NFP Advisors LLC

How to do a Simple Risk Assessment

Risk is inherent to all organizations. You can’t avoid it. What you can do is *mitigate risk.* Identifying risks and adopting policies and procedures that meaningfully mitigate those risks is the art of *risk management*.

Types of Risk:

☑ OPERATIONAL

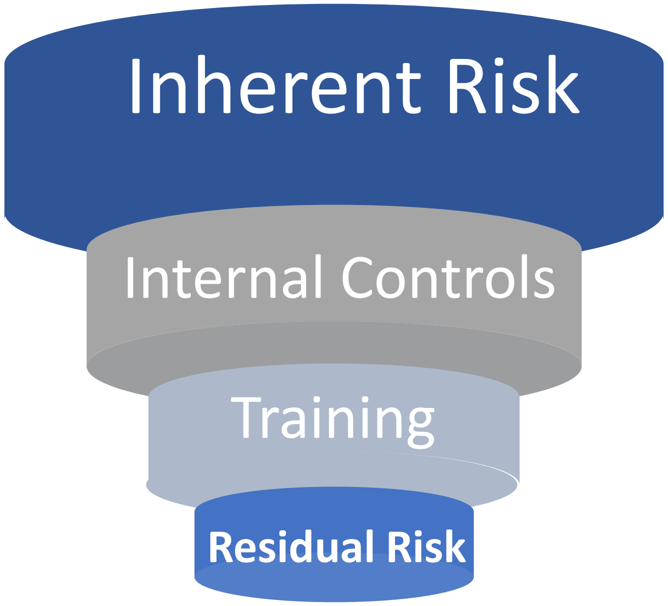
☑ FINANCIAL

☑ COMPLIANCE/LEGAL

☑ FRAUD

☑ IT/CYBER

☑ REPUTATIONAL



Inherent Risk

Internal Controls

Training

Residual Risk

Mitigants:

☑ Policies and Procedures

☑ Internal Financial Controls

☑ Segregation of Duties

☑ Training

☑ Employee Policies

☑ Whistleblower Policy

☑ Documented Reporting Procedures

☑ Cybersecurity Training

☑ Physical security

☑ Job Descriptions

☑ Internal Audit function

☑ Engaged Board

☑ External Communication Training

Asking Management and Department Heads a series of simple questions can help to identify organizational weakness and gaps and provide a road map to further audit or review.

The following set of questions should be posed to all Department heads. It can be administered as a survey or as face-to-face interviews. Make sure that the employee knows the purpose of the questions and that all responses will be held confidential. Keep it casual and have a real dialogue any areas of concern.

- ✓ What is the objective and business strategy of your Department?
- ✓ How many employees in your Department?
- ✓ Are there documented employee policies?
- ✓ Does the Department of a SOP manual?
- ✓ Are all employees aware of the policies?
- ✓ Do you have clearly defined, documented job descriptions?
- ✓ Does the organization offer formal training for all job functions?
- ✓ Are department personnel cross-trained for key activities?
- ✓ Is there clear segregation of duties?
- ✓ Do you have a whistle blower policy?
- ✓ What are the security issues relevant to this Department?
- ✓ Does this department handle cash transactions?
- ✓ How is interaction with the public, the press or other external stakeholders managed?
- ✓ What are the regulations, laws, reporting or other compliance issues that affect your Department?
- ✓ Are you aware of any instances of management override that may affect the organization?
- ✓ Are you aware of any IT issues, breaches or glitches that may put the organization at risk?
- ✓ What do you perceive as the largest risk to the organization?
- ✓ What does your Department need to effectively reach its goals?
- ✓ Is there a specific process area that you believe should be strengthened/audited?

Do not ignore the warning signs. Give yourself a risk rating by identifying the risk, applying the mitigants, and assessing the residual risk. Take action on all inherent risks that have not been addressed. Your best defense is an honest and open dialogue, documented policies and procedures, training and segregation of duties.