1-2-3
Risk Assessment

WHY

COSO/NYS Internal Control Standards/B-350

COSO

Principle 6: Specify objectives with clarity
Principle 7: Identify and analyze risks across the entity
Principle 8: Consider the potential for fraud in assessing risks to the achievement of objectives
Principle 9: Identify and assess changes that could significantly impact the system of internal control

COSO/NYS Internal Control Standards/B-350

New York State Standards for Internal Control

- "One of the most important components of an organization's internal control program is the process used to identify and evaluate the risks and internal controls associated with specific functions, objectives, and assessable units."
- …a formal assessment of all inherently high-risk functions should occur at least annually , and lower risks categories should be reviewed at least every three years.
- The formal report of deficiencies should be directed to the ..head of agency …
- Presentation of Enterprise risks based on analysis of reported deficiencies

COSO/NYS Internal Control Standards/B-350

B-350

- Report Plan for reviewing and testing of Controls
- How monitoring corrective actions
- High risk areas tested.

But really—Risk assessments are good because…

- Recognize and control risk that could impede objectives in your organization
- Ensure that high priority risks are aggressively managed and that allidentified risks are cost-effectively managed by deliberately allocating resources to address risk.
- Identify controls that do not mitigate risk and may be eliminated.
- Create awareness among employees – and use it as a training tool as well.
- Reduce number of events that negatively impact the organization.
- Save funds by being proactive instead of reactive.
- Provide management at all levels with the information required to make informed decisions on issues critical to success.
- Provide documentation and transparency to decisions addressing risk.

Who

Management

- Responsible for establishing objectives that align and support the organization in pursuit of its mission.
- Establish acceptable variances
- Considers risk at all levels both by unit and entity.
- Considers both inherent and residual risk
- Responsible and accountable for risk identification and analysis.
- Responsible for ensuring appropriate personnel participate in the risk assessment
- Management determines how to respond to risk and implementing response
- Most importantly: Values and utilizes the risk assessment

ICO role

- Set up requirements for Risk Assessments with Management
- Establish schedule with Management
- Facilitate risk assessment, testing and corrective action plan
- Performs or assists with enterprise risk assessment and summary
- Report results to head of agency
- Report on status of corrective action plan

WHAT

Risk

Risk

- Risks are circumstances that threaten the accomplishment of objectives
- Can be both internal and external

RISK

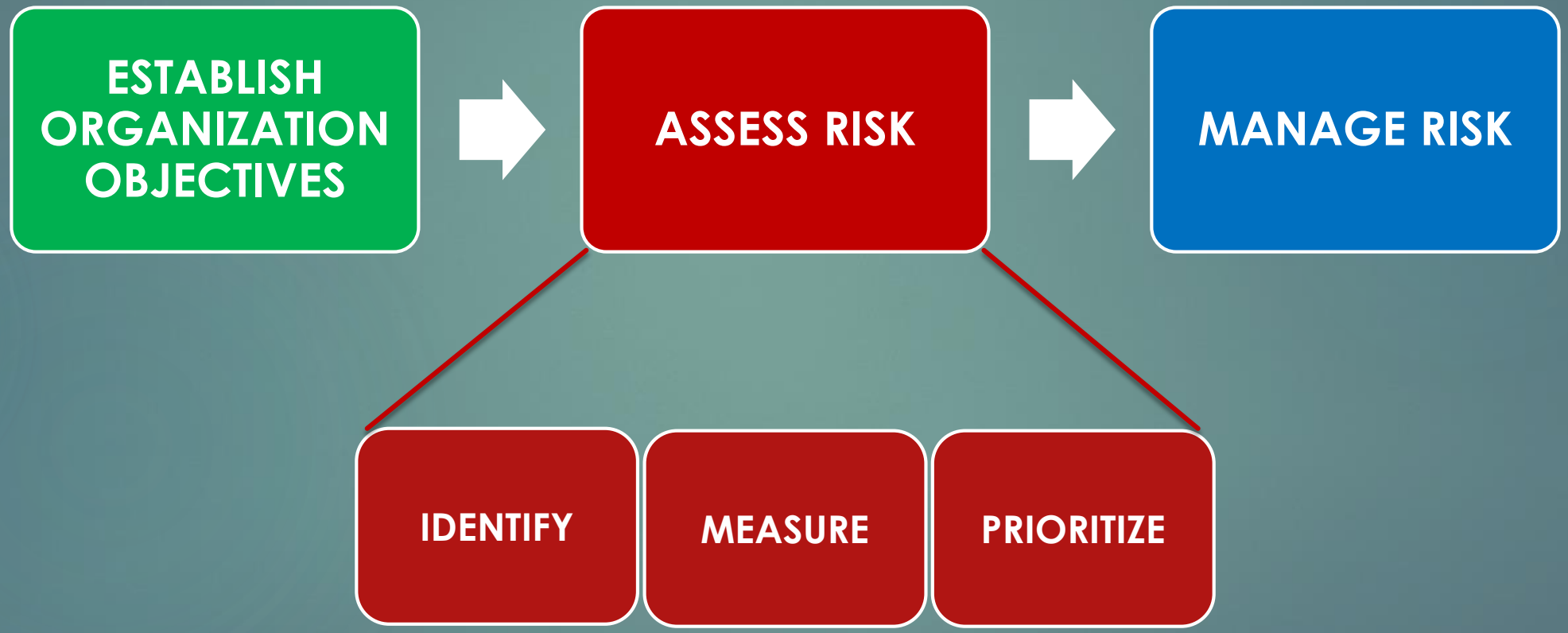
- Getting to work on time

- Cooking at home

- Driving a car

How

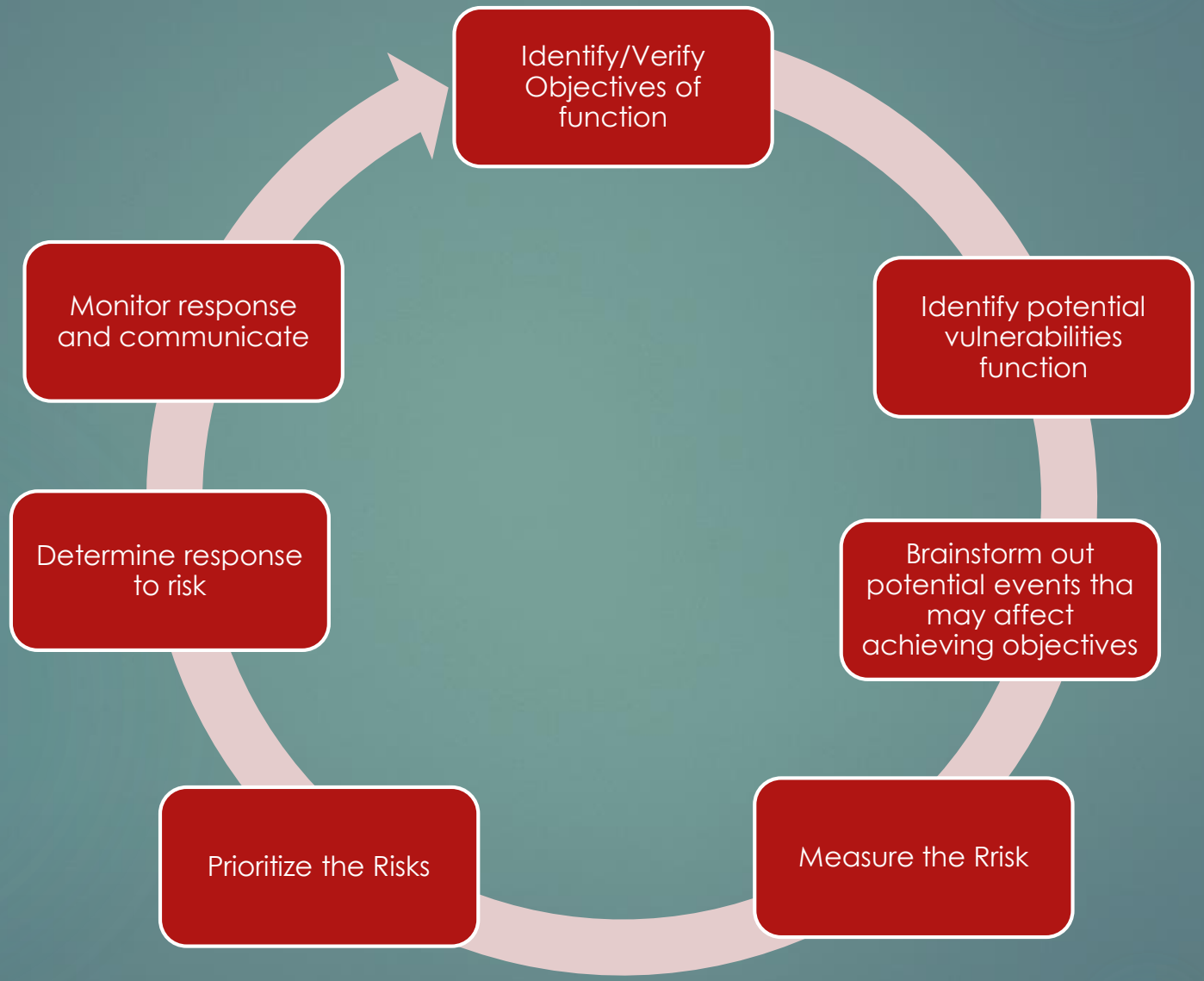
The Process of Risk Management



Risk Assessment Process

- What could go wrong?
- What are the chances of it happening? How often? (likelihood)
- What are the consequences if it does happen? (impact)
  - Include cost of missed opportunities
- What would cause it to happened?

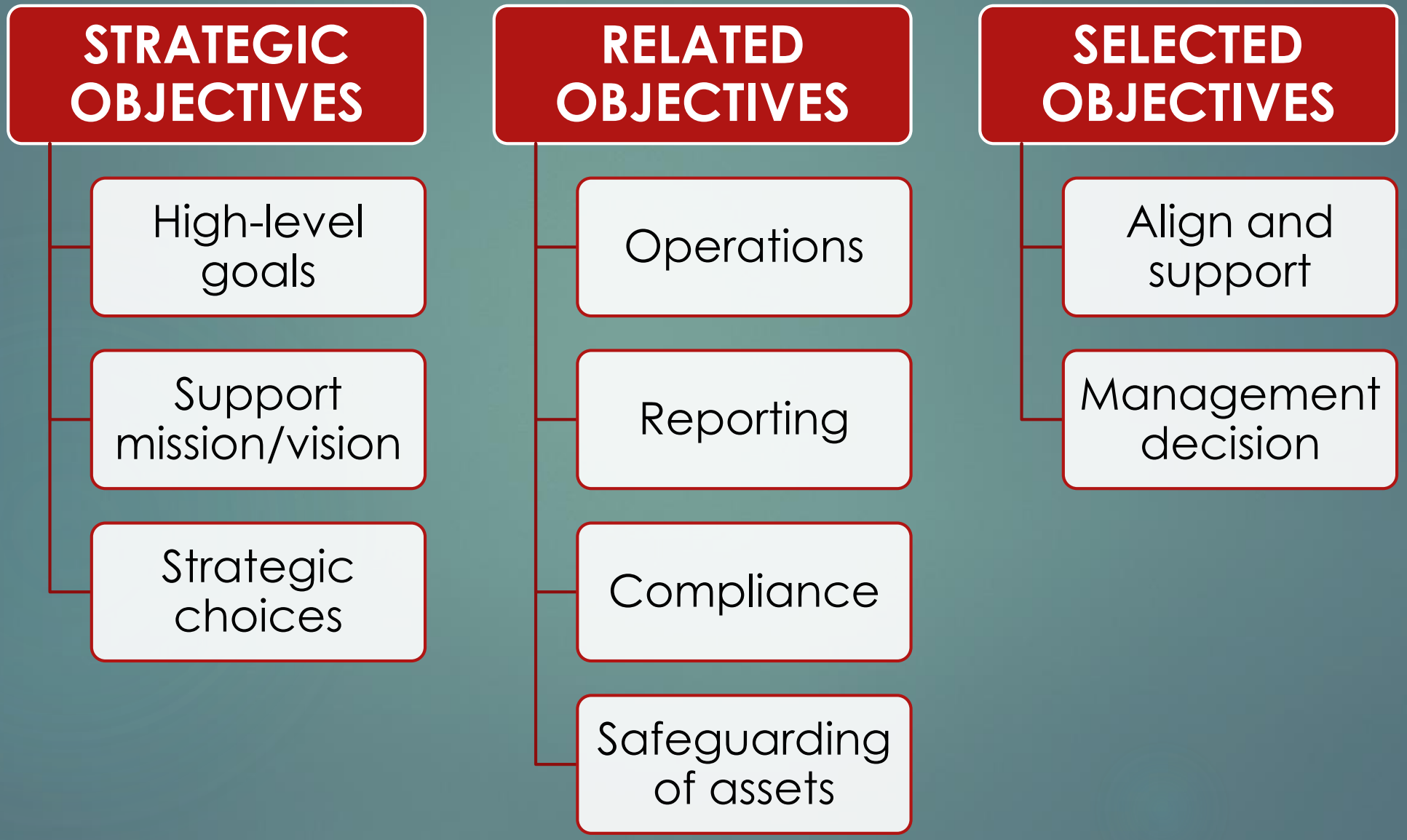
Risk Assessment Process



Objective Setting

- Every entity faces a variety of risks from external and internal sources, and a precondition to effective event identification, risk assessment and risk response is establishment of objectives, linked at different levels and internally consistent.
- Objectives are set at the strategic level, establishing a basis for operations, reporting, and compliance objectives.
- Objectives are aligned with the entity's risk appetite, which drives risk tolerance levels for the entity's activities.

OBJECTIVE SETTING



Risk Appetite

- The amount of risk, on a broad level, an organization is willing to accept in pursuit of its objectives
- It reflects the organization's established risk philosophy and influences the culture and operating style

Unacceptable Events

Unacceptable Events

- Fraud/Corruption
- Actions that cast public doubts on the organization's integrity, ethics, competency, accuracy and/or professionalism
- Violation of the public trust because of Management's unethical behavior
- Events that would endanger employee safety
- Illegal discrimination of any kind

Unacceptable Events (cont'd)

- Widespread failure of an agency mission critical operation
- Unauthorized disclosure, access or loss of personal/private information maintained by the agency
- Failure to plan for and strive for an adequate and skilled work force
- Actions that cause a hostile work environment

Risk Assessment

- Evaluate inherent risk
- Determine risk response
- Evaluate residual risk

Functional Vulnerability (Risk) Assessment

Step 2 - FUNCTIONAL VULNERABILITY ASSESSMENT

Function: _____ Office/Unit: _____

Responsible Individual: _____ Telephone: _____

For each characteristic listed below, rate the function's vulnerability from 1 to 5, with 5 being the highest degree of risk.

For example, a highly sensitive, technical or administratively complex function should be rated a 5 for the first category listed below.

Characteristic	1 Low Risk	2 Low to Moderate Risk	3 Moderate Risk	4 Moderately High Risk	5 High Risk
1. Sensitive/Complex Operations					
2. Personnel					
3. Policies & Procedures					
4. Financial Assets					
5. Authorizations					
6. Influence					
7. Operational Stability					
8. Organizational Structure					
9. Frequency of Reviews					
10. Impact of Failure					
11. Physical Assets					
12. Reliance on Information Systems					

TOTAL SCORE (add ratings 1 thru 12): _____

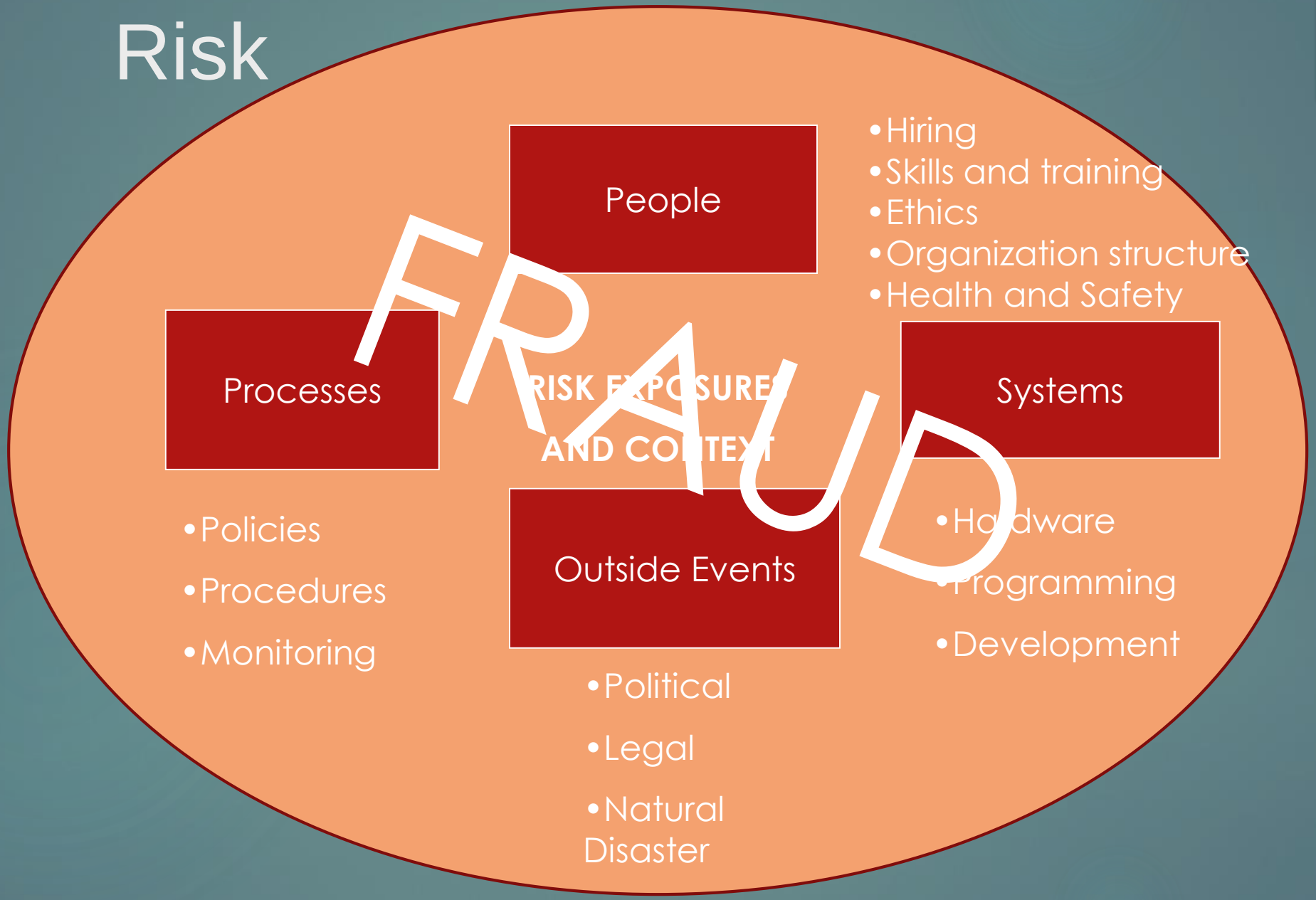
Overall Level of Vulnerability

Total Score of 48+ indicates **HIGH**

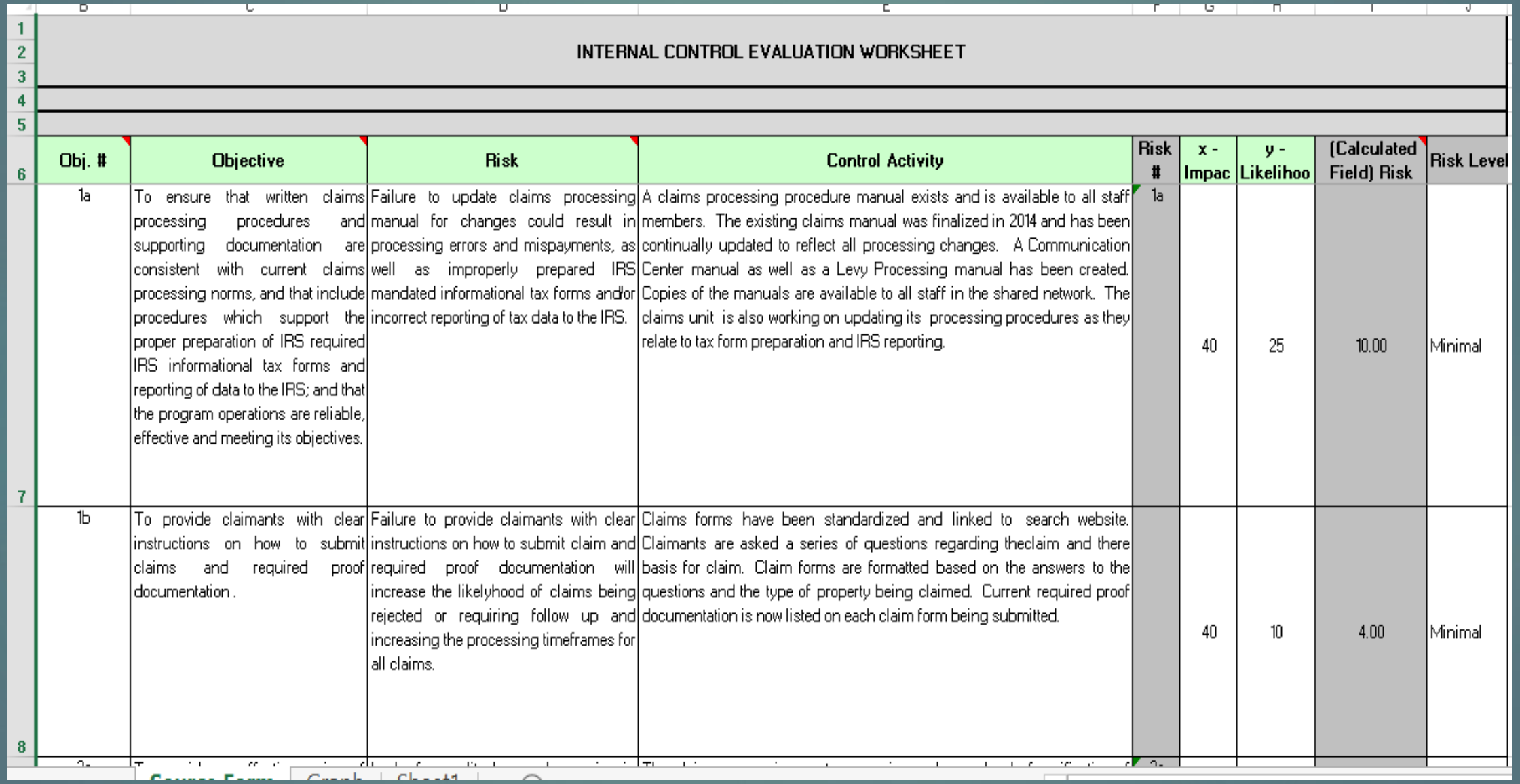
Total Score of 25-47 indicates **MODERATE**

Total Score under 25 indicates **LOW**

Risk


People
•Hiring
•Skills and training
•Ethics
•Organization structure
•Health and Safety
Processes
•Policies
•Procedures
•Monitoring
RISK EXPOSURE
AND CONTEXT
FRAUD
Systems
•Hardware
•Programming
•Development
Outside Events
•Political
•Legal
•Natural Disaster

How do you assess it

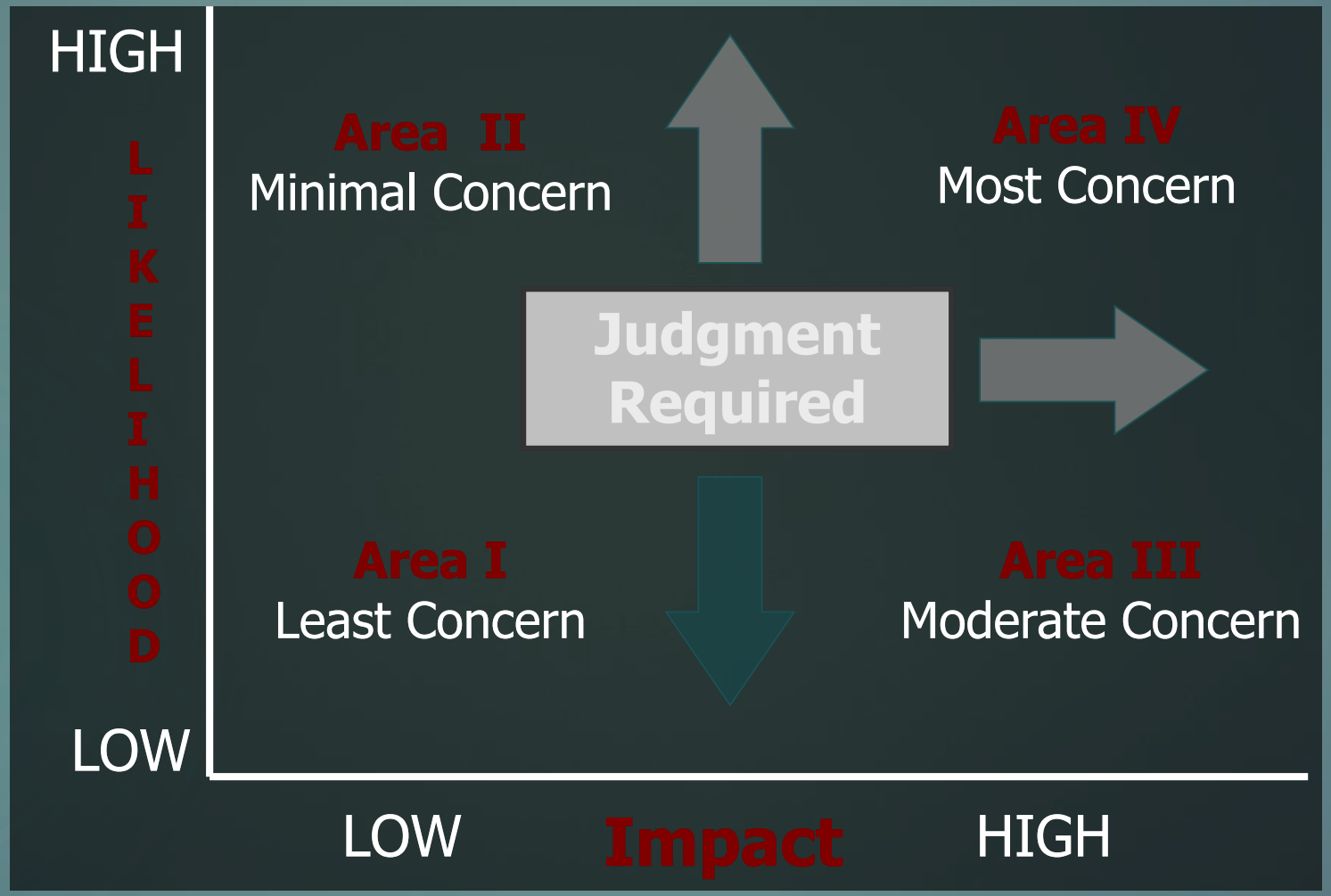


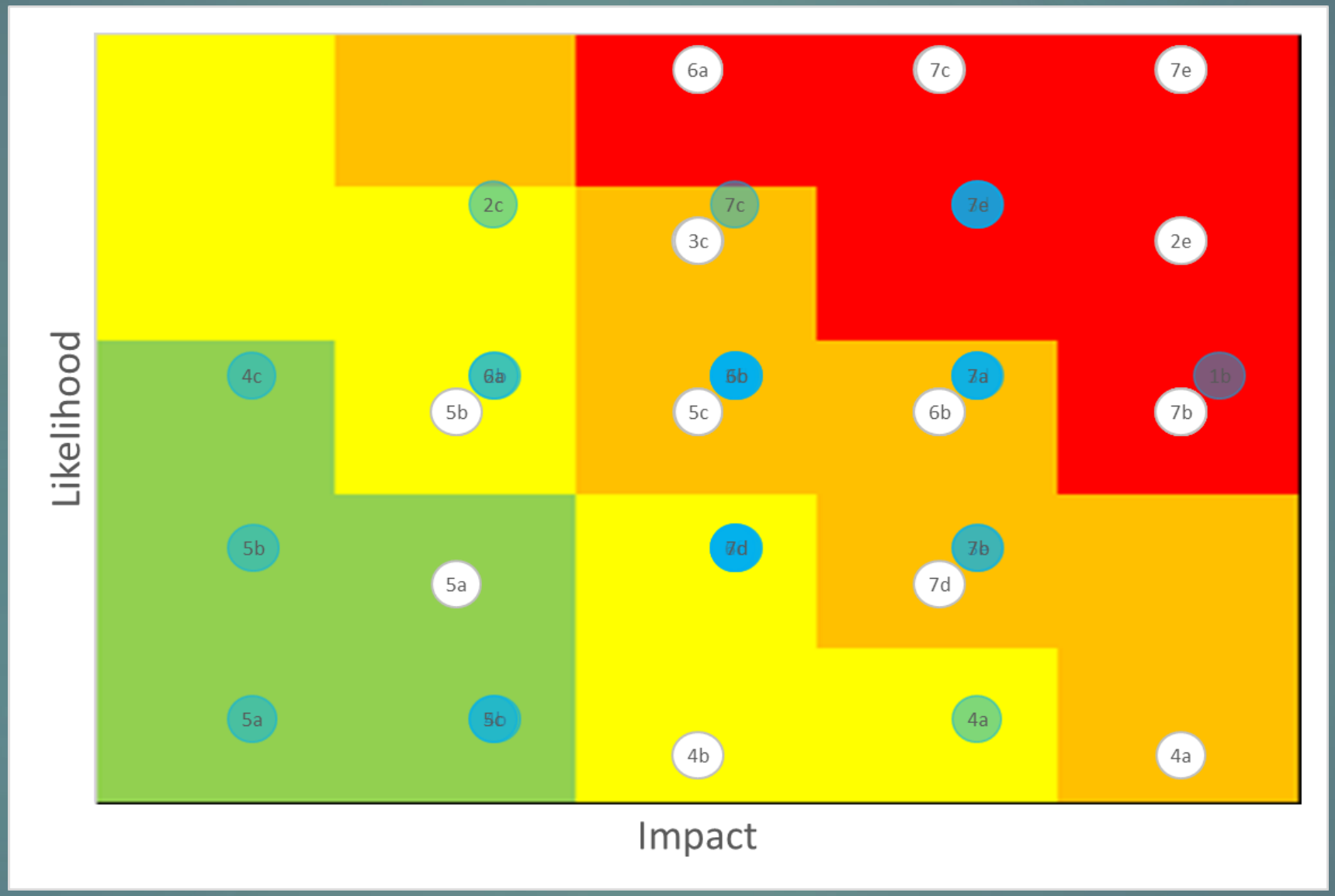
INTERNAL CONTROL EVALUATION WORKSHEET

Obj. #	Objective	Risk	Control Activity	Risk #	x - Impac	y - Likelihoo	(Calculated Field) Risk	Risk Level
1a	To ensure that written claims processing procedures and supporting documentation are consistent with current claims processing norms, and that include procedures which support the proper preparation of IRS required IRS informational tax forms and reporting of data to the IRS; and that the program operations are reliable, effective and meeting its objectives.	Failure to update claims processing manual for changes could result in processing errors and mispayments, as well as improperly prepared IRS mandated informational tax forms and/or incorrect reporting of tax data to the IRS.	A claims processing procedure manual exists and is available to all staff members. The existing claims manual was finalized in 2014 and has been continually updated to reflect all processing changes. A Communication Center manual as well as a Levy Processing manual has been created. Copies of the manuals are available to all staff in the shared network. The claims unit is also working on updating its processing procedures as they relate to tax form preparation and IRS reporting.	1a	40	25	10.00	Minimal
1b	To provide claimants with clear instructions on how to submit claims and required proof documentation .	Failure to provide claimants with clear instructions on how to submit claim and required proof documentation will increase the likelyhood of claims being rejected or requiring follow up and increasing the processing timeframes for all claims.	Claims forms have been standardized and linked to search website. Claimants are asked a series of questions regarding theclaim and there basis for claim. Claim forms are formatted based on the answers to the questions and the type of property being claimed. Current required proof documentation is now listed on each claim form being submitted.		40	10	4.00	Minimal

Objective	Risk	Inherent Likelihood	Inherent Impact	Inherent Rating	Inherent Ranking	Control	Residual Likelihood	Residual Impact	Residual Rating	Residual Ranking
To receive funds on behalf of a company and applying it towards their current pending balances.	Payment applied to incorrect account.	3	3	9	High	Check reconciliation at month end.	3	2	6	Medium
To pay money owed by a business to its suppliers, vendors, or employees.	Duplicate invoices paid.	5	4	20	Very High	Consistent invoice numbering convention. Automated matching based on multiple factors (invoice number, vendor name, amount, etc)	5	3	15	Very High
Recording of transactions to a company's assets, liabilities, owners' equity, revenue, and expenses accounts.	Transaction amount incorrect.	3	5	15	Very High	Financial statement out of balance.	3	3	9	High
The sum of money allocated for a particular purpose and the summary of intended expenditures along with proposals for how to meet them.	Spend plan coding error.	4	3	12	High	Spending cannot exceed account balance.	3	3	9	High
The calculation and payment of salaries, wages, benefits, and taxes.	Salary inflated for a friend.	5	3	15	Very High	Run match of payroll amount by employee title. Anomolies are researched.	3	2	6	Medium

Evaluating Risk

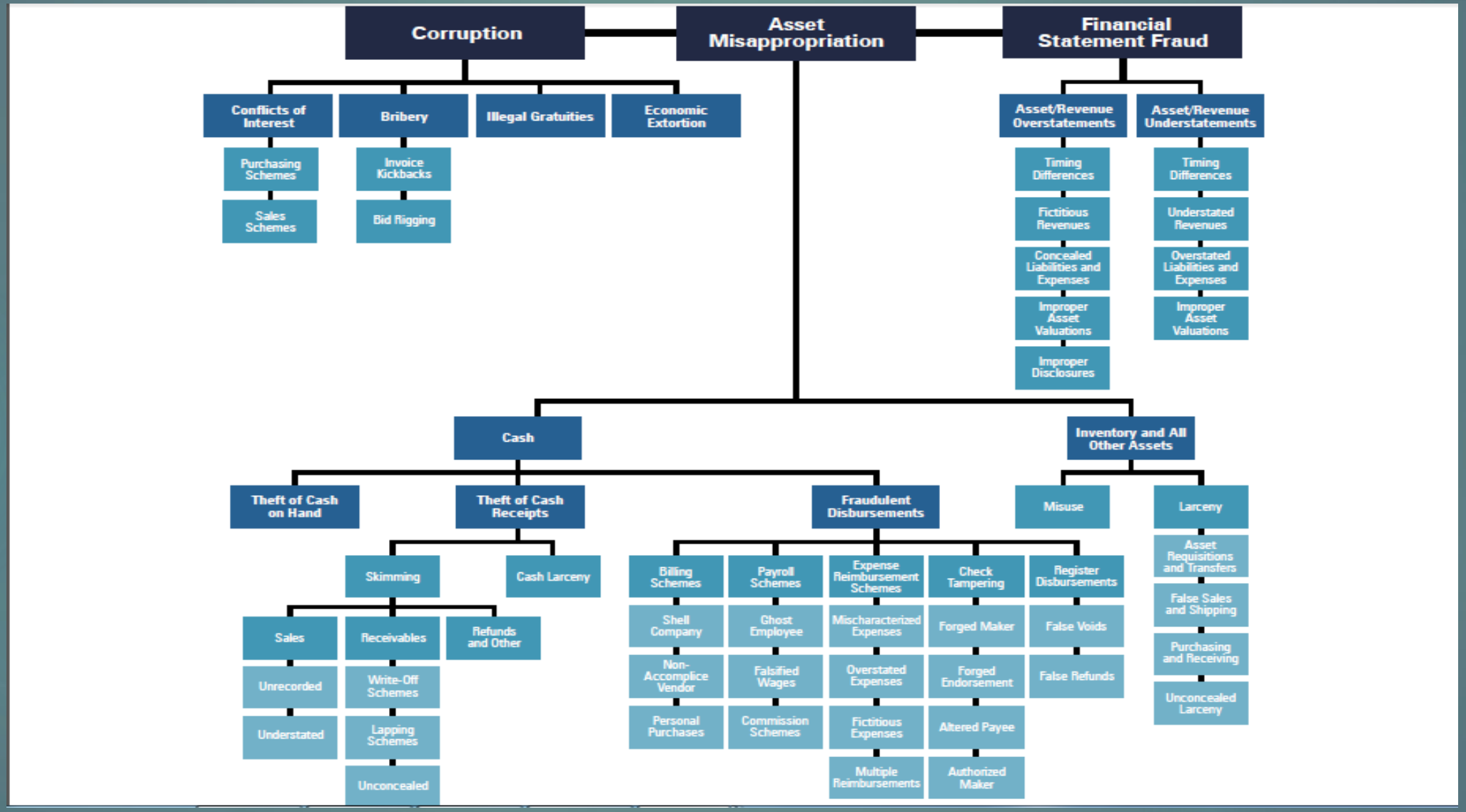



Likelihood
Impact
6a
7c
7e
2c
7c
7e
3c
2e
4c
6a
6b
7a
1b
5b
5c
6b
7b
5b
7d
7b
5a
7d
5a
5b
4a
4b
4a

Incorporate fraud risk in your annual risk assessment.

- How might a fraud perpetrator exploit weaknesses in the system of controls?
- How could a perpetrator override or circumvent controls?
- What could a perpetrator do to conceal the fraud?

Occupational Fraud Tree



Identified Fraud risks and Schemes[1]	Likelihood [2]	Significance [3]	People and/or Department [4]	Existing Anti-fraud Controls[5]	Controls Effectiveness Assessment[6]	Residual Risks[7]	Fraud Risk Response[8]
FINANCIAL REPORTING:							
Revenue Recognition							
Recording receipts in incorrect periods	Remote	Insignificant	Accounting	Manager year end review of receipts.	Tested by Independent staff.	Risk of Management Override.	No further action, receipts are minimal and no benefit to agency of management to record in error.
Expenditure Recognition							
Holding bills	Reasonably possible	Material	Accounting	Input of bills and approval are segregated.	Tested by Independent staff.	Risk of Override.	Independent staff tests year end expenses.
Improper coding of bills	Reasonably possible	Material	Accounting	1) Input of bills and approval are segregated.	1) Tested by Independent staff.	1) Risk of Override.	1) Independent staff tests vouchers.

Control Activities to focus on

- Physical Access
- Job Descriptions
- Reconciliations and Analysis
- Supervision

Risk Response

- Identifies and evaluates possible responses
- Evaluates options in relation to entity's risk appetite
- Selects and executes response based on evaluation of the portfolio of risks and responses.

Risk Response

- Accept
- Avoid
- Reduce
- Share

Risk Response

- Accept
  - Monitor the situation
- Avoid
- Reduce
- Share

Risk Response

- Accept
- Avoid
  - Just what it sounds like!
- Reduce
- Share

Risk Response

- Accept
- Avoid
- Reduce
  - Add or modify controls
- Share

Risk Response

- Accept
- Avoid
- Reduce
- Share
  - Partner with someone else

    (e.g. Insurance)

Risk Response

- Key questions:
  - What risks will the organization not accept?
  - What risks will the organization take on new initiatives?
  - What risks will the organization accept for competing objectives?

Reasonable Assurance

Internal controls are to provide a reasonable assurance that the objectives of the system will be accomplished

The cost of internal control should not exceed the benefit derived.

When

Risk Assessment

A continuous and interactive process that takes places throughout the organization

Pulling it together

Portfolio View (organization)

- Risk is assessed from the entity level
- Considers the interdependence of risks
- Decisions are based on the whole package

Red Flags a Risk Assessment is not Adequate

- Management has not assessed risk in relation to major changes (reorganizations, funding cuts, system changes)
- There are not well defined objectives
- There are not well defined measures
- Management has not consider fraud issues
- The organization is unable to prioritize work appropriately
- The organization is unaware of or cannot overcome obstacle to its mission
- Management will not acknowledge or discuss risks