HARVARD
Financial Administration
RISK MANAGEMENT AND AUDIT SERVICES

# Conducting a Risk Assessment

A risk assessment can be a valuable tool to help your unit identify, evaluate and prioritize its risks in order to improve decision-making and resource allocation. Harvard's Institutional Risk Management (IRM) program recommends the following process for conducting risk assessments. We are here to consult with and assist in the development and facilitation of risk assessments for all Harvard groups. To learn more or request assistance, please contact Nick Hambridge at nick_hambridge@harvard.edu or (617) 496-8980.

## Step 1: Risk Identification Workshop (1 – 1.5 hours)

An interactive workshop in which participants brainstorm the risks that could impact their unit's ability to meet its objectives. Participants are asked to first brainstorm on their own and write down risks on Post-it Sticky Notes; then categorize each of the risks as academic, compliance, financial, operational, reputational or strategic by posting them on flipcharts situated throughout the room. Small groups are then formed to further consolidate the risks within each category by thematic areas. Finally, each group provides a quick report-out on their thematic groupings of risks. These thematic groupings become the first draft of the unit's risk inventory.




## Step 2: Refinement of risk inventory and development of risk statements (1 – 3 hours)

One or more individuals review, refine and finalize the risk inventory that was developed during the risk identification workshop. Then for each risk, a clear and concise risk statement should be written to help your team better understand, assess and manage the risk. At Harvard, we use the "if / then" format for risk statements: If [event] occurs, then [negative consequences] may result. The IRM Program keeps a master list of risk statements which you can utilize to develop your risk statements.

*Example risk statement for 'Research Integrity'*

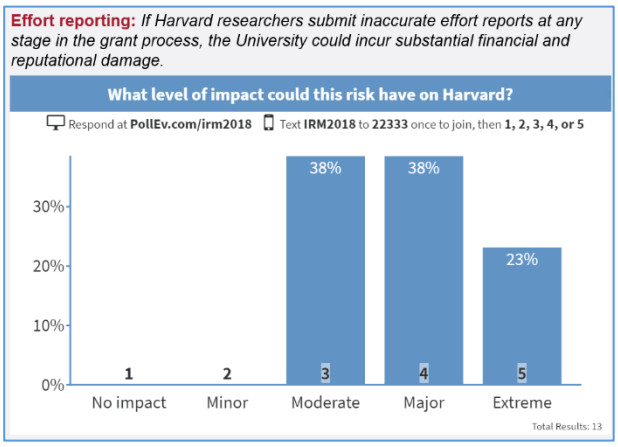
*If research is falsified, plagiarized, fabricated, or seriously deviates from commonly accepted practices, then failure to achieve Harvard's mission, reputational harm and financial losses may result.*

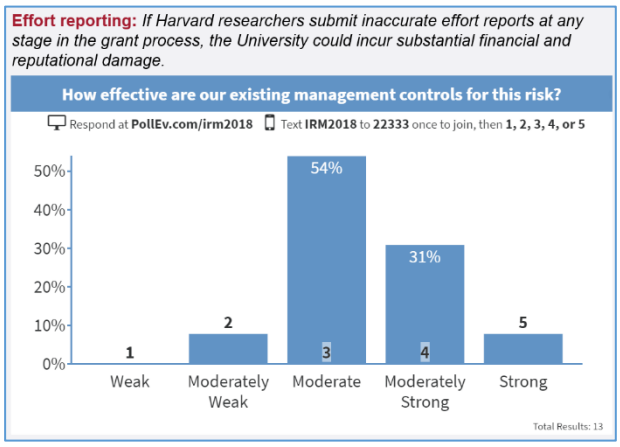
## Step 3: Risk Scoring Exercise (1 – 1.5 hours)

An interactive exercise (done as a group or individually) where participants score each risk based on predetermined risk scoring criteria. The IRM program recommends scoring each risk on a 1 to 5 scale (1 being lowest, 5 being highest) using the following criteria (see attachment for a recommended risk criteria scoring rubric):

- Impact were the risk to occur
- Likelihood of the risk occurring
- Effectiveness of our ability to manage the risk

If the exercise is done as a group, participants use their smartphones and the PollEverywhere technology to score each risk in real-time. Aggregated results are instantly available for the group to see and discuss. If done individually, each participant is emailed a link to a Qualtrics survey where the risks can be scored and compiled at a later time.



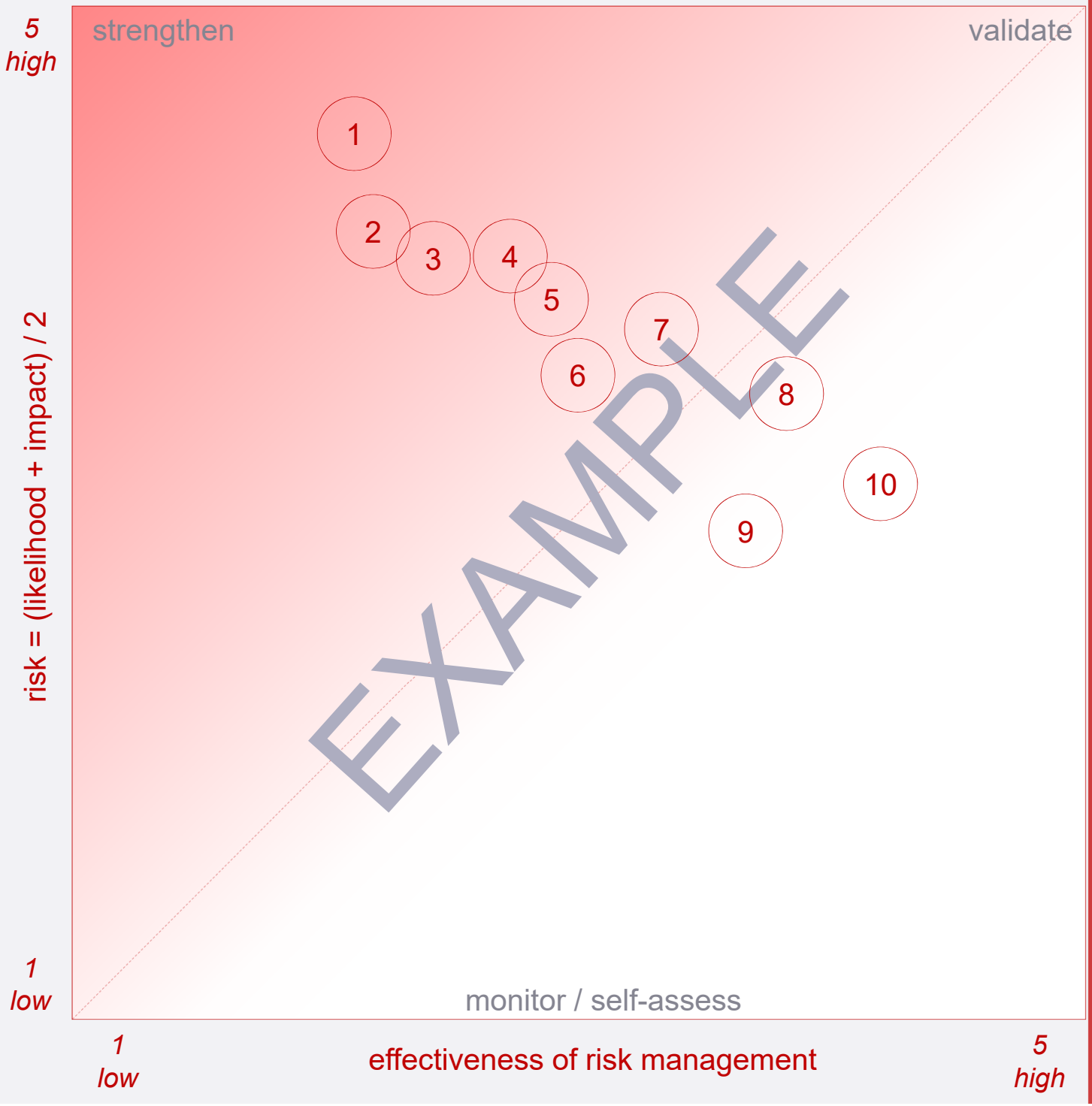




## Step 4: Risk Heat Map (0.5 – 1 hours)

Using the data from the risk scoring exercise, a risk heat map (scatterplot graph) is produced with each risk's inherent risk level (average 'impact' and 'likelihood' scores) on the y-axis and its average 'effectiveness of management controls' score on the x-axis (see attached sample heat map). An IRM program staff member will be happy to create the heat map for you. The heat map will help your team determine where it would be most beneficial to focus your time and attention on risk mitigation (i.e., risks in upper left area of the heat map with high inherent risk and low management controls scores).

# Risk Assessment Criteria

| | Low | | Medium | High | |
|---|---|---|---|---|---|
| ***IMPACT*** | **(1) No impact** | **(2) Minor** | **(3) Moderate** | **(4) Major** | **(5) Extreme** |
| **Human Impact** **The possibility of injury, illness, or death to University community members, visitors, or guests** | No injuries | Injuries are minor and treatable with first aid | Injuries are treatable with out-patient medical care | Injuries/Illnesses are treatable with limited in-patient care; injuries are not permanent | Injuries require extended in-patient care; injuries (including mental anguish) are permanent and could lead to death |
| **Asset Impact** **Physical and/or financial losses and damages to campus facilities, infrastructure, reputation, and/or balance sheet** | No loss | Minimal damage or loss | Significant isolated damage or loss to buildings facilities, and/or other assets, including reputational damage | Major or recurring damage or loss to buildings, infrastructure, and/or other assets including regulatory noncompliance, litigation and reputational damage | Widespread, critical financial loss and/or damage to buildings, infrastructure, and/or other assets, including disaster, regulatory noncompliance, litigation and reputational damage |
| **Mission Impact** **The disruption of and/or adverse impact of University operations, including the essential mission of research and teaching** | No disruption | Minimal disruption or adverse impact to operations | Significant disruption or adverse impact, but manageable with a moderate level of resources | Faculty, students, staff temporarily unable to carry out operations | Critical damage to campus and/or loss of other essential facilities or people requiring temporary or permanent suspension of normal daily operations |
| ***LIKELIHOOD*** | **(1) Rare** | **(2) Unlikely** | **(3) Moderate** | **(4) Likely** | **(5) Almost certain** |
| **Odds of occurrence** | ~ every 10 years | ~ every 5 years | ~ yearly | ~ quarterly | ~ monthly |
| ***EFFECTIVENESS OF MANAGEMENT EFFORTS*** | **(1) Not at all effective** | **(2) Slightly effective** | **(3) Moderately effective** | **(4) Very effective** | **(5) Extremely effective** |
| | None of the risk is being managed | Very little of the risk is being managed to an acceptable level | Some of the risk is managed to an acceptable level | Most risk is managed to an acceptable level | Best Practice |




## risk heat map example

1. **Information Security**
2. **Funding Uncertainty**
3. **International Programs**
4. **Safety & Security**
5. **Research Compliance**
6. **Employee & Manager Skills**
7. **Diversity & Inclusion**
8. **Student Behavior & Wellbeing**
9. **Facilities Adequacy**
10. **Business Continuity**

*The risk assessment process is designed to identify and assess a wide variety of potential areas of operational and other risks upon which University officials may wish to focus management attention. The identification of a matter for consideration does not imply that the University or any individual has failed to take appropriate action, or that the matter warrants action by any University official.*