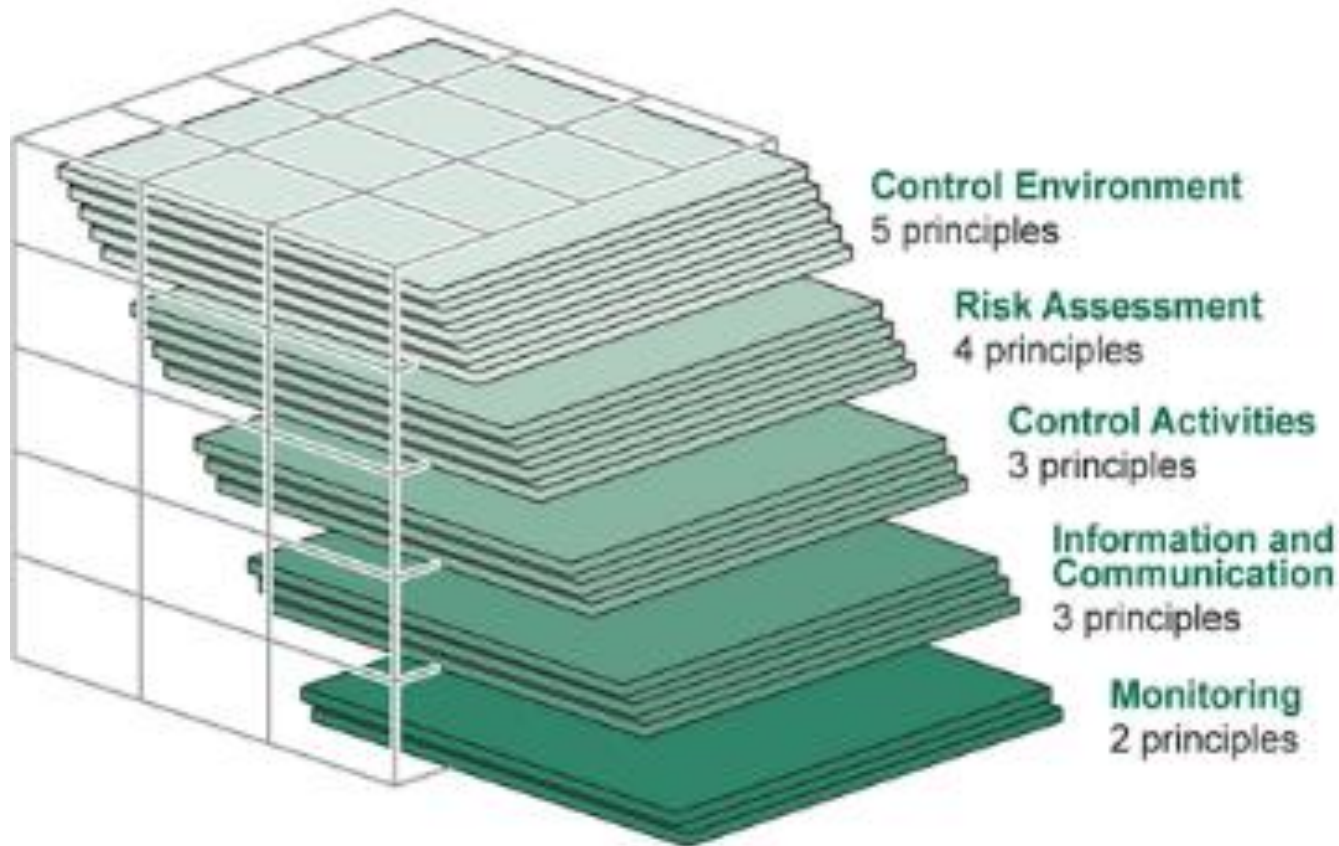
WHAT YOU SAID...

- “Our policies are being drafted.”
- “We have a small staff, and many people have collateral duties.”
- “I need to check around to find that document.”
- “You can use my logon to review system records.”

WHAT THE AUDITOR HEARD...

- “The program may not be administered effectively. Let’s increase our testing sample.”
- “No segregation of duties, potential for fraud.”
- “There is no document management system. The records are not accurate.”
- “There are no controls over systems. There is potential error, fraud, and unauthorized use.”

COSO: 5 Components and 17 Principles of Internal Controls



Source: GAO. | GAO-14-704G



Control Environment Principles

1. A commitment to integrity and ethical values
2. Independent oversight over the development and performance of internal controls
3. Clearly defined organizational structure, clear reporting lines, appropriate authorities
4. A commitment to attract, develop and retain competent individuals
5. Maintain a level of competence that allows personnel to accomplish their assigned duties (and holding individuals accountable)

Control Environment Examples



Well-written policies and procedures manuals

Addressing employee responsibilities, limits to authority, performance standards, hiring practices, whistleblower policies, conflict of interests, etc.



Organizational chart

Clear lines of authority and responsibility



Accurate job descriptions



Adequate training programs and performance evaluations

Risk Assessment Principles

1. Clear objectives to enable the identification and assessment of risks
2. Identify risks to achievement of objectives across the entity and analyze risks as a basis for determining how the risks should be managed
3. Consider the potential for fraud
4. Identify and assess changes that could significantly impact the system

Risk Areas

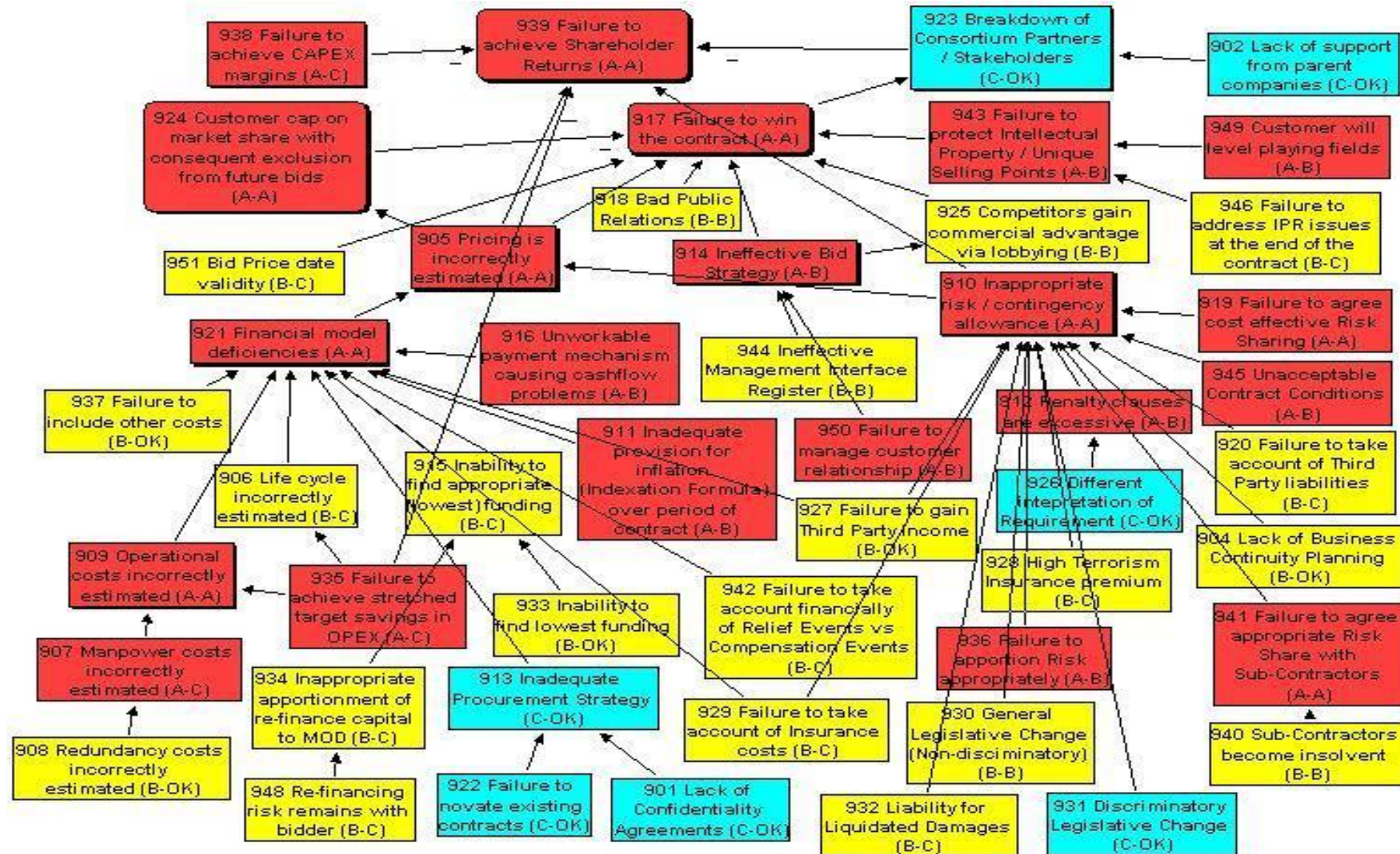
Risks are not stagnate; they increase and change as laws and operational environments change

- New personnel
- Experienced personnel
- Lack of personnel
- Reorganizations
- Rapid growth/Changes in population



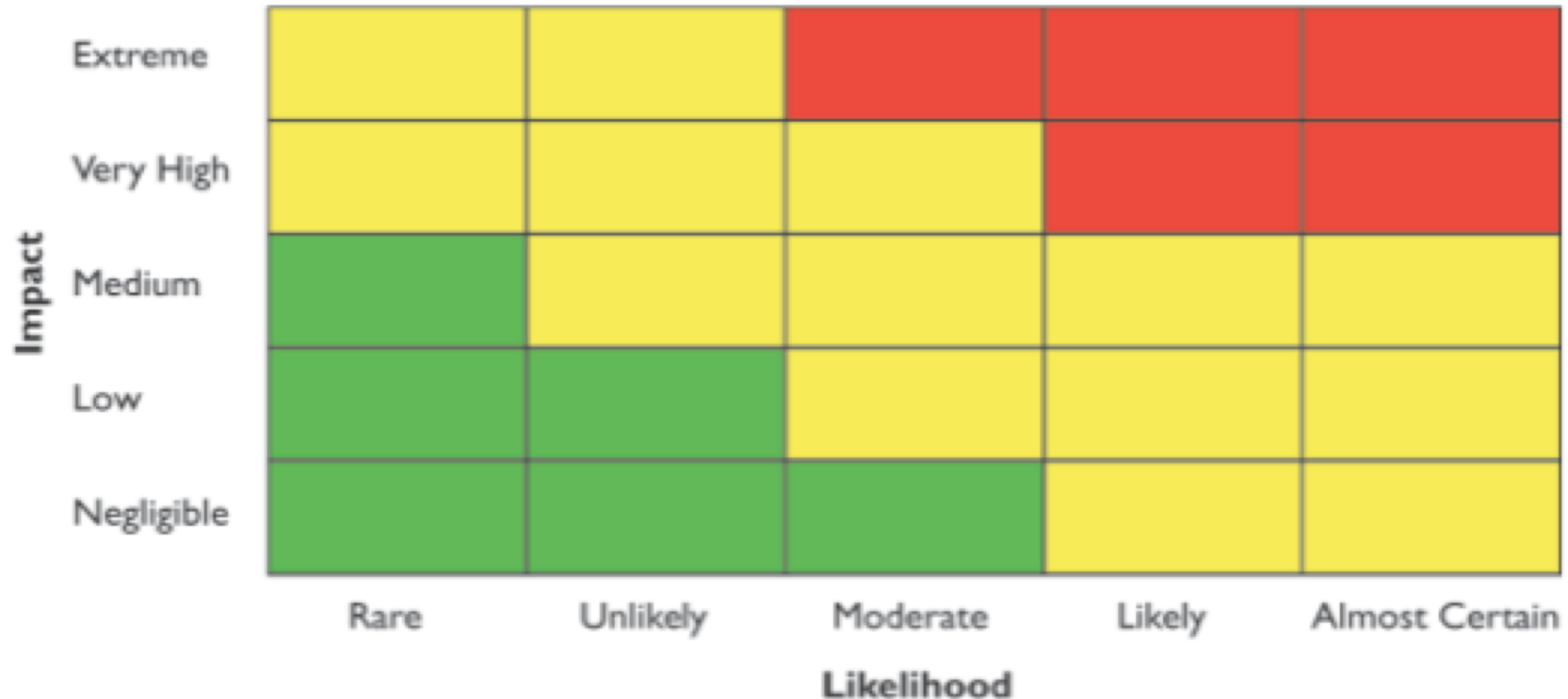
- Leadership Changes
- Change in Laws / Regulations
- New Grants
- New Technology
- High Crime Area

Risk Mapping



Example: "Current Risk Severity Map" graphically shows the level of risk prior to mitigation.

Let's Try That Again! Risk Mapping



Control Activities Principles

1. Select and develop control activities that contribute to the mitigation of risk and achievement of objectives to acceptable levels
2. Select and develop general control activities over technology to support the achievement of objectives
3. Deploy control activities through policies that establish what is expected and procedures that put policies into action

Control Activity Examples

Preventive Controls:

- Control that helps management avoid issues before they occur.
 - Approval for purchases
 - Restricting Access (Passwords)
 - Training
 - Security and surveillance systems
 - Segregation of Duties
 - Safeguarding Assets

Detective Controls:

- Control that discover issues after they occur.
 - Match receiving to POs
 - Compare actual expenditures to budgeted
 - Reconciliations
 - Physical inventory count
 - Review activity logs

Information and Communication Principles

1. Obtain, generate, or use relevant, quality information to support the functioning of the entity
2. Internally communicate info, including objectives and responsibilities necessary to support the entity
3. Communicate with external parties regarding matters affecting the functioning of the entity

Develop procedures for identifying pertinent information and distributing it in a form and timeframe that permits people to perform their duties efficiently.

Monitoring Principles

1. Select, develop, and perform ongoing and/or separate evaluations to ascertain whether the components of internal controls are present and functioning
2. Evaluate and communicate internal control deficiencies in a timely manner to parties responsible for taking corrective action

Monitoring Examples

Ongoing program and fiscal monitoring

Regular oversight by supervisors

Record reconciliation

Formal program reviews/audits

Annual single audits

Include policies and procedures for correcting any findings in a timely manner



Internal Controls Risk Self-Assessment

32

What is an internal controls risk self-assessment?

- A management technique that reviews whether an organization's internal controls system is reliable
- That is, individuals within an organization perform effectiveness testing to verify whether key controls are functioning properly, resulting in the detection or elimination of weaknesses



Be Honest With Yourself!



Be Prepared!

- Set tone that compliance is important and critical for success
- Identify key goals and objectives of the review
- Set clear timelines and communicate expectations
- Make certain you have the proper people involved
- Document findings and recommendations

Internal Controls Risk Assessment Tool

- Aim for an annual review
- Consider adding in additional areas to address based on recent audit or monitoring findings, or other concerns raised by District staff
- Requirements are based on federal rules, so consider changes/additions based on more restrictive state or local rules
- Risk rating for each question: low, moderate, or high

Low Risk

- What does a “low” risk rating mean?
 - District has current, updated internal controls in place that foster compliant administration of federal grants
- Example: Does the District ensure all lost, stolen and damaged property is investigated?
 - Response/Notes: Yes, the District has internal controls in place (check in/out forms, maintenance plans, investigative process, etc.). The District maintains a record of investigations showing few instances of loss, damage, or theft.
 - Employee interview and/or documentation reviewed would reflect these strong internal controls.

Moderate Risk

- What does a “moderate” risk rating mean?
 - District has some existing internal controls in place, but they may require updating or may not fully cover the breadth required under the federal rules
- Example: Does the District ensure all lost, stolen and damaged property is investigated?
 - Response/Notes: The District has some internal controls in place but the record of such investigations is not clear and/or the investigation procedures are not in writing.
 - Employee interview and/or documentation reviewed might reflect some knowledge of how to maintain federal equipment, but a lack of clarity on what the procedures are to investigate instances of loss, damage, and theft.

High Risk

- What does a “high” risk rating mean?
 - District either has no internal controls or they are so outdated that staff are untrained on them (also unresolved findings, likely to be high risk)
- Example: Does the District ensure all lost, stolen and damaged property is investigated?
 - Response/Notes: The District does not have internal controls. There is no record of the District’s investigations, or a high volume of instances involving loss, damage, or theft.
 - Employee interview and/or documentation reviewed might reflect a lack of knowledge of how to maintain Federal equipment, especially around the process for investigating instances of loss, damage, and theft.



Using the Risk Levels

- Use the ratings to identify areas that may require further attention
- Update policies and procedures in that section (or create them) to reduce risk
- The ratings should:
 - inform decision-making
 - prioritize action steps to mitigate risk
 - contribute to overall compliance with federal requirements

The Risk Assessment Tool

Questions: Overall LEA Risk

Has the LEA had any significant systems changes in the past fiscal year, or does the LEA anticipate any systems changes in the next year? Significant systems might include financial management or accounting systems, grants management systems, etc. 2 CFR § 200.303(a)

Does the LEA currently have high carryover from the prior year in any Federal program (50% or greater)?

In the last 2 fiscal years, has the LEA expended all federal grant funds without lapsing any at the end of the period of performance?

Has the LEA previously received all Federal awards currently being administered (*e.g.*, none of the awards are new to the LEA this year)?

What is the average relevant experience in years of the federal program staff and fiscal staff?

Questions: Overall LEA Risk (cont.)

If there were any vacancies at the LEA within the past fiscal year, did the LEA successfully fill those positions?

Does the LEA provide training (or permit staff to attend training) on Federal grants compliance for staff administering federal grant funds at least annually?

Does the LEA have all the required policies and procedures and ensure they are reviewed at least every 3 years? Have all relevant staff members received training on written policies in the past 12 months? 2 CFR §§ 200.318; 200.403; 200.302(b)(7)

Is there generally a separation of duties across grants-related offices? If not, what controls are in place to ensure compliance?

Did the LEA timely submit its applications, budgets and any required amendments, per the awarding agency deadlines? 34 CFR §§ 76.708; 76.710; 2 CFR 200.308

Questions: Financial Management and Allowability

Does the financial management system permit the tracing of funds to a level of expenditures adequate to establish that such funds have been used only for allowable purposes under each program and budget line item? 2 CFR § 200.302(b)

Does the LEA timely request reimbursements (e.g., monthly)? Does the LEA track reimbursements and cash advances and ensure interest is calculated on any cash advances (remitting any interest back to USED, as required?) 2 CFR § 200.305

Does the LEA ensure that costs are only incurred during approved budget periods? 2 CFR § 200.403(h)

Does the LEA have a process to ensure costs are adequately documented to demonstrate costs are necessary and allowable under applicable programs? 2 CFR § 200.403(g)

Questions: Financial Management and Allowability (cont.)

Does the LEA ensure all travel expenses are allowable (e.g., obtain prior approval for travel, track advances, etc.)? 2 CFR § 200.475

Does the LEA ensure that applicable credits are applied to the appropriate Federal grant? 2 CFR § 200.406

Does the LEA request prior written approval from the SEA (or USDE as required) for purchases of equipment, capital expenditures, and other costs where prior approval is required? 2 CFR § 200.407

Does the LEA have a process for tracking matching or cost sharing contributions? 2 CFR § 200.306

Does the LEA ensure all federal funded (in part or in whole) employees complete time and effort documentation in a timely manner and that the documentation is used to reconcile budgets to actual time worked? 2 CFR § 200.430(i)

Questions: Purchasing/Procurement

Does the LEA ensure all employees understand and comply with the LEA's conflict of interest requirements? 2 CFR § 200.318

Does the LEA ensure that the proper method of procurement is used for each purchase made at the LEA? 2 CFR § 200.320

When possible, are minority businesses, women's business enterprises, and labor surplus area firms considered? 2 CFR § 200.321

Does the LEA, to the greatest extent provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States? 2 CFR § 200.322

Does the LEA include the contract provisions described in appendix II of 2 CFR Part 200 when contracting with vendors and providers? 2 CFR § 200.327; Appendix II

Questions: Equipment and Property Management 200.313-314

Does the LEA ensure that a physical inventory of the property is conducted, and the results reconciled with the property records at least once every two years? 2 CFR § 200.313

Does the LEA ensure all equipment and other items, as required, are inventoried (placed on an inventory listing) and that the inventory listing includes all the required information? 2 CFR § 200.313

Does the LEA ensure all lost, stolen and damaged property is investigated? 2 CFR § 200.313

Does the LEA ensure that all equipment and supplies purchased with Federal funds comply with the disposition requirements when no longer needed? 2 CFR §§ 200.313; 200.314



Questions: Reporting, Monitoring, and Audits

Does the LEA submit all financial, performance, and other reports as required, no later than 90 days after the period of performance? 2 CFR §§ 200.329; 200.344(a)

Does the LEA review its school-level activities (each program, function, or activity) under Federal awards to ensure compliance with applicable Federal requirements and performance expectations are being achieved? 2 CFR § 200.329(a)

Does the LEA obtain an annual single audit as required by Subpart F? 2 CFR § 200.332(f)

If the LEA received audit or monitoring findings within the last fiscal year, has it resolved the findings or implemented a corrective action plan?

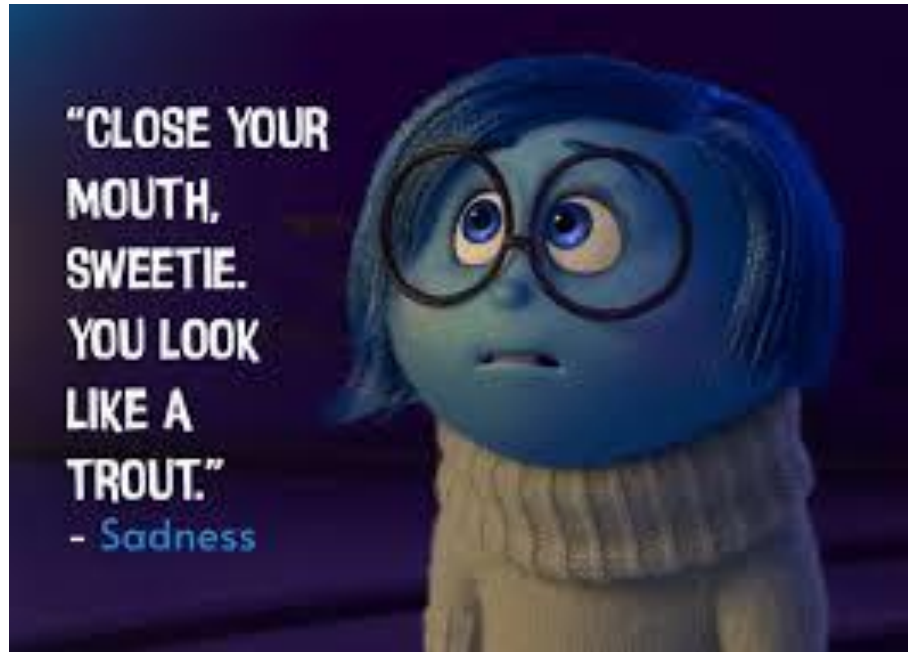
Questions: Monitoring and Audit

Did the LEA have any cross-cutting monitoring findings within the last year? If so, did the LEA ensure that all corrective actions were made in a timely manner? 2 CFR §§ 200.339; 200.340

Does the LEA have record retention policies and procedures that have been updated in the last 3 years? Including collection, transmission, and storage of information, protection of protected personally identifiable information (PII)? 2 CFR §§ 200.336; 200.338; 200.334

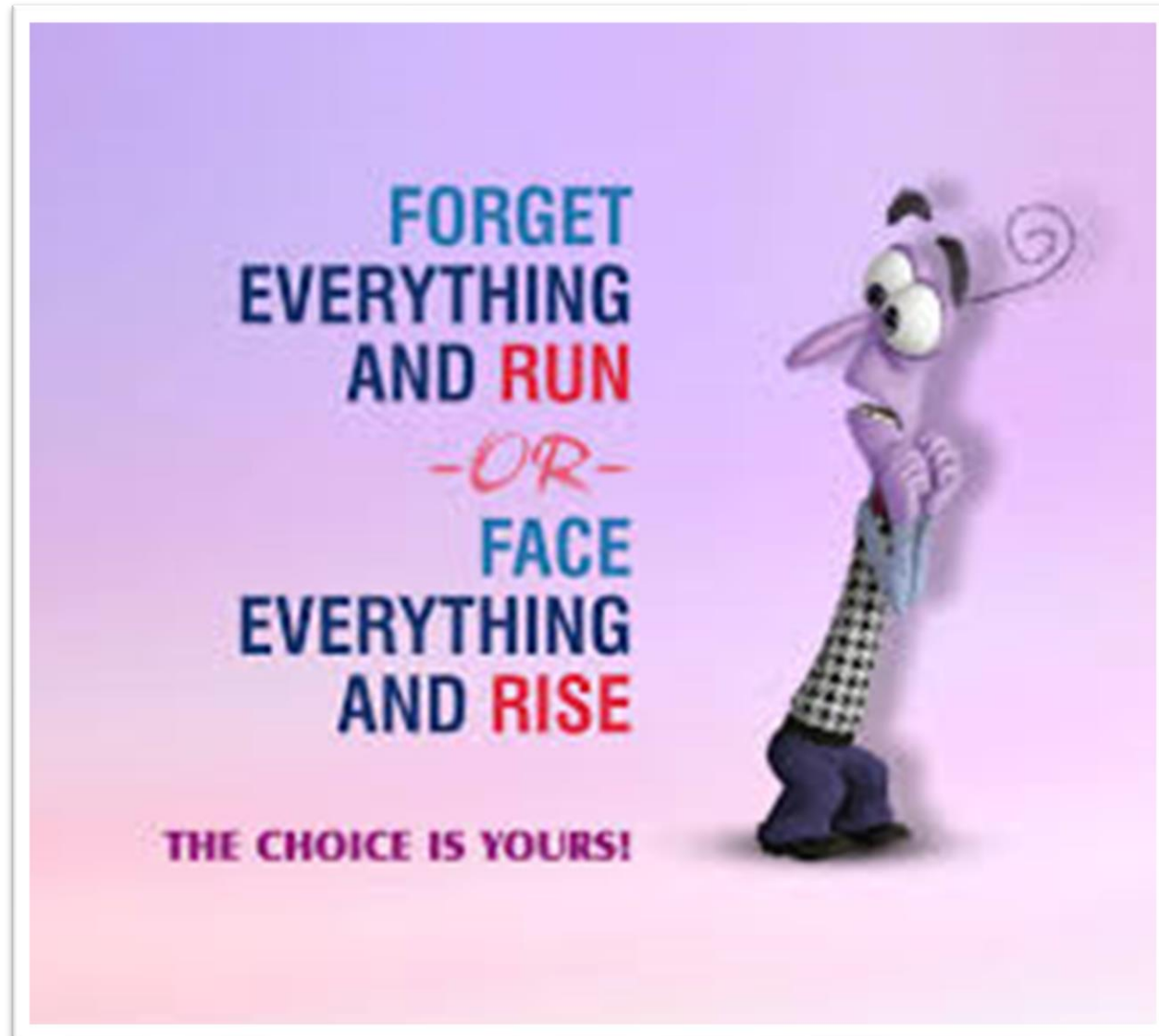
Has the LEA taken any reasonable cybersecurity or other measures to safeguard information, including personally identifiable information (PII) or other information designated as sensitive by the LEA or SEA? 2 CFR § 200.303(e)

Documentation is Key!



- Auditors and Monitors only have the documentation to tell the story
- Reviewer can not reconstruct what has happened without documentation

Utilizing the Results for Success



Self Assessment Completed – What Now?

- Document findings
- Determine Risk Level
- Assess your Risk Tolerance
- Discuss the results with management and inform them of any deficiencies that need immediate attention.

Mitigation

Improve controls to reduce likelihood/impact

Transfer

Shift responsibility to an external party

Acceptance

Accept the risk!



What controls are currently in place to address or prevent identified weaknesses?

Training

Approvals

Authorizations

Verifications

Reconciliations

Performance
reviews

Segregated
duties

Security
measures

Maintenance of
appropriate
documentation

Self Assessment Completed – What Now? (cont.)

- If any review reveals that control activities do not satisfy the weakness, the severity of the problem should be described as well as the action steps being undertaken to resolve the issue(s)
- Make adjustments as determined necessary to clarify procedures or systems
- Change timelines or requirements
 - For example, maybe you've discovered that you struggle to meet closeout deadlines, so you set an internal deadline for schools to submit all expenditures up to a certain date. This way you're not trying to closeout for the entire period in 90 days.
- Report any instances of fraud, conflict of interest, bribery/gratuity violations

Prioritize and Improve Weaknesses



To Improve the Weakness, the Control MUST:

- Address the risk in question
- Be required by the organization (i.e., addressed in policies and procedures)
- Be embedded in the operational functions (e.g., has occurred within the last 12 months)

2024 Compliance Supplement

- 2024 Compliance Supplement Part 6
Internal Controls:
 - <https://www.whitehouse.gov/wp-content/uploads/2024/05/Part-6-Internal-Control.pdf>



Internal Control Examples: Procurement

- District creates and requires the use of standard forms and templates for purchase orders, contracts, requests for proposals/bids, cost/price analyses, bid evaluation, etc.
- Supervisors review and approve procurement and contracting decisions for compliance with federal and organizational policies.
- A supervisor reviews applicable award agreements, contracts, budgets, and other appropriate sources to identify potential covered transactions. Standard forms or templates are used to document verification that parties are not suspended or debarred.
- Responsible staff reconcile goods/services received with those procured including evaluating performance in accordance with terms, conditions, and specifications of contracts or purchase orders.
- Individuals who initiate procurements are different from those recording the resulting transactions in the general ledger or making disbursements.

Inform Staff of the Requirements and any Changes Made

Communicate the right information to the right people at the right time!

- Include internal and external communications
- Develop procedures for identifying pertinent information and distributing it in a form and timeframe that permits people to perform their duties efficiently
- Clear message from top down

The single biggest problem with communication is the illusion that it has taken place.



Learn the Law/Staff Training

- Training for Staff
- Certification/Grants Testing

Legal Requirements (may include references in policies and procedures):

- EDGAR / Uniform Grants Guidance 2 CFR Part 200
- Program Statutes, Regulations, and Rules
 - May link to ed.gov websites
- State and Local Law

Enforce the Rules



- Self-evaluations can be routine, periodic, or random
 - Regular oversight by supervisors
 - Spot Checks
 - Record reconciliation
- Retain documentation and be prepared to share and explain during your next monitoring/audit visit!

Repeat Next Year!



Questions???

Disclaimer

This presentation is intended solely to provide general information and does not constitute legal advice or a legal service. This presentation does not create a client-lawyer relationship with The Bruman Group, PLLC and, therefore, carries none of the protections under the D.C. Rules of Professional Conduct. Attendance at this presentation, a later review of any printed or electronic materials, or any follow-up questions or communications arising out of this presentation with any attorney at The Bruman Group, PLLC does not create an attorney-client relationship with The Bruman Group, PLLC. You should not take any action based upon any information in this presentation without first consulting legal counsel familiar with your particular circumstances.