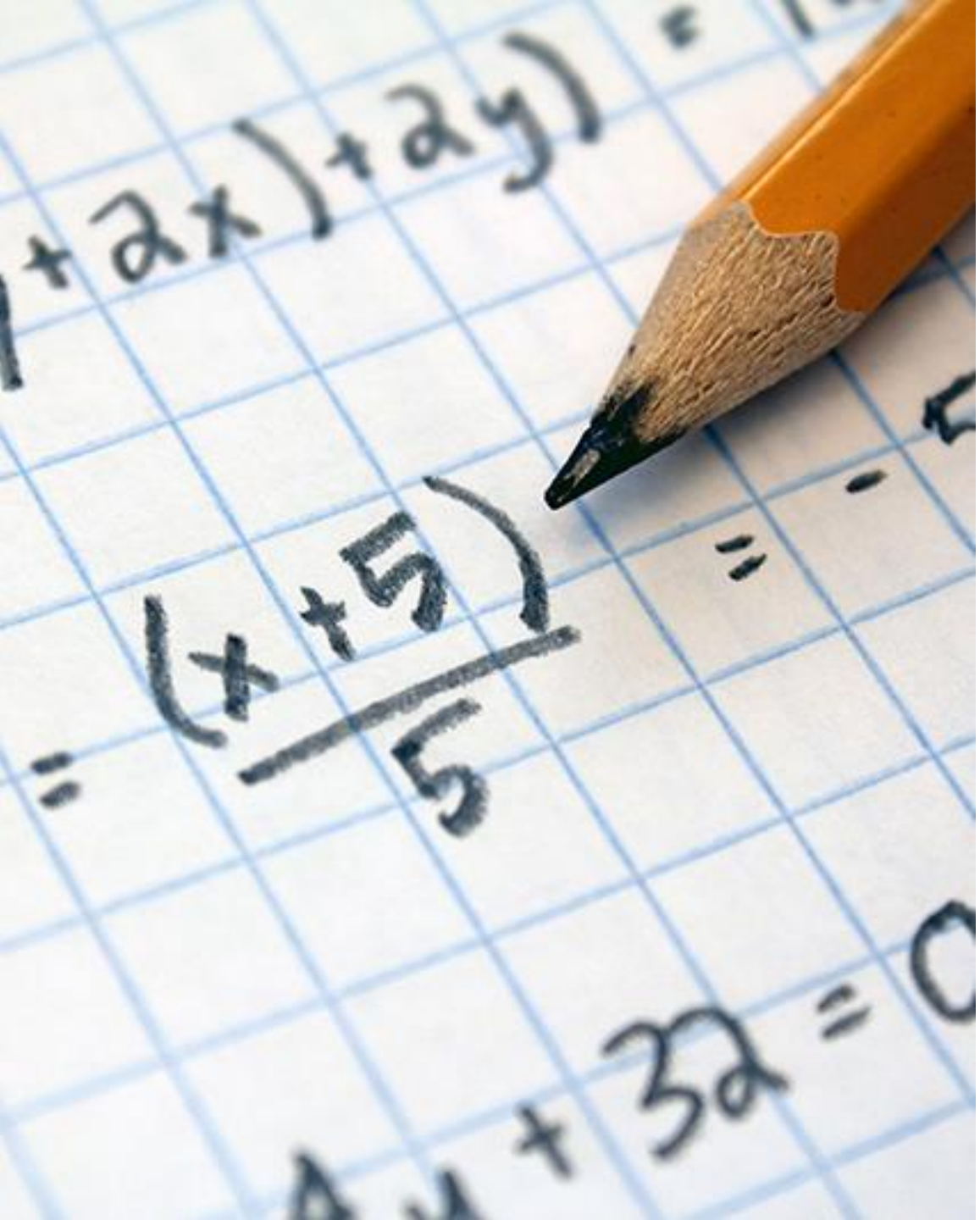


THE BRUMAN GROUP PLLC

Virtual Spring Forum 2023

Internal Risk Assessment Creation and Implementation

Michael Brustein, Esq. & Madelaine Cleghorn, Esq.

mbrustein@bruman.com; mcleghorn@bruman.com

www.bruman.com

May 4, 2023

Agenda

- Introduction: What is a risk assessment and why do we need it?
- Developing an Internal Risk Assessment
- Applying EDGAR and the UGG
- Case Study: Indiana Department of Education

What is a Risk Assessment?

"[A risk assessment] assesses the risks facing the entity as it seeks to achieve its objectives. This assessment provides the basis for developing appropriate risk responses…assesses the risks the entity faces from both external and internal sources."

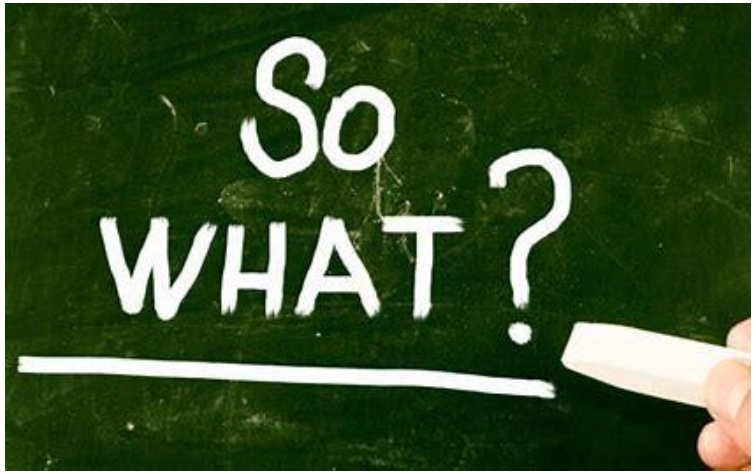
- GAO Standards for Internal Control

https://www.gao.gov/assets/gao-14-704g.pdf

Why do we Need a Risk Assessment?

- Self-assessment (2 CFR 200.329)
- Compliance with all requirements of federal award (2 CFR 200.300(b))
- Financial management (2 CFR 200.302(b))
- Internal controls (2 CFR 200.303)

Why do we Need a Risk Assessment?



- Federal grant rules require self assessment, internal controls, and oversight of subrecipients

- Can use a risk-based approach at all levels
  - Subrecipients
  - LEAs
  - SEAs
  - Institutions of higher education
  - Non-profits

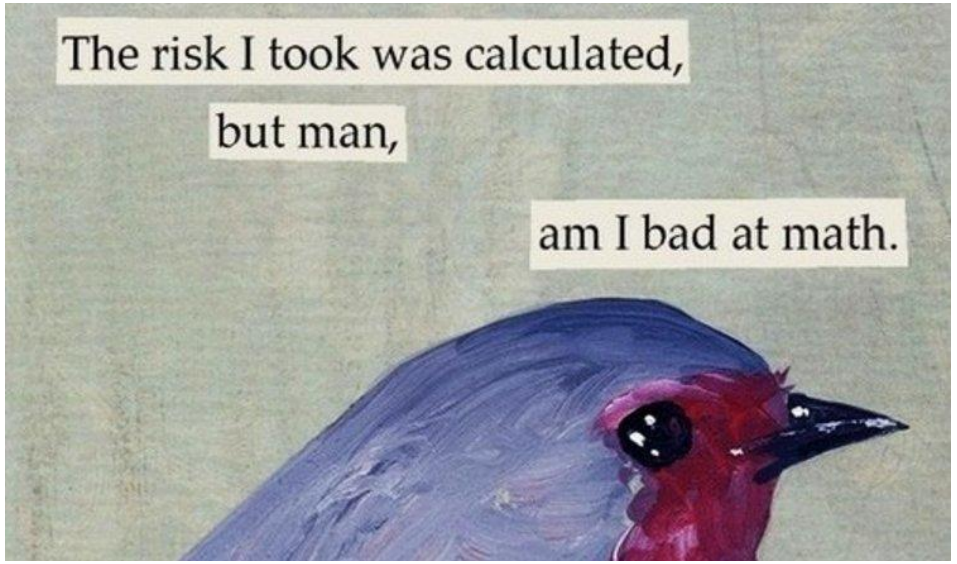
Why do we Need a Risk Assessment?

Lessons learned from a recent State performance review:

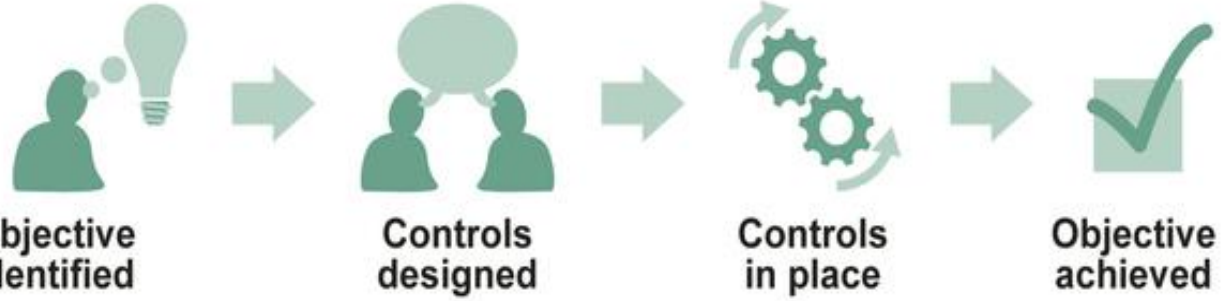
- "[The SEA] was unable to describe a formalized internal risk assessment process as required in both the GAO Green Book and the Treadway Commission/COSO. In addition, [the SEA] stated that it relies on communication from [the State's Department of Finance and Administration] and annual audits as a means of evaluating the performance of its internal controls system. Without a formal process in these areas, there is a risk that [the SEA] will be unable to sufficiently identify risks to agency operations, develop targeted strategies to mitigate identified risks, or make timely determinations regarding the ability of the controls that are already in place to protect against identified risks."

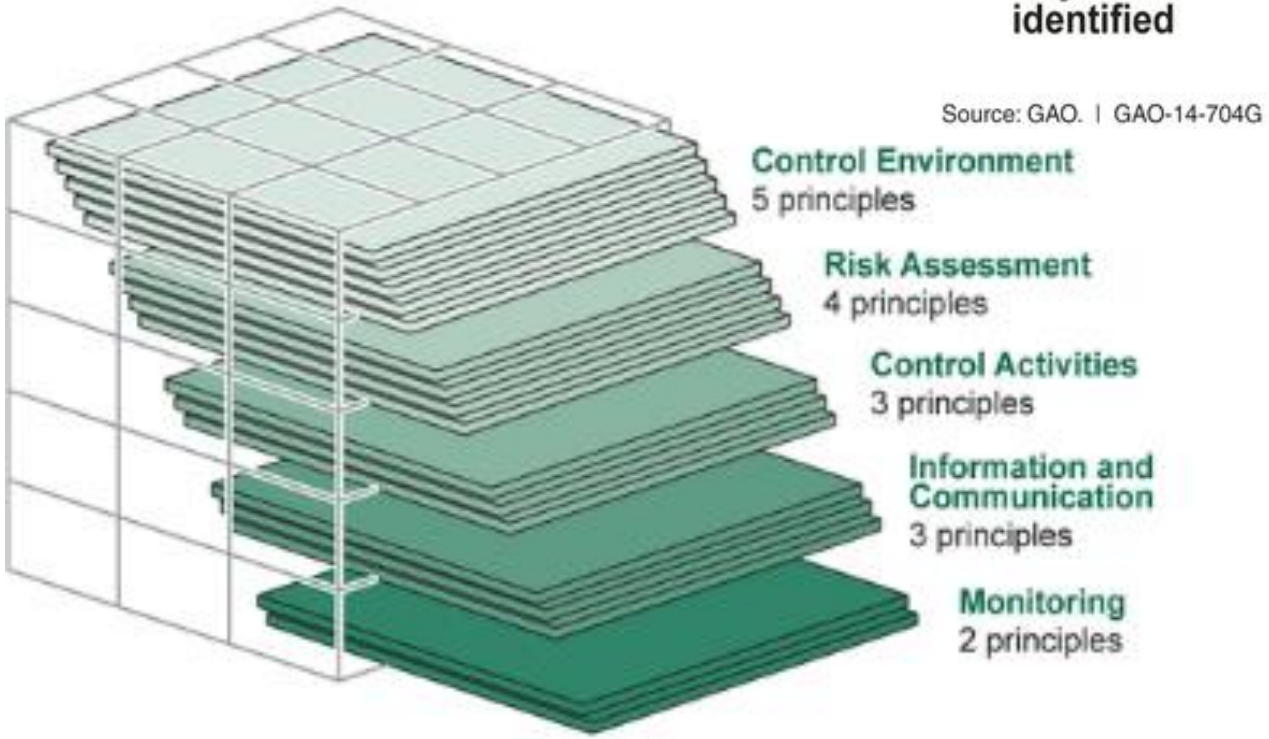
Why do we Need a Risk Assessment?

- Bottom line: A risk-based approach helps you prioritize needs and identify solutions
- More grants (stimulus funds!) = more rules to follow and higher risk
- Mitigate risk before auditors find it!



Developing a Risk Assessment





Source: GAO. | GAO-14-704G

Risk Assessment Principles

1. Develop clear objectives to enable the identification of risks and risk tolerance levels
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.

GAO Standards for Internal Control:
https://www.gao.gov/assets/gao-14-704g.pdf

Example Areas of Risk

- New personnel
- Lack of personnel
- Reorganizations
- Rapid growth / Changes in population
- Leadership Changes
- Change in Laws / Regulations
- New Grants
- New Technology
- High Crime Area

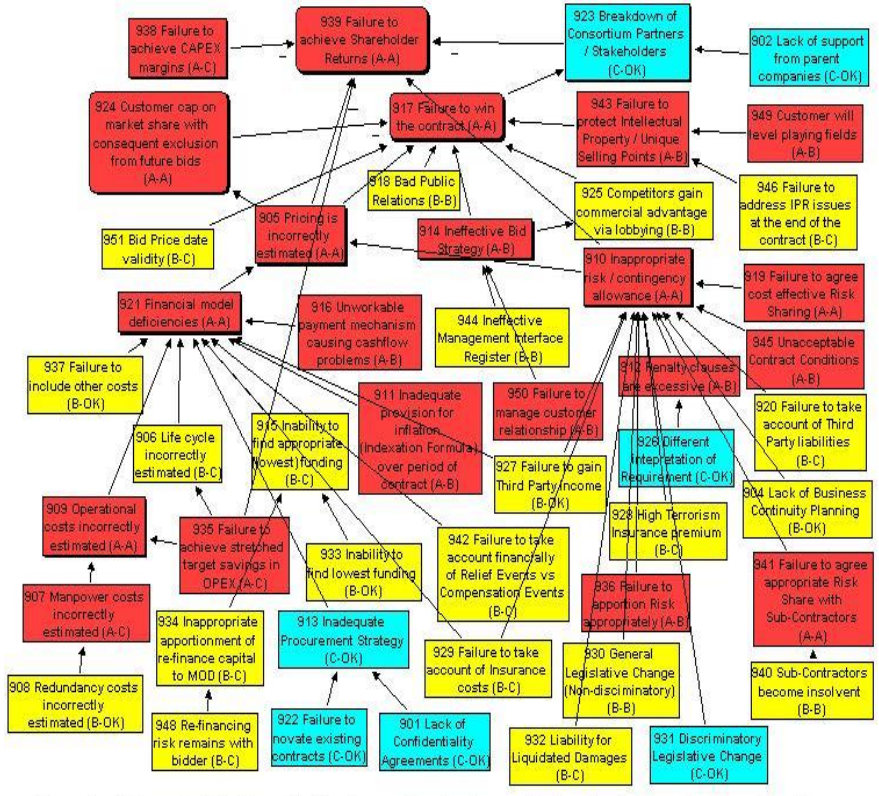
Risks are not stagnate; they increase and change as laws and operational environments change.

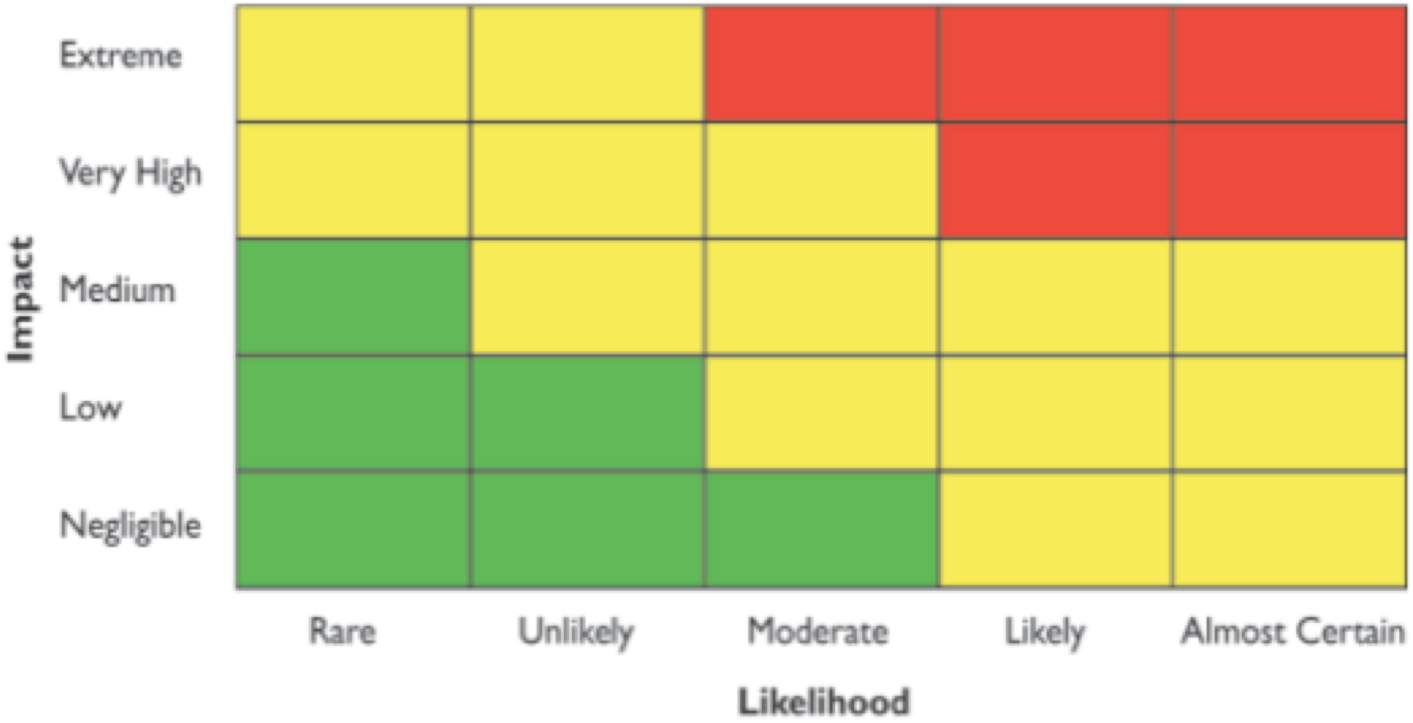
Federal Risk Evaluation - 200.206(b)(2)

Federal agencies **may** use the following items when reviewing applicant risk:

1. Financial stability
2. Management systems and standards
3. History of performance (including timeliness or compliance with reporting requirements)
4. Audit reports and findings
5. Ability to effectively implement requirements

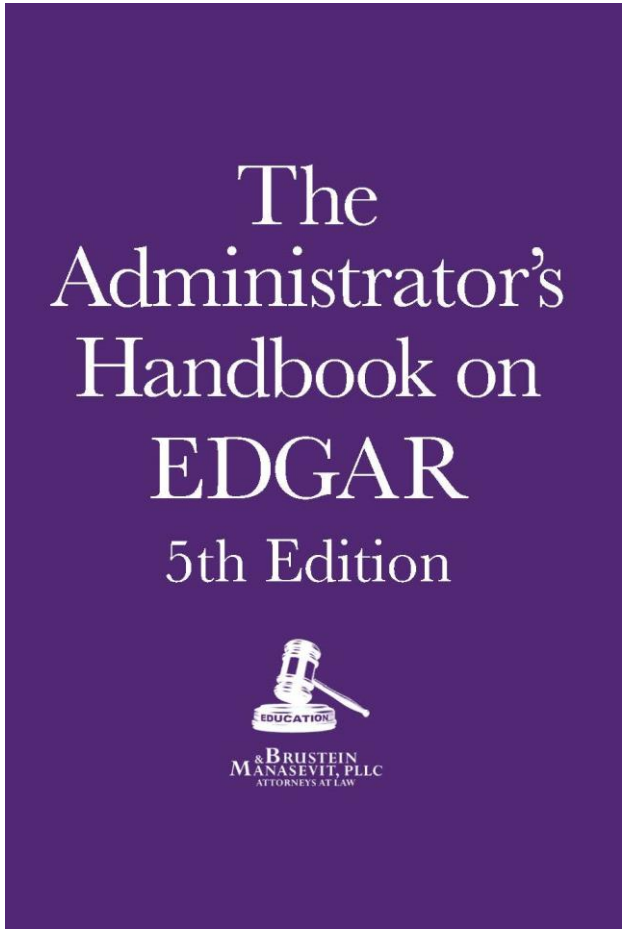
Risk Mapping





Applying EDGAR and the UGG

Which areas should be included in your risk assessment?



Uniform Grant Guidance (p. 105)

- Subpart A – Acronyms and Definitions (p. 108)
  - Examples changes: added "budget period," "renewal award", revised "period of performance," etc.
- Subpart B – General Provisions (p. 118)
- Subpart C – Pre-Federal Award Requirements and Contents of Federal Awards (p. 123)
- Subpart D – Post Federal Award Requirements; Standards for Financial and Program Management (p. 130)
- Subpart E – Cost Principles (p. 153)
- Subpart F – Audit Requirements (p. 184)

Financial Management

The Rules

- States - 200.302(a)
- Everyone else - 200.302(b)
  - (1) Identification of awards
  - (2) Financial reporting - 200.328 & 200.329
  - (3) Accounting records
  - (4) Internal controls - 200.303
  - (5) Budget controls - 200.308
  - (6) Written cash management procedures - 200.305
  - (7) Written allowability procedures - 200.403
- Federal Payment - 200.305

Risk Examples:

- Failure to track budget line items
- Missing budget amendments
- Late reporting
- Delayed drawdowns
- Lapsed funds

Procurement Standards

The Rules

- Procurement by states - 200.317
- General procurement standards - 200.318
- Competition - 200.319
- Methods of procurement - 200.320
- Domestic preferences - 200.322
- Awards to responsible contractors - 200.318(h)
- Suspension and debarment - 200.214
  - 2 CFR 180.300; 180.220

Risk Examples:

- Failure to compete
- Unallowable prioritization
- Vendor complaints re: processes
- Significant use of noncompetitive procurement

Inventory Management

The Rules

- Definitions - 200.1
  - Equipment, supplies, computing devices, etc.
- Equipment - 200.313
  - Use 200.313(b)-(c)
  - Management and inventory - 200.313(d)
  - Disposition - 200.313(e)
- Supplies - 200.314
  - Disposition - 200.314(a)

Risk Examples:

- Missing property
- Significant police reports
- Failure to submit inventory reports
- Lack of disposition records
- No evidence of depreciation calculation
- Prices exceed standard market value

Cost Principles

The Rules

- Factors affecting allowability - 200.403
- Applicable credits - 200.406
- Prior written approval - 200.407
- Direct and Indirect (F&A) Costs - 200.413; 200.414
- Selected Items of Costs
  - Time and effort documentation - 200.430(i)
  - Telecommunications and video surveillance costs - 200.471
  - Travel - 200.475

Risk Examples:

- Purchases lack tie to program objectives
- Number of items purchased not justified
- Lack of required documentation (time and effort)
- Failure to obtain prior approvals, when required
- Utilizing wrong indirect cost rate (or applying the rate incorrectly)

Other Risk Areas

The Rules

- Federal awarding agency review of risk posed by applicants - 200.206
- Single Audit - 200.501
- Subrecipient monitoring - 200.332

Risk Examples:

- Amount of federal funding
- History of past performance
- Staff turnover
- Monitoring findings
- Audit findings
- Failure to obtain a single audit
- Lack of policies and procedures
- Financial stability

Test Your Internal Controls!! (200.303)

The non-Federal entity **must**:

a. **Establish and maintain effective internal control** over the Federal award that provides reasonable assurance that the non-Federal entity is managing the Federal award in compliance with Federal statutes, regulations, and the terms and conditions of the Federal award

These internal controls should be in compliance with guidance in:

- "Standards for Internal Control in the Federal Government" issued by the Comptroller General of the United States, or
- The "Internal Control Integrated Framework," issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO).

Internal Controls - 200.303 (cont.)

b. Comply with Federal statutes, regs, and the terms and conditions of the Federal awards

c. **Evaluate and monitor the non-Federal entity's compliance** with statutes, regs and the terms and conditions of Federal awards

d. **Take prompt action when instances of noncompliance are identified including in audit findings**

e. Take reasonable measures to safeguard protected personally identifiable info (PII) and other information designated or deemed sensitive

Self-Assessment - 200.329

- The non-Federal entity **must**:
  - Monitor its activities under Federal awards to assure compliance with applicable Federal requirements and performance expectations are being achieved
  - Monitoring must cover each program, function or activity

Case Study: Indiana Department of Education

Case Study: Indiana Dept. of Ed.

- **RFQ - Internal Risk Assessment, Statement of Work:**
- Develop and implement an internal risk assessment across the agency
  - The internal risk assessment should provide assurance of compliant use of funds, appropriate safeguards, and proper accounting and reporting
  - Elements of effective internal control should include segregation of duties, personnel authorizations, policies and procedures, established systems and adequate staffing
  - Objectives include proper authorizations, accounting, security of assets, data, monitoring, and documentation including policies and procedures

Case Study: Indiana Dept. of Ed.

- Step One: Information gathering
  - Documentation (org chart, compilation of existing policies and procedures, recent audits/monitoring reports)
  - Interviews
    - CFO
    - Chief of Staff
    - Director of Financial Services
    - Director of School Finance
    - Director of Program Compliance
    - Director of Title I

Case Study: Indiana Dept. of Ed.

- Step Two: Identifying the types of risks to be evaluated
  - **Operations Risk Factors**
    - Staff turnover
    - Staff shortages
    - Lack of segregation of duties
    - Inconsistent or lack of staff training; PD opportunities
    - Receipt of new federal grants or significant increase (including stimulus)
    - Lack of uniform grants management system
    - Lack of policies and procedures re employee performance, oversight, reporting, and other procedures related to technology controls such as use access controls

Case Study: Indiana Dept. of Ed.

- Step Two: Identifying the types of risks to be evaluated
  - **Financial Management Risk Factors**
    - Lack of transparency of financial information (carryover balances, budget visibility) internally and externally, as needed
    - Lack of protocols on budget-to-actual reporting
    - Lack of consistency/schedule of federal draws
    - Significant carryover of funds
    - Lapsing of funds
    - Lack of written financial management procedures, including on timeliness; payment methods, collecting and evaluating financial data, maintaining accounting records

Case Study: Indiana Dept. of Ed.

- Step Two: Identifying the types of risks to be evaluated
  - **Allowability Risk Factors**
    - Time and effort is incomplete and/or noncompliant
    - Employees allocating time to two or more cost objectives on real time funding system
    - Inconsistent reconciliation of time and effort documentation to budgeted amounts
    - Lack of or inconsistent review process for time and effort
    - Lack of required travel documentation
    - Incorrect calculations of MOE/MSF/Moequity, as required
    - Incorrect calculations of match and in-kind contributions
    - Lack of updated written allowability policies and procedures

Case Study: Indiana Dept. of Ed.

- Step Two: Identifying the types of risks to be evaluated
  - **Procurement and Asset Management Risk Factors**
    - Lack of approvals on procurement documentation
    - Failure to obtain required quotes, bids or sole source verification documentation
    - Inconsistent maintenance of procurement record-keeping
    - Inconsistent oversight of contractors
    - Reports (internal and/or external) of conflicts by employees involved in procurement
    - Inadequate security or internal controls over assets
    - Lack of updated written policies and procedures related to management and disposition of equipment, safeguarding assets, conflicts of interest, including reporting conflicts and related disciplinary steps for violations

Case Study: Indiana Dept. of Ed.

- Step Two: Identifying the types of risks to be evaluated
  - **Compliance Risk Factors**
    - Inconsistent completion of required corrective actions
    - Lack of internal audit office and/or clear reporting structure and reporting options for internal audit office
    - Lack of updated written record retention policies and procedures
    - Inconsistent or lack of training on IDOE policies and procedures
    - Inconsistent or lack of familiarity on EDGAR/UGG requirements

Case Study: Indiana Dept. of Ed.

- Step Three: Identifying relevant documentation and evidence to review in conducting the assessment of risk
  - For example:

    Risk factor: Lapsing funds

    - Prior audits and/or monitoring; documentation of lapsing funds year-to-year; approved plans and budgets; budget amendments and related approvals; policies and procedures related to communication of financial information internally and with LEAs; proof of communication of financial information

    Risk factor: Inconsistent staff training on grants policies and procedures

    - Documentation of current trainings in place; new employee onboarding materials; employee handbook; other documents with policies and procedures distributed to employees

Case Study: Indiana Dept. of Ed.

- Step Four: Develop scoring rubric; factor in internal priorities, impact, likelihood
  - 5-point scale; +1 point for agency prioritization or repeated issues
  - For example:

    Risk factor: inconsistent oversight of contracts

    0 = Process for contract oversight in place and consistently followed

    3 = Process for contract oversight in place but requires updates

    5 = No process in place for contract oversight

    Risk factor: significant staff turnover

    0 = Less than 10% turnover

    3 = 10%-30% turnover

    5 = More than 30% turnover

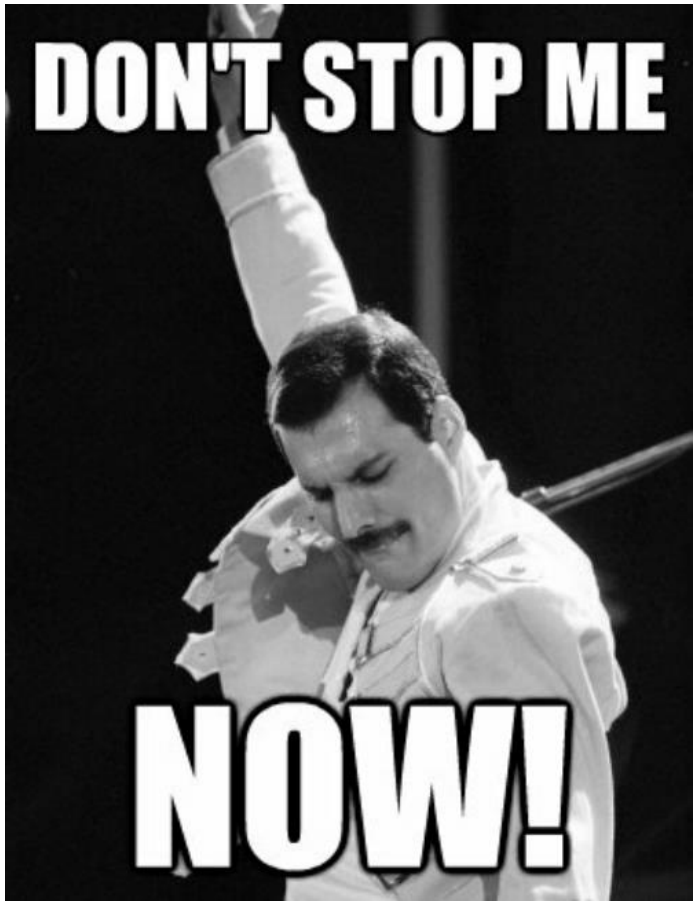
Case Study: Indiana Dept. of Ed.

- Step Five: Score the risk assessment
- 5+ points = high risk (red)
- 2-4 points = medium risk (yellow)
- 0-1 points = low risk (green)

  - ⋆Included "notes" section to provide additional context regarding risk factor or level
  - ⋆ Included recommended actions section for risk mitigation
  - Tailor rubric to your entity's needs

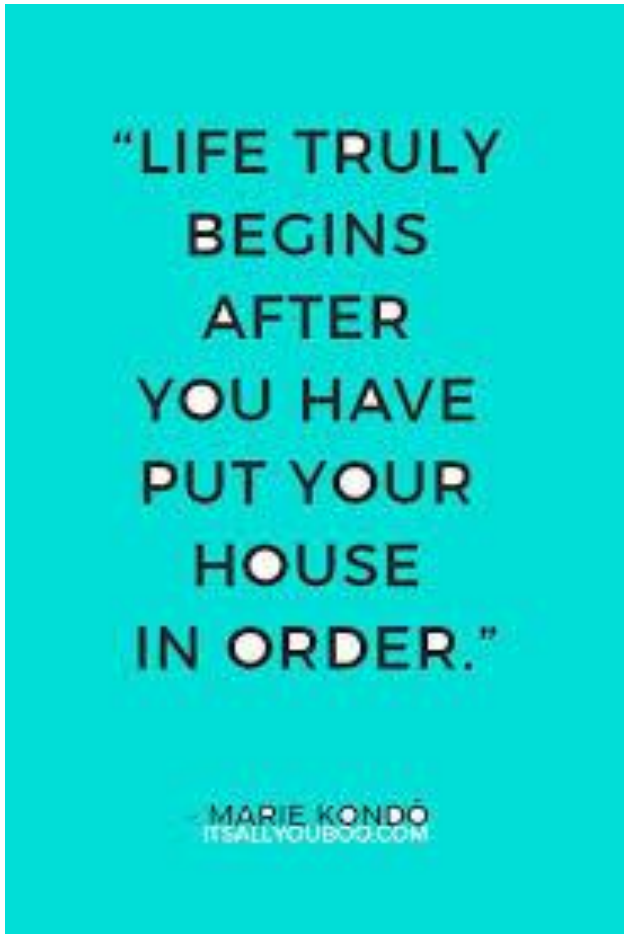
But Don't Stop There!

- Once the risk assessment is complete, don't forget the next step—take steps to mitigate the risks!
- Start with highest risk areas
- Implement strategies to mitigate risk
- For example, if inconsistent contract oversight is a high-risk area, a mitigating action would be to develop contract administration procedures and train employees



Now what?

- Need an internal risk assessment?
  - Develop and implement one tailored to your agency!
- Can I use federal stimulus funding?
  - Probably. Can use funds broadly, including for maintaining operations and employing SEA staff, but need COVID link
- Effective risk mitigation strategies?
  - Training!! Consider testing your staff on EDGAR/UGG
  - Written procedures (that are useful, updated, available)



Questions???

LEGAL 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.