RoadMap
Strengthening Organizations. Advancing Social Justice.

(1/5/17 rev)

A Guide to Getting and Keeping Your House in Order

This is the starting point for implementing the practices necessary to protect your organization against opposition attacks. RoadMap has prepared this checklist to help you assess your organizational vulnerabilities as a whole, and to help you identify the concrete practices and systems you will need to have in place to ensure that your organization is prepared.

This checklist covers preparation for the two types of attacks that occur: *known risks or attacks* that take advantage of noncompliance issues, and *fabricated risks or attacks* that directly threaten the reputation of the organization and/or the safety of its staff and constituents regardless of compliance issues.

We recommend that you identify one staff person as the primary "holder" of this checklist and that at least once a year and/or when there is turn over in key positions you conduct internal reviews based on this checklist.

By discussing and sharing this check list and other security protocols with your team you can identify "weaknesses" and gaps, lift up worrisome or suspicious activities that may be taking place that you are unaware of, build confidence among your staff that everything is in order, and ensure that ongoing training is taking place. Creating frequent opportunities to increase organization-wide awareness and build reassurance will go a long way towards minimizing any risks your organization may face.

1. Governance Practices

		Risks to Watch For	Status at My Organization
Board Meetings and Minutes	Regular, well-attended board meetings are conducted. Minutes document decisions and demonstrate active oversight by the board. Minutes are up-to-date, on file. Minutes are distributed to all board members in a packet before the next board meeting and minutes are approved during the board meeting.	Lack of board minutes comes up in audits or legal challenges. Minutes reflect whether or not you have an engaged board, which can be the first flag someone might look for. Minutes are also important when the board itself has disputes over actions.	

		Risks to Watch For	Status at My Organization
Articles of Incorporation & By-Laws	Organization has articles of incorporation & bylaws and any amendments on file. Bylaws clearly state mission of the organization including nonpartisan civic engagement work and speak to term limits. Board members are familiar with and have copies of articles of incorporation and bylaws.	Overly complex bylaws can lead to problems or confusion in following proper process. Out-of-date or not following bylaws indicate lack of compliance	
Board Members	Organization can demonstrate that board members and officers are elected in accordance with the bylaws.	Board members need training in their roles and responsibilities.	
Whistleblower, Conflict of Interest & Confidentiality Policies	Board has adopted these policies as encouraged by the IRS.		
Document Retention and Destruction	Organization has a policy in place that includes language requiring suspension of destruction in the event of legal disputes or investigations. Staff understands and follows regular filing practices; files and folder names on servers are clear. A senior staff person can answer questions and staff should do regular cleanups. Computer backups are regular and are held offsite, email records are deleted after a set period of time. Sensitive files are locked.	During legal disputes it is crucial to manage document searches properly and not destroy records. Email and electronic records are a major weakness in many organizations. (See Litigation Hold Policy below)	
Litigation Hold Policy	Circumstances may arise where normal and routine destruction of records must be suspended in order to comply with Federal & State legal requirements as well as present future records that are involved in litigation or reasonably anticipated in foreseeable legal action.		

		Risks to Watch For	Status at My Organization
Annual Report to Membership	If organization is a membership corporation, it meets state requirements regarding reporting and rights of members. This usually means an annual meeting where members elect board members.	Often groups do not have defined membership lists or they are out of date.	
Personnel Policies	Board has approved personnel policies including procedures to assure nondiscrimination in hiring and termination decisions and in all other terms and conditions of employment and compliance with all other applicable laws, such as those concerning wage and hours and required leave.	Board members often have little orientation prior to personnel conflicts and need immediate support to understand their role and time to brush up on policies.	

2. Business Practices and Accounting Systems

		Risks to Watch For	Status at My Organization
Accounting System	Meets GAAP (Generally Accepted Accounting Principles) requirements (for larger organizations). Have an external CPA or qualified financial advisor review systems not just to meet audit standards but to ensure timely reporting/filing of financial documents.	Many groups only do annual reconciliations and allocations; monthly or quarterly is preferable.	
Fiscal Policies	Organization has written fiscal policies and procedures including internal controls for handling deposits and cash.		

		Risks to Watch For	Status at My Organization
Internal Controls	Key separation of duties is clear to senior managers, board treasurer and accounting staff. Essential practices are followed to appropriately approve and pay bills, sign contracts, sign checks and reconcile bank statements. More than one staff person understands internal controls and how to take care of daily transactions and accounting backups.	This is a common area of weakness or inconsistencies, making the organization vulnerable to theft and fraud.	
Cash Controls	Cash donations and petty cash both need close tracking and prompt reconciliations.		
Audit/Audit Committee	Completed for most recent fiscal year (in some states audits not required by law, but most groups over $500,000 should have an annual or biannual audit. Determine your state's requirement). Create audit committee that meets directly with auditor (or CPA providing similar service such as a review or compilation) and an independent relationship between the board or officers and legal counsel.	For example, can be helpful if once a year the board chair calls legal counsel to ask, "Is there anything new we should be aware of?" Helps keep organization aware of any potential issues of concern.	
State and Local Registration and Reporting	Know all state and local operating and registration/reporting requirements applicable to organization's tax status. Organization meets all legal requirements to operate in the state and locality(ies) e.g. business permit etc.	Late filing of required reports & registrations makes your organization an easy target to be accused of operating "illegally."	

		Risks to Watch For	Status at My Organization
Liability Insurance	Insurance policy in place. Other specialized insurance coverage may be advisable depending on the nature of the organization's activities.	When holding events off-site, groups may need add-ons to their general liability policy.	
Director and Officers Insurance	Insurance policy in place.	This is mostly used to pay for legal services or settlements when the organization is sued or in disputes with an employee. Does not cover unlawful acts or gross negligence by the board.	
Workers Compensation Insurance	Insurance policy in place and staff know how to respond in case of injuries or other claims.	Make sure employees are covered in all locations where they actually work.	
Unemployment Insurance	State requirement vary. Know your local, state and federal requirements regarding unemployment insurance. Most 501(c)(3) organizations are required to have this insurance.		
Auto Insurance	Auto insurance may be needed if activities regularly involve transporting staff, volunteers or members to activities.		
Payroll Taxes	Payroll taxes are paid each pay period and payroll reports are filed quarterly and annually. Board treasurer and/or auditor verify this quarterly.	This is a common area for liability during financial crises and high penalties can be incurred.	

		Risks to Watch For	Status at My Organization
Information (Tax) Returns and 990s	Properly filed public disclosure version of last three 990s readily available upon request.		
Budget Process	Board approves annual budget and mid-year adjustments. Expenditures over a set amount are subject to additional approval (e.g., large contracts or liabilities over $10,000).		
Time Sheets	Must be kept in real time, completed daily/weekly and indicate lobbying vs. non lobbying hours and (c)(3) vs. (c)(4) hours as appropriate. Also needed to track leave time etc	Time sheets are a critical piece of defense to show that policies and practices are in place.	
Salary policy	Board approves salary scale for categories of staff positions (not by person). Board approves benefits package. Board ensures that compensation arrangements with organizational insiders (e.g., CEO, Executive Director, Board members) are reasonable, as supported by appropriate data.	Rationale for ED compensation is a question on the 990.	

3. Lobbying and Non-Partisan Advocacy

		Risks to Watch For	Status at My Organization
Lobbying	Organization has system in place for tracking, documenting and reporting lobbying expenses ("H" election, plus)	Staff needs regular training in this. Timesheets must be timely and complete.	
	Staff has been trained on lobbying limits, restrictions and reporting requirements.		
	Does your state or local government require that you register as a lobbying organization? If so, is your org registered? Then, keep up on quarterly and annual filings.		
"H" Election for 501(c)(3) (IRS form 5768)	Completed / Copy on file to declare lobbying within IRS limits is strongly recommended	Accusations of exceeding lobbying limits is a common form of attack.	
Lobbying / Ballot Initiatives	Organization has reporting process in place for direct lobbying on ballot initiatives, if applicable. In some states, ballot work requires setting up a political action committee (PAC).	Lack of accurate record keeping and tracking in real time is a huge vulnerability.	
State and Local Laws	Organization has researched and understands state and laws for civic engagement work and reporting requirements; Organization is in compliance.		
Relationships with 501(c)(4)s	If affiliated with a 501(c)(4), bylaws, contracts and cost-sharing agreements have been reviewed by legal counsel when established, and all board records are kept up to date.		

		Risks to Watch For	Status at My Organization
Implementation of Cost Sharing Agreements for 501(c)(3) / (c)(4) Organizations	Cost sharing agreements are implemented and where (c)(3) pays for things up front, the (c)(4) gets billed monthly or quarterly and invoices are paid in a timely way.	Want to avoid impression that the c3 is subsidizing the c4 organization which is not allowed.	
Training for Staff and Leaders	Organization can document training provided to staff and leaders on voter registration; voter education; GOTV, etc.	Senior staff and field staff need regular training/ refreshers on these guidelines especially with turnover.	
Documentation of Process	Organization can document the steps that it takes to ensure that civic engagement work is nonpartisan	Accusations of engaging in partisan activities are a very common form of attack and can result in loss of IRS tax exempt status	
Employee Statements	Employees have signed a statement confirming that they are not allowed to engage in partisan work while on duty or on behalf of the organization. Organizational policies, such as those addressing permissible outside activities, use of organizational resources and systems, and use of and references to the organization's name and the employee's affiliation, require clear separation of personal partisan work from association with the organizations.		
Public Communications	Copies of all appeals, web content and issue educational materials use consistent language around non-partisan work, lobbying and c4 advocacy work where applicable.		

4. Fundraising

		Risks to Watch For	Status at My Organization
Registration and Reporting	The organization is registered and/or has obtained necessary permits to fundraise with each state and locality it is fundraising in, as required. Reporting requirements are met in a timely manner.	Lack of compliance leads to accusations of "illegal" fundraising and penalties	
Record Keeping	Organization has records of all donations; donor information is kept secure and confidential. Sample appeal letters, printed materials, and phone scripts are kept organized.		
Tax-deductible Donation Records	Organization complies with all applicable charitable contribution rules. Donors are informed if the donation is tax deductible or not and which portion is deductible. All donations are recorded and acknowledged. All donations (single or cumulatively within a tax year) of $250 or more must be acknowledged in writing, including a statement (if true) that no goods or services were provided to the donor in return for the contribution.		
Public Communications	Copies of all appeals, web content and issue educational materials use consistent language around non-partisan work, lobbying and (c)(4) advocacy work if applicable.		
Defense Fund	A small percentage of the organizational budget is set aside in the case of unforeseen emergencies, for legal assistance, communications assistance, or other support. This could also be the same as your reserves.		

5. Employment Practices

		Risks to Watch For	Status at My Organization
Personnel Policies / Employee Manual	Organization provides new employee orientation. Organization also provides updated personnel policies / employee manual to all employees. Employees acknowledge receipt in writing. Policies preserve at-will employment, unless an explicit decision is made to modify it. Clear grievance procedure is spelled out. Organization documents that all staff have received policies and notice of changes. Policies periodically reviewed for compliance with current laws. Ideally, an attorney has reviewed policies. Board has approved personnel policies including procedures to assure nondiscrimination in hiring and termination decisions and in all other terms and conditions of employment and compliance with all other applicable laws, such as those concerning wage and hours and required leave.	Annual check in with an attorney regarding any changes in employment laws is recommended. A full legal review every 3-5 years in recommended.	
Employment Forms	All employment forms required by Federal, State and local government (e.g. I-9s and W-4s) are completed before adding employees to payroll. Copies are available.		
Independent Contractors	Sign contracts and get W-9 from each independent contractor. File 1099 tax reports annually.	Ensure contractors are not doing work in ways that would make them employees.	
Classification	Ensure that individuals are appropriately classified as employees or independent contractors and as exempt or nonexempt for purposes of federal and state wage and hour laws.	Improper classification of temporary, seasonal, or part-time workers. Failure to pay minimum wage or overtime. Appropriate treatment of interns.	

		Risks to Watch For	Status at My Organization
Anti-Discrimination and Anti-Harassment Policies	Organization has policies and employees have read policies. Senior staff and board have been trained on how to respond to claims/grievances.	Senior staff and board need regular training/refreshers on how to avoid inappropriate conduct and how to respond to claims/grievances.	
Confidentiality	Organization has policies and/or signed agreements with employees and contractors requiring them to keep confidential all nonpublic organizational materials and information and to return all organizational material and property on separation from employment.	Policies should protect organizational interests, but must also comply with rules allowing concerted activity of employees.	
Equipment, Internet, Email, Social Media policies	Organization has policies in place making clear its ownership of equipment, materials, and communication systems, spelling out appropriate use of those items, and disclaiming any employee expectations of privacy while using those items.	Usage of the organization's equipment by employees or volunteers for their personal communications creates risks and vulnerabilities for the organization.	
Recruitment, Selection and Hiring	Organization has developed fair, consistent and thorough hiring process. Organization carefully reviews resumes and employment applications and prepares specific interview questions focused on ability to perform the job and skills needed. Organization checks references carefully. Organization knows legal obligations about acceptable and unacceptable interview questions and reference inquiries.	Hiring the right staff is critical for program success, organizational reputation, and legal compliance. Be on the lookout for moles and individuals who will cut corners, not produce, or violate legal obligations. Be alert for leading questions or inquiries designed to entrap. Consider requiring new hires to sign confidentiality agreements and other types of statements to deter moles.	

		Risks to Watch For	Status at My Organization
Employee Training and Supervision	Make sure you can verify employees receive job orientation and appropriate training, as needed and effective supervision.		
Exit Interview	Conduct exit interview for feedback & positive closure. Be sure to use checklist & obtain keys and equipment. Be sure to change all passwords and close accounts to which exiting employee had access.		
Volunteer Management	All volunteers are screened, trained in key protocols and procedures and supervised. References of all volunteers are checked. Limit volunteers' access to sensitive files, data and information. All volunteers should sign confidentiality agreements	Volunteers or staff working with minors under age 18 may need to be fingerprinted. Refer to precautions in the Recruitment, Selection and Hiring section above.	

6. Civic Engagement Work

		Risks to Watch For	Status at My Organization
Board Support	Organization has documented support of board of directors for civic engagement work. Board minutes reflect process for endorsing events, ballot propositions, etc.		
Attorney Relations	Organization has relationships or contacts with one or more attorneys familiar with (c)(3), (c)(4), labor law and crisis management.		

		Risks to Watch For	Status at My Organization
Significant Donors	Organization has support from significant donors for civic engagement work. Rules are followed regarding confidentiality and proper disclosure of donors where required (990 private pages, (c)(4) donation rules, PAC rules, etc.)		
Allied Organizations	Organization has support from allies and can call on them in time of crisis.		
	Share best practices from this checklist with your allies. Consider joint training or peer learning to prevent and respond to crises.		
Volunteer Management	All volunteers are screened, trained in key protocols and procedures and supervised.	Volunteers and staff working with minors under age 18 may need to be fingerprinted. Refer to precautions in Recruitment, Selection and Hiring under Section 5 Employment.	

7. Crisis Management Planning

		Risks to Watch For	Status at My Organization
Create a Crisis Management Plan / Create a Crisis Management Team	Organization has a board approved written "**Crisis Management Plan"** and team in place for crisis management and media inquiries. All staff and key volunteers are trained and have a copy of the plan, which is reviewed and updated periodically. The plan clearly designates delegation of responsibilities, notification protocols, how to handle inquiries and messaging guidelines.	Keep a copy of keys, corporate documents, software backups and passwords off-site in case of theft or fire.	
Cultivate Communication and Legal Relationships	Proactively develop relationships with knowledgeable communication, organizational development, finance and legal professionals who can help assess and implement readiness and compliance practices, and assist you in the event of an attack.		
Allied Organizations	Organization has support from allies and can call on them in time of crisis.		
	Share best practices from this checklist with your allies. Consider joint training or peer learning to prevent and respond to crises.		

8. Crisis Communications Planning

		Risks to Watch For	Status at My Organization
Goals and Success Indicators	Organizations should conduct a risk assessment and prepare crisis communications plans accordingly. For most crisis communications, the overall goal is to preserve and promote the organizational brand and values while fostering accurate and contextualized public discourse.	Goals should be specific, achievable and measurable through milestones.	
Opposition Assessment	Organization has assessed credibility, allies, traditional, online and social media activity and likely next moves of opponents.	Audit broadly – opponents might not appear in familiar channels but might still have influence.	
Communications Channels	Organization understands all channels available for proactive communication and has plans for engagement across platforms.	Don't forget about newsletters, meetings or events and direct outreach.	
Audience Assessment	Organization has identified major audience groups (staff, supporters and volunteers, the media etc.)	Remember the board and major donors. Specific communication to these audiences is critical.	
Message Strategy	Organization has developed overall brand messages as well as crisis-specific messages, tailored for groups identified in audience assessment.	All messaging should align with overall crisis and organizational messaging.	

		Risks to Watch For	Status at My Organization
Media Strategy	Organizations should have outlined project goals and crisis communication goals. Media assessment must include current environmental factors and an issue-specific media plan.	Media strategy should align with your target audiences and communications goals; consider both proactive and reactive strategies.	

Digital Security Readiness Assessment: Do you have these Baseline 8 practices in place? ✔

1. Have regular and adequate technical support provided either by staff assigned via job description or contracted with outside agencies.
If your existing hardware and software are not well supported, introducing new tools and practices will likely meet with significant barriers, as new technologies and tools often demand significant ongoing technical support for proper setup and functioning. There are as many ways to secure technical support as there are organizations. Talking to peer organizations in your area is a good way to find quality help.

2. Have a culture of training and learning, including strong technology training and follow-up as part of new staff orientation procedures.
New tools and practices demand end user training. If your organization doesn't have established practices around training, implementing improved and possibly complex secure practices is nearly impossible. Beginning with documentation and training for new hires is a wise first step in this area. Following up with new employees at 30-day intervals will ensure they continue to get the support they need to do their work effectively and securely.

3. Have a common and clearly communicated set of information systems that all staff use effectively: Know all the platforms you are using for organizational communications.
If your staff are using personal file-sharing, email, task management, or other accounts without knowledge or guidance from the organization, not only will your efficiency suffer but also the environment becomes impractical to secure. How can you protect things you have no access to at an administrative level or, worse yet, don't even know are in use?

4. Have a recurrent line item for technology in your budget.
Security is an ongoing process and will require ongoing investments in computer equipment and software to be effective. Work with your technical support provider to determine an appropriate amount to put into this line item.

5. Provide relatively new and adequately powered computers to all staff
Industry standard best practice is to replace laptops and desktops every 3 to 5 years. Encryption tools use a lot of power and can bring older, inadequately powered computers to a near halt, making some security steps untenable for staff. Money for replacing 1/3 to 1/5 of your computers each year should be part of your recurring technology budgeting.

6. Have some baseline non-technical security practices
If you do not control your office space and access to your computers, your other digital security steps can be easily circumvented by walking into your office. Rotate alarm system codes, door codes, wireless network passwords and other sensitive access procedures such as emergency building access when staff leave the organization.

7. Make sure the computers and other devices you use, including personal devices that staff may use to access organizational information, are not compromised by malware, viruses or other intrusive software. As a first step ensure you are running antivirus software on all computers.
Antivirus software for Macs and Windows computers is available to non-profits at a discounted rate through Tech Soup Global (http://techsoup.org). If you haven't been running antivirus software or otherwise aren't sure about the status of your devices, you can have the operating system (OS) on it reinstalled to help guarantee the computer is free of malware and viruses. If reinstalling, use a copy from the OS provider, NOT the computer manufacturer, as manufacturers often bundle dangerous software in their installs. There are other ways in which your device can be compromised that will not be remedied by OS install. If you suspect such an issue, get a new computer and call a security professional.

8. Have a disaster recovery plan that includes making regular backups of organizational data that are stored away from your main offices. Do not rely exclusively on third parties to back up and hold your information.
This actually is a digital security practice itself, but straightforward and critical enough that it needs to come before any other digital security steps. Talk to your technical support provider about the status of your backups. Refer to the guide at the following link for ideas on how to improve your disaster preparedness http://www.techsoup.org/disaster-planning-and-recovery.

If you have these baseline practices in place, you are ready to improve other practices:

Please Note: Although these practices are highly recommended they do not in and of themselves constitute a successful security practice. Information security is an ongoing process of managing risk and no list of procedures is an adequate replacement for a thorough review of what information you are protecting, why and from whom paired with an organizational commitment to shifting operations to mitigate risk. Information Ecology, RoadMap Consulting and Common Counsel are not liable for negative outcomes associated with following these practices.

To request assistance from RoadMap contact: info@roadmapconsulting.org