2021 RISK ANALYSIS

Dean Bushmiller CISSP+32

Why RISK?

Exam requires 20% Application of process

This activity is how translate risk scenario

Translation is your job as a CISSP

Required inputs at these proficiency levels

- CISSP definitions 90-95%
- Knowledge of the process

Class activity

Students read a statement

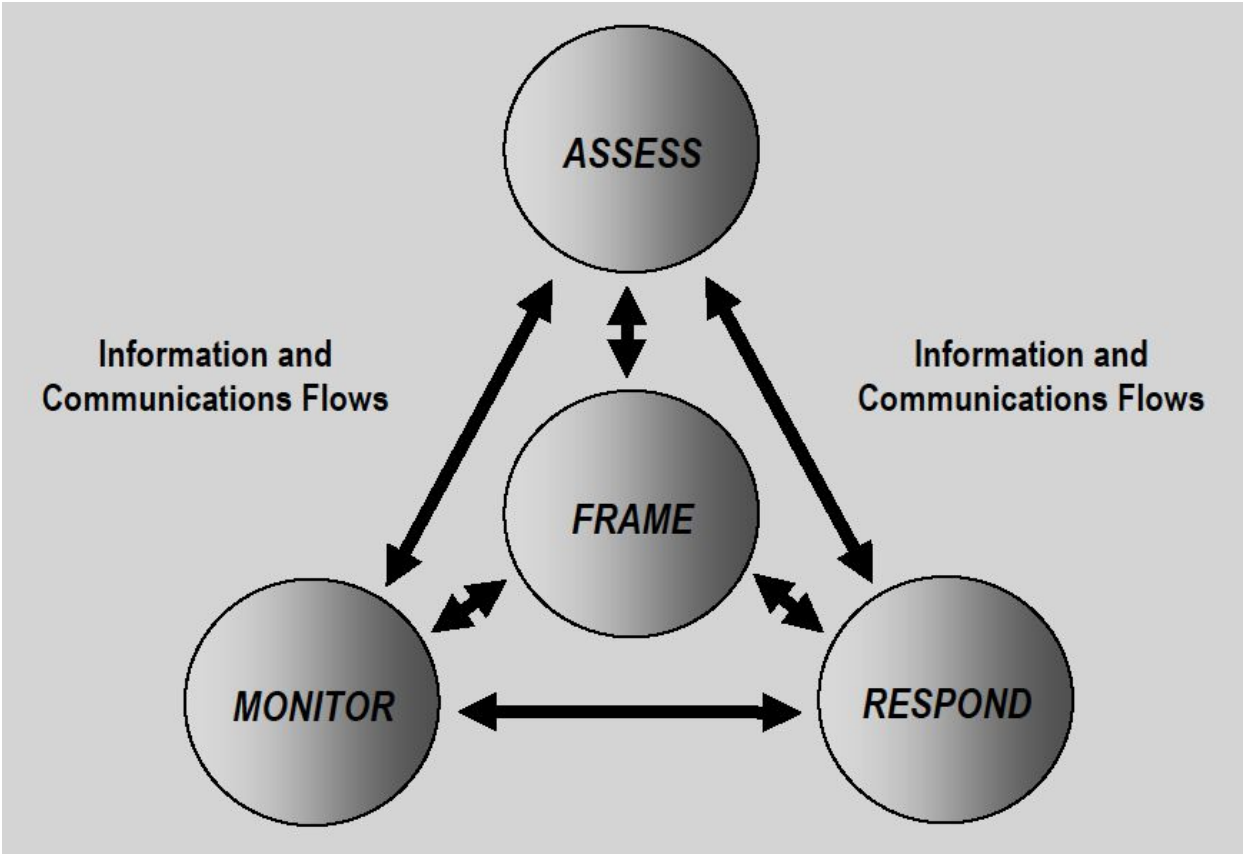
Students convert this to a risk management step

Students choose a next level detail

We discuss

REPEAT per subdomain

You must use these choices in exercises



Frame

Assess

Respond

-Alternatives

Monitor

NEXT STEP IS TO GIVE MORE DETAIL ON ONE OF THE CHOICES

Framing = Scope

- Tactical / System
- Operational / Business process
- Strategic / whole business

Assessing

- Choose scope of Assessment
- Identify threat sources
- Identify threat events
- Identify vulnerabilities
- Determine likelihood
- Determine impacts
- Determine risks

Response with Biz in put

- Developing alternatives
- Evaluating alternatives
- Determining course of action
- Implementing

Monitor

- Determine effectiveness of responses
- Identify risk-impacting changes
- Verify controls and compliance

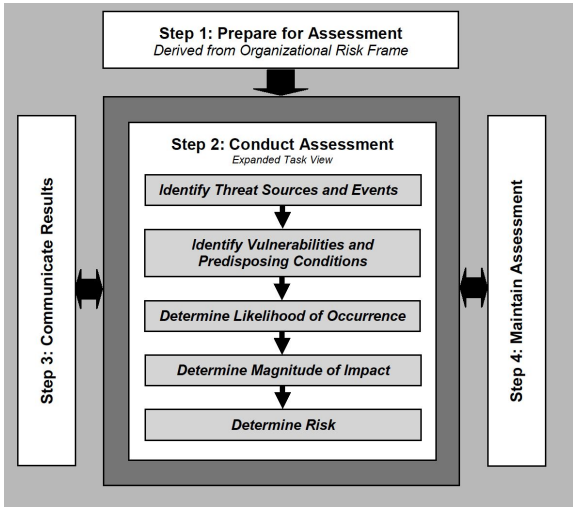
Alternatives

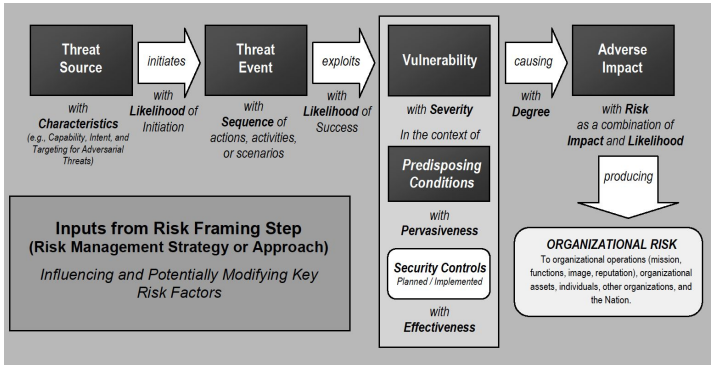
- Avoid=Stop Doing
- Accept=Do Nothing
- Transfer=Buy Insurance
- Mitigate=Control

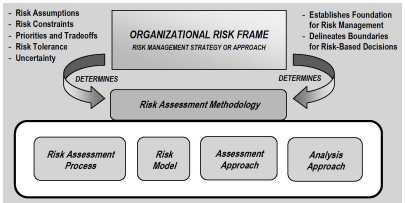
RISK – WHERE IS THIS FROM?

Whole framework: https://csrc.nist.gov/Projects/risk-management/about-rmf

NIST Sp800-30r1 pages 29-30 https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final







ANALYSIS ACTIVITY HINTS

Who is saying the statement?

Security, Management, Sales, Human resources.

Do you know Management and Assessment ?

Can you tell difference between

Is one of these steps part of another process?

BCP, SDLC, Change control

Do you know the logical order?

Policy, Management, Technical

Is this an example | best/worst | first/last?

If example – they will not use the term "example"

Best/Worst – means ALL of them are relevant/true

First/Last – More than one option will be true

Dean.Bushmiller@ExpandingSecurity.com