Updated 8/2018

# Risk Assessment

Risk is inherent in life. While inevitable, not all risks are necessary, and, not all risks have the same potential for harm or the same likeliness of occurrence.

Not all risk is bad. Through calculated risks and developed safety nets, we challenge ourselves, practice our training, and stretch our capacities – we grow.

Organizations are responsible for creating safe, nurturing spaces for program participants, volunteers, and employees. They must mitigate catastrophic risks and balance competing risks, while having programing that allows participants to grow and employees and volunteers to do their job and achieve program goals.

Risk assessments assist organizations in identifying risks and potential threats in order to nullify and mitigate potential harm. While all risk will never be eliminated, forethought, planning, education, and awareness are "Controls" which will create safer environments and allow organizations and people to react quickly to contain active threats and disable harmful situations. By identifying specific risks, organizations can implement relevant controls to address these risks. "Forewarned is forearmed."

There are many ways to analyze and visualize risk. Start with a basic assessment of risk to prepare for threats and manage risk.

The Part 1 presents terminology and ways to visualize risks and threats. Part 2 contains two basic worksheets which suggest likely threats and provide space to rate them in terms of probability and impact. Use these worksheets as a guide to draft a Security Plan and Child Protection Safeguarding Policy in Part 3.

- What Threats are there to my organization, people and assets? (Part 2)
- What Vulnerabilities can be exploited by these Threats? (Part 2)
- What Controls can be implemented to mitigate these Threats? (Part 3)

## Part 1: Background on Risk

### Terminology & Visuals

Asset – Tangible and intangible things such as people, property, and information that have value to the organization.
*Ex- staff, participants, buildings, computers, information, equipment*

Vulnerability – Weakness or flaws in a system that can be exploited by a threat. Critical vulnerabilities are flaws with already devised methods of exploitation. For instance, known security holes in a financial software package for which an easily available virus exists to exploit this known flaw.
*Ex- location, unlocked doors, out-of-date anti-virus software, hazardous materials, poverty, poor governance*

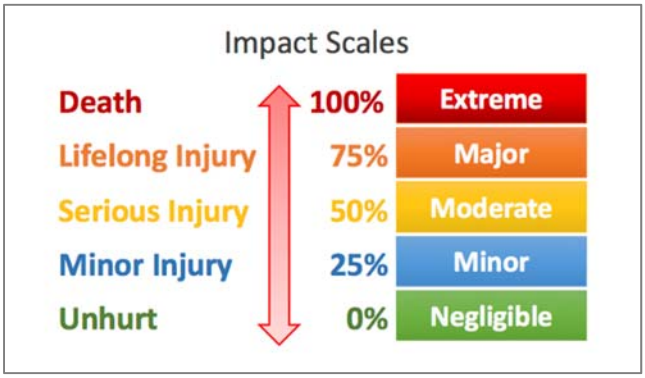
Threat – Anything that can exploit a vulnerability, intentionally or accidentally, and obtain, damage, or destroy an asset. Potential harm that can come to a system. A threat can be intentional or unintentional, internal or external.

Hazards are the dormant object which have the potential to be a threat.

*Ex– natural disasters, cybercrime, disease, computer viruses, accidents, incompetence*

Impact – The effect of the threat on the asset.
*Impact can be assessed in a variety of ways. Some of the most common methods use numeric scale, assign percentages for computation, or use a basic color coding scale.*

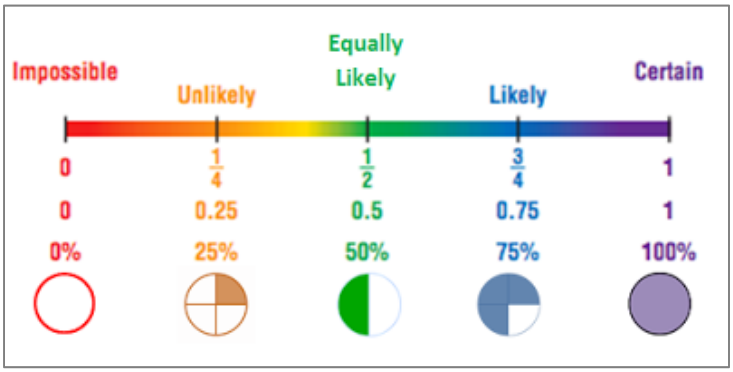
**Visual #1: Impact Scale Example**



Probability – The likelihood that a threat will occur. The probability of threat is based on the exposure length, amount, and frequency. Something generally innocuous could be dangerous if the exposure is abnormally high.

*Probability can be assessed in a variety of ways. Some of the most common methods use numeric scale, assign percentages for computation, or use a basic color coding scale.*

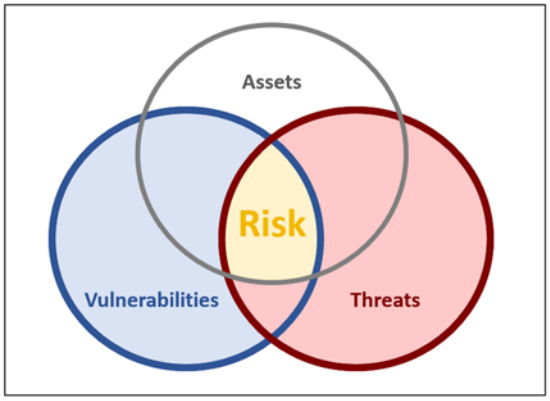
**Visual #2: Probability Scale Example**




http://samanthamaths8x.blogspot.com/2015/11/probability.html

Risk – an assessment which factors in the impact and probability of a threat exploiting a vulnerability of an asset. Some people look at it as a combination of threats, vulnerabilities, and assets (Risk = Threats + Vulnerabilities + Assets) where if you are missing one of those components you nullify your risk. Risk is the intersection of assets, vulnerabilities and threats.

**Visual #3: Risk = Vulnerability + Threat + Asset**




Other experts use the mathematical equation Risk = Threat x Vulnerability x Consequence/Impact. The idea being that if the impact or consequence is likely to be nothing or close to nothing, then the risk will be rendered almost nothing and can be disregarded.

The reality is that it's more conceptual than a true formula. To understand the risk to an asset requires judgment and subjectivity. It is helpful to create a basic metrics to help standardize analysis, though. Therefore, CPT recommends creating a rating system for impact and probability to apply to threats on an asset(s) based on current vulnerabilities using the Impact x Probability Chart or Formula model.

**Visual #4: Probability x Impact Chart**

| | Negligible | Minor | Moderate | Major | Extreme |
|---|---|---|---|---|---|
| Rare | Low | Low | Low | Medium | Medium |
| Unlikely | Low | Low | Medium | Medium | Medium |
| Equally Likely | Low | Medium | Medium | Medium | High |
| Likely | Medium | Medium | Medium | High | High |
| Certain | Medium | Medium | High | High | High |

*For this chart, impact is measured on the x axis and probability on the y. Using both probability and impact, the chart shows the level of risk associated with threats. Organizations should address those threats that present high and medium risk. It is possible to create a more detailed risk scale between "Low" and "High" to distinguish better between risk.*

**Visual #5: Probability x Impact Formula**

| | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 0 | 0*0=0 | 1*0=0 | 2*0=0 | 3*0=0 | 4*0=0 | 5*0=0 |
| 1 | 0*1=0 | 1*1=1 | 2*1=2 | 3*1=3 | 4*1=4 | 5*1=5 |
| 2 | 0*2=0 | 1*2=2 | 2*2=4 | 3*2=6 | 4*2=8 | 5*2=10 |
| 3 | 0*3=0 | 1*3=3 | 2*3=6 | 3*3=9 | 4*3=12 | 5*3=15 |
| 4 | 0*4=0 | 1*4=4 | 2*4=8 | 3*4=12 | 4*4=16 | 5*4=20 |
| 5 | 0*5=0 | 1*5=5 | 2*5=10 | 3*5=15 | 4*5=20 | 5*5=25 |

*Similar to the Probability x Impact Chart above, this formula rates those with higher numerical values as higher risk. The color coding helps to reinforce that. While it does not completely mirror the Probability x Impact Chart, it shows similar rankings and risk.*

Controls – A practice, policy, procedure, method, or device which is employed to mitigate or nullify risk.

*Ex- Fire lock box, fence with locked gate, protective policies, training, first aid kit*

Child "Protection" Safeguarding Policy – Often known as child protection policies within the United States, child safeguarding policies are policies for protecting children from risks and procedures for how to handle an incident if a child is put at risk or harmed.

Emergency or Security Plan – A policy which outlines the procedures and protocol for dealing with an emergency or security threat. The plan should address what steps to take and when to take them for incidents such as political unrest, natural disaster, missing person, car accident, medical emergency, etc. It provides well thought out plans and benchmarks for action when employees or volunteers might not be able to think clearly. The plan may include safeguards for mitigating harm, such as registering with an embassy when outside of the home country and carrying travel insurance.

## Part 2: Risk

There are many ways to mitigate and address risks. For organizations that work with children, it is important to have a Child Protection Safeguarding Policy and an Emergency or Security Plan. The Emergency/Security Plan is more general than the Child Protection Safeguarding Policy which is specific to children and interpersonal abuse.

Emergency/Security Plans provide a protocol for actions to be taken in the case of situations or alerts such as large scale as a natural disasters, political unrest, or epidemics or as small scale as a death or medical evacuation. Most emergencies happen quickly and allow little or no time for planning. Emotions can be running high, communication may be impaired, and information might be scarce. Having a well-thought-out plan in place, while it may not be perfect, will create the best chance of positive outcomes for everyone involved.

Therefore, the two worksheets below will be focused in terms of threats on those two issues. If your organization has other needs, this can help you think about them as well, however, you may need to create a different worksheet specific to those needs for writing those policies in order for threats to be broken down into smaller more specific issues to be addressed by the specific person or department where the threats are relevant. [*Ex- financial and technology risks*]

Additionally, it is important to remember that, even within your organization, not all threats pose the same risk to:

- populations
- locations
- programming areas

You will need to consider each threat in terms of the various groups that will be impacted as well as evaluating the impact and probability of each threat when giving a rating.

Table 1 in the appendix contains a chart listing examples of Assets, Vulnerabilities, Threat Actors, and Threats. Please remember that these lists are not exhaustive.

**Child Protection Safeguarding**
This is for looking at specific threats to children which cause harm and prevent them from thriving. This looks at everyday situations.

Please see Worksheet 1: Child Safety Risk Assessment in the Appendix for additional assistance evaluating these risks.

**Security or Emergency**
This examines emergencies and security concerns which may arise and threaten your organization and its assets – adults, children, finances, property, & information.

Please see Worksheet21: Security & Emergency Risk Assessment in the Appendix for additional assistance evaluating these risks.

## Part 3: Creating Controls

Controls address risk by reducing the impact of a negative outcome. Impact is reduced through 4 strategies:

- Avoidance: eliminate cause of risk -- the vulnerability, asset, or threat
- Mitigation: reduce risk probability and impact (ex- safety gear, restricted access, training)
- Acceptance: contingency plan for risks which include:
    - preparedness (ex- first aid kits, emergency funds, practice drills, training)
    - prediction & warning systems (ex- State Department SMART Traveler registration, natural disaster warning system)
    - protocols (ex- emergency or security plan, child protection safeguarding policy, financial or information protection policy)
- Transference: have a third party take on the responsibility for risk (ex- contract, outsource, insurance)

Table 2 in the Appendix offers examples of possible controls. Please remember that the lists are not exhaustive.

When creating a protocol, run the most likely scenarios to test the robustness and usefulness of the plan. Create a plan to handle communication, decision-making, safety, and loss that can be adapted to whatever emergency arises. Provisions specific to a risk can be included but as an addendum to a strong basic protocol or policy.

Multiple threats acting simultaneously or in rapid succession can create more impact or risk than one occurring in isolation. Similarly, one threat may cause a new vulnerability and a cascading chain of events.

> *Ex.- Election violence may lead to property damage due to increased lawlessness from civil strife and reduced ability of government of government services such as police. Resulting property damage or riots causes banks to close, medical access to limited or obstructed, and supplies to be limited or unavailable. Now low threat disease and medical conditions become medium or high risks.*

## Appendix

1) Table 1: Assets, Vulnerabilities, Threats, and Risks
   These are examples, not an exhaustive list.
2) Worksheet 1: Child Safety Risk Assessment
3) Worksheet 2: Security & Emergency Risk Assessment
4) Table 2: Controls
   These are examples, not an exhaustive list.

**Table 1: Assets, Vulnerabilities, Threats, and Risk**

These are examples, not an exhaustive list.

| Assets | Vulnerabilities | Threats & Hazards | Risks |
|---|---|---|---|
| People | Poverty | Pedophiles/Sexual Abusers | Abuse: Physical, Sexual, Psychological & Neglect |
| Local Staff | Inequalities | Pornography | |
| International Staff | Economic | Physical Abusers & Bullies | Domestic Violence |
| Participants | Social (class, tribe, disabled, etc.) | Substance Abusers | Exploitation |
| Donors | Political | Mental Abusers | Transactional Sex |
| Volunteers | Gender | HumanTraffickers (labor, sex, organ) | Child Labor |
| Community Relations | Age | Gangs, Mafia, Hackers, & Thieves | Child Soldiers |
| Buildings | Religious | Militias & Armed Groups | Teen Pregnancy |
| Computers & Technology | Poor Governance | Drug & Weapons Dealers | Female Genital Mutilation/Cutting |
| Cell/Mobile Phones | Corruption | Natural Disasters | Harrassment & Discrimination |
| Animals | Lack of or Inconsistant Rule of Law | Flood | Addictions & Substance Abuse |
| Farm & Crops | Poor Construction (buildings, roads, etc.) | Hurricane/Monsoon | Behavioral Problems |
| Vehicles | Poor Infrastructure | Landslide | Psychological Problems |
| Equipment | Medical | Drought | Poor Health, Illness, & Disability |
| Cash | Transportation | Earthquake | Death, Drowning, Dismemberment |
| Personal Data & Information | Sanitation | Tsunami/Tidal Wave | Bribery, Corruption, & Fraud |
| | Communication | Volcanic Eruption | Financial Loss |
| | Open Water Sources | Environmental Hazards | Productivity Loss |
| | Malnutrition & Poor Health | Animals (domestic & wild) | Reputation Damaged |
| | Poor Education System | Poisonous Plants | Expulsion from the Country |
| | Poorly Trained Work Force | Bodies of Water | Homelessness |
| | Social Taboos | Holes/Uneven Ground | Joblessness |
| | Unreliable/Surging Electricity | Sewage | Missing Persons & Kidnapping |
| | Adults who were/are Abused | Hazardous Materials | |
| | Lack of Close Relationships | Gasoline & Oil | |
| | Separation from Parents | Toxic Chemicals | |
| | Foreigners/Outsiders | Medicine | |
| | Language Barriers | Matches | |
| | Handicaps & Learning Difficulties | Sharp Implements & Weapons | |
| | Open Access to Networks & Information | Disease, Infection, Epidemic | |
| | Unrestricted Access (data, children, cash, etc.) | Fire | |
| | Weak information security | Work Accident | |
| | Mono- crop agriculture or industry (org. & country) | Vehicle Accident | |

## Safety Threats for Child Safeguarding

*Threats to well-being and ability to thrive*

In order to write a child protection safeguarding policy, prevent incidents and injuries, and keep children safe, it is important to assess the risks. Not all threats carry the same impact or probability thus the risk varies. Use either the Probability x Impact Chart or Formula to score each threat or threat actor's risk of occurrence. Write in or circle specific threats beside the general ones listed.

Consider the immediate site location, as well as the general local or country infrastructure, and any locations that the organization might visit (field trips, transportation, etc.). Afterwards, go back through the risk scores and circle or highlight the highest risk scores and the most likely threat actors or hazards so that you address them first in creating controls or planning for them in the Safeguarding Policy.

| | **Risk Score** |
|---|---|
| Physical Abusers (staff, volunteers, community members, care-givers, sex-tourists, teachers, donors, children/peers, other: _____) | ____ |
| Pedophiles/Sexual Predators (staff, volunteers, community members, care-givers, sex-tourists, health care professionals, donors, children/peers, other: _____) | ____ |
| Pornography & Sexually Inappropriate Content (videos, internet, books, magazines, conversations, radio, other: _____) | ____ |
| Human Trafficking (labor, sex, organ, other: _____) | ____ |
| Harmful Ingestible Substances (substances: drugs, alcohol, medicine, glue/huffing, other: _____) | ____ |
| Mental abusers (other: _____) | ____ |
| Drug & Weapons Dealers (_____, _____, _____) | ____ |
| Gangs & Mafia (_____, _____, _____) | ____ |

## Safety Risks for Child Safeguarding

*Threats to well-being and ability to thrive*

| | Risk Score |
|---|---|
| Employers (_____, _____, _____) | ____ |
| Illness & Disease (infections, malaria, dengue fever, cold/flu, stomach problems, typhoid, river blindness, yellow fever, other: _____) | ____ |
| Animals (farm, wild, stray dogs, other: _____) | ____ |
| Health & Sanitation (contaminated water, stagnant water, open sewage, open trash/garbage, used hygiene products/needles, other: _____) | ____ |
| Hazardous Materials Storage (gasoline, oil, toxic substances, medicine, matches, weapons, other: _____) | ____ |
| Sharp & Dangerous Implements (machetes, knives, farm tools, guns, other: _____) | ____ |
| Environmental Hazards (trees – falling/climbing, holes, animals, poisonous plants, bodies of water, other: _____) | ____ |
| Other: _____ | ____ |
| Other: _____ | ____ |
| Other: _____ | ____ |
| Other: _____ | ____ |

## Safety Risks for Child Safeguarding

*Threats to well-being and ability to thrive*

The risks, which rated higher on your scale, need to be incorporated into your organization's child protection safeguarding policy. Think carefully about the situations in which these threats exist – off/on campus, special events, guest on campus, breaks, recess, travel from activities, bed-/bath-times, car rides, after-/before-program, etc.

When writing the policy, make sure to test the policy by running scenarios from the most likely cases. This will help you think of complexities which you might encounter and how to mitigate problems before they occur. Some questions to think about when writing and planning:

- ❑ **How can hazards be minimalized or corrected to reduce risk? What physical changes to the environment can we make to mitigate these risks?** Some examples may include: storing hazardous materials and sharp tools in secure areas, using safety gear, filling in holes, covering garbage, creating drainage for stagnant water, implementing sanitation practices, securing clean water, etc.
- ❑ **How is the program and organization structured to avoid risks?** Create rules & guidelines which will help structure the organization, programs, and activities to minimize risks. This may include focusing on supervision and trainings and having strong screening procedures for volunteers and employees. Trainings on child abuse, policies, safety with hazardous materials, and use of safety equipment can help avoid risks.
- ❑ **Does the child protection safeguarding policy provide a framework for handing a situation of these risks if it were to occur? Would staff know what to do if a situation occurred?** It is important to have a clear, transparent, standardized, and well-thought out plan for handling any situations or accusations which might occur. This does not necessarily mean having standardized penalties but rather a standardized process. Transparent policies and processes help build confidence in the organization's commitment to keep children safe. Remember: policies only work if the staff and children know and use them!

* 1 There are different risks to children's health, development, likelihood of abuse of substances, and likelihood of being assaulted or abused based on who is using the addictive or barred substances. For example, if children witness substance abuse by an adult, they are at greater risk of being physically or sexually abused or neglected as well as more likely to be substance abusers when they are adults and more likely to have various health problems. Children using but in groups with non-users mean that there is a higher risk of child on child abuse, especially sexual abuse.

2 There are different risks to children based on if they are witnessing a parent or sibling being abused vs. being the victim. Also, there is the question of risk that a staff member or volunteer is a perpetrator of domestic violence and how that may carry over to the children they work with at your organization. Please also see information about ACEs (Adverse Childhood Experiences) to understand more.

3 Parent and family are important for children's psychological health and ability to be resilient after trauma or adverse circumstances. Even when it is in the best interest of the child to be separated (ex- a parent is abusive), separation can cause a set of psychological traumas and problem. In general, parents and families are important protective systems for children.

4 If a child does not have a long-term stable caregiver with whom to develop a close relationship, a child can develop many psychological problems, from attachment disorders to addiction problems to depression and suicide. Often children will try to attach themselves to short-term volunteers and visitors quickly and without caution; this is both a warning sign and also a result of an attachment disorder.

# Security & Emergency Risk Assessment

*Threats to Safety*

Analyze the biggest hazards and threat actors to the security of to your organization. Below are examples to help you think about your organization and country situation. This list is not exhaustive. Not all threats carry the same impact or probability thus the risk varies. Similarly, not all threats will impact all groups within your organization the same.

Use either the Probability x Impact Chart or Formula to score each threat's risk of occurrence. Make sure you think about how it might be relevant to each group within your organization: participants, local staff, international staff, home office, donors, volunteers, etc. Circle or write-in beside each general threat, the specific ones that most threaten the safety and security of your organization. You may also want to note who within the organization will be most impacted. Afterwards, go back through the risk scores and circle or highlight the highest risk scores so that you address them first in creating controls or planning for them in the Security or Emergency Plan.

| | **Risk Score** |
|---|---|
| Epidemic (affecting) | |
| People: ebola, hemorrhagic fever, zika, cholera, HIV, malaria, dengue fever, typhoid, river blindness, yellow fever, STIs, other: _____ | ____ |
| Animals: rabies, avian flu, hoof & mouth, measles, other: _____ | ____ |
| Plant: blight, infestation, other: _____ | ____ |
| Gangs & Mafia (_____, _____, _____) | ____ |
| Human Trafficking (labor, sex, organ, other: _____) | ____ |
| Militias & Armed Groups (_____, _____, _____) | ____ |
| Drug & Weapons Dealers | ____ |
| Thieves & Hackers (pickpocketing, scams, hijacking, mugging, kidnapping, robbery, malware, computer virus, other: _____) | ____ |

# Security & Emergency Risk Assessment

*Threats to Safety*

| | Risk Score |
|---|---|
| Corruption (local & national governmental bodies and representatives, other: _____) | ____ |
| Civil Unrest (strikes, rioting, disputed elections, gang warfare, other: _____) | ____ |
| Economic Collapse (inflation, embargoes, funds transfers, bank runs, other: _____) | ____ |
| Natural Disaster (earthquake, drought, hurricane, tsunami, flood, tornado, volcanic eruption, mud slide, other: _____) | ____ |
| Environmental Hazards (water, holes, poisonous plants, other: _____) | ____ |
| Wild Animals ( _____, _____, _____ ) | ____ |
| Sharp Implements & Weapons (machetes, saws, hoes, blades, knives, guns, other: _____) | ____ |
| Hazardous Materials (gas/petrol, oil, kerosene/paraffin, chemicals, medicines, matches, other: _____) | ____ |
| Fire (wild fire, cooking, electrical, controlled burn, garbage, other: _____) | ____ |
| Other: _____ | ____ |
| Other: _____ | ____ |
| Other: _____ | ____ |
| Other: _____ | ____ |

# Security & Emergency Risk Assessment

*Threats to Safety*

You need to come up with a security protocol for what to do when an emergency happens. The risk scores should help you prioritize what your organization's biggest risks are and should be balanced by thinking about the impact each has. You cannot, nor would you want to, have a very specific security plan for EVERY possible situation. You want a basic plan with contact tree and decision-making assistance to guide you. Run a few scenarios to test your protocol and practice thinking about how to handle and emergency situation. Think about how it impacts children, staff (local & foreign), community, the organization's mission, and volunteers. Some recommended scenarios for testing and planning:

- Car accident (highly likely and potential for high impact to organization if there is a death or major injury)
- Death of a volunteer, staff member, or child during an organization program
- Natural disaster or Civil unrest
- Highest rated threat (risk and impact) from worksheet above

Here are some questions to ask when creating an emergency/security protocol:

❑ **Do you have up-to-date emergency numbers easily available?** (embassies –almost always a first call for help, hospitals, partners, allies/similar groups in the area, etc.) Who are your natural allies and partners that could work with you during an emergency?

❑ **Who should those on-site call – point of contact (POC)? When should they call? What is the reporting chain?** Your organization does not want too many people giving directions, asking questions, distracting, etc. Make a streamlined process of decision- making and disseminating information. Designate one POC at the site of the incident and one POC at headquarters or the main. You want to have a trigger or level of severity for a staff member to know to activate emergency protocol.

❑ **How are you keeping people, especially children, safe?** This includes both those not directly involved and possibly sick or injured, as well as those who were not involved. Who is immediately at risk and who will be at secondary risk? Do you have an assembly point or check in method?

❑ **Do you have an enough cash on hand or resources in reserve in the case of an emergency?** Extra cash, food, gasoline, and medical supplies should be stockpiled before an election or predicted weather event in case of the banking or physical infrastructure suffers disruption. What sort of emergency kits should you have and where should they be located? Build kits to match the most likely threat situations and the particular context for your organization (ex- food, light, medical kit, power supply/fuel, communication, water filter, multi-tool, etc.)

## Security & Emergency Risk Assessment

*Threats to Safety*

- ❑ **What situations might this one initial incident trigger**? (ex. Natural disaster could shut down banks or cause civil unrest, etc.)

- ❑ **What is your plan for handling the press, public, and donors?** Your organization needs to be open and transparent while also cautious about sharing too much information too soon. It is important to consider how the information shared might affect an on-going situation, both positively and negatively. Create a decision hierarchy and locate possible public relations resources ahead of time to assist when you have a specific incident.

- ❑ **How will the emergency protocol be practiced and remembered so that when an emergency happens, people know what to do, where to go, or how to find the protocol?** A protocol is only useful if it is available and can be followed!

**Table 2: Controls** These are examples, not an exhaustive list.

| CONTROLS | | | |
|---|---|---|---|
| **Avoidance** | **Mitigation** | **Acceptance** | **Transference** |
| Review & Remove Physical Hazards (holes, weapons, etc.) | Good Nutrition | **Preparedness** | Contractors & Services |
| | Vaccinations & Prophylaxis Medications | First Aid Kits | 3rd Party Payment System |
| Centralize, Burn, Cover, &/or Remove Garbage | WASH: Water, Sanitation, & Health | Stockpile Supplies (nonperishable food, medicine, emergency kits, etc.) | Accounting Services |
| | Hand Washing Stations | | External Auditors |
| End High-Risk Programming | Drilled & Covered Wells | Training & drills for Disasters & Emergencies (CPR, swimming lessons, assembly points, training on protocols, etc.) | (financial, safety, etc.) |
| Change Locations | Good Health & Hygene Practices | | Employee & Volunteer |
| Filter &/or Treat Water | Pest Control (rats, mice, etc.) | | Vetting Service |
| Drain Stagnant Water | Safe Food Storage (covered, refrigerated) | Redudnant Communication Systems | Cloud Storage |
| Repair Facilities | Proper Ventilation | | Data Security & IT |
| Maintain Equipment | Safety Gear & Work Equipment | **Prediction & Warning Systems** | Insurance |
| | Education and Training | Alarm or PA System | Programming by Gov't |
| | Strong, Long-term, Caregiver Relationships | US State Dept. SMART Traveler | Programming by Other Organizations |
| | Birth Registration | Embassy Registration | |
| | Good Community & Gov't Relations | Regional Early Warning System | |
| | Monitoring & Supervision | | |
| | Personnel Assigned with Oversight | **Protocols** | |
| | Scheduled Reviews of Protocols | Child Protection Safeguarding Policy | |
| | Physical & digital Information Backup | Emergency and/or Security Plan | |
| | Criminal Background Screenings | Whistleblower Policy | |
| | Reporting Chains & Systems | Information Protection Procedures | |
| | Fire Boxes for Critical Document Storage | Code of Conduct | |
| | Restricted Access | | |
| | Location (fence, locked doors, security, sign-in/out, etc. | | |
| | Information (passwords, encyption, locked cabinets, "Need to Know," etc.) | | |
| | Materials (equip., vehicles, etc.) | | |

## Sources

Langham, Gary. “Threat vs Risk.” IMSL. 20 Feb 2013. http://intelmsl.com/insights/other/threat-vs-risk/.

Lowder, Jeff. BlogInfoSec.com. https://www.bloginfosec.com/2010/08/23/why-the-risk-threats-x-vulnerabilities-x-impact-formula-is-mathematical-nonsense/.

Nonprofit Risk Management Center. https://www.nonprofitrisk.org/

Samantha Maths 8X Blog. http://samanthamaths8x.blogspot.com/2015/11/probability.html.

Threat Analysis Group. https://www.threatanalysis.com/2010/05/03/threat-vulnerability-risk-commonly-mixed-up-terms/.

Wikipedia. “Risk Management.” https://en.wikipedia.org/wiki/Risk_management