



# Introduction

---

## OVERVIEW

The news reports are full of stories about nonprofits in trouble. Senator Charles Grassley (R-IA) and the U.S. Senate Finance Committee have held hearings into nonprofit accountability, and Governor Arnold Schwarzenegger of California has signed a bill into law that holds nonprofits accountable for governance, financial, and fundraising activities. Today's legislative expectations have raised the bar for the private sector and the nonprofit sector alike. Nonprofits are being scrutinized at the federal level not only by the Senate Finance Committee, but by the Internal Revenue Service, with greater inspection of 990 forms. The California Nonprofit Integrity Act applies not only nonprofits domiciled in California, but to any nonprofit that solicits donations or otherwise does business in the state.

The nonprofit world's response to these heightened expectations is not always astute. Dean Zerbe, senior aide to Senator Grassley, commented in an interview with the *Chronicle of Philanthropy* that he routinely encounters these three groups of nonprofit people: “[o]striches . . . deny problems; Luddites believe there is no need for change but advocate stiffer enforcement of nonprofit laws; and fig-leaf reformers come up with ideas that appear to offer solutions but actually allow problems to persist” (Wolverton, 2005, p. 38).

How can nonprofits address these changes in requirements and expectations? Risk management and business continuity planning are two techniques that have the potential for facilitating growth and

strengthening the internal structure of nonprofits. But as with any good-for-you regimen, there are always plenty of excuses not to engage in these healthy activities.

## Five Common Myths about Risk Management

Often nonprofits defer risk management planning because they are apprehensive about beginning the process. Many times this fear stems from five common myths about risk management and business continuity planning:

1. It takes forever.
2. It involves a lot of navel gazing.
3. It will step on toes.
4. The finished plan will have to be at least four inches thick.
5. It gathers dust on the shelf once it is finally completed.

Bonus myth:

6. If we do it right, we can eliminate risk altogether.

Of course, none of these myths is true, but they all are significant in their power to keep nonprofits from engaging in risk management and business continuity planning. The truth about these myths points to the need for nonprofits to take a more streamlined approach to this type of planning:

### The Truth

- *It takes forever.* The Done in a Day (DIAD) method of risk management and business continuity planning accelerates the process by allowing for a structured preparation with a concentration of time dedicated to assembling the plan and developing strategies for execution.
- *It involves a lot of navel gazing.* With DIAD, there is no “paralysis by analysis.” The preparation time is structured to identify the necessary data, information, and other resources. Decision making is

compressed to focus on what is needed for a specific time frame. Because risk management and business continuity planning follow a recurring course, there will be opportunities in the next scheduled round to review decisions made today.

- *The process will step on toes.* The best interests of the nonprofit and the community it serves trump any individual egos. The nonprofit’s insurance professional, insurance carrier, auditor, banker, and legal counsel will be pleased that the organization has committed to this type of planning.
- *The finished plan will have to be at least four inches thick.* Not using today’s technology! An effective risk management plan and/or business continuity plan can fit into the memory of a PalmPilot or BlackBerry. Because one of the themes of DIAD is “less is more,” planners focus on the *important* information. The plan must always be user-friendly because staff and volunteers will be expected to fully understand how to participate in its execution.
- *It gathers dust on the shelf once it is finally completed.* Absolutely not! Risk management and business continuity planning need to be woven into everyone’s job description and performance objectives. These plans can also serve to strengthen internal controls and facilitate the implementation of Sarbanes-Oxley best practices.

Bonus myth:

- *If we do it right, we can eliminate risk altogether.* Risk can never be eliminated—all of life is a risk. The intent of risk management is to recognize that risks can be neutralized to some extent so that the frequency and severity of losses can be managed.

Despite seemingly nonstop scandals that have affected nonprofits, many leaders are committed to making their nonprofits stronger and more viable entities. Done in a Day planning for risk management and business continuity can serve to build and strengthen their organizations.

An important assumption in this book is that *nonprofits are businesses*. The nonprofit sector is an industry in its own right. Nonprofits’ identity of “not for profit” lies solely in their tax classification of 501(c) (3, 4, or

whatever). Nonprofits do not stay in operation very long if they lose money. The business models of private companies and nonprofit organizations are more closely aligned today than ever before. Public sector expectations of accountability apply to private companies and nonprofits, as evident from the findings of Senator Grassley's hearings in 2004 and 2005 on nonprofit accountability. Many nonprofits have "for-profit" subsidiaries or related operations, such as ownership of commercial property. Private companies routinely partner with nonprofits on contractual ventures or as part of corporate philanthropy.

This book sets on a mission to:

- Explain what risk management and business continuity planning are and how this type of planning can add value to a nonprofit.
- Illustrate why these plans are *essential* to your nonprofit in today's business environment.
- Describe the most efficient and cost-effective ways to design and execute these plans.
- Present risk management and business continuity planning templates to facilitate the design of the first edition of your nonprofit's plans.
- Show how risk management and business continuity planning can help your nonprofit come into compliance with Sarbanes-Oxley legislation and state legislation, such as California's Nonprofit Integrity Act.
- Present methods to add further value to your planning, such as offering training to your staff and leveraging planning for competitive and marketing advantage.

## **BASIC ASSUMPTIONS**

### **Board and Senior Management Collaboration**

Before you begin a DIAD plan, we should review some basic assumptions. The most important assumption is that the nonprofit's board and senior management are fully committed to providing the time, space,

and resources to the staff and volunteers who are constructing the plan. The board needs to hold itself and senior management accountable for contributing to the plan in terms of new methods and policies. The board and senior management also need to commit to being visible in modeling the desired behavior and practices that are associated with risk management and business continuity planning.

## **Pre-Session Preparation**

The DIAD plans can be completely assembled in one day with some preparatory work in the two to three weeks prior. The preparatory work is essential to the success of the DIAD session. However, it is important to complete the preparatory work quickly and not engage in paralysis by analysis. If your team wants to construct the plan in one day, then you need to commit to completing the (not complex) prep work prior. Chapters 4 and 8 provide detailed descriptions of the preparation methods and include checklists and timelines to simplify the process. The chapters include practical advice for dealing with risks and developing strategies for resuming business operations.

Each DIAD session presumes that your nonprofit has assembled a team to do the preparatory work and to assemble the plan. The team should be large enough to complete the preparatory work in a short time, but not so large as to bog down decision making. The team can be comprised of staff, volunteers, and/or board members—whatever works for your nonprofit. All of the staffing and preparatory work suggestions are just that—suggestions. It is important that your nonprofit put together a team that works for your organization and does the prep work that is relevant to the needs of your organization. The preparatory work and the structure of the plan are intended to be generic and user-friendly so they can be tailored to meet the needs of nonprofits of all sizes.

## **Template**

The DIAD method uses templates as basic tools. Using a template to begin your nonprofit's risk management or business continuity planning is an important way to jump-start the planning process by eliminating

the need to design a structure for the plan. The template is a fill-in-the-blanks tool that can be used to design the first edition of your nonprofit's risk management or business continuity plan. If your team decides it would like a different structure for the second round, great! At least your risk management or business continuity planning process has been launched, and your team has had the experience of a round of risk management planning. You can customize the generic components of the template to meet the structural needs of your nonprofit. If some aspect of the template does not apply to your organization, you can simply ignore it.

## **OVERVIEW OF THE CHANGES IN THE LEGAL ENVIRONMENT**

In order to design effective risk management and business continuity plans, planners need to be conscious of the changes in the legislative environment at the federal and state level. These requirements, best practices, and expectations need to be built in to risk management and business continuity plans and will be highlighted in the discussions of plan content.

The Public Company Accounting Reform and Investor Protection Act, commonly referred to as Sarbanes-Oxley (SOX) after its sponsors, Senator Paul Sarbanes (D-MD) and Representative Michael Oxley (R-OH), was passed in 2002 in the wake of the Enron corporate scandal. Although SOX initially was intended to raise the bar for integrity and competence for publicly traded companies, its effect has been to promote greater accountability within both the nonprofit and the private sector.

Currently, only two of the provisions in SOX apply directly to nonprofit organizations. Nonprofits are required to adhere to “whistle-blower protection,” which provides protection to employees who report suspected fraud or other illegal activities. Employees or volunteers of a nonprofit are shielded from retaliation for making reports of waste, fraud, or abuse.

Nonprofits are also expected to have a fully functioning document preservation policy in place. This policy has two aspects: preservation and archiving of documents for the purpose of timely retrieval and a prohibition against the destruction or falsification of records or documents.

## **Whistleblower Protection**

The first obligation from SOX that applies to all organizations is the requirement for a documented whistleblower protection policy. SOX requires all organizations, including nonprofits, to establish a means to collect, retain, and resolve claims regarding accounting, internal accounting controls, and auditing matters. The system must allow for such concerns to be submitted anonymously. SOX provides significant protections to whistleblowers and severe penalties for those who retaliate against them.

The policies and procedures that a nonprofit develops must contain at least these features:

- There is a confidential avenue for reporting suspected waste, fraud, and abuse.
- There is a process to thoroughly investigate any reports.
- There is a process for disseminating the findings from the investigation.
- The employee or volunteer filing the complaint will not be subjected to termination, firing, or harassment, or miss out on promotion.
- Even if the findings do not support the nature of the complaint, the employee or volunteer who made the complaint will not face any repercussions.

All employees and volunteers should have a copy of the whistleblower policy, and it should be posted in clear view. This policy should also be covered in any orientation or training programs the organization offers for employees and volunteers.

## Document Management and Preservation Policy

Document storage and retention is another area within SOX that applies to all organizations. Some key areas for consideration include:

- What documents and records should be preserved and why?
- Are the documents paper only, or are electronic files included? Which ones?
- What about e-mail and instant messaging?
- What are the expectations about the way in which documents are stored or archived and the ability to retrieve documents?
- How long are you supposed to keep these documents?
- Is there a protocol for disposing of documents once their storage time has elapsed?
- When should you not destroy materials?
- How can you make sure that everyone in the nonprofit—staff and volunteers—understands and adheres to these requirements?
- What happens if your nonprofit is in violation?

The executive team must develop a statement that contains these talking points:

- What the document retention policy is—and why it is required by law. It is important that the staff and volunteers understand that document preservation is a component of SOX that applies to all organizations.
- What new procedures emerge from the policy? Staff and volunteers need to understand how to be in compliance, and what specific actions are required.
- What are the obligations of individuals to ensure that your nonprofit is in compliance? Requirements for individual staff and volunteers should be presented in writing. Because this is probably a very new requirement in your organization, the more user-friendly the guidelines, the better.

- What is expected in terms of new behaviors and procedures, and what are the consequences for individual employees and volunteers for failing to adhere to the new procedures? It is particularly important that the executive team be prepared to carry out unpleasant consequences swiftly to send a strong message throughout the organization.

## **Sarbanes-Oxley Best Practices**

SOX best practices are designed to enhance the completeness and reliability of all aspects of your nonprofit's operations. These practices include:

- Audit committee whose role is to oversee the annual audit or financial review (for small nonprofits) and to upgrade the financial literacy of the board of directors
- Enhanced detail and accuracy in the preparation of IRS Form 990
- Improved governance and a nonprofit board that understands its role as ultimately accountable for the actions of the nonprofit and is willing to take steps to enhance professional development for each member
- Conflict of interest policy and code of ethics that facilitates greater focus on decision making for the good of the nonprofit
- Internal controls, particularly as these relate to financial operations, and compliance with all laws and regulations at the federal, state, and local level
- Transparency at all levels of management
- Adherence to policies and procedures—and enforcement

The nonprofit's commitment to adopting and maintaining SOX best practices can be demonstrated in the deliverables of a review of internal controls. The process and outcomes can be used to measure the development of the platinum standard. Compliance cannot simply be a rote operation; the commitment to excellence must transcend all levels of the

organization and be evident in all of the operational systems and in the symbiotic relationship that exists among the various systems within the organization.

### **Example of State Legislation: California's Nonprofit Integrity Act**

In addition to federal legislation and regulatory scrutiny, nonprofits can be subject to state legislation even if they are not domiciled in that state. The state of California passed a Nonprofit Integrity Act (SB1262) in 2004 that imposes many of the features of Sarbanes-Oxley legislation on nonprofits with budgets in excess of \$2 million operating in that state. Of particular significance is that this law also applies to *any nonprofit that solicits donation in the state of California regardless of where the nonprofit is domiciled*.

### **Provisions That Apply to Nonprofits with Revenues in Excess of \$2 Million**

The law has specific provisions that apply to nonprofits with revenues in excess of \$2 million. These provisions include:

- Nonprofits will be required to have an annual audit performed by a certified public accountant (CPA) who is “independent,” as defined by U.S. Government auditing standards.
- The results of the audit will need to be made available to the public and the State Attorney General.
- Nonprofits will be required to have an audit committee whose membership cannot include staff and must not overlap more than 50 percent with the finance committee. The audit committee can include members who are not on the organization’s board of directors.

### ***What This Means for Nonprofits Operating in California***

Nonprofits whose revenues exceed \$2 million will be required not only to file an annual audit with the Attorney General’s office, but will have

to demonstrate that the audit was conducted by an auditor who is independent of the organization. The auditor cannot perform any other services for the nonprofit, including tax preparation. Nonprofits covered by this provision of the law will be required to have an audit committee that conforms to the standards described in the law.

To ensure greater accountability in executive compensation, the law requires that the board approve the compensation, including benefits, of the corporation's president or chief executive officer and its treasurer or chief financial officer for the purposes of assuring that their compensation package is reasonable.

The law also requires disclosure of written contracts between commercial fundraisers and nonprofits. These contracts must be available for review on demand from the Attorney General's office. Fundraisers must be registered with the Attorney General's office.

### **Provisions That Apply to All Nonprofits, Regardless of Size, Operating in California**

Nonprofits are required to:

- Make their audits available to the public on the same basis as their IRS Form 990 if they prepare financial statements that are audited by a CPA.
- File at least 10 days before the commencement of the solicitation campaign, events, or other services notice of the campaign/events/services by a "commercial fundraiser for charitable purposes." This time provision is lifted in emergency cases. Each contract must be signed by an official of the nonprofit and include the contract provisions specified in the law.
- For fundraising activities, not misrepresent or mislead anyone about their purpose, or the nature, purpose, or beneficiary of a solicitation. There must be specific disclosures in any solicitation that the funds raised will be used for the charitable purpose as expressed in articles of incorporation or other governing documents. The nonprofit is expected to ensure that fundraising activities are adequately supervised to make certain that contracts and

agreements are in order and that fundraising is conducted without intimidation or undue influence.

### ***What This Mean for Nonprofits Operating in California***

Nonprofits in California, regardless of their size, need to review their fundraising practices, particularly if some or all of their fundraising is outsourced to commercial fundraising firms. Nonprofits will be liable for abuses by vendors of fundraising services. As a practical matter, boards should insist that due diligence activities be conducted before contracting with any vendor, particularly those providing fundraising services. The California law, however, places strict parameters on third-party fundraising.

### **Bottom Line**

The days of the “mom and pop” nonprofit are over—you have an obligation to your donors, your clients, your board, and your staff to ensure that your organization is in compliance with the relevant provisions SOX legislation (and SB1262 if you operate or solicit donations in California). It’s not just a “best practice”—it’s the *law*, and it applies to all organizations in this country, including your nonprofit.

### **SUMMARY**

The DIAD concept is predicated on the values that preserve the nonprofit’s mission and preserve its resources. Risk management and business continuity planning need not be resource intensive in terms of time, staff, or money. It is important to look on DIAD activities as the launching pad for *ongoing* risk management and business continuity planning. It’s *done* in a day, *but not over* in a day.