

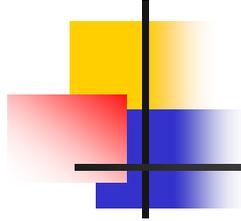


NISTy Business

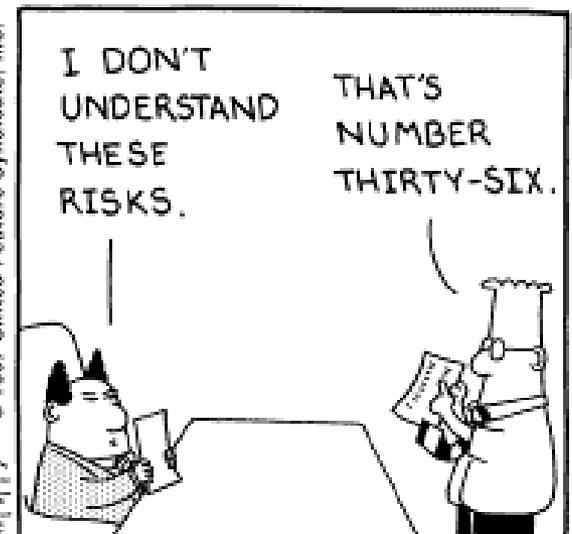




Poor Communication of Risk



How to Communicate Risk?



Copyright © 1997 United Feature Syndicate, Inc.
Redistribution in whole or in part prohibited



Management Relates To:

- Ensure Business Continuity
- Calculate Risk For Critical Assets
- Improve Security
- Maintain Regulatory Compliance

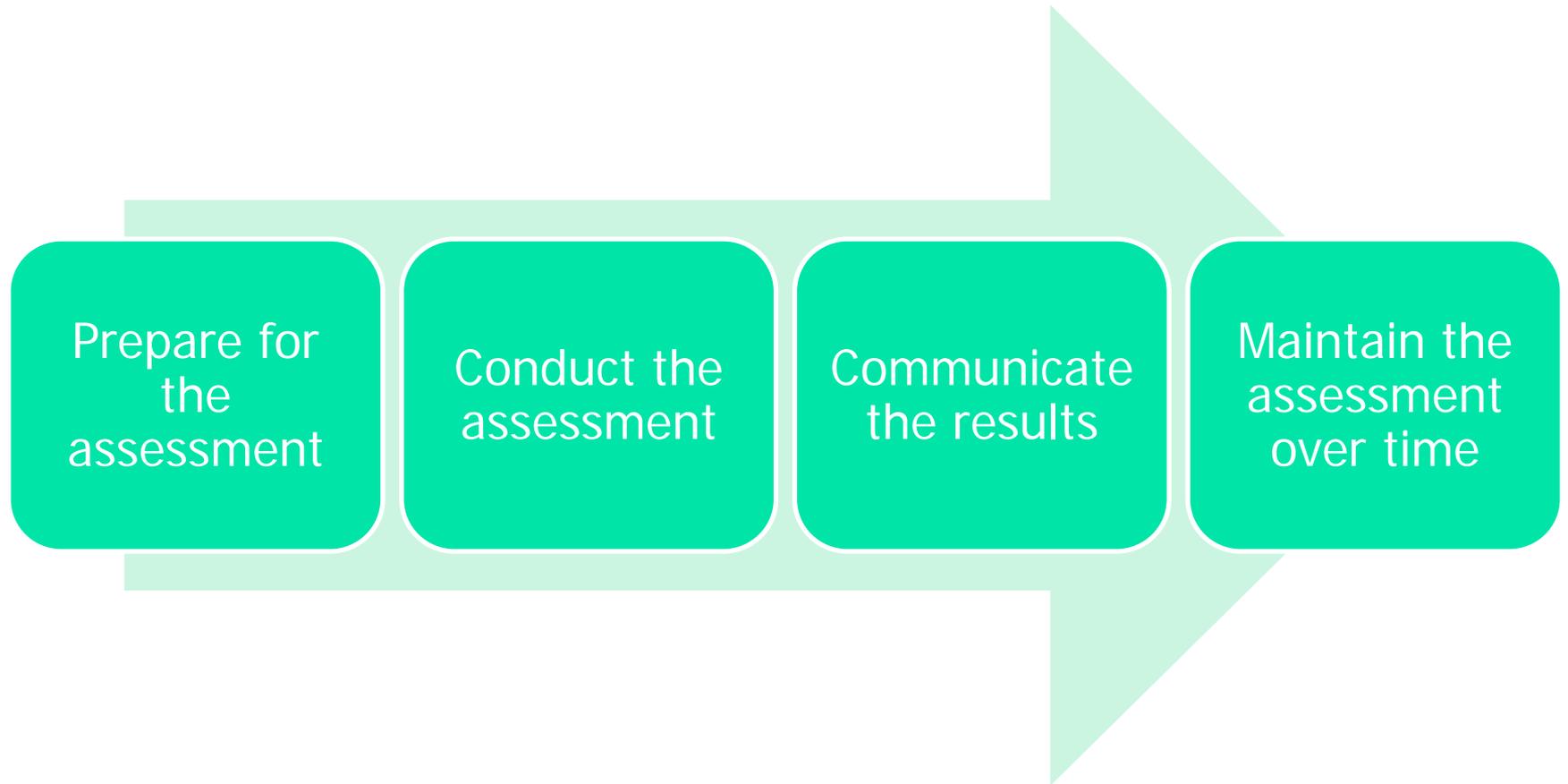


Managing risk (NIST)





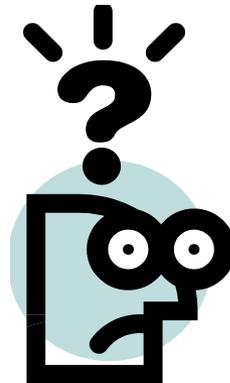
Assess risk





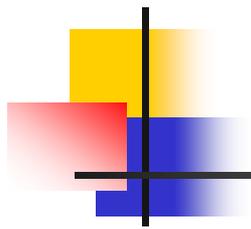
Prepare for the assessment

- Identify purpose & scope
 - What is your system trying to accomplish?
 - Must be aligned with a business objective
 - Allows you to focus on what Assets really need to be protected
 - Repeat: Pick objectives that are important to management





Example





Threats and Vulnerabilities

- Threat \neq Vulnerability
- Threat Assessment \neq Vulnerability Assessment \neq Risk Assessment
- Vulnerability Management \neq Risk Management



Conduct the risk assessment

- Identify or determine
 - Threat
 - Vulnerability
 - Effect
 - Likelihood
 - Risk
 - Uncertainty



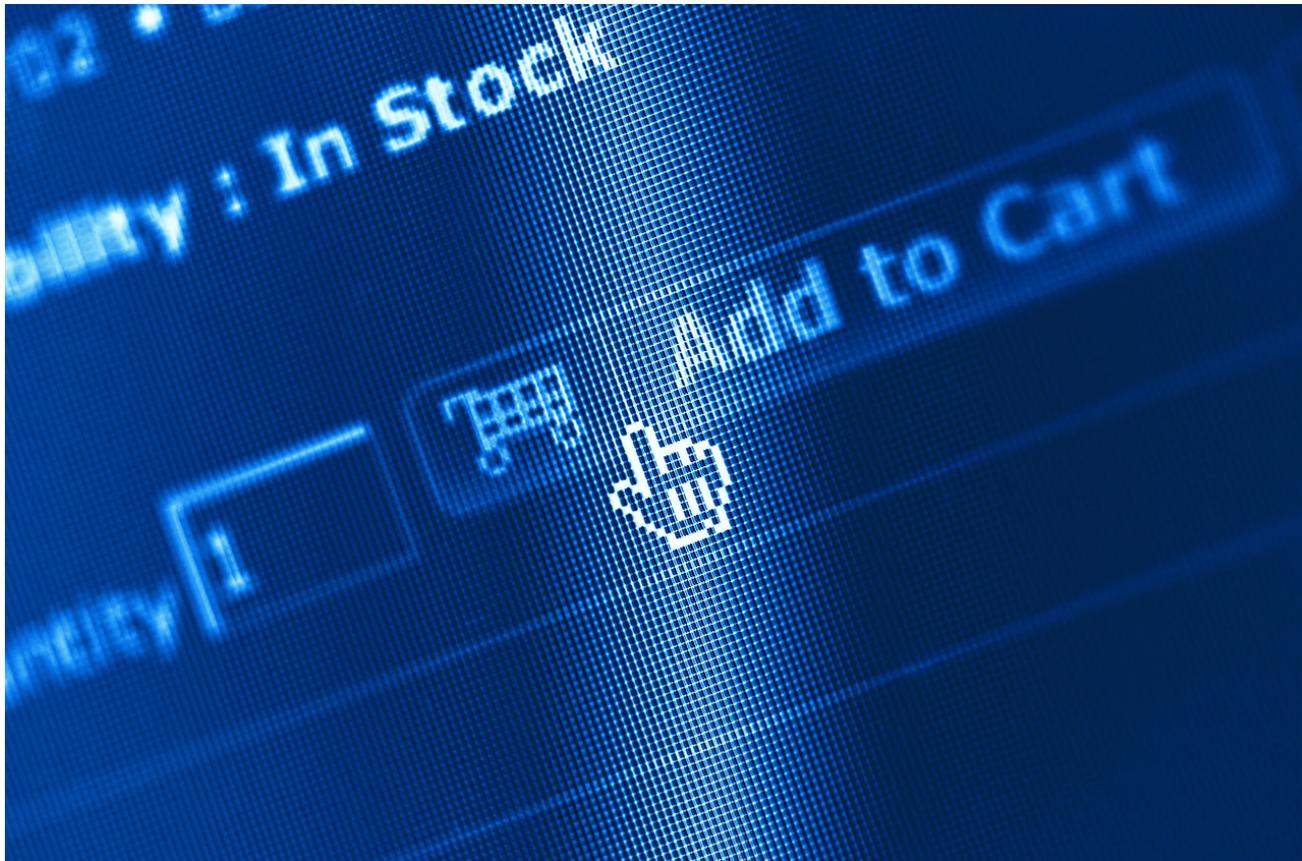
Example

- Threat
- Vulnerability
- Effect
- Likelihood
- Uncertainty





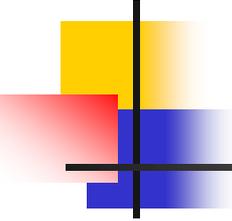
eCommerce example



Adversarial threat sources & events

- Consider:
 - Capability
 - Intent
 - Targeting





Adversarial Threat Sources

<i>Threat Source</i>	<i>In Scope</i>	<i>Capability</i>	<i>Intent</i>	<i>Targeting</i>
Insider attack	Yes	High	High	High
External individual attack	Yes	Medium	Medium	Medium
Other organization attack	Yes	Medium	Medium	High



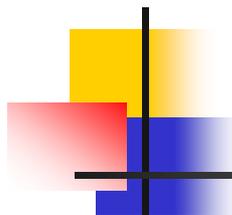
Identify Non-adversarial threat sources & events

- Accidents, acts of God, etc





Identification of Threat Events

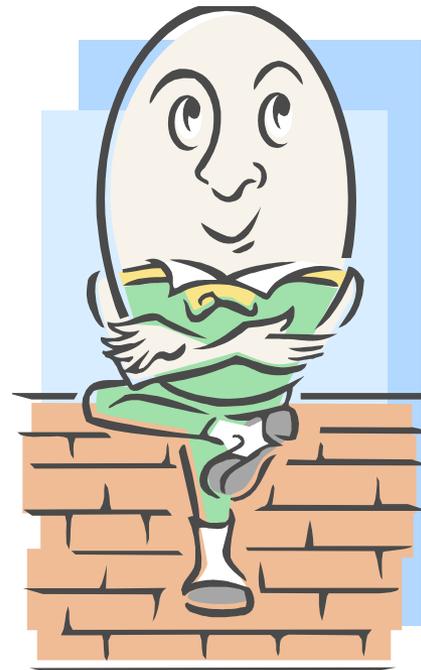


<i>Threat Event</i>	<i>Threat Source</i>	<i>Relevance</i>
Credit card numbers released	Individual hacker	High
Slow response time	Poor database maintenance	Medium
Slow response time	Poor ISP contract terms	Low



Vulnerability

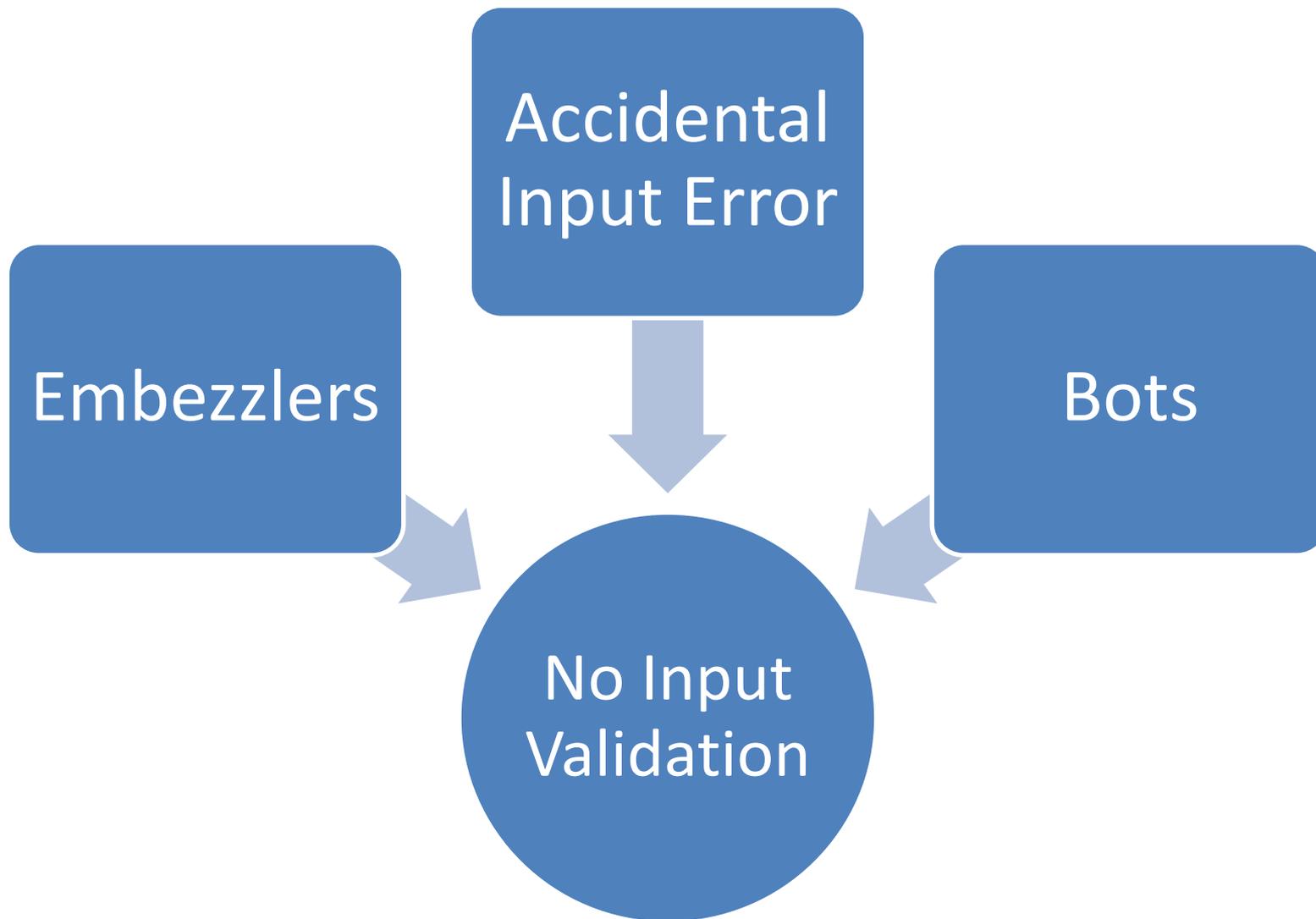
- Something a threat could exploit
- Even if it's already controlled – the control could fail

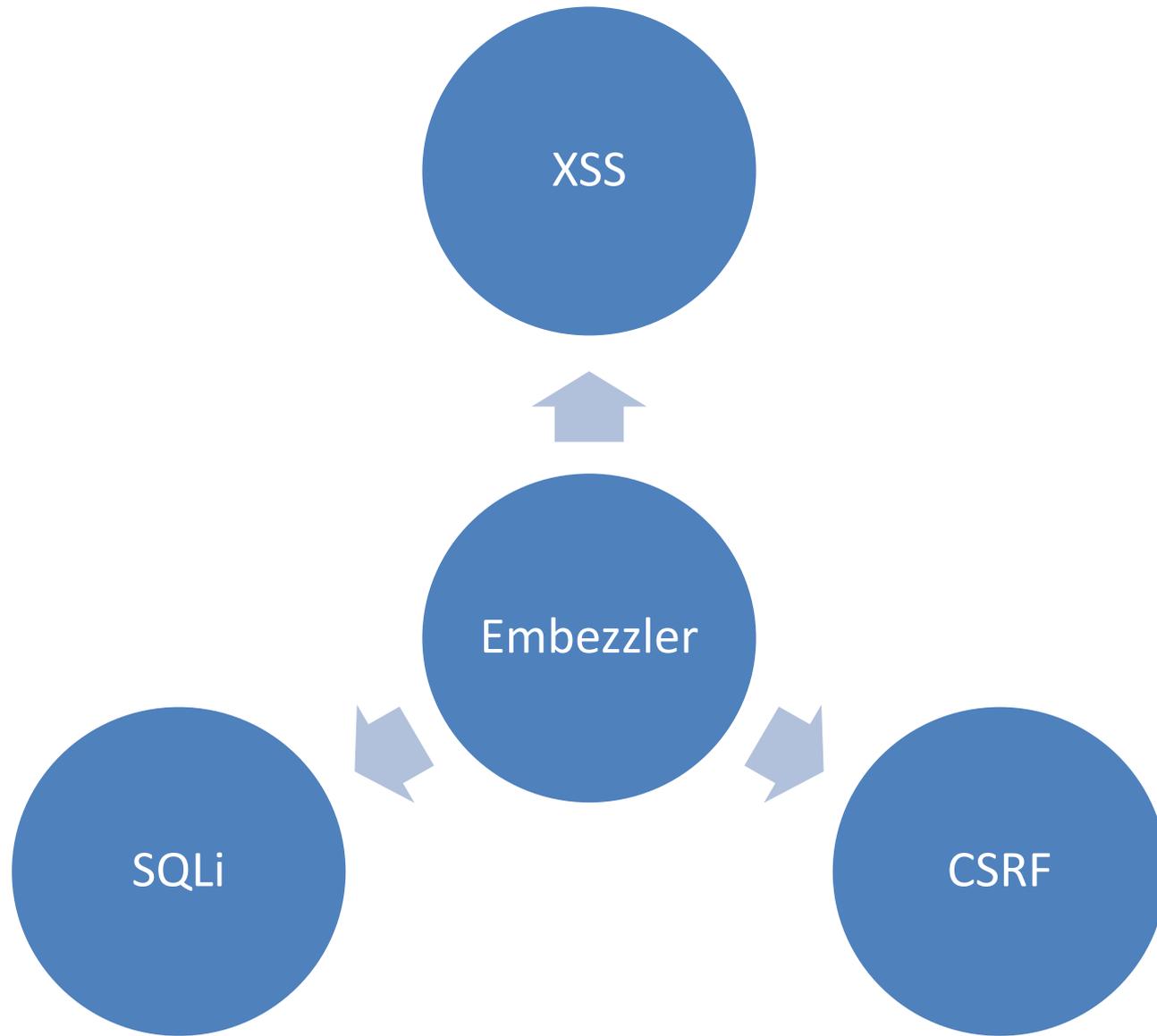




Threats And Vulnerabilities

- An executed Threat against a Vulnerability is an Attack







Try Not to Assume Something Cannot Happen





Likelihood And Effect

- Likelihood = Probability
- Effect
 - *Not* the same as Risk!
 - Affects Information
 - *Integrity*
 - *Confidentiality*
 - *Availability*



Determine likelihood

Adversarial

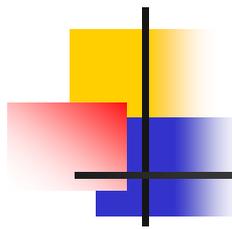
- initiation

Non-
adversarial

- occurrence



Estimating Effect And Likelihood - Ask Questions

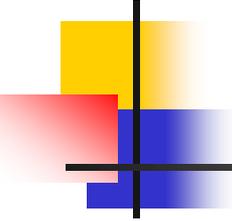


- Could the information be manipulated for personal gain?
- Could business decisions be affected?
- Could you fail to take action: process orders, pay invoices?
- Can you discover the problem?
- How much information loss would make a material difference?



Estimating Effect and Likelihood – More Questions

- Would disclosure lead to public embarrassment?
- Is there a difference between internal and external disclosure?
- Can you permanently lose business?
- Could there be fines or penalties?
- Do non-employees have access to the information?



Determine effect (harm)

- To *operations*
- To *assets*
- To *individuals*
- To *other organizations*



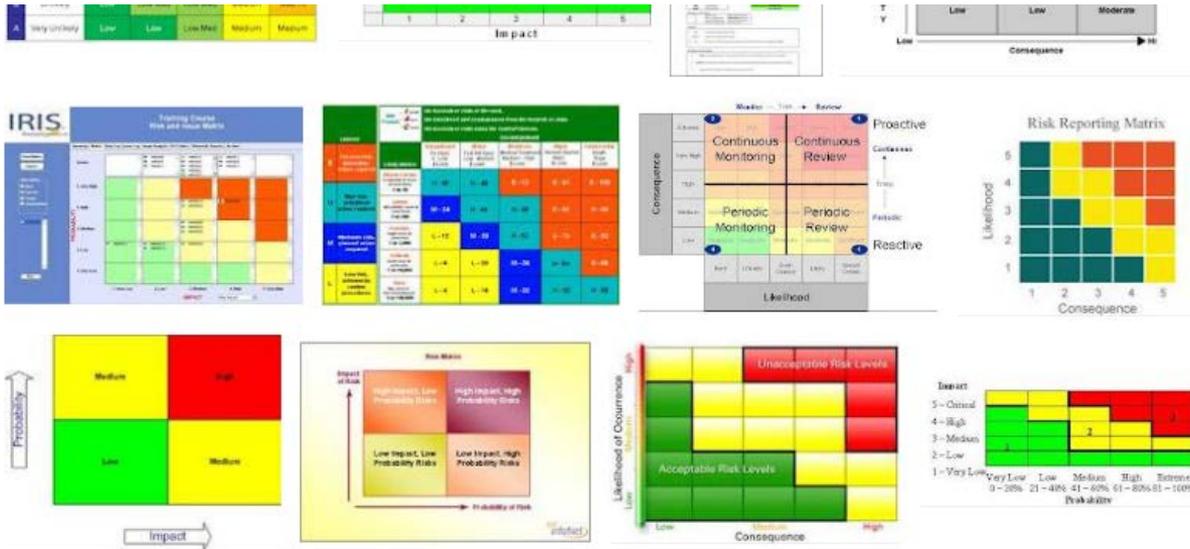


Determine risk

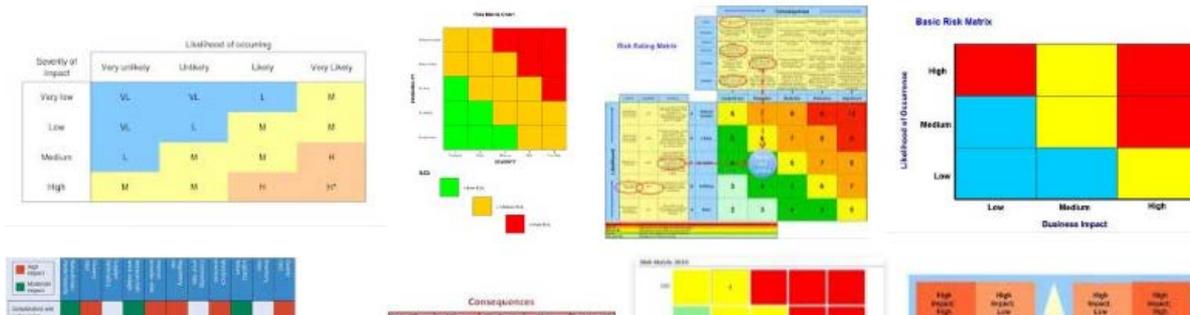
- Generally, the combination of likelihood of the event and its harmful effect

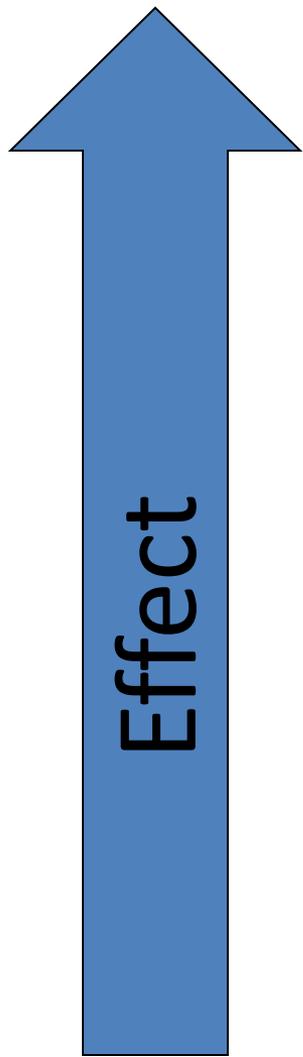


Risk Charts



Page 3





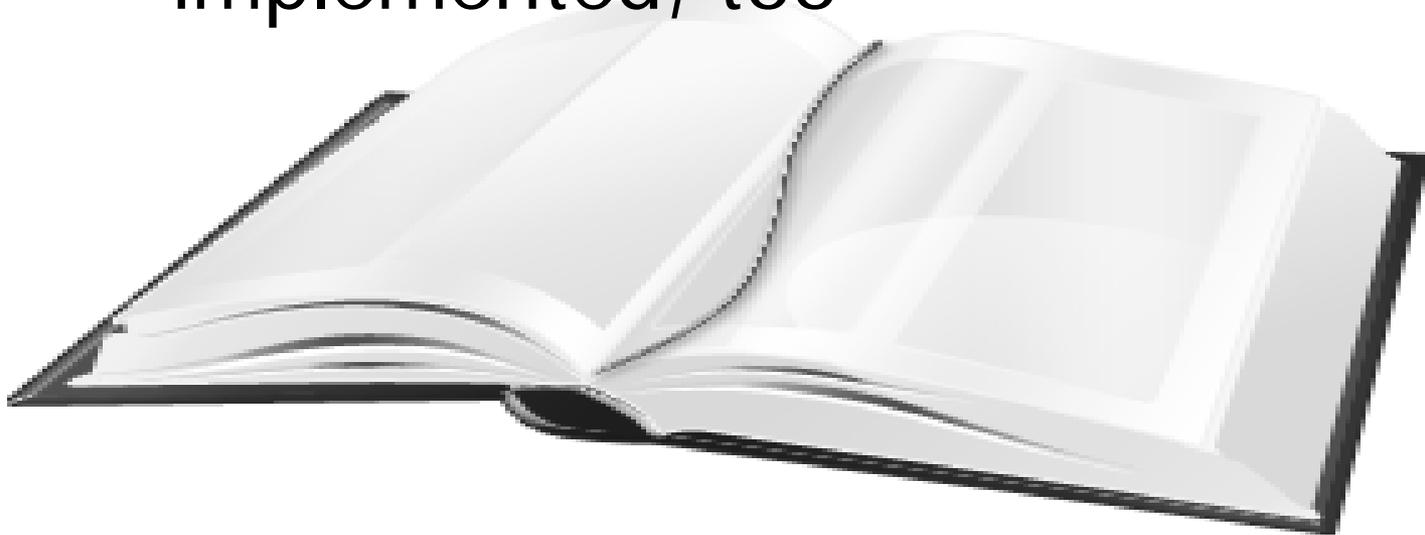
Med Risk	High Risk	High Risk
Low Risk	Med Risk	High Risk
Low Risk	Low Risk	Med Risk





Documentation

- For the sake of audit and future reviews, document controls not implemented, too

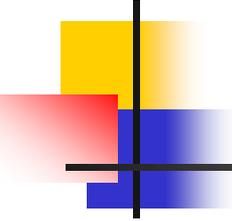




Communicate results to key personnel

- Communicate results to decision makers to support risk responses.





Success!

- Now we have a measurement of Risk that management can relate to
- Management's job to decide what level of Risk they are willing to live with
- This will define how they respond to Risk



Managing risk (NIST)



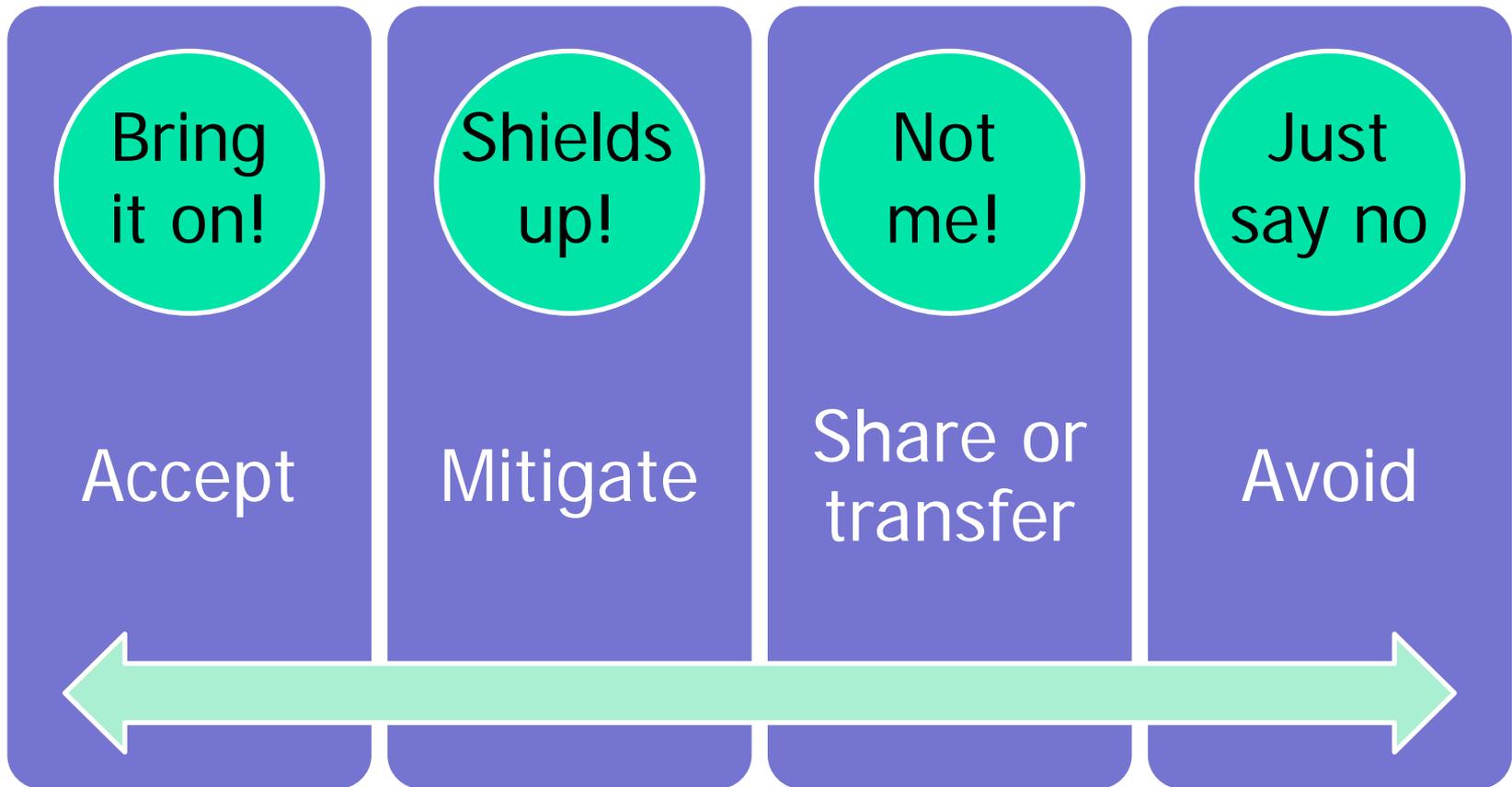


Respond to risk

- What are we going to do with this information?



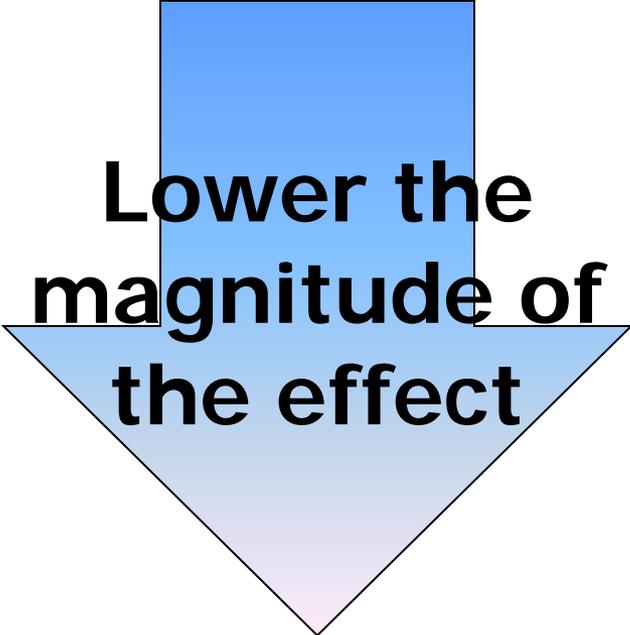
Identify alternative courses of action



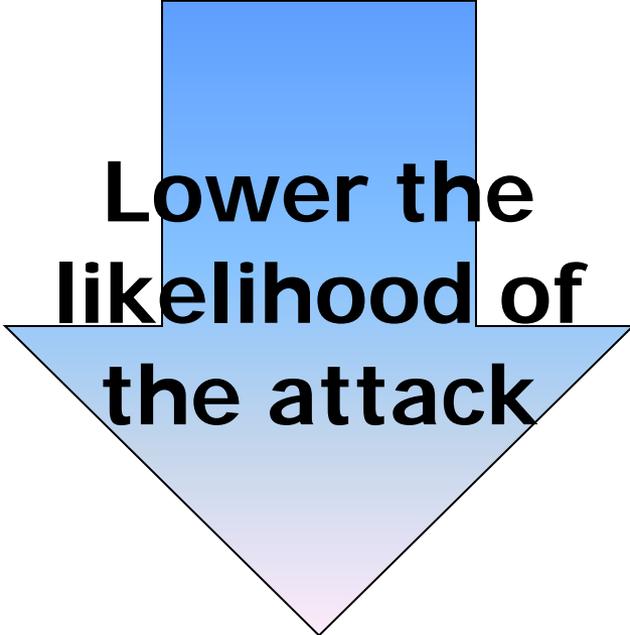


Controls

- There is no bank that cannot be robbed



**Lower the
magnitude of
the effect**



**Lower the
likelihood of
the attack**



Monitor risk



Ensure
accountability



Periodic review



Get Management Sign-off



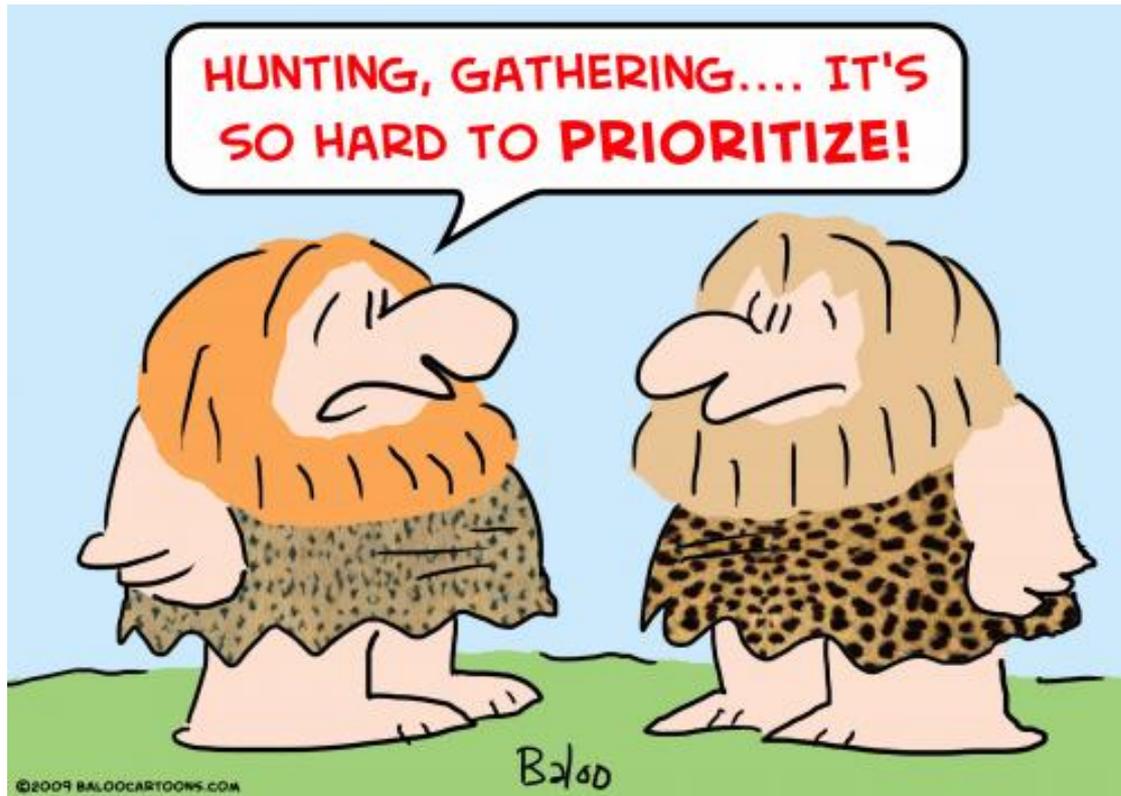


Maintain assessment over time

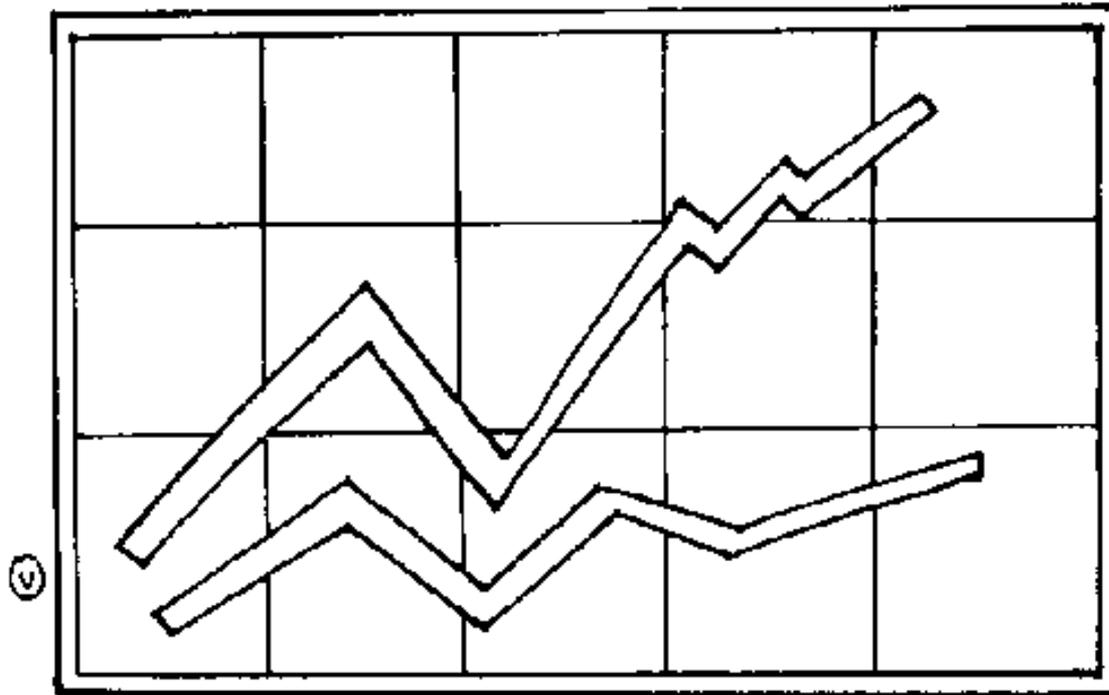
- Ongoing monitoring of risk factors that contribute to changes in risk
- Update existing assessment using the results from monitoring of risk factors



What are you going to do with this information?



What are you going to do with this information?



What are you going to do with this information?





What can go wrong?





What can go right?

