Information Risk Management

Mick Atteberry

NebraskaCERT Conference 2006

What is Risk?

- *Risk* – An uncertain event or condition that, if it occurs, has an impact on a project's or business' objectives.
- *Threat* – Any circumstance or event with the potential to cause harm.
- *Vulnerability* – A weakness that makes a threat possible.
- *Exploit* – An action taken that harms an asset usually by taking advantage of a vulnerability or weakness.
- *Risk Assessment* – The act of identifying potential threats to and vulnerabilities in an information system or business process.
- *Risk Management* – The process of determining an acceptable level of risk, assessing the current level of risk, taking steps to reduce risk to the acceptable level, and maintaining that level of risk.

Information Risk Management (IRM)

> *Information risk management is a process designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.”*

Why IRM is Important

Underlying Principles:

- Every entity, whether for-profit or not, exists to realize value for its stakeholders.
- Value is created, preserved, or eroded by management decisions in all activities, from setting strategy to operating the enterprise day-to-day.

Why IRM is Important

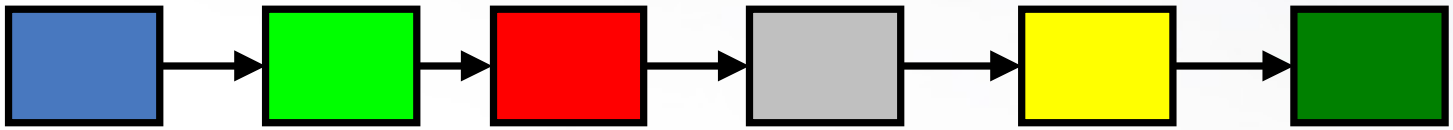
IRM supports value by enabling management to :

- Deal effectively with potential future events that create uncertainty.
- Respond in a manner that reduces the likelihood of downside outcomes and increases the upside.

The Value Chain

X # of revenue streams

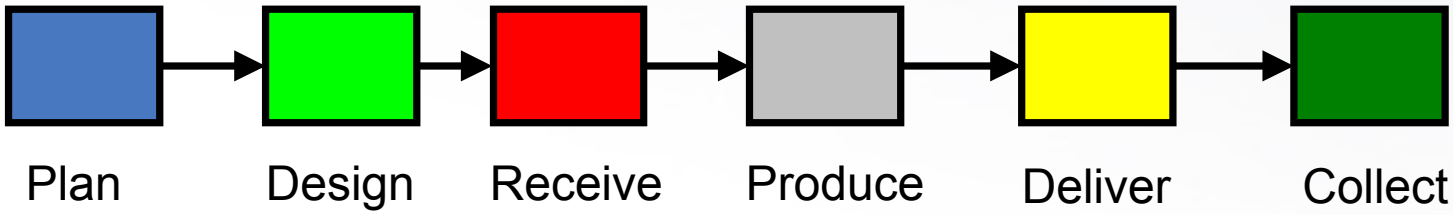
Dependent Processes



Dependent Processes

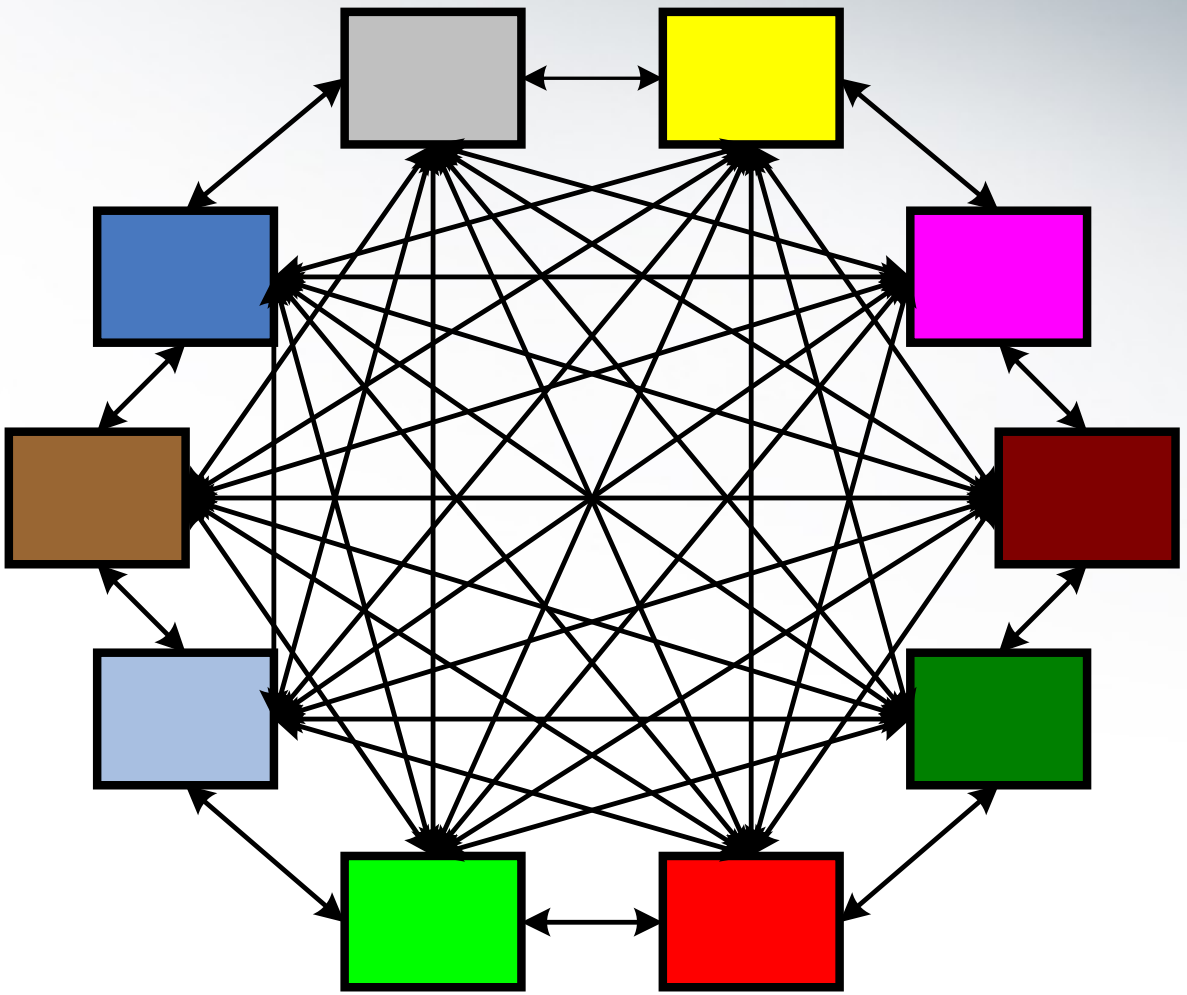
a primitive macro view example
for discussion

Sale



Revenue

Interdependent Processes



Value per Day

$$\frac{\text{Cash In}}{\text{\# Days}} = \$ \text{ per Day}$$

Corporation ~ Gross Revenue

Agency ~ Budget Allocation

12,000,000,000 / 365 = 32,876,712.33 / 24 = 1,369,863.01

Business Risk Exposure

$ per Day

\+ revenue growth

\- unexpected expenses

$ Adjusted

Objective Setting

- Is applied when management considers risk strategy in setting objectives.
- Forms the risk appetite of the entity — a high-level view of how much risk management is willing to accept.
- Risk tolerance, the acceptable level of variation around objectives, is aligned with risk appetite.

Event Identification

- Involves identifying those incidents occurring internally or externally, that could affect strategy and achievement of objectives.
- Think of the risk categories surrounding the asset – business processes, human, and technology (network, host, application).
- Map the actual data flow; identify failure points.
- Document risks, threats and vulnerabilities on a Risk Profile.

Information Identification

- Identify information categories and the dependent information system and business process.
- Information types:
  - Financial — Sarbanes-Oxley Mandate
  - Private — Laws and Regulations
  - Operational — Performance and efficiency
  - Trade Secret — Product Design

Issues List for Discussion

	Issue	Effect	Action
01	Financial	Integrity of financial reporting has a direct relationship to the public's perception of value	Maintain adequate controls to assure integrity. Use the CoBIT framework as an input.
02		Premature release of financial information can lead to negative public perception	Restrict access to financial reporting data with appropriate release reviews
03	Private	Inadvertant release of private information can lead to violation of state or national laws on privacy resulting in unexpected expenses	Restrict access to private data. Review business processes for the flow of information and identify the multitude of systems where the data is stored.
04		Individual perceptions to the definitions of privacy can lead to conflicts and discussion.	Clearly state the entities direction in the control of private information.
05	Operational	Availability of information is key to successful execution of dependent business processes; failure to deliver can lead to process failure.	Maintain system design, implementation, and maintenance controls to meet availability targets.
06			
07	Trade Secrets	Loss of trade secrets can lead to unfair competition or counterfit products that take market share away from the owner.	Maintain adequate controls to assure confidentiality and release of trade secret information.
08			
09			
10			

Risk Assessment

- Determine the impact to the business in terms of high, medium and low
  - Exposure / Damage potential
  - Cost (in both time and dollars) / Value
  - Affected users (internal & external)
- Determine the probability of occurrence in terms of high, medium and low
  - The likelihood a threat will be realized or a vulnerability will be exploited with a limited timeframe (year).

- Risk = Impact X Probability

Impact vs. Probability

IMPACT	Low Probability	High Probability
High	*Medium Risk* ***Share***	*High Risk* ***Mitigate & Control***
Low	*Low Risk* ***Accept***	*Medium Risk* ***Control***

PROBABILITY

Security Risk Decision Matrix

Probability options

- Extremely Low
- Necessary
- Acceptable
- High

Risk Response

- Identifies and evaluates possible responses to risk.
- Evaluates options in relation to entity's risk appetite, cost vs. benefit of potential risk responses, and degree to which a response will reduce impact and/or likelihood.
- Selects and executes response based on evaluation of the portfolio of risks and responses.

Risk Response

- Decide on a Mitigation Plan
  - Controls or safeguards that will
    - reduce the likelihood of occurrence,
    - decrease the impact, or
    - minimize the risk.
  - May include accepting the risk

Why ERM is Important

Information risk management provides enhanced capabilities to:

- Align risk appetite and strategy
- Link growth, risk, and return
- Enhance risk response decisions
- Minimize operational surprises and losses
- Identify and manage cross-enterprise risks
- Provide integrated responses to multiple risks
- Seize opportunities for investment
- Rationalize capital expenditures

War Stories

Examples of Information Risk Management in action

Questions?

Mick Atteberry

mick.atteberry@conagrafoods.com

402-577-3846