NATIONAL ASSOCIATION FOR STATE COMMUNITY SERVICES PROGRAMS

45th ANNIVERSARY

# Risk Management

HANCOCK™ SOFTWARE
PLATINUM SPONSOR

2023 ANNUAL TRAINING CONFERENCE
SEPTEMBER 25 - 29

# RISK ASSESSMENT & MITIGATION

Kevin C. Myren, CPA

# Agenda

- What is risk?
- Types of risk
- Risk in the *Uniform Guidance*
- Assessing risk
- Mitigating risk
- Enterprise Risk Management (ERM)
- Cyber

# Risk Defined

- **Risk** is the possibility of something bad happening.
  - *Wikipedia.com*
- Generally, it is the ***uncertainty*** of something happening or the implications of an activity
- This uncertainty gets in the way of our plans or expected outcomes
- So, it is an impediment to our goals
- Usually focuses on negative or undesirable outcomes

# Risk Quantified

Risk = Probability of event occurring
X  Expected loss

# Eliminating Risk

- Only ONE way to *completely* eliminate risk in your organization

If we can’t eliminate it, then we need to manage it….

# Types of Risk

1. Environmental
   - *Funding*
   - *Legislative change*
   - *Economy*
2. Organization
   - *Governance*
   - *Weather*
   - *Brand*
   - *Lawsuit*
   - *Employees*
3. Transaction
   - *Fraud*
   - *Error*

- Internal
  - *Operational*
  - *Financial*
  - *Technology*
- External
  - *Social*
  - *Market*
  - *Political*
  - *Legal*
  - *Environmental*
  - *Economic*

- Facilities & Buildings
- Human Resources and Employment Practices
- Financial Reporting & Internal Controls
- Contracts
- Client and Participant Safety
- Transportation
- Technology & Privacy
- Special Events
- Crisis Management & Business Continuity
- Volunteers
- Fundraising and Resource Development

# Top 10 Risks to Non-profits

1. Loss of Government funding
2. Reduction in Foundation funding
3. Lack of succession
4. Workplace injury
5. Fraud
6. Data security
7. IT downtime
8. Unrelated business activities
9. Disgruntled former employee
10. Natural disaster

# Risk in the *Uniform Guidance*

2 CFR 200

## _.206 *Federal awarding agency review of risk posed by applicants*

- *Prior to making an award, whether competitive or not, the Federal agency shall evaluate **risks** to the program posed by each applicant*
  - Financial stability
  - Quality of management systems
  - Ability to meet the management standards
  - History of performance
  - Reports and findings from single audits

# 2 CFR 200

- ***_.208 Specific conditions***
  - *When awarding agency review of risk posed by applicant or recipient history indicates potential failure to comply with performance goals:*
    - Payments as reimbursements, rather than advances
    - Withholding authority to proceed to next phase
    - More detailed financial reports
    - Additional project monitoring
    - Receipt of technical assistance
    - Establishing additional prior approvals

# 2 CFR 200 – Pass-through Entities

- ***_. 332 Requirements for pass-through entities,***
  - *All pass-through entities shall:*
    - Evaluate each subrecipient's **risk of noncompliance** with Federal statutes, regulations and terms and conditions of the subaward, which includes consideration of:
      - *Subrecipient's prior experience with same or similar subawards*
      - *Results of previous audits*
      - *New personnel or new or changed systems*
      - *Federal agency monitoring*

*All pass-through entities shall:*

- *Depending upon pass-through entity's assessment of risk posed by the subrecipient, the following monitoring tools may be used to ensure proper accountability and compliance with program requirements and achievement of performance goals"*
  - *Performing on-site reviews of operations*
  - *Providing training and technical assistance*
  - *Arranging for agreed-upon-procedures engagements*

# 2 CFR 200 – Single Audits

- ***_.514 Scope of Audit***
  - *Shall be conducted in accordance with GAGAS*
  - *Audit shall cover the entire operations of the auditee*
  - *Auditor shall determine whether the financial statements are presented fairly in all material respects in conformity with generally accepted accounting principles*
  - *Auditor shall also determine whether the schedule of expenditures of Federal awards is presented fairly*
  - *Auditor shall obtain an understanding of internal control over Federal programs sufficient to plan the audit to support a low assessed level of control risk for major programs*
  - *Determine whether the auditee complied with laws, regs. and terms and conditions of awards that might have a direct and material effect on each major program*

# 2 CFR 200 – Single Audits

- _.518 Major Program Determination
  - *Risk-based approach to determine major programs*
  - *Step 1. Determine Type A programs*
  - *Step 2. Determine which Type A programs are low-risk*
  - *Step 3. Determine which Type B programs are high risk*
    - Auditor uses professional judgment and criteria in _.519
    - Auditor only required to perform risk analysis on Type B programs that exceed 25% of Type A threshold
  - *Step 4. Determine major programs*
    - At a minimum, the following shall be identified as major
      - *Type A – High Risk*
      - *Type B – High Risk*

# 2 CFR 200 – Single Audits

- ***_.518 Major Program Determination***, continued
  - *Percentage of Coverage Rule*
    - If a Low Risk Auditee, Major programs must encompass 20% or more of total Federal Awards expended
    - If other than a Low Risk Auditee, Major programs must encompass 40% or more of total Federal Awards expended
  - *Documentation of risk analysis process must be included*
  - *When documented, the auditor's judgment of risk shall be presumed to be correct*

# 2 CFR 200 – Single Audits

- ***_.519 Criteria For Federal program risk***
  - *Auditor's determination should be based on overall evaluation of risk of noncompliance occurring that could be material to the Federal program*
  - *Current and prior audit experience*
    - Prior findings indicate higher risk
    - Programs administered under multiple internal control structures
    - Programs not recently audited may be of higher risk
    - Monitoring reviews may impact assessment of risk
    - Federal agencies may identify programs with higher risk
  - ***Inherent risk***
    - Nature of Federal program – eligibility, allocation, etc.
    - Phase in life cycle

# 2 CFR 200 – Single Audits

- ***_.520 Criteria For a Low-Risk Auditee***
  - *Auditee meeting all of the following for each of the preceding two audit periods shall qualify as a low-risk auditee*
    - Full single audits were performed on an annual basis
    - Auditor's opinion on financial statements were unqualified
    - No deficiencies in internal control were identified as material weaknesses
    - Auditor did not report a going concern
    - No Type A program had audit findings in prior two audits that were:
      - *Internal control deficiencies that were identified as material weaknesses*
      - *Other than unqualified opinion on major programs*
      - *Questioned costs <5% of total*

# CSBG Organizational Standards

## Standard 4.6

An organization-wide, comprehensive risk assessment has been completed within the past 2 years and reported to the governing board.

## Key Points

- Must be organization-wide
  - *Not just one program or area*
- Must be comprehensive
  - *Not just one department or function*
- Must be communicated to the Board

# CAA Standards of Excellence

- ***Additional*** requirements beyond the Org. Stands.
  - Administrative and Financial risk assessments
  - Annually conducted
  - Board engagement must be formal part of agency operations

# Risk Assessment & Risk Management

1. Identify Potential Hazard (Risk)
2. Assess Impact
3. Examine Options
4. Implement Solution
5. Monitor Results

# 1. Identify Potential Hazard (Risk)

## Tools

- What-if analysis
  - *If we are hacked and data is compromised, we can not conduct business and our reputation is ruined.*
- Checklist
  - *Assumes the checklist is a valid list of all hazards*
- Brainstorming session
  - *What hazards might impact your organization?*
  - *What hazards might impact your infrastructure?*
  - *What hazards might impact your surrounding area (environment)?*

## Examples

- Fire
- Tornado
- Cyber attack
- Fraud
- Embezzlement
- Lack of employees
- Bad press
- Lack of money

# G O A L...

Trying to ascertain a challenge before it becomes a problem

# Risk Analysis

| |
|---|
| **AREA I: Governance and Leadership** |
| |
| **AREA II: Strategy and Outcomes** |
| |
| **AREA III: Regulatory and Environmental** |
| |
| **AREA IV: Human Capital** |
| |
| **AREA V: Internal Control** |
| |

# AREA I: GOVERNANCE & LEADERSHIP

**Governance and leadership is the direction setting function of the organization. The Board of Directors is responsible for setting the strategic direction of the organization and the Executive Director is key employee of the organization responsible for ensuring the organization follows that direction. Strong and clear leadership at the Board and Executive level are essential for the success of an organization. The lack of either of these elements puts the organization at severe risk.**

## A. The *composition* of the Board is appropriate to obtain the desired outcomes.

1. The Board has elected officers, such as Chair, Vice-chair, Secretary and Treasurer.
2. The Board members have knowledge and expertise in the activities of the organization.
3. The number of Board members is large enough to cover a diversity of opinion and input, but not too large to preclude effective operations.
4. If the organization administers CSBG funds, the tri-partite composition requirements followed.
5. Financial expertise present on the Board.
6. Human resource expertise on the Board.

## B. The Board members are *engaged* in their role as Board members.

1. There is a document that describes the roles and responsibilities of Board members, that is communicated to Board members.
2. A new Board member orientation is held so that Board members get clear expectations on the duties they are to perform.
3. Attendance at Board meetings is monitored.
4. Open participation is encouraged at Board meetings.
5. The Board asks relevant and pertinent questions at Board meetings.
6. The Board does *not* act as a 'rubber stamp' on issues before them.

## C. The Board *conducts* its business in an appropriate manner.

1. Minutes of Board meetings are maintained and reviewed and approved at subsequent meetings.
2. The Board operates professionally under a set of guiding principles such as Robert's Rules of Order.
3. The Board has a policy on confict of interest and follows it.
4. The Board receives trainings on topics relevant to Board leadership, such as fidiciary responsibility, and incorporates them into how it operates.
5. Board members hold each other accountable for their actions.
6. Board members review and approve the Form 990 annually before submission.

## D. The Board establishes the *strategic direction* for the organization.

1. The Board creates and/or approves the mission, vision and values for the organization.
2. The Board determines and/or approves the metrics for success or outcomes measures for the organization.
3. The Board is kept current on the organization's progress towards these outcomes, by dashboard or other outcomes reporting methods.
4. When the organization is lagging in performance (not meeting its outcomes), the Board requests and receives corrective action strategies.
5. The Board approves the annual budget for the operations of the organization, which is aligned with the strategic plan of the organization.
6. The Board approves the auditor, receives the audit report and approves the audit report annually.

   Also, the Board requires correction of findings, if any.

## E. The Board *oversees* the Executive Director of the organization.

1. The Board hires and fires the Executive Director.
2. The Board directs the work of the Executive Director.
3. The Board does not inappropriately direct the work of other employees within the organization.
4. The Board meets with the Executive Director routinely to appraise his/her performance.
5. The Board determines the compensation of the Executive Director through the use of market comparability studies and performance.

## F. The Executive Director *effectively leads* the organization.

1. The Executive Director determines the appropriate human capital (staffing) structure of the organization.
2. The Executive Director provides leadership and direction to the staff to encourage successful achievement of the organization's goals and objectives.
3. The Executive Director oversees the operations and maintenance of the organizations policies and procedures around key systems:
   - Program operations
   - Finance and budget
   - Human resources
   - Risk management
   - Regulatory compliance
4. The Executive Director has the requisite education, training and knowledge to carry out her/his duties.

# AREA II: STRATEGY & OUTCOMES

Strategy is the guiding force for the organization. Further, it is the reason the organization exists. Outcomes are the desired results of the work of the organization. Achieving the stated outcomes indicates the organization has achieved its goals. Clear, well articulated strategies and goals ensures resources are aligned to achieve the desired outcomes and that staff are unified in the ultimate work of the organization. The risk to the organization without clear strategy and outcome expectations is significant.

A. The organization's strategic plan is developed with **appropriate input** from stakeholders.

1. A community needs assessment was conducted.
2. The needs that relate to the work of the organization have been identified and prioritized.
3. The strategic plan was developed based on this input.

B. Strategic **outcomes** were determined that tie to the strategic plan.

1. Outcome measures have been developed that link back to the strategic plan.
2. Outcome measures are relevant and impactful.
3. Outcome measures can be measured and replicated.

C. Progress towards achieving the strategic plan are **monitored**.

1. Staff monitor progress towards the outcomes.
2. Outcome measures are reported to the Board, using tools such as a dashboard.
3. The Board operates at the strategic level versus the operational level of the organization.

## D. The strategic plan and outcomes directs the work of the organization.

1. Staff develop annual action plans that incorporate the strategic plan as the over-arching goal.
2. The annual budget for the organization is aligned with annual action plans and the strategic plan.
3. When satisfactory progress is *not* being made in furtherance of the strategic plan there is a method to adjust the on-going operations to realign the work of the organization.

## E. The strategic plan and outcomes are updated and refreshed.

1. The Board approves the strategic plan.
2. The strategic plan is redone or refreshed on a three to five year schedule.
3. Outcome measures are evaluated for adequacy, potentially adjusted and approved by the Board, annually.

# AREA III: REGULATORY & ENVIRONMENTAL

**The regulatory arena that the organization operates in guides and restricts the activities that an organization can perform. This restrictive sphere of activity is further constrained by the environmental realities that the organization operates within. The risk to the organization of not understanding and operating within the regulations and environment to which it is constrained are significant.**

## A. The organization understands and operates within the legal parameters available to it.

1. By-laws are reviewed at least every three years to ensure currency.
2. The organization has identified corporate counsel that is available for immediate attention for legal issues.
3. At least one Board member is an attorney or well versed in business law, such as a business owner.
4. Staff of the organization include someone charged with understanding and overseeing human resource (employment) legal issues and compliance.
5. The organization is not currently engaged in a signficant legal action.

## B. The organization is aware of tax law issues.

1. Leadership of the organization knows the tax exempt mission approved by the IRS and operates within it.
2. The organization avoids lobbying and other disallowed political activities.
3. The organization timely and accurtately submits its form 990 to the IRS.
4. The organization understands and complies with the public disclosure requirements for its form 990.
5. The organization knows all payroll related tax reporting requirements and has complied with them all.

## C. General grant requirements are understood and followed by the organization.

1. Relevant staff are aware of and understand the requirements of OMB's *Uniform Guidance*.
2. The necessary policies and procedures for entities administering Federal grants are in place.
3. Employees have been made aware of the requirements for administering Federal grants.
4. The policies and procedures are routinely reviewed and updated.
5. Employees receive training to stay current in recent developments for grants management.
6. Additional requirements for state grants management are also understood by employees and integrated into policies and procedures of the organization.

## D. Specific grant rules are understood and employed by program staff.

1. Program directors for major programs have the requisite training, knowledge and experience to manage their respective program.
2. Employees within each program understand the necessary rules and regulations for the program(s) they work in.
3. Employees knowledge is kept current by on-going professional development.
4. All necessary program outcome or deliverable reporting is timely and accurately submitted.
5. All financial reporting for individual grants is accurately and timely submitted.

## E. Financial aspects of grants are fully determined.

1. Grants are approved by either the Executive Director or the Board of Directors before submittal.
2. The organization's ability to fulfill grant requirements is analyzed and determined *before* grant applications are submitted.
3. The adequacy of grant resources to generate the required outcomes/deliverables of the grant are determined before grant submittal.
4. The method and sufficiency of indirect cost recovery is determined before grant application.

# AREA IV: HUMAN CAPITAL

People are the key component of any organization. The success or failure of an organization to deliver on its mission is directly dependent on the quality of people employed by the organization to carry out the mission. Regardless of how wonderful all the other systems of the organization are; without the right people in place, the organization has a great risk of failure.

## A. The organization hires well qualified people for all positions.

1. The organization has current job descriptions for all positions within the organization.
2. The organization requires appropriate education and experience, when filling vacancies.
3. The organization is able to generate adequate size pools to fill open positions.
4. The organization is intentional about hiring so that the employee demographics represent the demographics of those served.
5. Recent hires receive new employee orientation.

## B. Employees are appropriately trained for the positions they hold.

1. Individual performance is appraised at least annually with the employee.
2. Each employee has an individualized professional development plan specific to them and their position.
3. Employees have access to on-going training through internal methods or by attending outside opportunities.

## C. Employees are appropriately compensated for their service.

1. The organization understands the market compensation for each position and has a compensation philosophy or standard that considers market.
2. Compensation for each position is determined at an appropriate level that considers other similar positions within the organization.
3. The organization does not have a bonus component to its compensation plan.
4. Employees are eligible for an annual merit based compensation adjustment.
5. The organization provides adequate benefits to employees, based on internal satisfaction and/or external comparabilities.

## D. Employees are engaged in the work of the organization.

1. Employee engagement is assessed at least every three years via survey or other means.
2. Annual employee turnover is less than 10% annually.
3. The Executive Director position has not turned over in the past two years.
4. Program Managers for the two largest programs have been in their positions for at least one full year.
5. Each employee receives a copy of the employee handbook or employee policies and procedures.
5. A short-term vacancy backfill plan is in place for the Executive Director and all key senior management positions.
6. A succession management plan exists and is updated for key positions in the organization.

# AREA V: INTERNAL CONTROL

**Internal controls are the backbone of the financial reporting system of an organization. Without appropriate internal controls the risk of fraud and inaccurate financial reporting and decision-making is significant.**

## A. The organization has created a control environment that emphasizes ethics and values.

1. There is a code of conduct or anti-fraud policy that clearly articulates expected ethical conduct of business for the organization.
2. The conflict of interest policy includes employees and requires annual certifications.
3. The approval/authorization maximum threshholds are clearly established for the various levels of management throughout the organization.
4. Integrity and ethical values addressed in the annual employee performance reviews.
5. There is clear procedure on who employees should report suspected instances of fraud.

## B. The organization has a formal risk assessment process and follows it.

1. The budget and other financial objectives are clearly presented to all employees within the organization.
2. Periodic reporting regarding budget status and the attainment of financial objectives are reported out to employees of the organization.
3. A formal risk analysis process is conducted by the organization at least every three years.
4. Fraud and other risks identified in the formal risk assessment process are mapped to changes and modifications in policies and procedures.
5. The risk assessment and management's mitigation plans are reviewed and discussed with the Board of Directors.

## C. Accurate and timely information is communicated to right people

1. Internal financial information is accurate and error free.
2. Appropriate checks and balances are in place so that at least two people see and approve each transaction (Segregation of Duties).
3. Executive management receives financial information in a timely manner (information is received in a timeframe that allows action to be taken).
4. The Board of Directors receives the correct level of financial information in a timely manner and approves it.
5. Reporting of financial and other information to funding sources is timely and accurate.

## D. The organization conducts monitoring of its policies, procedures and information.

1. The organization conducts internal reviews to ensure that its policies and procedures are properly being followed.
2. Policies and procedures are routinely reviewed and updated to ensure compliance with regulations.
3. The single audit, management letter and external monitoring reports are reviewed and findings are corrected in a timely manner.

## E. The proper control activities are deployed to create sound internal controls.

1. Journal entries are approved by someone other than the creator before being entered in the general ledger.
2. Effective controls are in place so that 'ghost' employees would not be able to be paid (i.e. someone adds/deletes employees and someone else pays employees).
3. Controls are in place to ensure that only goods or services received are paid for (i.e. invoices are approved for payment by someone outside finance).
4. Fictitious vendors are not able to receive payment, as vendors are put on the system by someone other than those authorized to pay vendors.
5. Checks over a certain amount require second signatures.
6. Bank reconcilations are reviewed and approved by someone not authorized to sign checks.

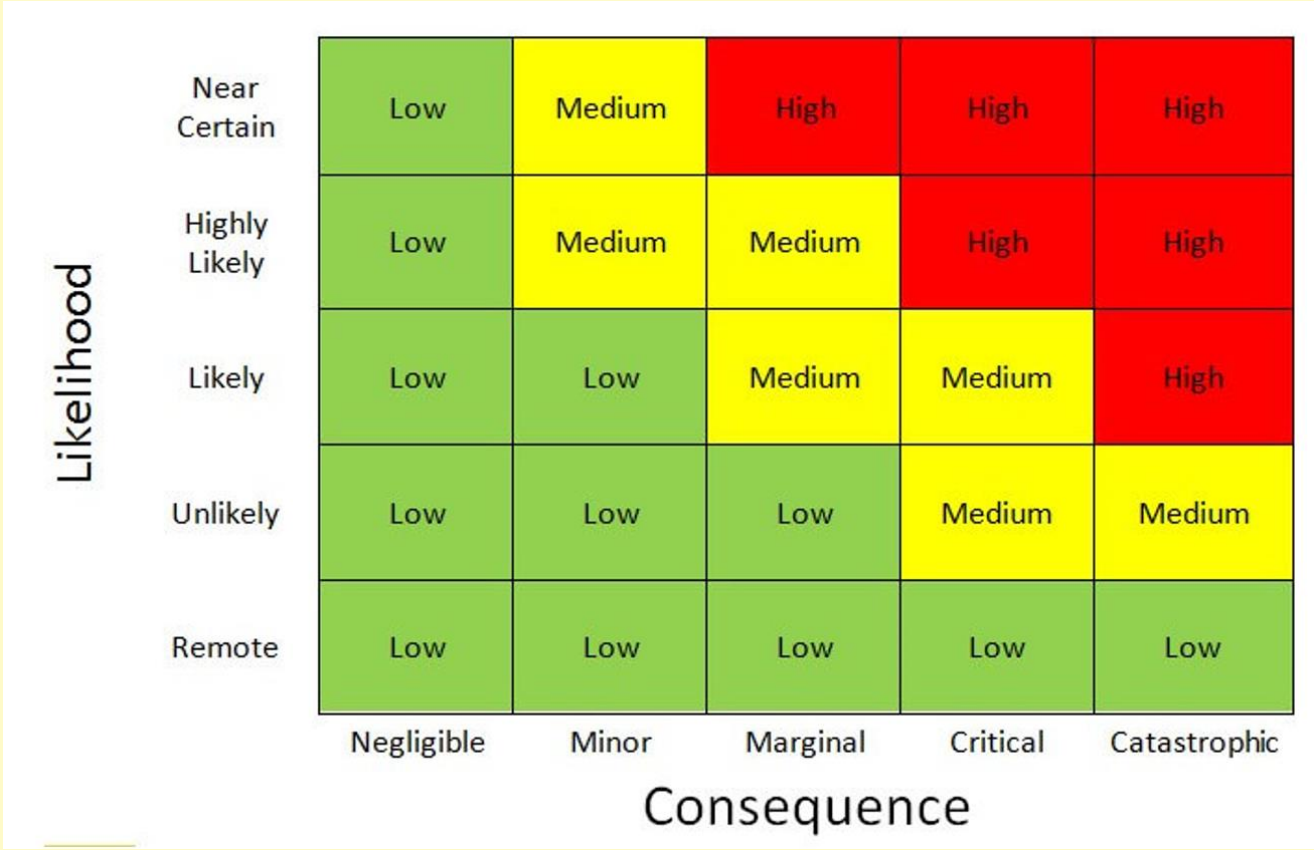
## F. Information technology has prudent controls in place.

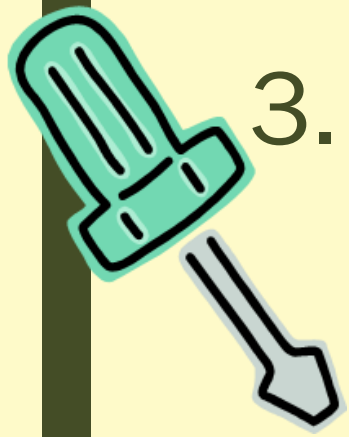
1. A disaster recovery plan has been created and tested.
2. Employees have been trained and reminded about on-going scams, such as phishing and other tactics.
3. Password integrity protocols are employed by the organization, such as required periodic changes, strong password elements and password education.
4. Anti-virus/anti-malware software is used and updated at the systems level.
5. Clear protocols are in place and understood by employees on protecting the privacy of client data and information.

# 2. Assess Impact

## Likelihood & Severity

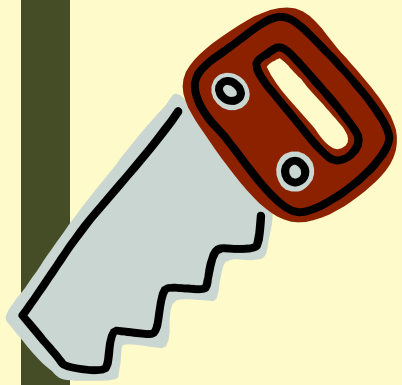
- How likely is the event to occur?
  - *Near certain*
  - *Highly likely*
  - *Likely*
  - *Unlikely*
  - *Remote*
- If event does occur, how severe would the impact be?
  - *Catastrophic*
  - *Critical*
  - *Marginal*
  - *Minor*
  - *Negligible*

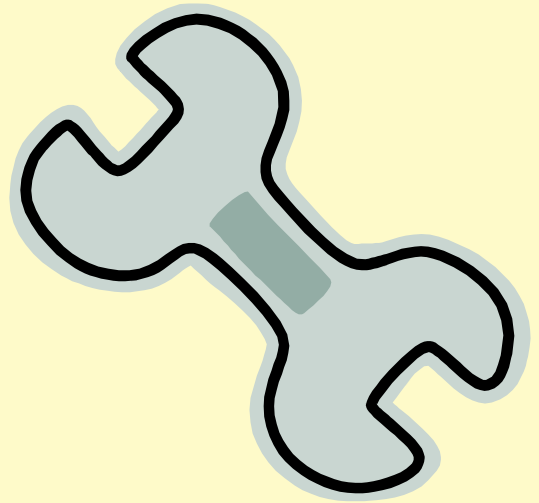




# 3. Examine Options

1. Avoidance
   - Exit the activity giving rise to the risk.
2. Reduction
   - Taking action to reduce exposure.
3. Modification
   - Taking alternative actions with less risk.
4. Sharing/Insuring
   - Transferring a portion or the risk (risk financing).
5. Acceptance
   - Agreeing to the risk (and the potential reward).





# 4. Implement Solution

- Select the ‘best’ risk management tool for each identified risk
- Consider Risk-Cost Analysis (ROI)
- Communicate
  - *Staff & Board*
- Things will go wrong
  - *Not always what we plan for*
  - *Black Swan events (e.g. COVID-19)*
- Develop contingency and recovery plans

# 5. Monitor Results

- Revisit risk assessment every X years
- Keep risk “fresh” in people’s minds
- “Practice” emergency management
  - *Table-top exercises*

# Enterprise Risk Management (ERM)

- 5 Elements of the Framework **plus:**
  - *ERM Objective Setting*
    - High level discussion of an organization's tolerance and appetite for risk
  - *ERM Event Identification*
    - Systemic evaluation of the types of risk events (internal and external)
    - Recognition that risk events are interdependent, not isolated events
  - *ERM Risk Response*
    - Evaluating using a "portfolio" view
    - Evaluate response opportunities
    - Consider risk and reward

# Cyber Risk

- $1.5 Trillion a year in losses
- If cyber-crime were a country, it would have the 13th highest GDP in the world!!!
- Employees account for 43% of data loss – whether intentional or accidental

# Mitigating Cyber Risk

- Three Pillars
  - *Business Continuity*
  - *Disaster Recovery*
  - *Incident Responses*
- KEY = Backup Strategies
- Cyber Insurance

# Risk Tolerance

- How much is too much?
  - *No one right answer to this, depends on:*
    - Your comfort
    - Your organization's financial position
    - Your Board's guidance
    - Your funders' perspectives
    - Your employees' skillsets
- Generally, NPOs are more risk adverse than for profit ventures
- Scaling risk tolerance
  - *Fully insured*
  - *Self-insured*
  - *Co-insured (risk sharing)*
  - *Uninsured ("going bare")*

# Is Risk Ever *Good?*

- Investments
  - *Higher risk may equal higher returns*
- Business opportunities
  - *Competitors are not willing to do*
- Non-profit missions
  - *The business return is not adequate, so NPOs can do*

# The End

EVALUATION QR CODE