Security Risk Management

Linking Security to Business

Mick Atteberry

Ron Woerner

NebraskaCERT Conference
2005

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.

Enterprise Risk Management (ERM)

“Enterprise risk management is a process, 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 risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.”

Source: COSO *Enterprise Risk Management – Integrated Framework*, 2004

Why ERM 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.

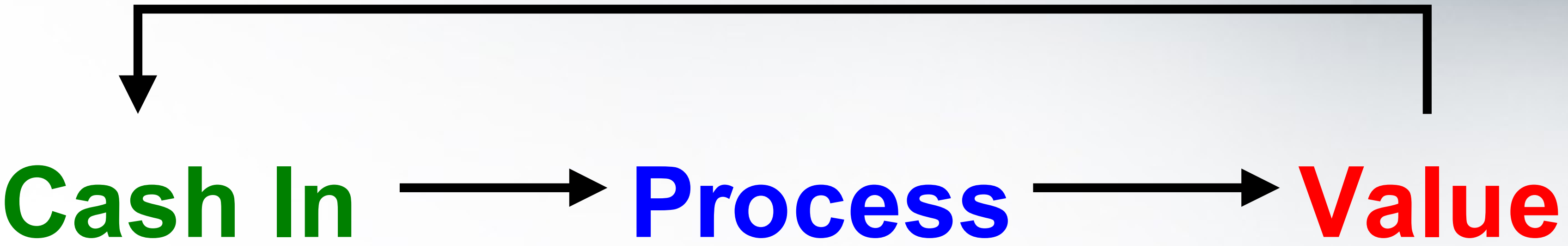
ConAgra Foods®

Why ERM is Important

ERM supports value creation 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.

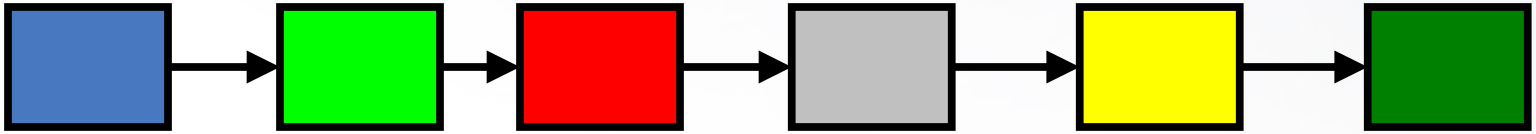
The Value Chain



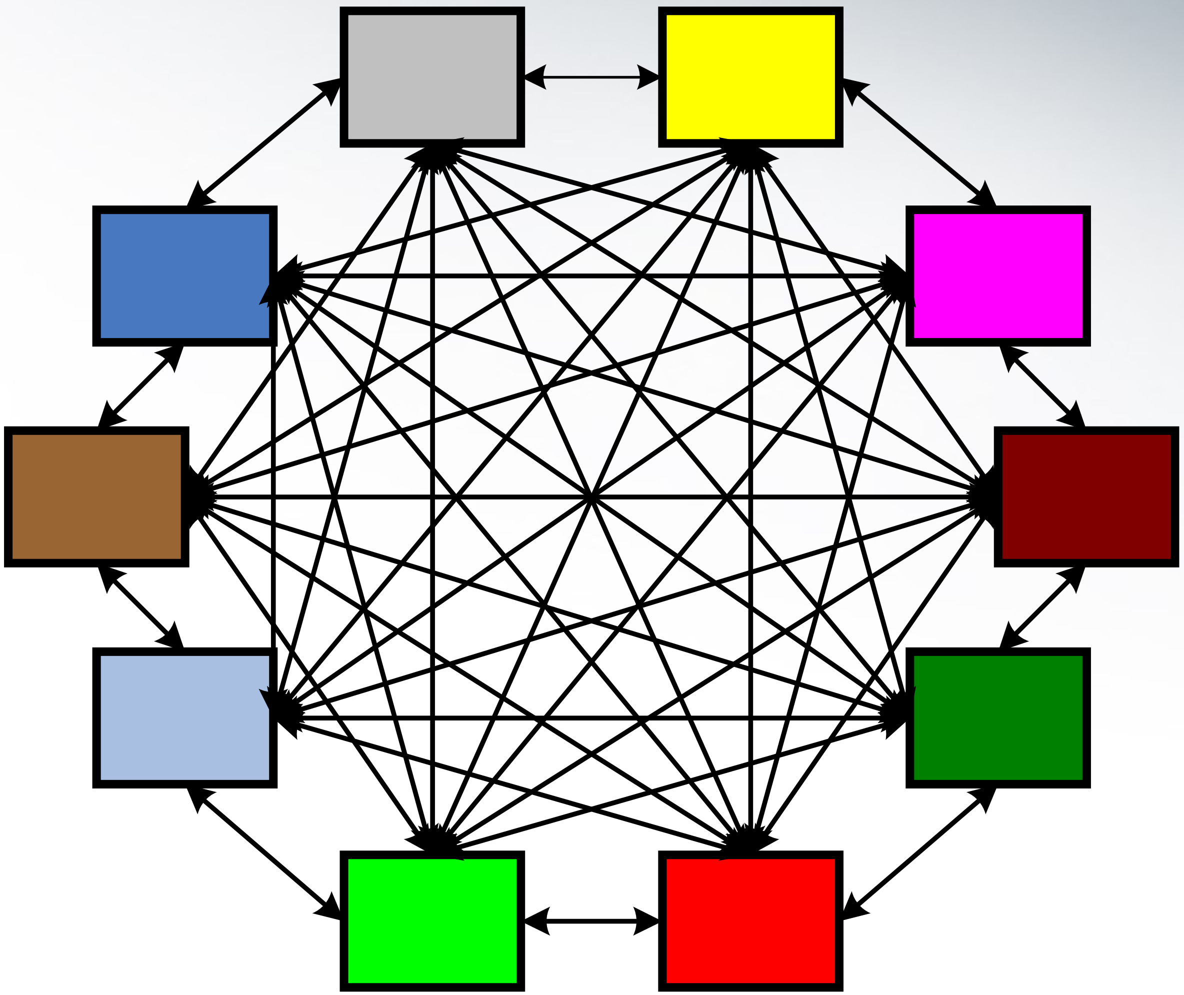
Cash In → Process → Value

X # of revenue streams

Dependent Processes



Interdependent Processes



ConAgra Foods®

Value per Day

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

Corporation ~ Gross Revenue

Agency ~ Budget Allocation

Business Risk Exposure

$ per Day

+ revenue growth

- unexpected expenses

$ Adjusted

Objective Setting

- Is applied when management considers risks strategy in the setting of objectives.

- Forms the risk appetite of the entity — a high-level view of how much risk management and the board are 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.
- Requires ongoing identification, evaluation and use of “what-if” and “worst-case” scenarios.
- Think of all the risk categories surrounding the asset – business processes, human, and technology (network, host, application).
- Identify trust boundaries, data flow and entry points. (How will the threat be realized?)
- Document risks, threats and vulnerabilities on the Risk Profile.

Event Identification

- Identify potential threats to and vulnerabilities in the information system or business process.
- Threat types:

Natural Disasters	System Failures	Human Error
Unauthorized Insiders	Former Employees	Competitors
Hackers	Cybercrime	Social Engineering
Virus / Worms	Spyware / malware	Trojan Horse
Spoofing / Repudiation	Tampering	Denial of Service

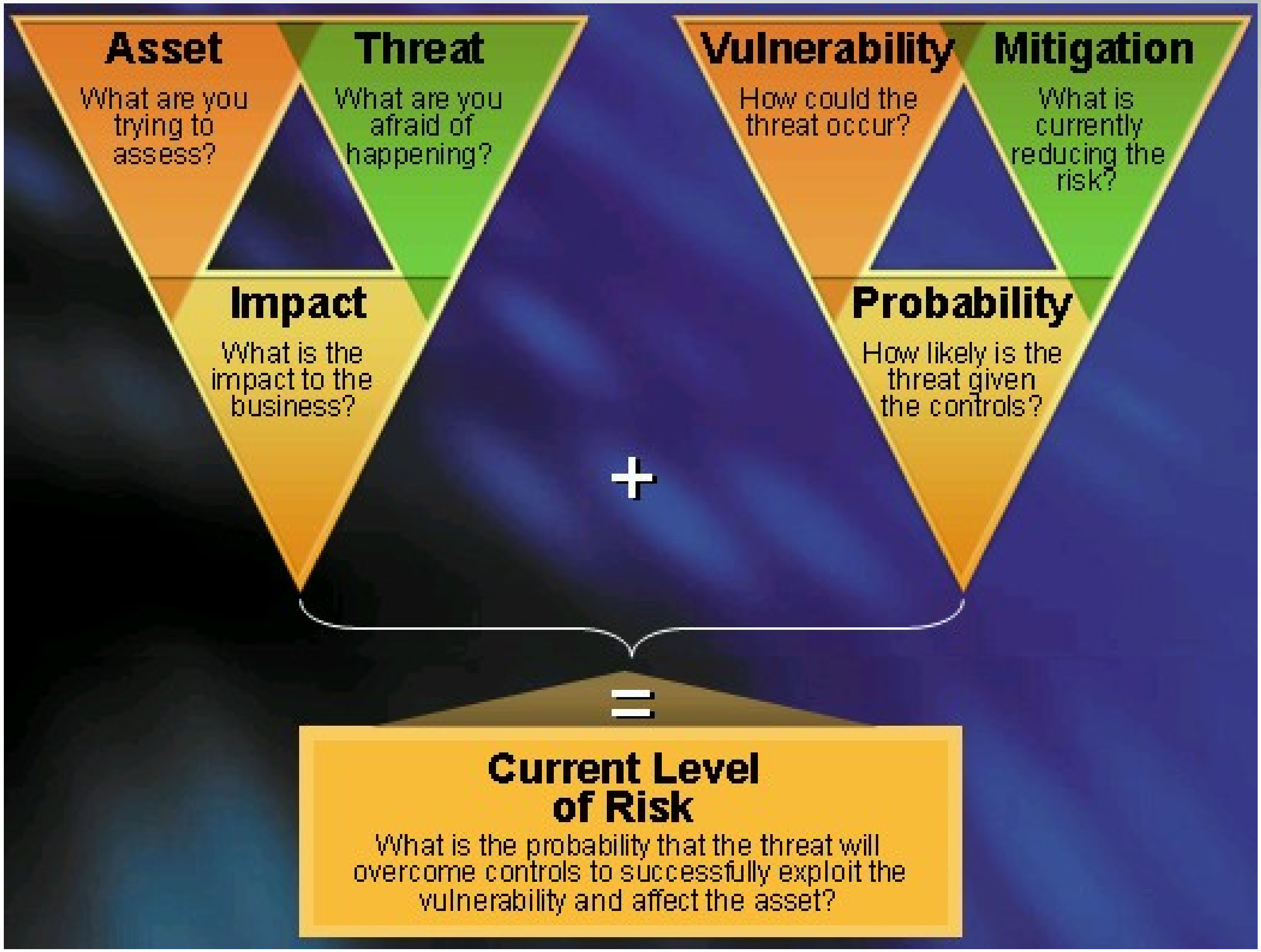
Risk Assessment

- 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

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

Components of Risk Assessment



Asset

What are you trying to assess?

Threat

What are you afraid of happening?

Vulnerability

How could the threat occur?

Mitigation

What is currently reducing the risk?

Impact

What is the impact to the business?

Probability

How likely is the threat given the controls?

+

=

Current Level of Risk

What is the probability that the threat will overcome controls to successfully exploit the vulnerability and affect the asset?

ConAgra Foods®

Security Risk Decision Matrix

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.

ConAgra Foods®

Risk Response

- Decide on a Mitigation Plan
  - Controls or safeguards that will lower the likelihood of occurrence, decrease the impact or minimize the risk.
  - May include accepting the risk
- Control / Safeguard types:

Policies / Standards	Procedures / Processes	Awareness / Training
Host / Network Defenses	Incident Detection	Logging / Auditing
Access Control	Password Protection	Encryption
Backup & Recovery	Patch Application	Security Software

Why ERM is Important

Enterprise 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
- Rationalize capital

War Stories

Examples of Risk Management in action

Resources

- ASIS International, *General Security Risk Assessment Guideline*, 2003.
- BITS, Kalculator: Key Risk Measurement Tool for Information Security Operational Risks, 2004,
- Berinato, Scott, “Enterprise Risk Management,” *CIO Magazine*, November 1, 2004, pp. 46-58, http://www.cio.com/archive/110104/risk.html
- Bernstein, Peter L., Against the Gods: The Remarkable Story of Risk, John Wiley & Sons, 1998.
- COSO (Committee of Sponsoring Organizations of the Treadway Commission), *Enterprise Risk Management – Integrated Framework*, September 2004, http://www.coso.org/
- Microsoft Corporation, *The Security Risk Management Guide*, 2004, http://www.microsoft.com/technet/security/guidance/secrisk/default.m
- Risk Management FAQ, Carnegie-Mellon Software Engineering Institute, http://www.sei.cmu.edu/programs/sepm/risk/risk.faq.html

ConAgra Foods®

Questions?

Mick Atteberry
mick.atteberry@conagrafoods.com
402-577-3846

Ron Woerner
ron.woerner@conagrafoods.com
402-577-3844