Larry's Cheat Sheet – Risk Assessment Basics

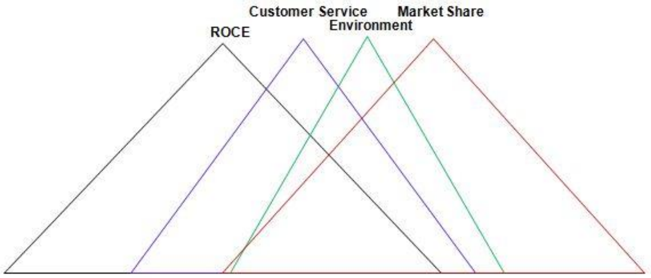
Definitions

Objective – Something an organization is trying to accomplish related to its mission, vision or values (VMV). Objective-setting is a control!
Risk - The uncertainty of an event occurring that could have a negative impact on the achievement of objectives. Risk is measured in terms of consequences/impact and probability/likelihood.
Response – Actions taken my management to either accept or alter the likelihood or impact of a risk. Risk responses are actually not part of the COSO internal control process.
Risk Assessment – 1. One component of both the COSO IC and ERM frameworks; 2. The method an internal audit department uses to develop their annual audit plan in order, or approach to an audit, to perform risk-based auditing. Risk assessment is a component, or type of, control!
Inherent Risk: A risk event that could occur in the absence of any actions management might take to alter either the risk's likelihood or impact.
Residual Risk: The risk that remains after management's responses to risks. If controls work perfectly, residual risks still exist. If a residual risk ever occurs, everyone second-guesses the risk taker's decisions.
Risk Management - A **process** to identify, assess and manage potential events or situations, to provide reasonable assurance regarding the achievement of the organization's objectives.
Enterprise Risk Management (ERM) and Internal Control are processes, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage controls and risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.
Moral hazard occurs when a party insulated from risk may behave differently than it would behave if it were fully exposed to the risk.

Risk Assessment for Management - Steps to follow, at each organization level:

1. Understand the environmental, or entity-level, controls
2. Identify risks to the Corporate VMV and Objectives
3. Prioritize business activities
4. For each important activity:
   - Identify the high-level process flow – 5 steps max
   - Identify process flow and non-process flow controls
   - Identify residual risk events
   - Compare controls to COSO components.
5. Test and evaluate activity-level controls (Auditors)
6. Test and evaluate entity-level controls (Auditors)

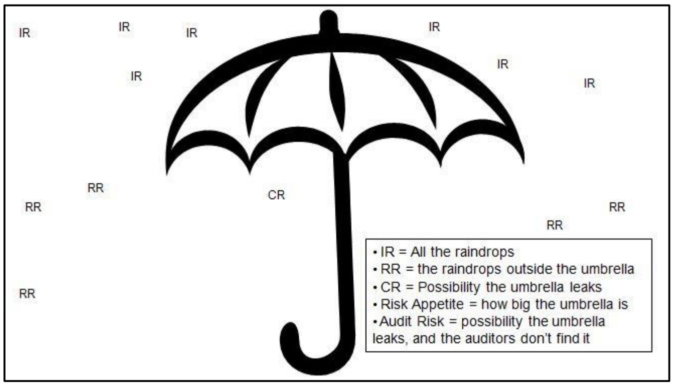
Objectives Flow Downward, and Collide



Process Flow Objectives (CAATSS) (if you must)
- Complete - Timely
- Authorized - Safeguarded
- Accurate - Segregation of Duties

Identify controls first, and then ask "What Else could go Wrong?" – a Residual Risk approach.

Risk Umbrella - Terminology


IR
IR
IR
IR
IR
IR
IR
RR
RR
CR
RR
RR
RR
• IR = All the raindrops
• RR = the raindrops outside the umbrella
• CR = Possibility the umbrella leaks
• Risk Appetite = how big the umbrella is
•Audit Risk = possibility the umbrella leaks, and the auditors don't find it

Objective-Setting Framework:

- Financial statement reliability
- Fiscal responsibility
- Customer service
- Product improvement
- Safeguarding assets
- Protecting the environment
- Preventing unintended exposure to risk
- Planning for the future
- Fraud prevention
- Business continuity
- Effectiveness and efficiency of operations
- Effectiveness and efficiency of process flows
- Compliance with laws, regulations and policies

Activities need objectives as controls (COSO Risk Assessment component). Link specific objectives to VMV: Vision (future way of accomplishing mission), Mission (purpose of company), Values (how to act while achieving mission). Ask "why do you want to do that" to move higher in objectives.

Risk Framework:

Internal

- Infrastructure (assets, capital, complexity…)
- Personnel (capability, fraud, judgment, safety …)
- Process (capacity, execution, dependencies…)
- Technology (data, availability, capacity, reliability…)

External

- Economic (credit, liquidity, market, capital availability…)
- Business (brand, fraud, competition, publicity…)
- Technological (external data, emerging technology…)
- Natural Environment (waste, energy, fire, natural disaster…)
- Political/Social (laws, regulations, demographics, change…)

Changes

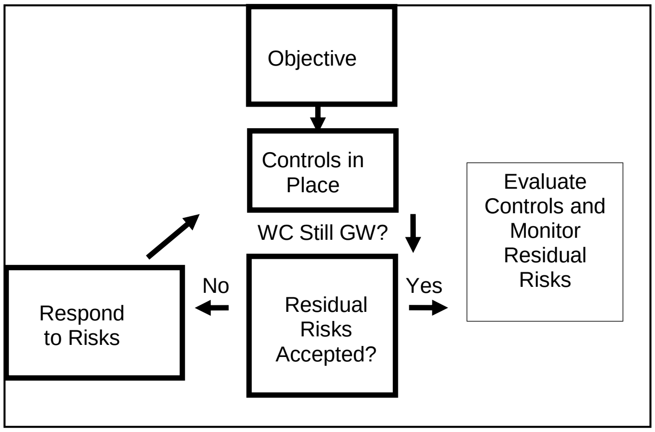
- Internal changes (people, processes, resources…)
- External changes (environment, competition, customers…)
- Voluntary changes (new products, opportunities…)
- Involuntary changes (laws, regulations, trends…)

Larry@LHubbard.com
In USA: (301) 529-8118
Larry Hubbard & Associates

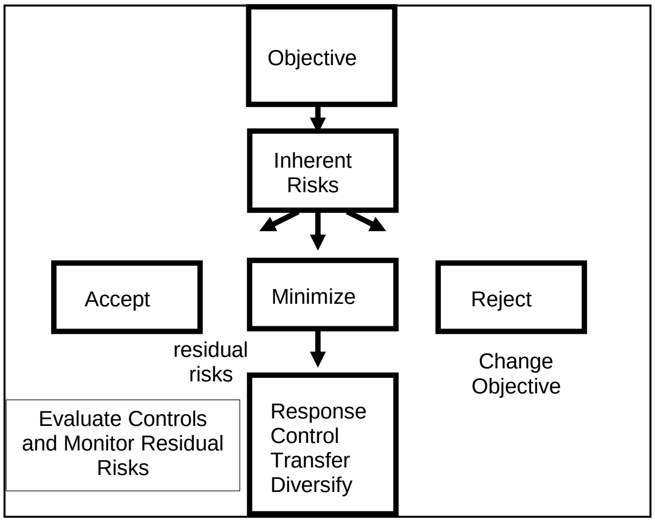
Larry's Cheat Sheet – Risk Assessment Basics

Risk Management Formulas

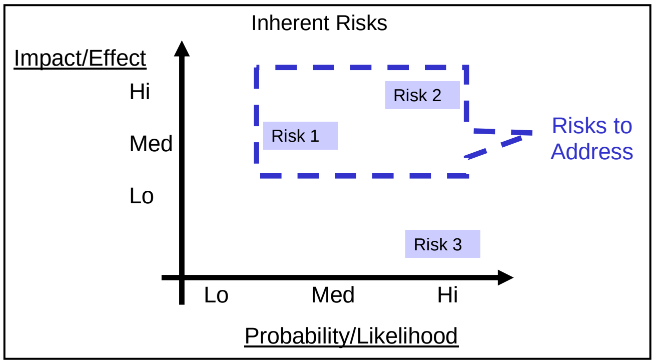
Best Way Most of Time → Residual Risks



Traditional Way – Good Theory → Inherent Risks


Objective
Inherent Risks
Accept
Minimize
Reject
residual risks
Change Objective
Evaluate Controls and Monitor Residual Risks
Response Control Transfer Diversify

Risk Mapping – It's about the Discussion!



Common Risk Assessment Errors:

- Don't confuse risk causes with risk impacts.
- A risk is different than an objective containing a "not".
- Controls that don't work are not "risks" – they are ineffective controls.
- Controls that are absent are not "risks" – there is a control design problem
- Existing problems are not the same thing as risks - Problem solving is different than risk assessment.

These are NOT risks:

- Poor training
- No segregation of duties
- Failing to approve a document
- A vault left unlocked
- Not maximizing market share
- No policies and procedures
- Lack of planning process

An "impact" is a result of a risk event occurring, or an objective not being met – it is not a risk.

Another error is saying management has no controls – there are always controls, but they may be called other things (ISO, TQM, BSC, Six Sigma, RACI, etc.)

Risk Assessment Tips and Thoughts:

- ERM is a management task; RA is a component of both COSO's IC and ERM frameworks and RA is also how IA selects audits to perform (confusing!)
- Objective-Risks-Control Alignment (ORCA) is only part of ERM and IC – the Risk Assessment components.
- Risk assessment starts with clarity of the objective.
- ERM and IC are all about achieving business objectives – not about the risks.
- Most organizations already do 80% of ERM – ERM is mostly a process of identifying existing controls, and determining how management knows those controls work as intended.
- Setting objectives is a control.
- You cannot flowchart risks – if you flowchart it, it is a process - just look for CAATSS controls over I PO, and then think about WCGW (What Could Go Wrong).
- Controls not working, instead of unknown risks, are what get organizations into real trouble.
- ERM and Internal Control are like opposite sides of the same coin.
- Real business problems are not on flowcharts.
- Most risk responses are part of I/T process flows.
- In Risk Assessment the discussion IS the value.
- Other efforts, like ISO, TQM, and BSC are also part of risk assessment, ERM, and internal controls.
- Be specific about risks – a generic list of risks is a starting point, not an end result.
- Don't spend time trying to predict the future – you cannot.
- Identify existing management controls first!
- Use an Inherent Risk approach to identify entity-level risks, and a Residual Risk approach to identify activity-level risks.
- A bad control environment yields too many risks to identify.
- Risk assessment is not about predicting the future.
- Don't spend too much time on "analytics" – spend time on discussions instead.
- Be sure and respond to known, obvious risks first.
- Most organizations have <u>no important residual risks</u>.

Larry@LHubbard.com
In USA: (301) 529-8118