

Assessing Your Organization's Risk Profile



Matthew Claeys, CPA, Principal
Craig Arends, CPA, Principal

LarsonAllen's 17th Annual Nonprofit & Foundation
Conference—May 6, 2010

LarsonAllen[®]
LLP

CPAs, Consultants & Advisors

Learning Objectives

At the end of this session, you will understand basic concepts related to assessing your organization's risk profile in the following categories:

- What is Risk
- Key Risk Areas of Risk
- Benefits of a Risk Assessment Program
- Examples of a Risk Assessment Program
- Concept of Enterprise Risk Management (ERM)



What is Risk?

- Risk assessment is a systematic process for utilizing professional judgments to evaluate probable adverse conditions and/or events and their potential effects on your organization
- The plan is developed through the execution of a risk assessment process whereby potential auditable areas are assessed using established risk factors



continued

- Areas make up the auditable universe can include:
 - Critical corporate processes,
 - Financial business cycles,
 - Strategic objectives or initiatives,
 - Major capital projects,
 - Significant contracts,
 - System applications and major system development projects and
 - Other key focus areas
- Assessing relative risk is based on several factors including:
 - Senior management input
 - Knowledge of significant events
 - Results of recent audits
 - The risk assessment process



Risk Infrastructure

- The process starts with identifying risks associated with business objectives linked through all levels of the organization whether it is entity or process level.
 - Entity level is the cornerstone for effective control and its objectives provide guidance on what the entity wants to achieve. It should be consistent with budget, strategy, and business plans.
 - Process level should align with entity level objectives, but differ in that they relate directly to goal setting with specific targets and deadlines. It provides guidance for management focus.



continued

- Within each layer of the organization, the following COSO elements should exist:
 - Control environment sets the tone of an organization, influencing the control consciousness of its people
 - Control activities are the policies and procedures that help ensure management directives are executed
 - Information and communications flow is the process of identifying, capturing and communicating pertinent information in a form and timeframe that allows management and staff the ability to execute their responsibilities
 - Risk assessment is the process of evaluating internal and external factors that impact the organizations performance and drives risk appetite
 - Monitoring is the process of monitoring internal control systems



Types of Risk

Strategic:

- The risk that business objectives will not be met due to poorly defined business strategies, poorly communicated strategies, or the organization's inability to execute these strategies due to inadequate organizational structure, infrastructure or alignment.
- Strategic risk is managed by appropriate organizational governance.

Financial:

- The risk that the organization's financial reporting is inaccurate, incomplete or untimely due to a variety of factors including the pace of change, the amount of uncertainty, the presence of a large error, or the pressure on management to meet investor expectations.



continued

Operational:

- The organization provides or is reliant on outsiders to provide processing activities supporting the delivery of services or products to their customers.
- This risk addresses barriers to the timeliness, accuracy, authorization and completeness of these processing activities.

Legal/Regulatory:

- The organization is subject to a variety of federal, state and local laws, regulations and directives, or accreditation agencies.
- Failure to follow prescribed directives may result in substantial fines, restrictions, loss of business, and/or legal action taken by regulators.



continued

Technology:

- This risk considers the level of use, sophistication, complexity, robustness, ease of use and speed and accuracy of recovery / replacement of systems.
- Addresses the overall importance of technology within the organization and the availability and quality of information the organization can access to support decision making, and the security of key information.

Human Capital:

- This risk addresses the type of behaviors encourage by management; the methods used to reward employees; the approach to consistently enforce policies and procedures; the selection, screening and training of employees; and the reason and frequency of turnover.



Risk Definition

Institute of Internal Auditors (IIA):

- “The uncertainty of an event occurring that could have an impact on the achievement of objectives.”
- Key words when discussing risk in an organization are – **likelihood / vulnerability** and **impact / consequences** to the nonprofit



Enterprise Risk Management

- The process of identifying and analyzing risk from an integrated, company wide perspective.
- It's designed to identify potential events that may affect an organization, and to manage these risks to provide **reasonable assurance** that the organization's objectives will be achieved.



Key Risk Areas

Governance

- How engaged are your board members?
- How effective are board members in aligning themselves with the organization's strategy and short/long term goals?
- Do they have the right skill sets, and stay up to date with current events that may or may not affect their organization/industry?



Strategic Planning

Goals of the Nonprofit:

In developing strategic plans, organizations should consider the risks associated with each strategy.

An adequate risk program framework should support the upside of risk (benefits) and protect against the downside of risks in all its endeavors.



Industry Stability / Competition

- Diminishing value of products / services
- Federal term contract conclusion (e.g., end of a government funding source leads to the nonprofit's ability to function)
- Vulnerability of industry to economy
- Decreasing market
- Consolidation of stakeholders



Compliance Risk

Laws and Regulations:

Noncompliance with external laws, regulations and rules can be costly.

Some of the most significant penalties have come from ineffective management of compliance risks.



continued

- Examiners and regulators tend to focus on compliance with new rules such as:
 - Red flags / ID theft prevention
 - PCI DSS compliance (security controls over credit card safekeeping and processing)
 - Federal and state tax compliance



Reputational Risk

Public Image:

Many organizations' images have been damaged and reputations tarnished by failure to effectively manage reputational risks.

Emphasis on employee and educational integrity and a clear statement of the ethics and moral values emanating from the top is an important component of this risk.

Reputational risk is the hardest to quantify as a simple rumor can spread and go viral over the Internet, causing irreparable damage to a company.



Operations Risk

Processes that Achieve Goals:

Nonprofits are dependent upon day-to-day operations for their success and as such, must assess operational risks.

Examples:

- The organization's ability to raise funds during its annual fund drive, maybe because member contributions may have gone to help earthquake or tsunami victims in a disaster-stricken area.
- Succession planning
- Human capital resources



Information Technology Risk

The risk of unexpected losses or expense to the nonprofit from inadequate systems, breaches in information technology security, and lack of a comprehensive disaster recovery (DR) and business continuity plan (BCP) document

- What is the organization's security posture?
- Is network security taken seriously?
- Are data backups performed consistently?
- Are backups tested periodically?
- Is there a need for a "hot/cold" site?



Financial Risks

Safeguarding Assets:

Finance and accounting divisions traditionally have focused on managing the risks of potential loss of physical assets and financial resources.

Examples:

- Lack of an annual financial audit
- Inadequate insurance coverage
- Adequacy of financial reporting systems
- Integrity / accuracy of financial statements



Benefits of an Assessment Program

- Helps ensure that the greatest risks to the organization are identified and addressed on a continuing basis.
- Helps personnel throughout the organization better understand risks to business operations and teaches them to avoid risky practices.
- Reduces the assumption of risk as it identifies key areas where actual risks lie.



continued

- Helps track risks and vulnerabilities to the organization as changes occur over time.
- Overall Organizational Value

Smaller organizations may update their programs every couple of years; this may be done annually if there are significant changes in business operations.

Larger nonprofits may seek assistance by outsourcing this task.



Assessment Framework

- A well-developed ***risk assessment*** component ensures that mechanisms exist throughout the organization to identify, manage, and mitigate unwarranted risks.



Assessment Activities

- Establish Goals & Objectives
- Identify Risks
- Analyze Risks
- Evaluate the Risks
- Address the Risks



Risk Descriptions

- **Nature of risk** – classification of risk, the potential impact and description as a hazard, opportunity or uncertainty
- **Stakeholders** – stakeholders, both internal and external, and their expectations
- **Risk evaluation** – likelihood and impact of an event



continued

- **Risk tolerance and appetite** – loss potential and anticipated financial impact of the risk
- **Risk response** – review of, and strengthening existing control mechanisms and activities
- **Strategy and policy** – responsibility for developing strategy related to the risk and procedures for monitoring and review of risk performance



Evaluation Criteria

Areas of Focus

Impact

Definitions

Financial
Stakeholder
Reputation
Legal / Regulatory
Operations

Each process within the functional unit is evaluated for cumulative impact and organizational vulnerability using a 3-point scale.

Vulnerability

Control Efficiency & Operating Effectiveness
Speed of Response
Complexity
People
Operational Efficiency
System Capability
Rate of Change

Scale

1.00 = High Risk
0.66 = Medium Risk
0.33 = Low Risk



Process Example

- Identify risk factors and assign weighted risk scores
- Use a multiplier to calculate average risk scores such as:
 - 0.33 - **Low**
 - 0.66 - **Moderate**
 - 1.00 - **High** Risk
- Identify objectives/assets/auditable activities
- Analyze the risks by considering their likelihood and consequence / impact



continued

- Assign ratings to the risks
- Review with the board, senior management and outside advisors
- Use rankings to develop risk mitigation and management action plans

Involve line managers in ERM process and roll up firm initiatives to the board and / or senior management)



IMPACT CRITERIA

	FINANCIAL	STAKE-HOLDER	REPUTATION	LEGAL / REG	OPERATIONS
HIGH 1.0	<ol style="list-style-type: none"> 1. Asset size > \$XX Million 2. Prior negative exposure 3. Rapidly increasing transaction volume 	<ol style="list-style-type: none"> 1. Management, employees, and customers affected by process inefficiencies or control breakdowns 	<ol style="list-style-type: none"> 1. Potential adverse issues are known to external parties (media and regulatory bodies) 	<ol style="list-style-type: none"> 1. Any federal, state, or other action 2. External audit reportable conditions 	<ol style="list-style-type: none"> 1. Current infrastructure cannot support business strategy.
MED .66	<ol style="list-style-type: none"> 1. Asset size < \$XX & > \$XX million 2. Major potential cost 3. Transaction volume stable 	<ol style="list-style-type: none"> 1. Management and employees may be affected ... 	<ol style="list-style-type: none"> 1. ... could impact customers. 	<ol style="list-style-type: none"> 1. Issues identified by federal, state, or other 2. Issues identified by external audit 	<ol style="list-style-type: none"> 1. ... is able to support business strategy with work-arounds.
LOW .33	<ol style="list-style-type: none"> 1. Asset size < \$XX million 2. Minor potential cost 3. Transaction volume stable 	<ol style="list-style-type: none"> 1. No customers or employees are affected ... 	<ol style="list-style-type: none"> 1. ... could impact employees. 	<ol style="list-style-type: none"> 1. No issues identified ... 2. No issues identified ... 	<ol style="list-style-type: none"> 1. ... is able to support business strategy.



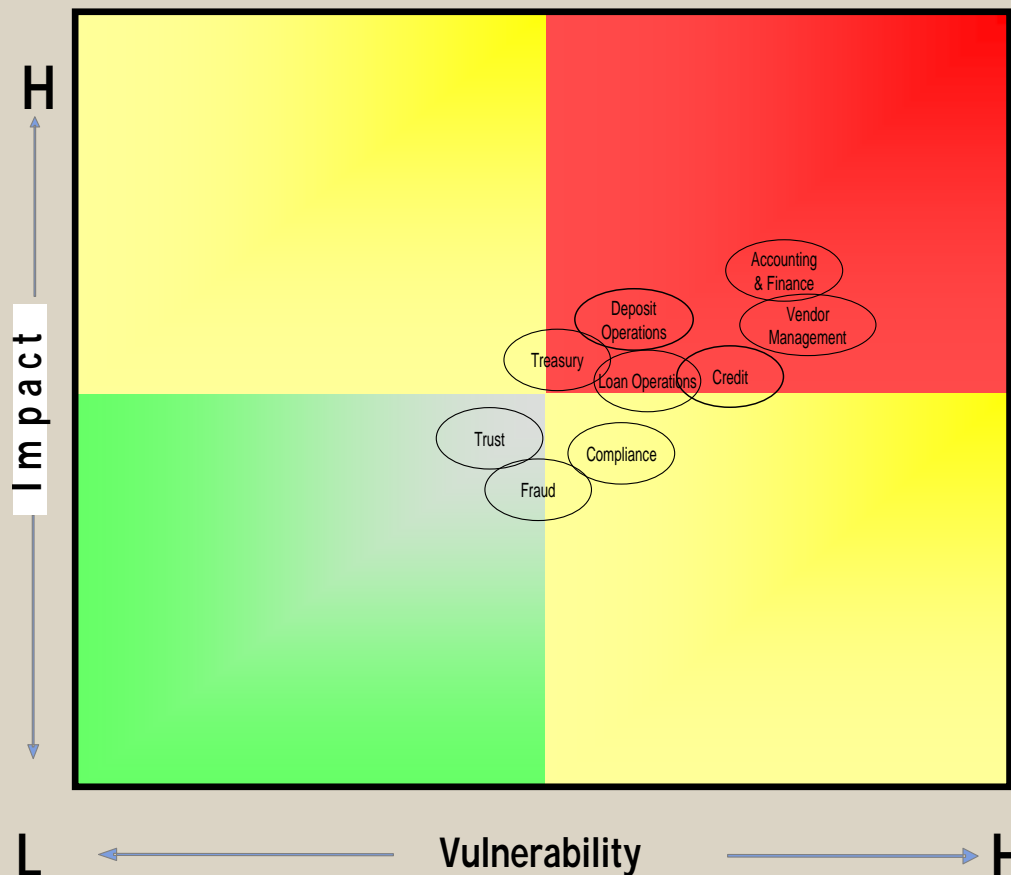
VULNERABILITY CRITERIA

	CONTROLS	SPEED OF RESPONSE	COMP-LEXITY	PEOPLE	OPERATIONS	SYSTEM CAPABILITY	RATE OF CHANGE
HIG H 1.0	Controls are not working or do not exist.	No method for anticipating and assessing specific risk events exists, issues are not escalated to the appropriate executives effectively.	Manual processes with many data transfer points and owners.	Limited staff or current have limited competency to manage risk events. Inadequate cross-training.	High / unmeasured cost of operations, many quality concerns, and unacceptable or unmeasured cycle/process time.	Systems are not operating as designed or design is flawed; very limited controls.	Risk is managed by or directly impacts people, processes, systems or businesses experiencing a HIGH rate of change over the last 6 months.
MED .66	Controls are detective but not preventative and there may or may not be effective reporting.	A method ... exists but issues are not effectively escalated to the appropriate executives.	Automated processes encompassing multiple systems and owners.	Limited staff and/or staff have moderate competency ...	Above industry average cost of operation, some quality concerns, and below industry average cycle/process time.	Systems are operating as designed, but design can be improved; controls are bolted on top of the system.	... a MODERATE rate of change over the last 6 months.
LO W .33	Controls are appropriately preventive and detective and there is effective reporting.	... exists and effectively escalates issues to the appropriate executives.	Automated processes with integrated systems.	Most staff have high competency ...	Low / average cost of operations, no quality concerns, and cycle/process times within standards.	Systems are designed, implemented and operating effectively; controls are embedded in the system.	... a LOW rate of change over the last 6 months.



Aggregate Results

Due to the inherent risk of the health care industry and the relative risk of ABC's processes, a number of the functional units were rated as high on the vulnerability and impact scales.



<u>Issue</u>	<u>Observations</u>
Role & Responsibility	Complex matrix organization Lack of formalized policies and procedures Unassessed staffing needs
Operational Metrics	Uncoordinated efforts No central data warehouse Lack of common definitions
Manual Processes	Over reliance on manual practices Limited leverage of automation within operations

Audit Frequency in Months

- Low Risk = 25 to 36 or not applicable
- Moderate Risk = 13 to 24 months
- High Risk = 1 to 12 months



Individual Results

- Low Risk
- Moderate Risk
- High Risk

Risk within critical areas has been measured based upon established risk criteria.

ABC Enterprise Risk Assessment		Accounting & Finance										Ave	
		Intercompany / Shared Services Accounting	Significant Accounting Estimates / Non-routine Transactions	Account Reconciliations	Period End / Close Process	Accrual/reserve/estimate analysis	Operational Accounting	TFR – Technical Accounting	Other Regulatory Reporting	Management Reporting / KPIs	Audited Financial Statements		
Area	Criteria												
Impact	Total Impact Rating	0.73	0.46	0.86	0.60	0.53	0.73	0.60	0.60	0.60	0.80	0.65	
	Financial	1.00	1.00	1.00	0.33	1.00	1.00	0.33	0.33	0.33	1.00		
	Stakeholders	0.33	0.33	0.66	1.00	0.33	0.33	0.33	0.33	0.33	0.66		0.66
	Reputation	1.00	0.33	1.00	0.66	0.33	1.00	1.00	1.00	0.33	1.00		
	Legal / Regulatory	0.66	0.33	0.66	0.33	0.33	0.66	0.66	0.66	0.66	0.66		0.66
	Operations	0.66	0.33	1.00	0.66	0.66	0.66	0.66	0.66	0.66	1.00		0.66
Vulnerability	Total Vulnerability Rating	0.81	0.52	0.90	0.76	0.66	0.71	0.81	0.57	0.86	0.61	0.72	
	Control Effectiveness	1.00	0.66	1.00	1.00	1.00	1.00	1.00	0.66	1.00	0.33		
	Speed of Response	1.00	0.33	1.00	1.00	0.33	0.66	0.33	0.33	1.00	0.66		
	Complexity	0.66	1.00	1.00	1.00	0.66	0.66	0.66	0.66	1.00	0.66		
	People	1.00	0.66	1.00	0.33	1.00	0.66	1.00	0.66	0.66	1.00		
	Operational Efficiency	1.00	0.33	1.00	1.00	0.33	1.00	1.00	0.66	1.00	0.66		
	System Capability	0.66	0.33	1.00	0.66	1.00	0.66	1.00	0.66	1.00	0.66		
Rate of Change	0.33	0.33	0.33	0.33	0.33	0.33	0.66	0.33	0.33	0.33			

©2010 LarsonAllen LLP





Case Study

LarsonAllen[®]
LLP

CPAs, Consultants & Advisors

Large Health System Organization

- 5 hospital sites and approximately 50 clinic sites
 - Negative publicity in the newspaper started this inquiry
 - Several thefts from the smaller clinics in the system
 - Assets stolen weren't huge, but publicity was problematic
- CFO approached us about an idea
 - Could we assess cash collection points and controls in place?
- Dozens of cash collection points for the hospitals in addition to each clinic site



Findings and Risks

- Identified
 - Lack of automation resulted in numerous “touches”
 - Little or no internal controls over the cash collections
 - Inefficient reconciliation process
 - Delayed cash flow or access to the cash
 - Cash collections were growing significantly due to growing deductibles and co-insurance
- Missing
 - Simple automation
 - ◇ Shared/secured file system
 - ◇ Collection software or even excel spreadsheets
 - ◇ Training due to not wanting to change
 - The right culture re cash collections



Results

- IT set up a few simple automation procedures
- Shared files opened up
- A collection software activated
- Basic training on the new procedures
- Lock boxes installed
- Internal controls tightened
- Secured depositing implemented throughout
- Enhanced reconciliation of cash reallocating 1.5 FTE's.
- Risk mitigated for bad publicity and stolen assets



Contact Information:

Matthew Claeys

267.419.1655 or mclaeys@larsonallen.com

Craig Arends

612.397.3180 or carends@larsonallen.com

LarsonAllen LLP

220 South Sixth Street, Suite 300, Minneapolis, MN 55402

Main 612/376-4500, Fax 612/376-4850, www.larsonallen.com

LarsonAllen is a member of Nexia International, a worldwide network of independent accounting & consulting firms.

.....
NOTICEABLY DIFFERENT

17th Annual Nonprofit and Foundation Conference



LarsonAllen
LLP
CPAs, Consultants & Advisors

