The Risk Management Process

Dr. Lyron H. Andrews

ISO/IEC 42001 AIMS Lead Implementor
CISSP/CCSP/SSCP/CRISC/CISM/CCSK/CCZT

@drlyronandrews | www.profabula.com

SSCP Certification Examination

Domains	Weights
Security Concepts and Practices	16%
Access Controls	15%
Risk Identification, Monitoring, and Analysis	15%
Incident Response and Recovery	14%
Cryptography	9%
Network and Communication Security	16%
Systems and Application Security	15%

SSCP Certification Examination

Domains	Weights
Security Concepts and Practices	16%
Access Controls	15%
Risk Identification, Monitoring, and Analysis	15%
Incident Response and Recovery	14%
Cryptography	9%
Network and Communication Security	16%
Systems and Application Security	15%

Overview

Overview

- Understand the risk management process
- Apply risk assessment and response techniques
- Demonstrate the monitoring and analysis tools and scenarios

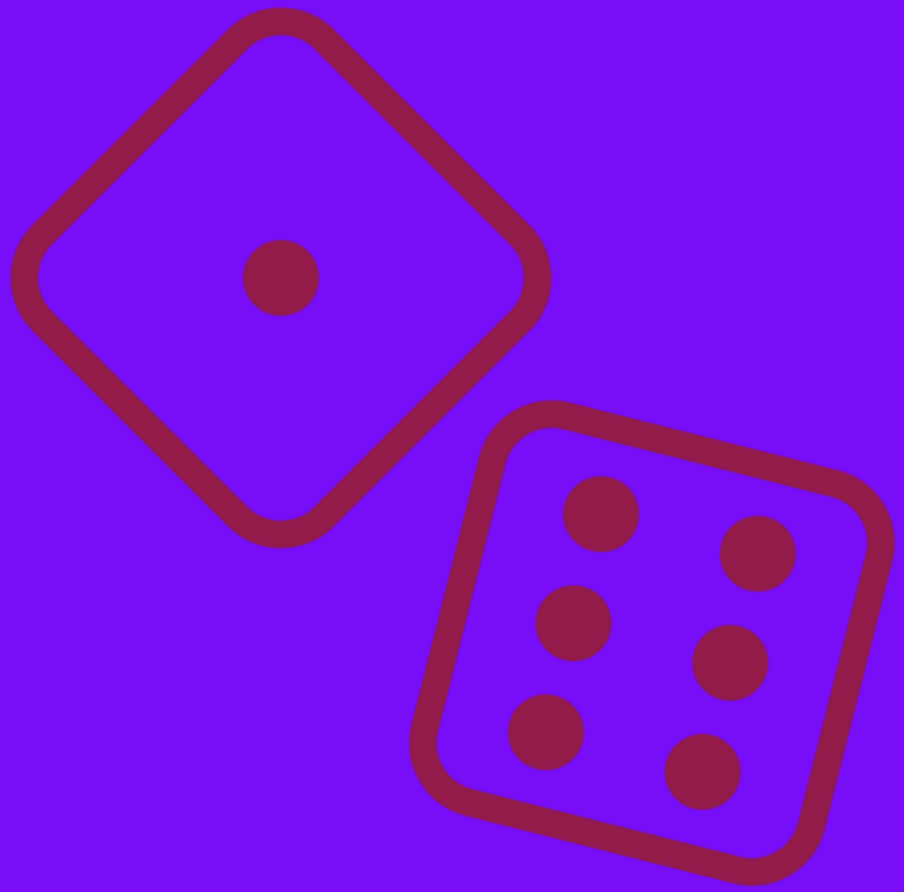
Defining Risk and Related Terms

Risk

Noun: a situation involving exposure to danger.

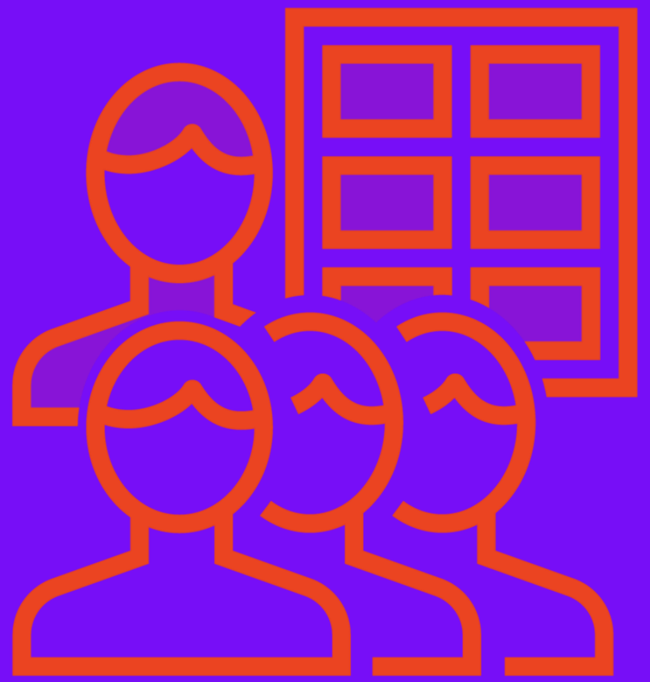
Verb: expose (someone or something valued) to danger, harm, or loss.

Citation: *Oxford Languages and Google*



Risk From Typical IT Perspective

Avoid, avoid, avoid.



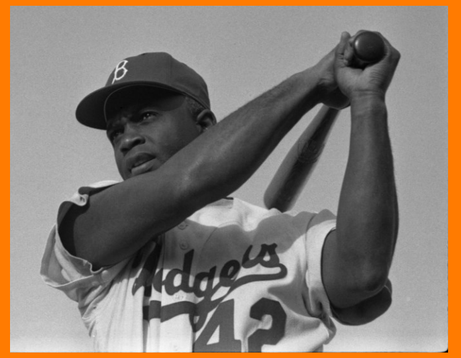
Risk From Typical Business Perspective

How much, how long, what kind...

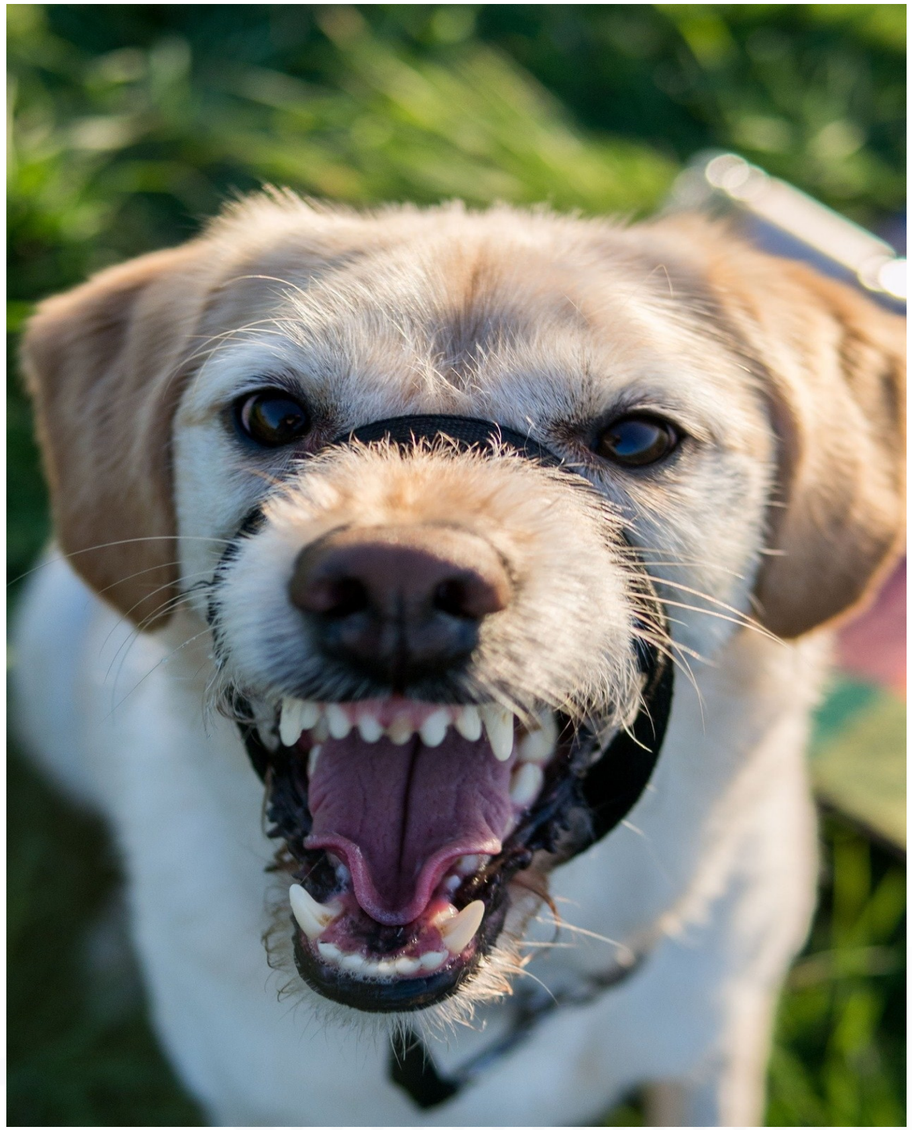
Risks are a combination of:

- Assets
- Threat agents and sources
- Vulnerabilities
- Impacts
- Safeguards
- Countermeasures

A Story to Understand Risk Elements



Threat Agent and Source



Name threat agent and source

- Dog is the threat, as is a hacker
- Threat source is dogs' teeth, as is malware

Safeguard

Name the primary safeguard

- The fence

Vulnerability

Name the primary vulnerability

- The fence

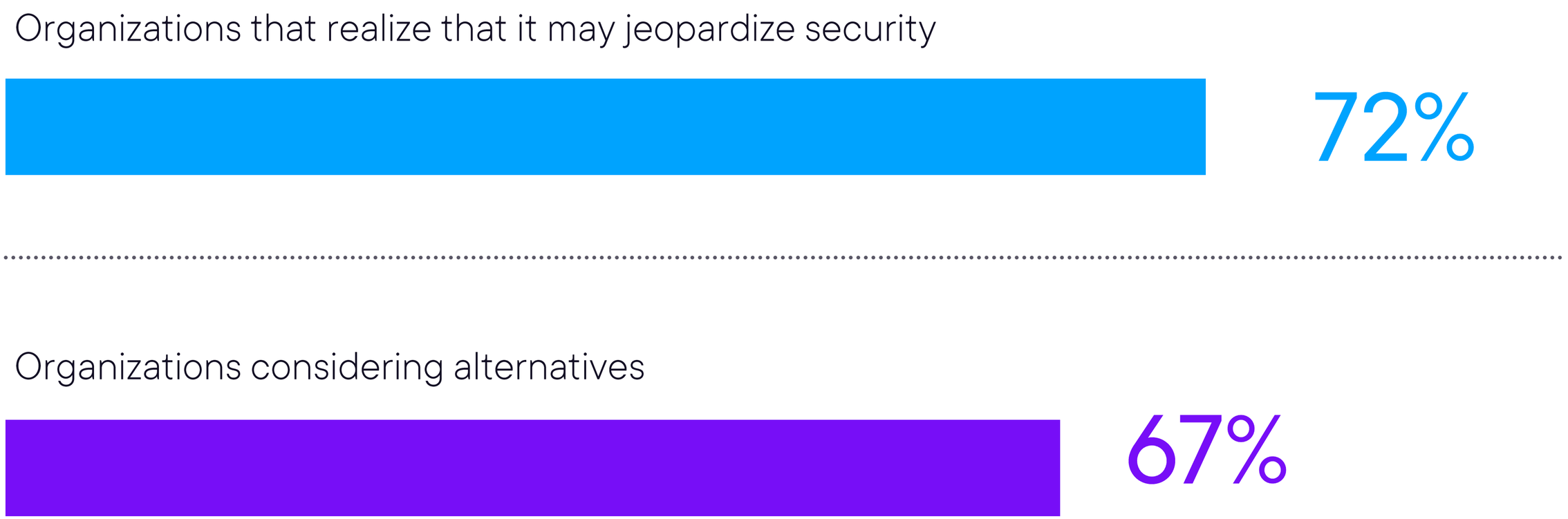
Can you list safeguards or controls that contain vulnerabilities?

VPN as Safeguard with Vulnerabilities

Organizations that use VPN service

Organizations aware that it is a cybercriminal target

VPN as Safeguard with Vulnerability



What would you state was the primary asset in the story?

Risk Management Frameworks

Major Frameworks and Guides

NIST SP 800-39
Managing information security risk

ISO/IEC 27005
Information security risk management

ISO/IEC 31000
Risk management guidelines

ISO 31000:2018 Risk Management - Guidelines

Not certifiable

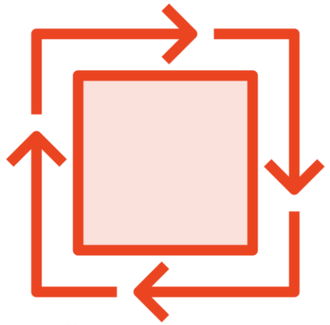
Addresses approach

Considers cloud

Five elements

Top management

ISO 27005 Information Security Risk Management



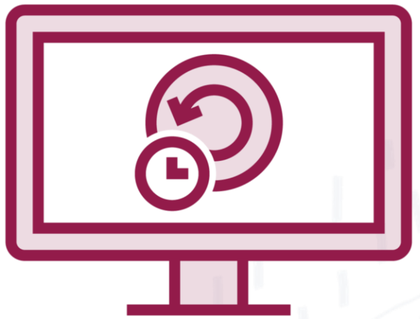
Context establishment

Risk assessment

Risk treatment

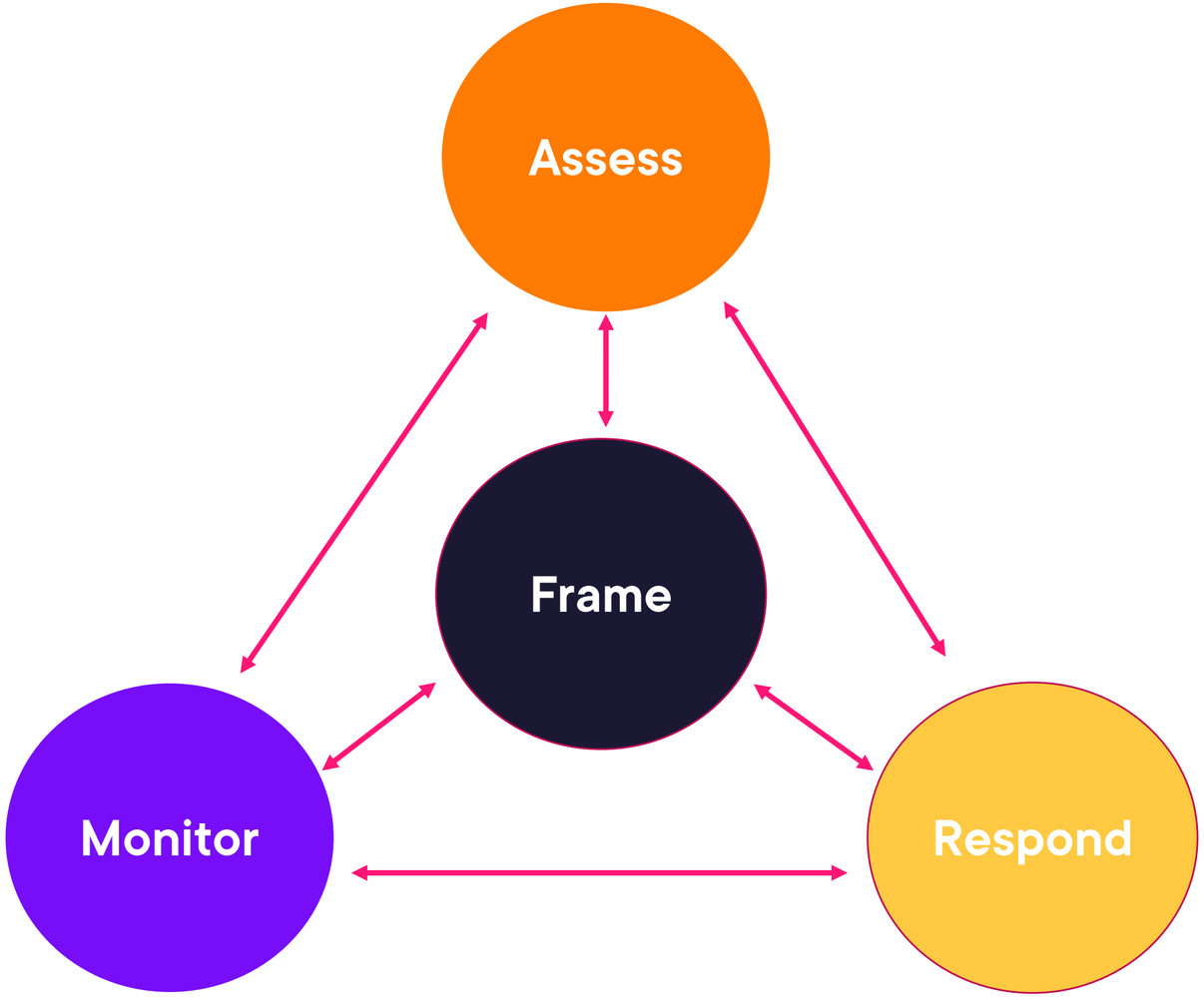
Risk acceptance

Risk communication



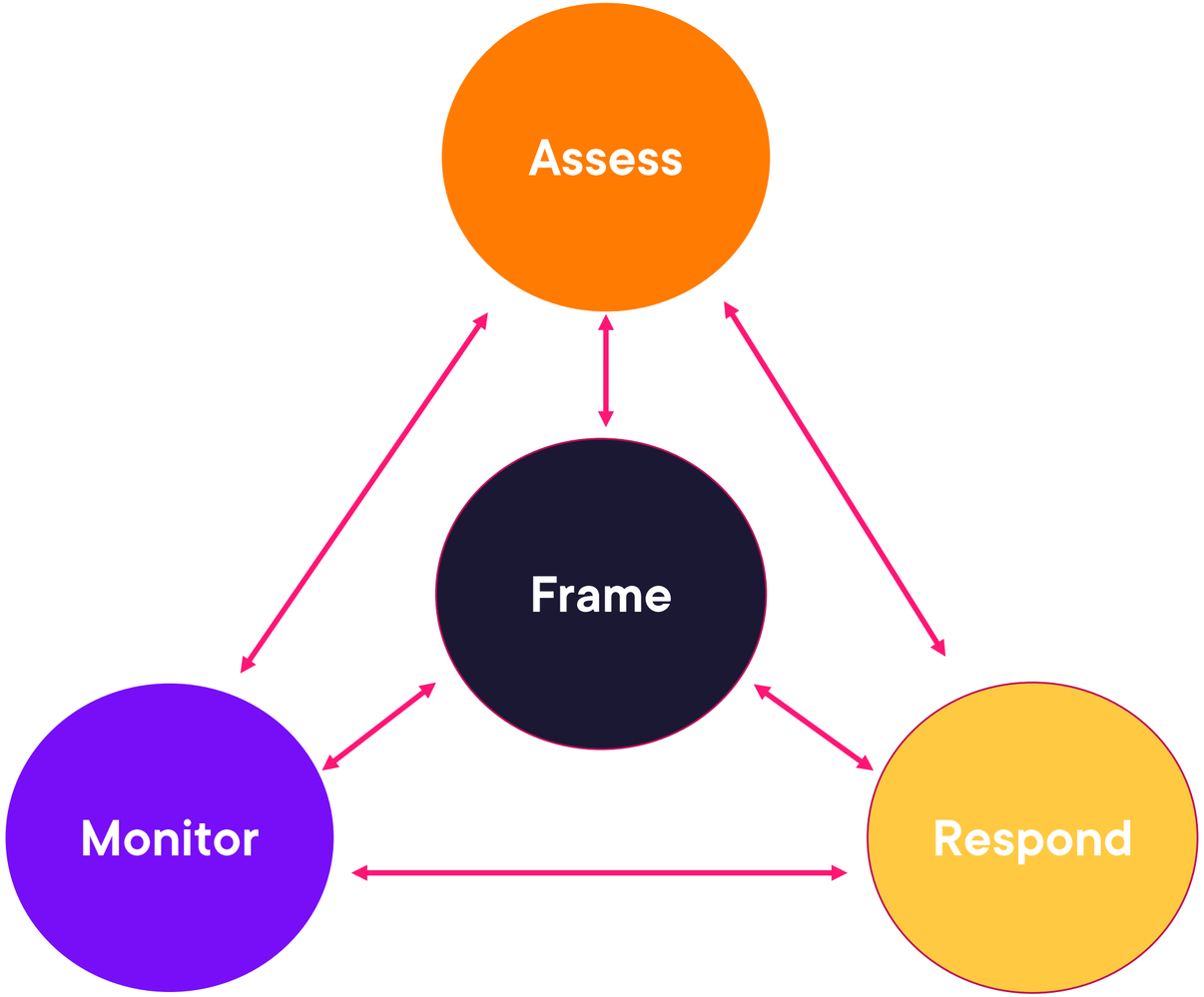
Risk monitoring

NIST SP 800-39 Managing IS Security Risk



Applying the Risk Process

Risk Process



Frame Risk

Aligned with business

Clear and continuous communication

Not a singular technological focus

Diverse and continuously changing landscape

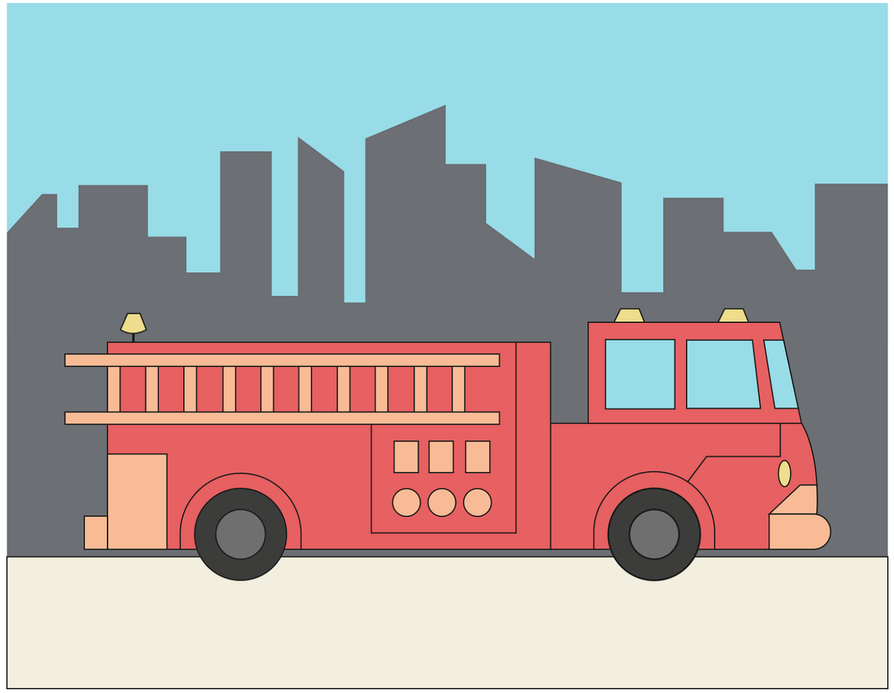
Assess Risk

Combining identification and assessment

Informed by the framing stage

Includes threat and vulnerability analysis

Risk Response



Avoid

Accept/retention

Reduce/mitigate/modification

Transfer/share

Monitor Risk

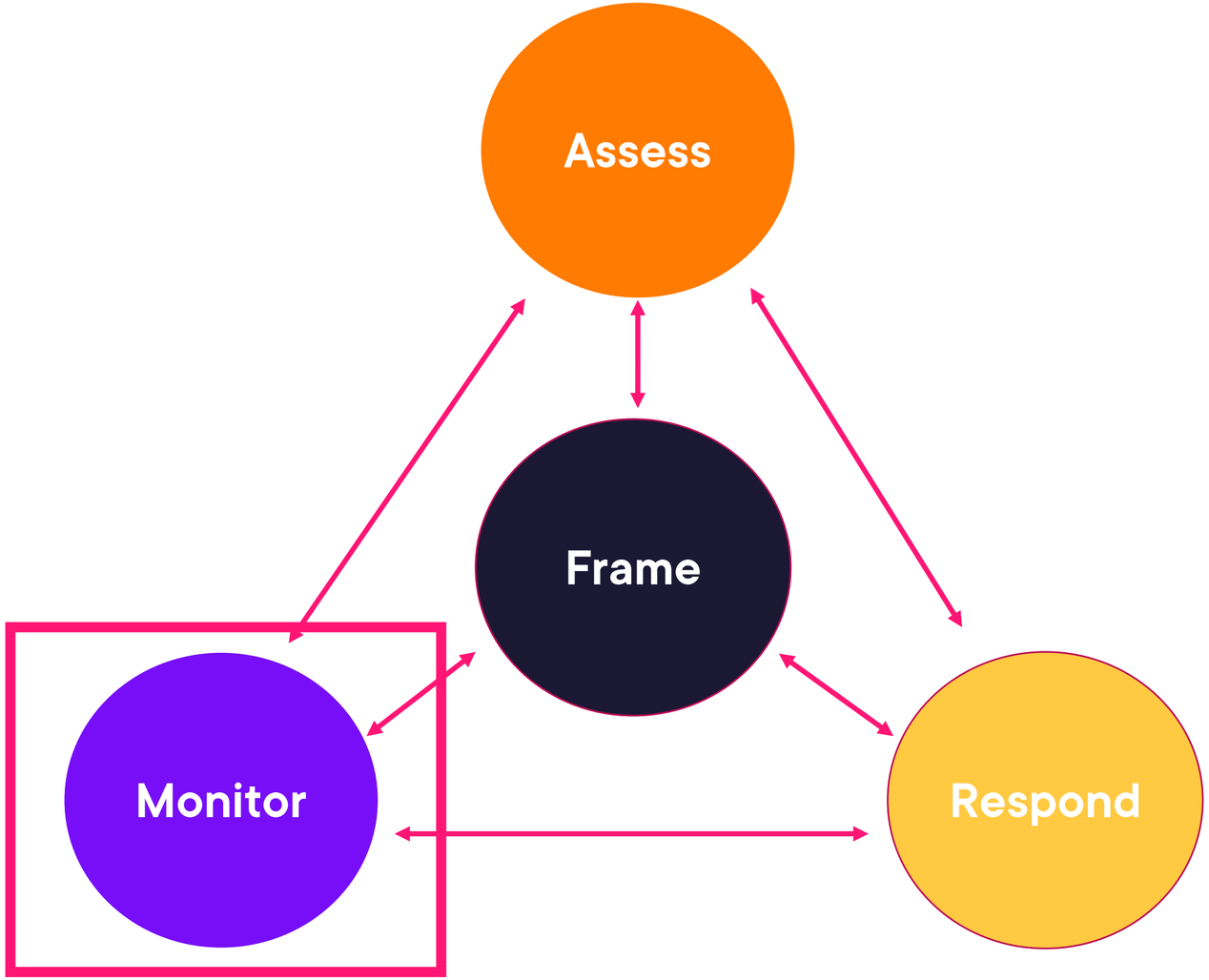
New vulnerabilities and threats

Change in asset value

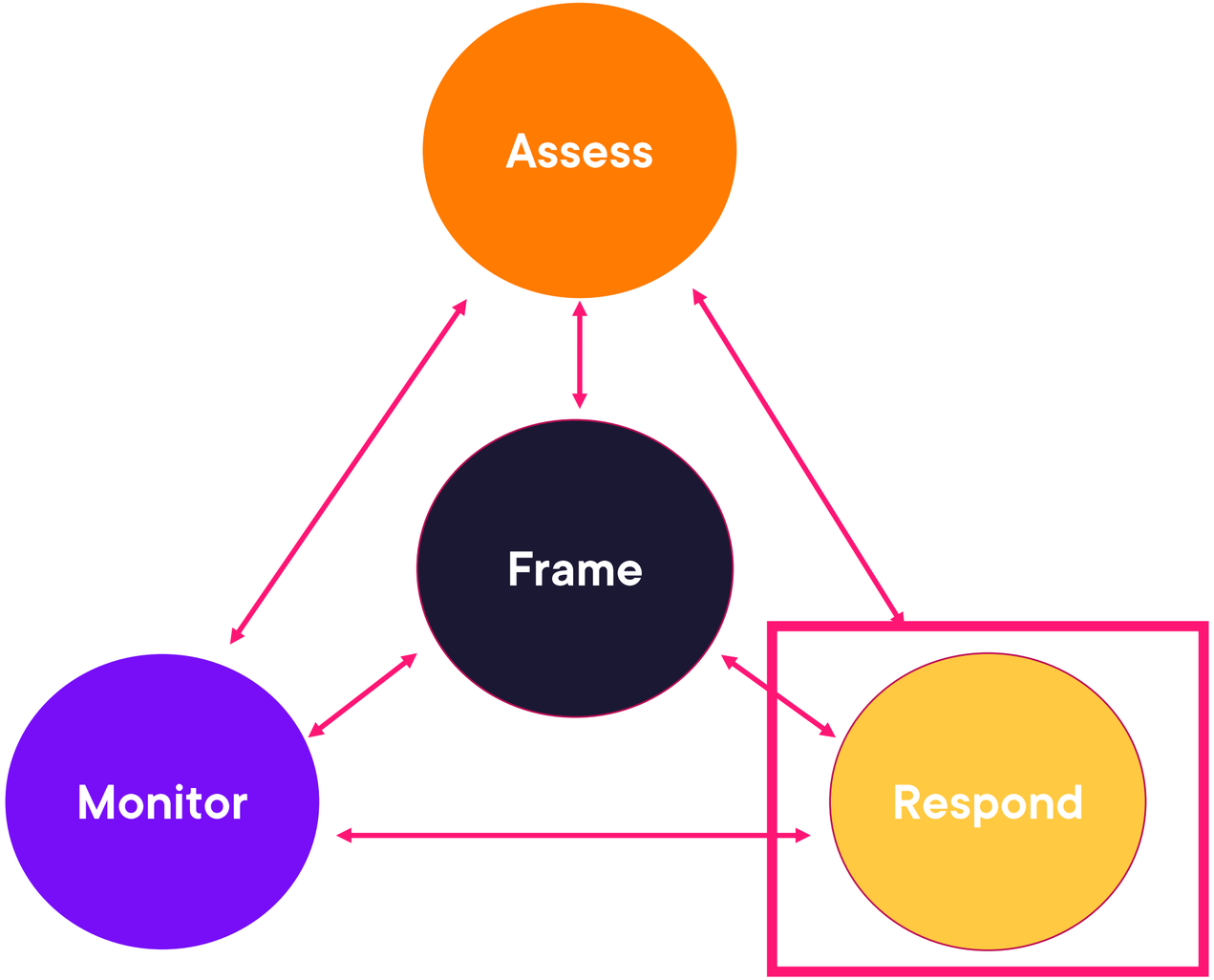
Legal and regulatory modifications

Organizational posture changes

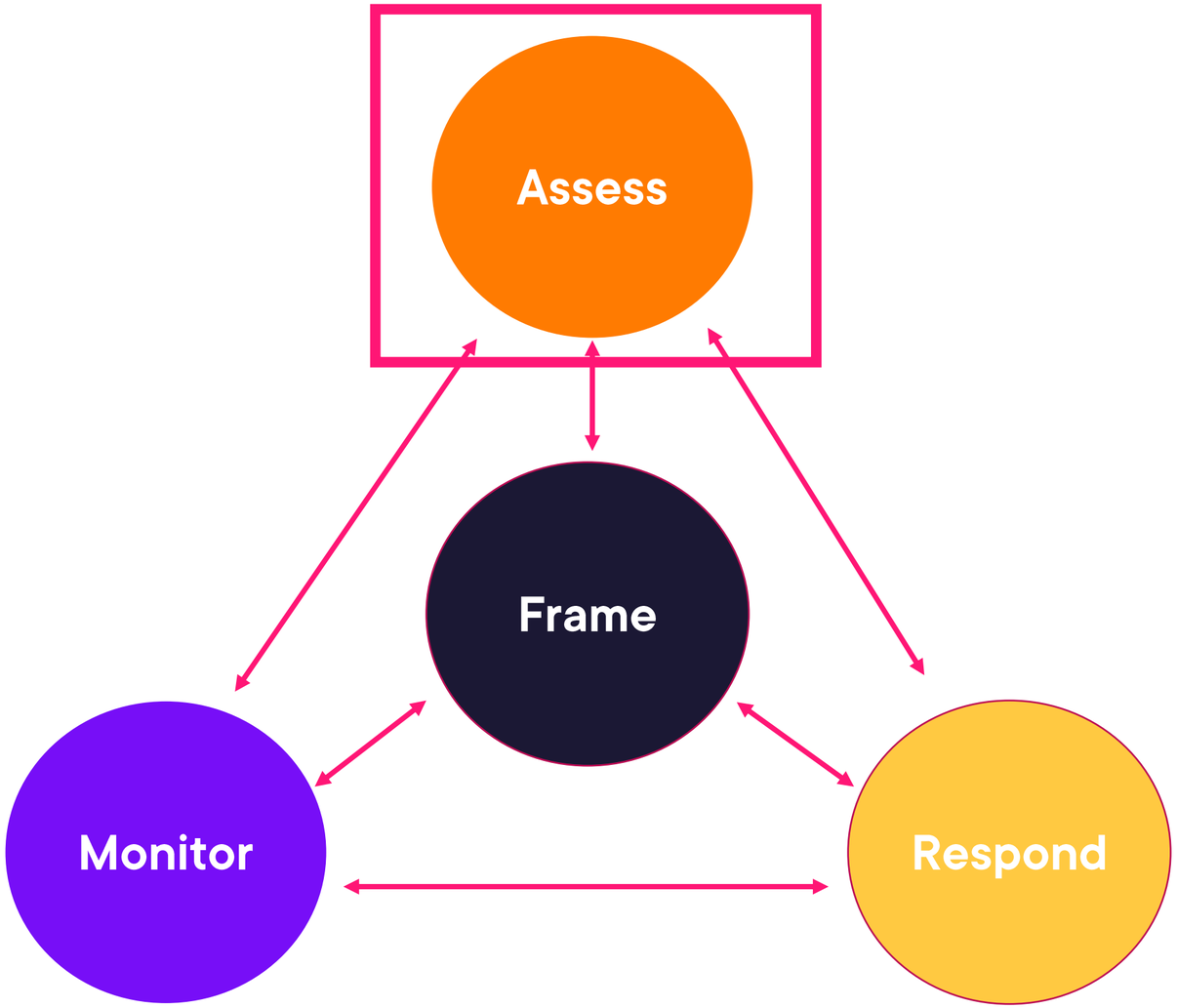
Risk Process Not Linear



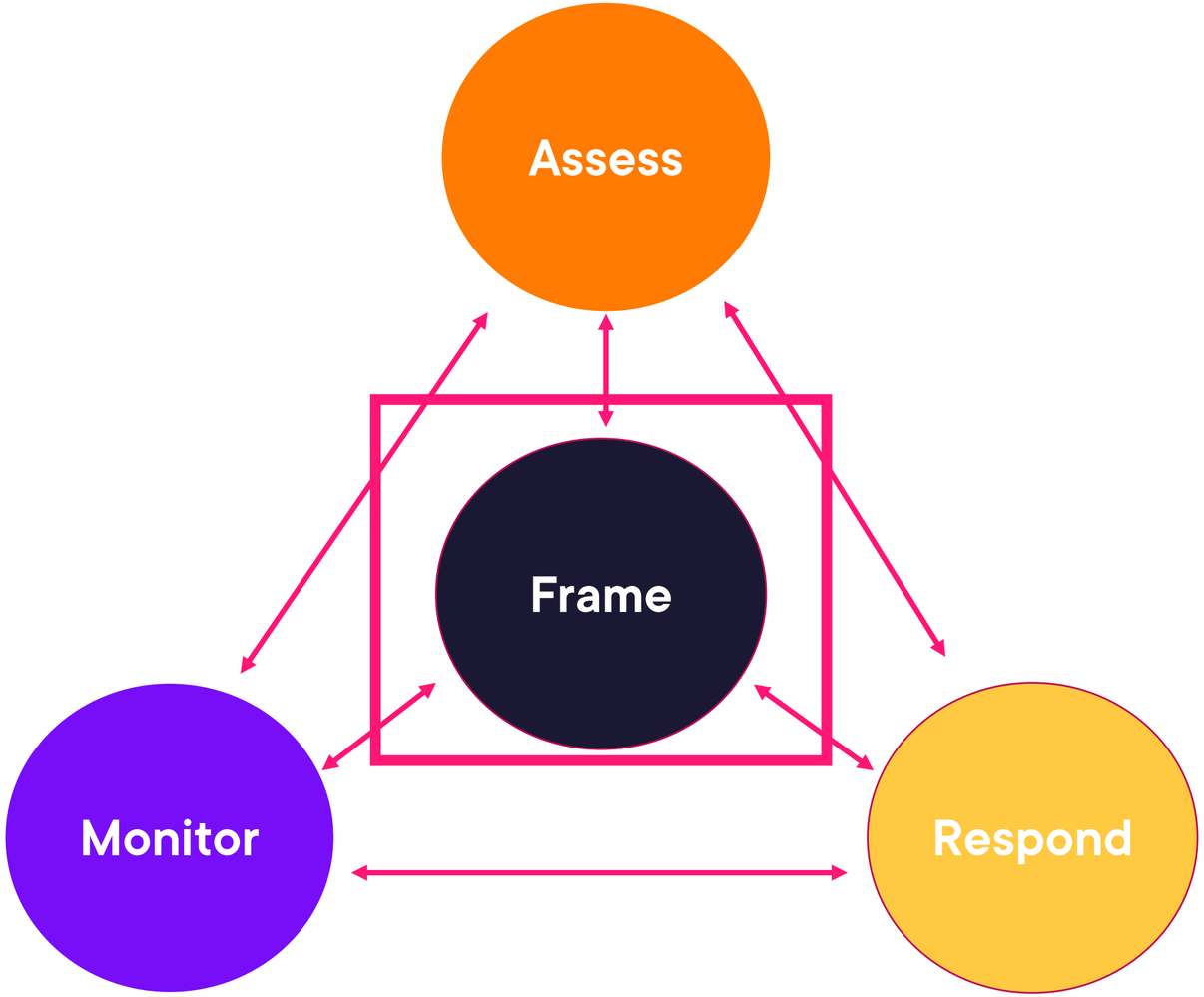
Risk Process Not Linear



Risk Process Not Linear



Risk Process Not Linear



Understanding Legal and Regulatory Concerns

Comparison: Legal vs. Regulatory

Legal	VS.	Regulatory
Established by government		Established by an oversight group
Applies to all citizens and visitors of a jurisdiction		Applies to an industry or practice
Violations can lead to civil and criminal charges		Violations can have penalties or participation exclusion

Primary Legal & Regulatory Risks

Privacy and data residency violations

1. Impactful financial penalties
2. Criminal accusations and imprisonment
3. Disbarment from association or removal of free movement

Course Summary

Summary

- Name specific threats, vulnerabilities, and assets related to your business
- Which risk framework best suites your business model
- What element of the risk process needs the most attention

Up Next:

Risk Assessment and Response