Risk Management

Prepared by: John D. Hernandez, CIA

Director of Internal Audit, Fred Hutch

Updated: September, 2017

Risk Management

Because … (PG version) “STUFF HAPPENS”

Risk Management

Because … (PG version) “STUFF HAPPENS”

Hint:
“Stuff” does NOT just “happen”!!!

Everyday Risk Management

- Do you check traffic before you cross a street?

Everyday Risk Management

- Do you check traffic before you cross a street?
- Do you adjust your driving in bad weather?

Everyday Risk Management

- Do you check traffic before you cross a street?
- Do you adjust your driving in bad weather?
- What steps do you take to ensure you don't burn yourself with a cup of hot coffee?

Everyday Risk Management

- Do you check traffic before you cross a street?
- Do you adjust your driving in bad weather?
- What steps do you take to ensure you don't burn yourself with a cup of hot coffee?
- Do you make sure your child is secure in his/her safety seat before you get behind the wheel?

Everyday Risk Management

- Do you check traffic before you cross a street?
- Do you adjust your driving in bad weather?
- What steps do you take to ensure you don't burn yourself with a cup of hot coffee?
- Do you make sure your child is secure in his/her safety seat before you get behind the wheel?
- Do you have insurance of any kind?

Everyday Risk Management

- Do you check traffic before you cross a street?
- Do you adjust your driving in bad weather?
- What steps do you take to ensure you don't burn yourself with a cup of hot coffee?
- Do you make sure your child is secure in his/her safety seat before you get behind the wheel?
- Do you have insurance of any kind?

We all "manage risk" everyday!

What is risk management?

Risk:

1: **possibility of loss or injury: peril**

2: **someone or something that creates or suggests a hazard**

3 a: the chance of loss or the perils to the subject matter of an insurance contract; *also* **:** the degree of probability of such loss **b:** a person or thing that is a specified hazard to an insurer **c:** an insurance hazard from a specified cause or source <*flood risk*>

4: the chance that an investment (as a stock or commodity) will lose value

Management:

1: the act or art of managing**:** the conducting or supervising of something (as a business)

2: **judicious use of means to accomplish an end**

3: the collective body of those who manage or direct an enterprise

So what is “risk management” for your enterprise?

Enterprise Risk Management

"… 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 risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."

Source: COSO Enterprise Risk Management – Integrated Framework. 2004. COSO.

Enterprise Risk Management

"… 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 risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."

Source: COSO Enterprise Risk Management – Integrated Framework. 2004. COSO.

This is what happens when definitions are created by committees of experts and consultants!

So … consider …

Enterprise Risk Management

A more useful and practical definition:

- A process in which everyone in the organization has a role
- That identifies events that may adversely affect the organization
- Provides reasonable assurance that risks are mitigated to an acceptable level

Let's spend a little time on that last one first!

Prerequisites for Effective Risk Management

"And provides **reasonable assurance** that risks are **mitigated** to an **acceptable level**"

Prerequisites for Effective Risk Management

"And provides **reasonable assurance** that risks are **mitigated** to an **acceptable level**"

- "Reasonable assurance" is NOT "absolute assurance" - absolute assurance is NOT the goal, and can not (practically) be achieved

Prerequisites for Effective Risk Management

"And provides **reasonable assurance** that risks are **mitigated** to an **acceptable level**"

- "Reasonable assurance" is NOT "absolute assurance" - absolute assurance is NOT the goal, and can not (practically) be achieved
- "Mitigated" does NOT mean "eliminated" – we take risks

Prerequisites for Effective Risk Management

"And provides **reasonable assurance** that risks are **mitigated** to an **acceptable level**"

- "Reasonable assurance" is NOT "absolute assurance" - absolute assurance is NOT the goal, and can not (practically) be achieved
- "Mitigated" does NOT mean "eliminated" – we take risks
- "Acceptable level" is subjective and implies we all know our "risk appetite" or "risk tolerance"
  - Board of Directors / Trustees / Regents
  - Senior management
  - Front line management
  - Every employee

Types of Risk

Strategic – A threat to the ability to achieve a strategic objective

Financial – Inadequate financing, erroneous financial reporting, financial fraud

Compliance – A failure to comply with federal, state, and local laws, terms of federal and non-federal sponsored awards, other contracts, etc. etc.

Operational – Ineffective or inefficient execution of day to day operations

- Potential to impact the organization's ability to achieve its objectives

- May also have an affect on its reputation
  - Do not underestimate the IMPACT of reputational damage!!!

Identifying and Evaluating Risk

- Identifying risk – understanding your operation
  - Chances are you know risks when you see them
  - But you must be able to anticipate them

Identifying and Evaluating Risk

- Identifying risk – understanding your operation
  - Chances are you know risks when you see them
  - But you must be able to anticipate them

- Evaluating risk – applying a technique
  - Impact – What will happen if this risk is realized?
  - Likelihood – How likely is it this risk will occur?

- Inherent risk vs. residual risk

Evaluation Approach

Standard approach

- Assign a value to each risk using some type of scale
- Determine relative importance of individual risks

Pro ejemplo:

Impact – Min - max values

- 1 - risks which have negligible impact
- 10 - those with truly catastrophic impacts

Likelihood – Min - max values

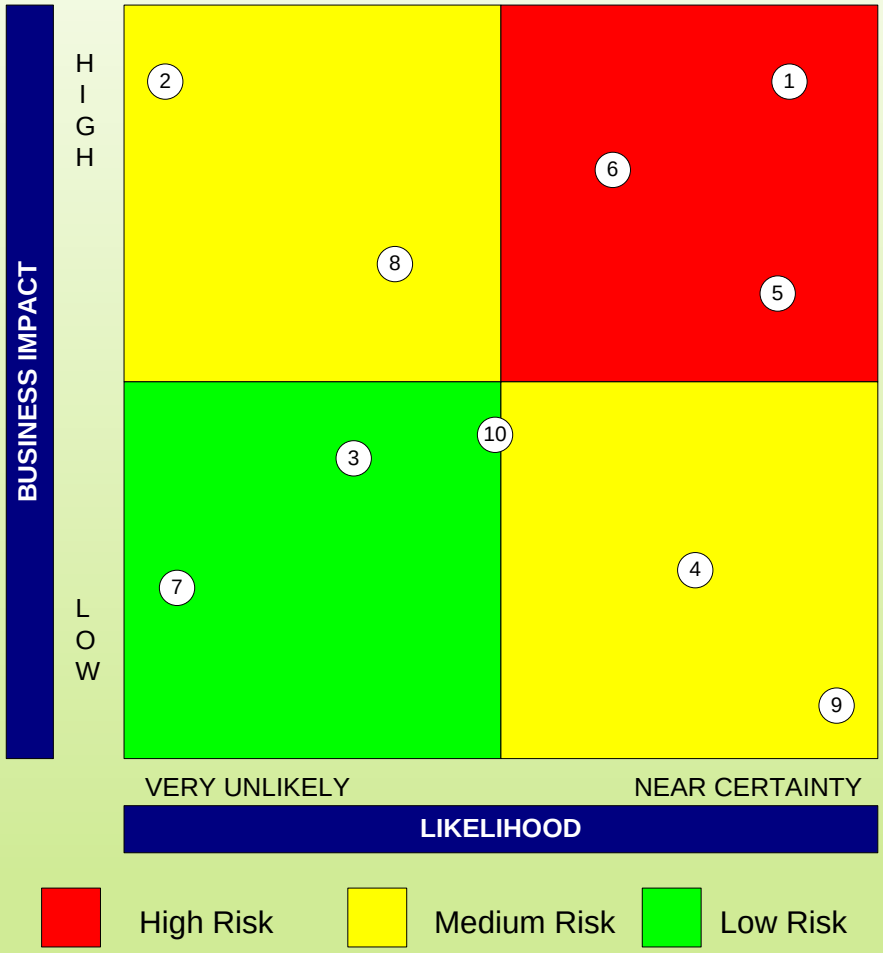
- 1 - risks which are highly unlikely to ever happen
- 10 - those which are almost certain to happen

Prioritizing Risks

Plot the results on a “heat map”. Your results might look like this. Some quick conclusions can be drawn:

1. Risks 1, 5, and 6 are all likely to occur and have a serious impact when they do occur.

2. Risks 3 and 7 are neither likely to occur nor are their impacts significant if/when they do occur.



Mitigating Risks

"Risk mitigation" processes and controls are like brakes on a car.

The brakes on your car allow you to _____.

Mitigating Risks

"Risk mitigation" processes and controls are like brakes on a car.

The brakes on your car allow you to _____

a) Bring the car to a stop

Mitigating Risks

"Risk mitigation" processes and controls are like brakes on a car.

The brakes on your car allow you to _____

a) Bring the car to a stop

b) Drive as fast as conditions and limits allow

Mitigating Risks

"Risk mitigation" processes and controls are like brakes on a car.

The brakes on your car allow you to _____.

a) Bring the car to a stop

b) Drive as fast as conditions and limits allow

c) Both of the above

Mitigating Risks

"Risk mitigation" processes and controls are like brakes on a car.

The brakes on your car allow you to _____.

a) Bring the car to a stop

b) Drive as fast as conditions and limits allow

c) Both of the above

Well designed controls are not "bureaucracy" or "red tape". They are essential enablers to:

- Stop or avoid an activity that is deemed too risky,

Mitigating Risks

"Risk mitigation" processes and controls are like brakes on a car.

The brakes on your car allow you to _____.

a) Bring the car to a stop

b) Drive as fast as conditions and limits allow

c) Both of the above

Well designed controls are not "bureaucracy" or "red tape". They are essential enablers to:

- Stop or avoid an activity that is deemed too risky,
- While proceeding in a controlled and judicious manner to your goals

Mitigating Risks

"Risk mitigation" processes and controls are like brakes on a car.

The brakes on your car allow you to _____.

a) Bring the car to a stop

b) Drive as fast as conditions and limits allow

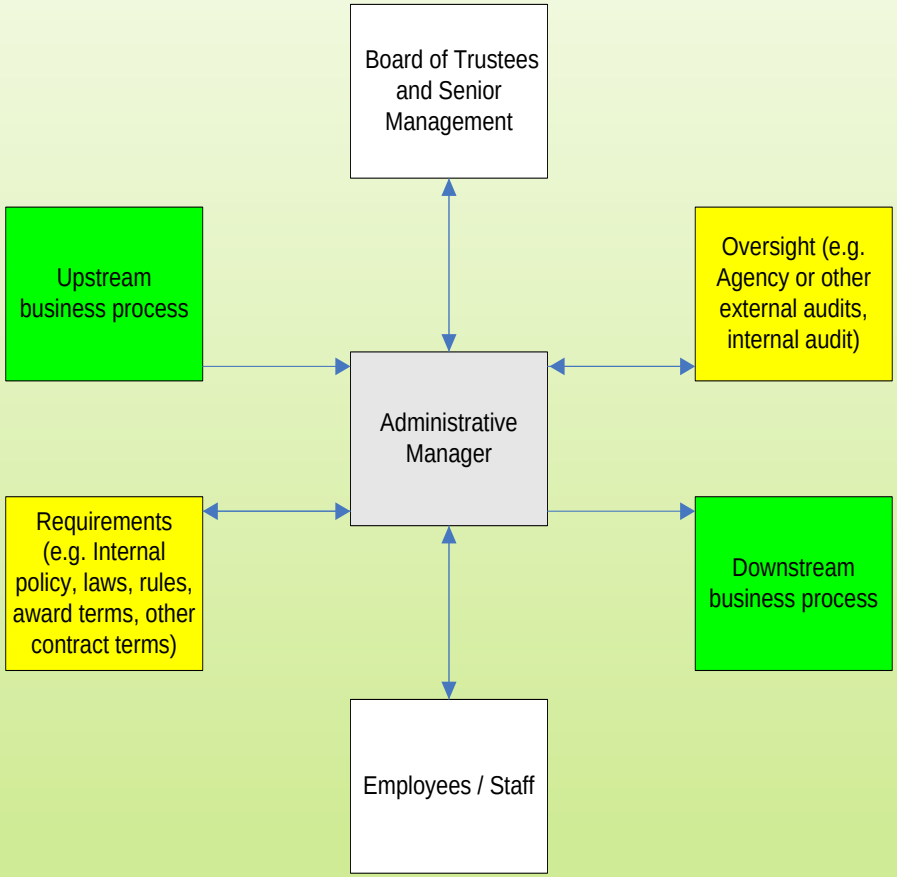
c) Both of the above

Well designed controls are not "bureaucracy" or "red tape". They are essential enablers to:

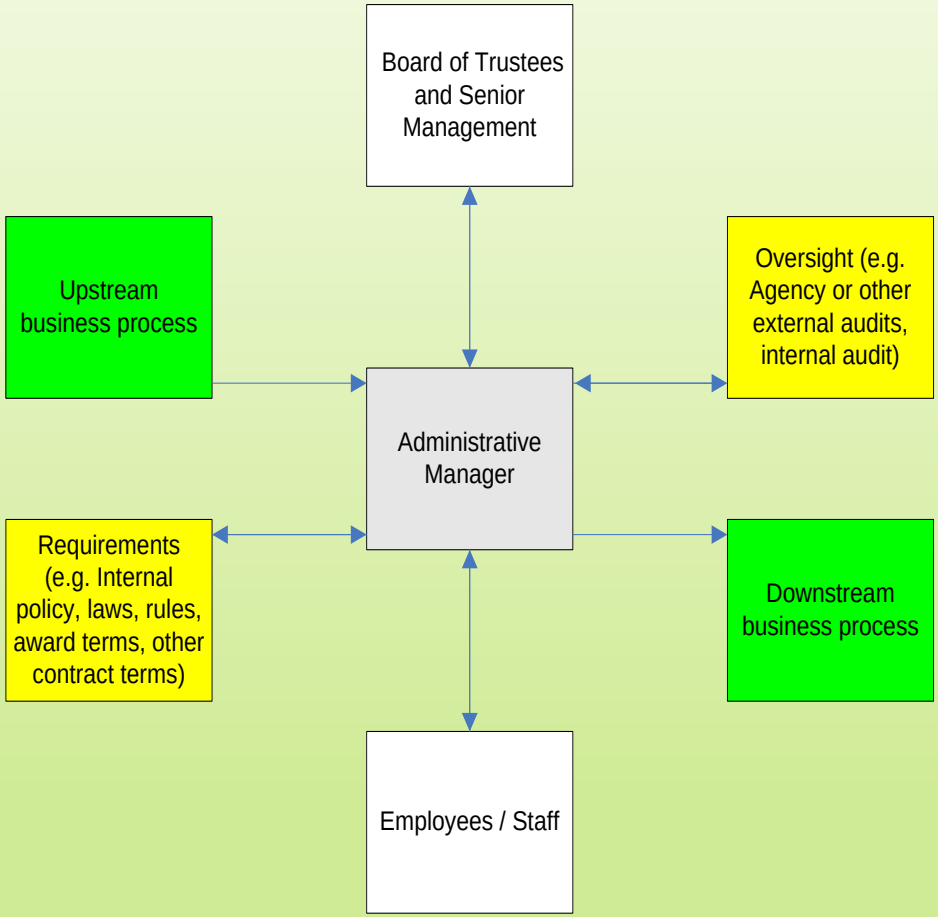
- Stop or avoid an activity that is deemed too risky,
- While proceeding in a controlled and judicious manner to your goals
- At the maximum safe speed .. .within the law, of course!

Mitigating Risks

Starts with **communication**



Mitigating Risks



These discussions MUST happen regularly:

1. Does everyone agree the impact or likelihood is as small or as large as I think it is?
2. BTW, something with virtually no financial impact could seriously impact reputation.
3. How will I know if I have mitigated a risk to an acceptable level?
4. Do I know what is expected of me and my department / staff?
5. If I do not have complete control over managing a risk, where do I turn?
6. Something can be unlikely in the short term but a near certainty in the long term - how should I treat that sort of event?
7. Are there other factors to consider?

Mitigation Strategies

Some ways to mitigate risk:

1. **Transfer/share** the risk – e.g. insurance, outsourcing, strategic partnering/alliances
2. **Reduce the likelihood** of risk occurrence – e.g. business process improvements, documentation, training and cross training, compliance awareness
3. **Reduce the impact** of risk occurrence – e.g. contingency planning, contractual language, public and governmental relations activities
4. **Avoid the risk** – e.g. "adverse events" practices re: clinical trials
5. **Accept the risk** – e.g. almost everything we do, but with full knowledge and reasonable / appropriate controls
6. **Combination** – e.g. fire extinguishers, alarms, CPR training for employees, fire drills … but we still buy insurance!

Mitigation Strategies

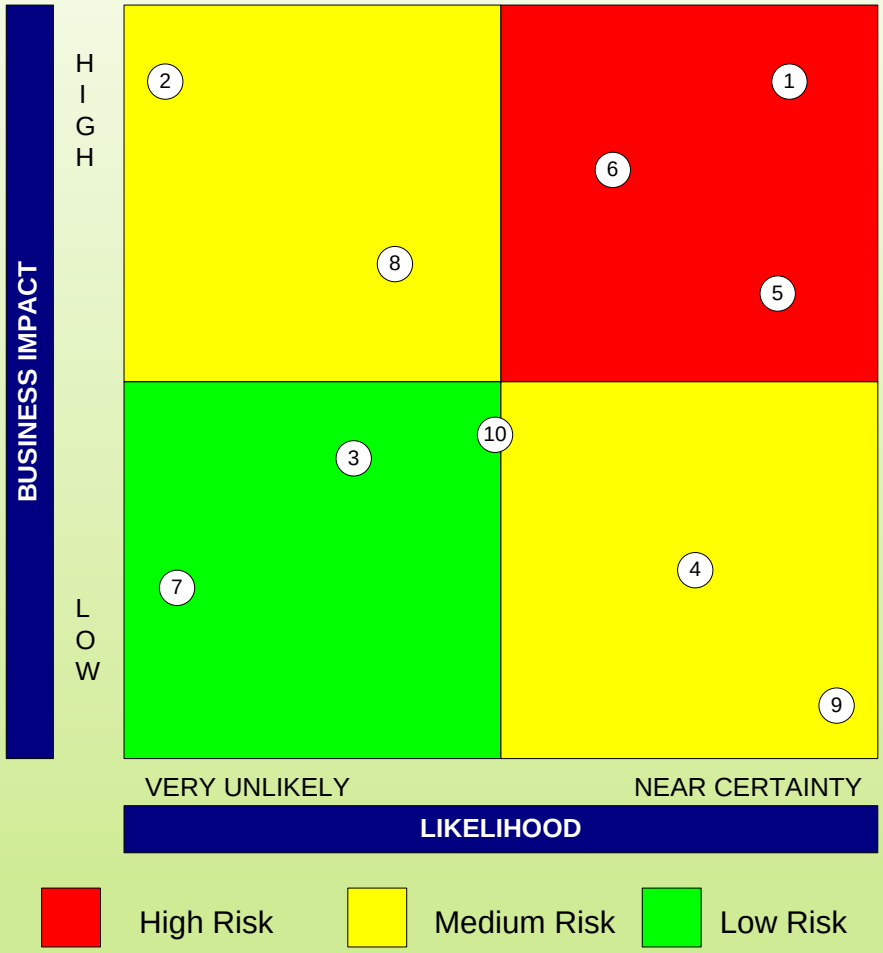
So back to our “heat map” …

What should be done, assuming avoidance is not possible or desirable?

Risks 1, 5, and 6 – **Mitigate and control**. Strong controls, regular oversight, lots of attention and resources

Risks 3 and 7 – **Accept**. Limited controls, limited oversight, little day to day attention, few resources

Risks 2, 4, 8, 9, and 10 – **Share or control**. These are the ones that require discussion. Share items 2 and 8? Control 4, 9 and 10? How? At what level? What is “acceptable” risk level?



What is an Effective Control?

- Ensures that a significant adverse event
  - Is detected on a timely basis
  - Is evaluated and corrected on a timely basis
  - As people perform their normal job functions
  - Cost is less than the risk of not having the control

  - Remember:

    Do not ignore the risk to reputation!!!

Prioritize, Prioritize, Prioritize

- It is **NOT** sufficient to do things right the first time
- You must do the **RIGHT THINGS** right the first time
- What risks should you be working on?
- More importantly, how do you know … ???

Summary

"Stuff" does not just "happen"

- Stuff gets done
- Stuff gets neglected
- Stuff is allowed to happen

- So when "stuff" does "happen" …

Will you be ready?

Summary

Effective Enterprise Risk Management (ERM)

- Requires constant communication … with everyone!
- Has highly subjective components
- Requires prioritization
- Affects how scarce resources are allocated
- Requires new strategies as conditions change

ERM … IS EVERYONE'S JOB !!!

Questions ?

John D. Hernandez, CIA

Director of Internal Audit

Phone: 206-667-5824

E-mail: jhernand@fredhutch.org