

Risk Assessments & Internal Controls

Kelly A. Nueske
Managing Director
Enterprise Risk Services
Internal Audit & Compliance

1

Nature of Risk



- R = risk is relative because perception of downside and upside risk is individual, and that applies to people and organizations.
- I = risk is intuitive because we learn with experience and time.
- S = risk is significant because everything we do has positive and negative consequences.
- K = risk is kinetic because it changes relative to situations, events, time and space.

2

Nature of Risk (continued)



- Risk is universal
- Risk is not properly identified and managed by most organizations, including governments
- Need a common risk vocabulary
- Need improved risk management methodologies
- Risks are diverse & inherent to the business operations
- If non-clinical risks are not managed they are just as hazardous as clinical risks

Common Healthcare Internal Risks



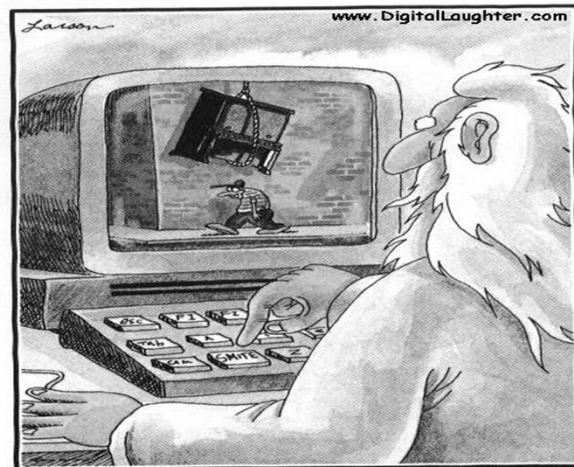
- Policies and Procedures
 - Document internal control structure
- Contracting
 - Vendor Relationships
 - Physician Relationships
- Financial Reporting
 - Financial Statements
 - Tax Returns
 - Cost Reports
 - 990 Reporting
 - Credit Risk
 - Liquidity Risk
- Crisis Management Program
 - Business Continuity Plan
- Human Resource Management
 - Hiring & Terminations
 - Employee Relations
- Governance
 - CEO Succession planning
 - Director Succession planning
- Clinical Practices
 - Quality
 - Core Measures
 - Evidence Based
- Information Technology
 - Security
 - Disruptions
- Document Management

Common Healthcare External Risks



- Office of the Inspector General
- CMS
- State Health Department
- OSHA
- EPA
- Investors
- CCAC
- Litigators
- Past Employees
- HIPAA
- IRS
- Auditors
- Competition
- Integrity Program Contractors

Unknown Risks



God at His computer



CHANGE = RISK!!

People, Process, Tools, Regulations, etc.



Internal Controls

What is an internal control?



■ COSO Definition

- Internal control is a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories
 - Effectiveness and efficiency of operations
 - Reliability of financial reporting
 - Compliance with applicable laws and regulations

Control Elements



- Control environment – the tone of a company and its audit committee, which influences the control consciousness of its personnel
- Risk Assessment – from a financial reporting perspective, a company's assessment of its identification, analysis and management of risks relevant to the preparation of financial statements.
- Control Activities – the policies and procedures to ensure that the company's directives are carried out.
- Information and Communication – the company's information systems, which includes the accounting systems
- Monitoring – a process to assess whether controls are operating as intended and whether they are modified as appropriate for changes in conditions.

Types of Control



■ Preventive Controls

- Designed to prevent errors or irregularities before they have occurred.
- Examples:
 - Regular balancing and reconciling are completed by an individual independent of the transactions processed through the account.
 - Passwords and physical safeguards are established to restrict access to appropriate personnel.
 - Authorization and limits are established to ensure the appropriate oversight of significant transactions

■ Detective Controls

- Designed to detect errors or irregularities after they have occurred.
- Examples:
 - Exception reports are reviewed and cleared by persons with appropriate authority.
 - Systems maintenance reports are reviewed to ensure changes are completed properly and authorized.
 - Documentation reviews are completed to ensure files are complete.

Types of Control (continued)



■ Business Controls

- Can be preventive or detective
- Executed by people
- Examples:
 - Review and approve Expense Report

■ Application Controls

- Input: logic to prevent key errors in a system
- Process: controls that ensure that the operation methods are correct
- Output: controls that detect errors in processing of data

Risk Continuum & Internal Controls

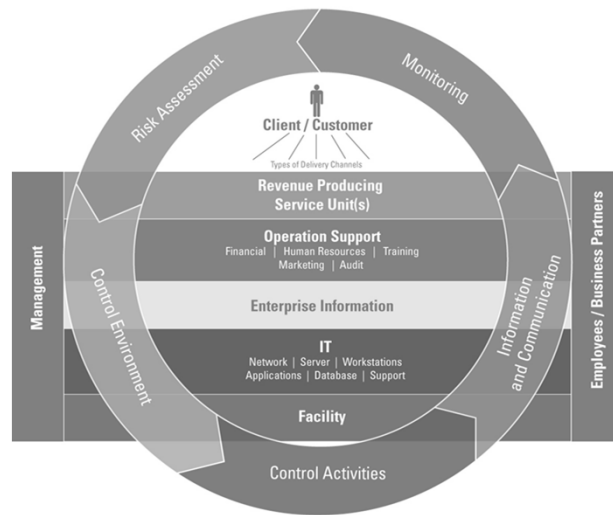


Risk Assessments



- Process of identifying, analyzing and managing risks relevant to objectives
- Consideration of the risk's significance, likelihood of occurrence and how they should be managed.
- Management may initiate plans, programs or actions to address risks or accept the risk due to cost or other considerations
- Elements to consider:
 - Changes in operating environment
 - New personnel
 - New or revamped information systems
 - Rapid growth
 - New technology
 - New lines, products or activities
 - Corporate restructuring
 - Accounting pronouncements

Risk Assessment Approach

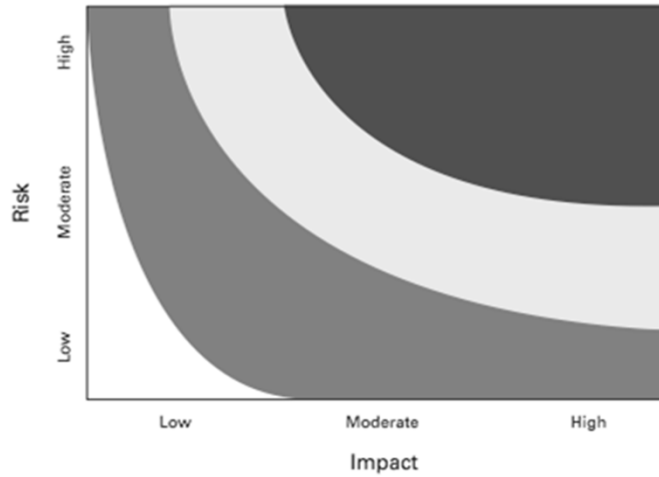


Risk Domains



- **Operational** – core business including systems and processes.
Example: outpatient care
- **Financial** – ability to earn, raise or access capital. Example:
bonds
- **Human** – recruiting, retention and managing workforce.
Example: worker's compensation
- **Strategic** – ability to grow and expand. Example: joint ventures
- **Legal/Regulatory** – statutory, regulatory compliance, licensure,
accreditation. Example: HIPAA, OSHA, JC
- **Technology** – biomedical & information technologies.
Example: CPOE

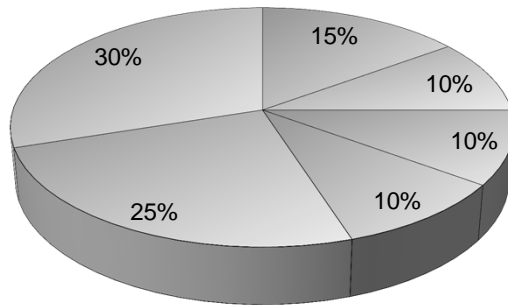
Risk Matrix



Internal Audit Work Plan Balance



Internal Audit Work Plan Percentage of Plan

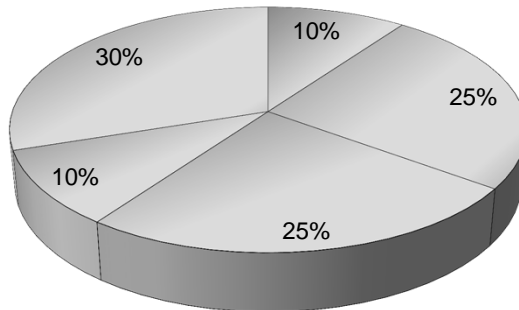


- Operational
- Financial
- Human Capital
- Strategic
- Legal/Regulatory
- Information Technology

Compliance Work Plan Balance



Compliance Work Plan Percentage of Plan



- Education
- Monitoring
- Investigative/Hotline
- Policies & Procedures
- Response

Things to Remember About Risk & Control



- Do not use the concepts of risk, control and governance to strangle the life out of an organization.
- Risk assessment and internal controls are tools.
 - Use them wisely and in a manner that supports the mission and vision of the organization.
 - Like the organizations served, these tools are as unique as they are similar.
- Internal controls should be balanced to the risk addressed.
- Internal controls are often better at keeping honest people honest than they are at preventing criminals.
- Don't expect to control all risks.

Contact Information



Kelly A. Nueske, CIA, CMA, CPA, CHC, RN
kelly.nueske@altegrahealth.com
(612) 730.7782