Organizational and Cloud Risk Management

Dr. Lyron H. Andrews
CISSP/CCSP/SSCP/CRISC/CISM/CCSK

https://www.profabula.com/whyprofabula

Overview

Explain risk management taxonomy

Review risk management frameworks

Provide quantitative and qualitative analysis

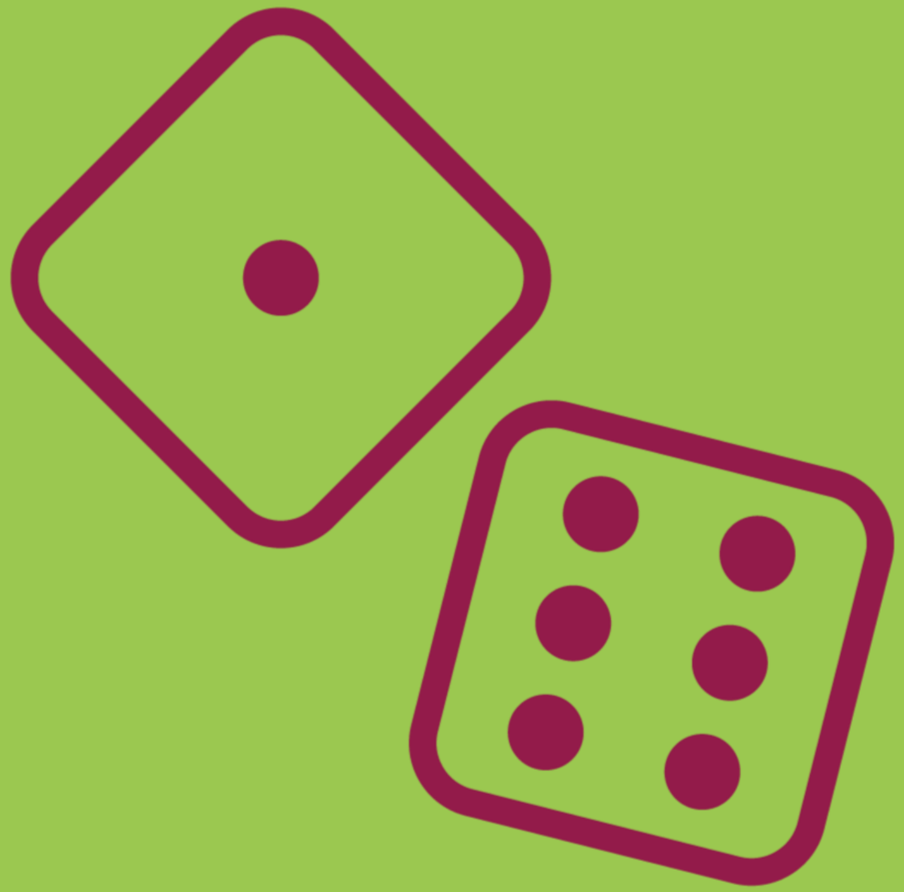
Defining Risk and Related Terms

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

Threat sources

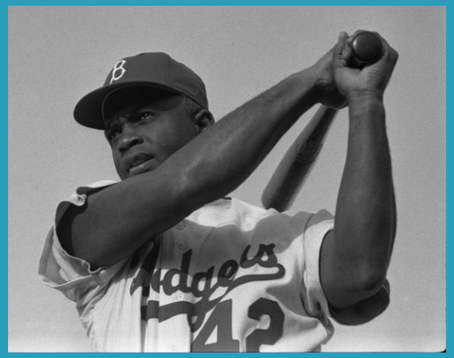
Vulnerabilities

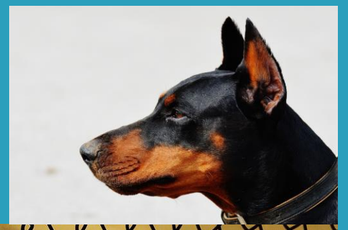
Impacts

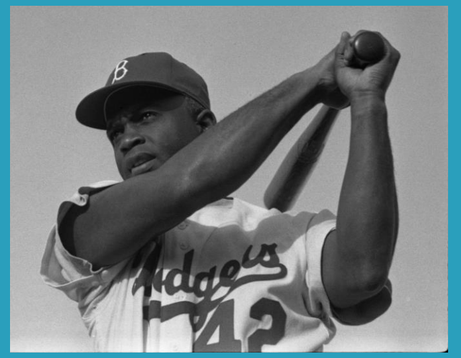
Safeguards

Countermeasures

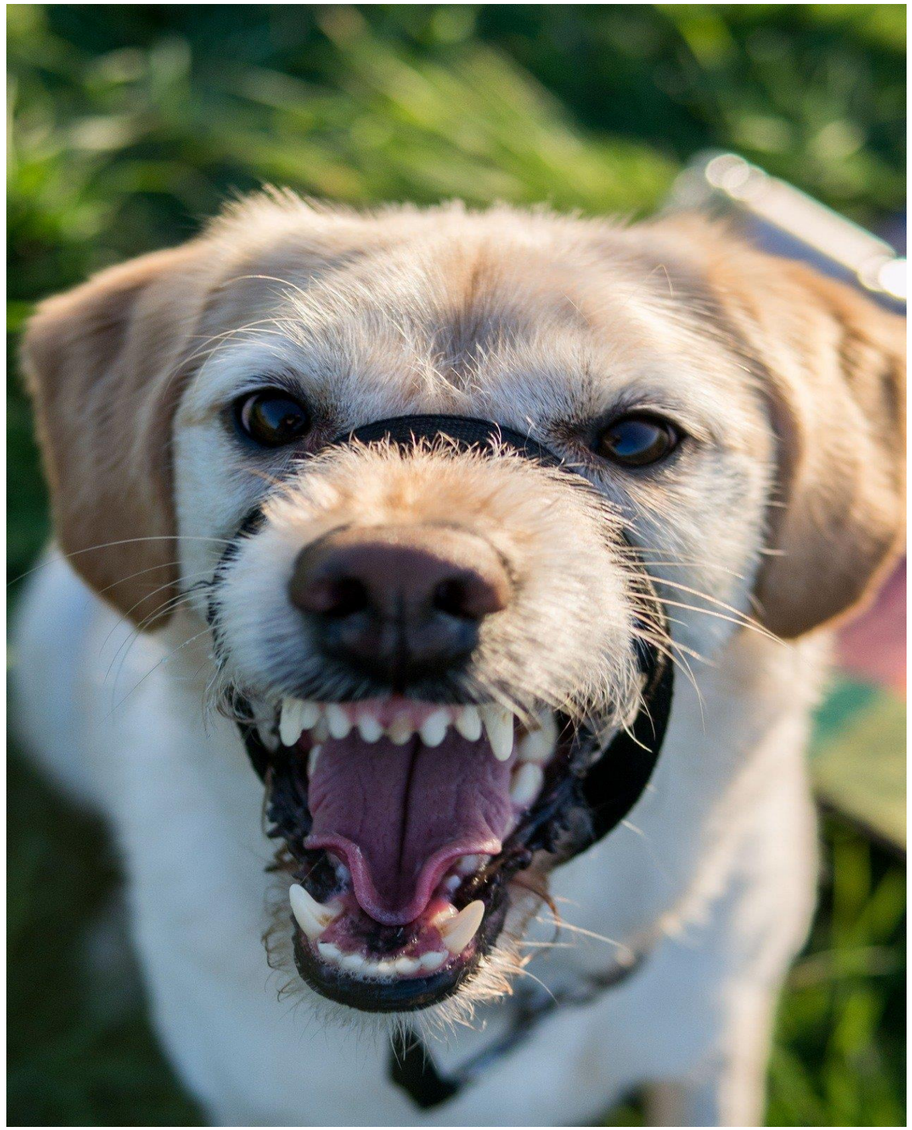
A Story to View the Elements of Risk in Motion


Dodgers
42





Threat Agent and Source



Name threat agent and source

- Dogs are threat agent as is a hacker
- Threat source is dogs' teeth as is malware

Safeguard

Name the primary safeguard

- The fence

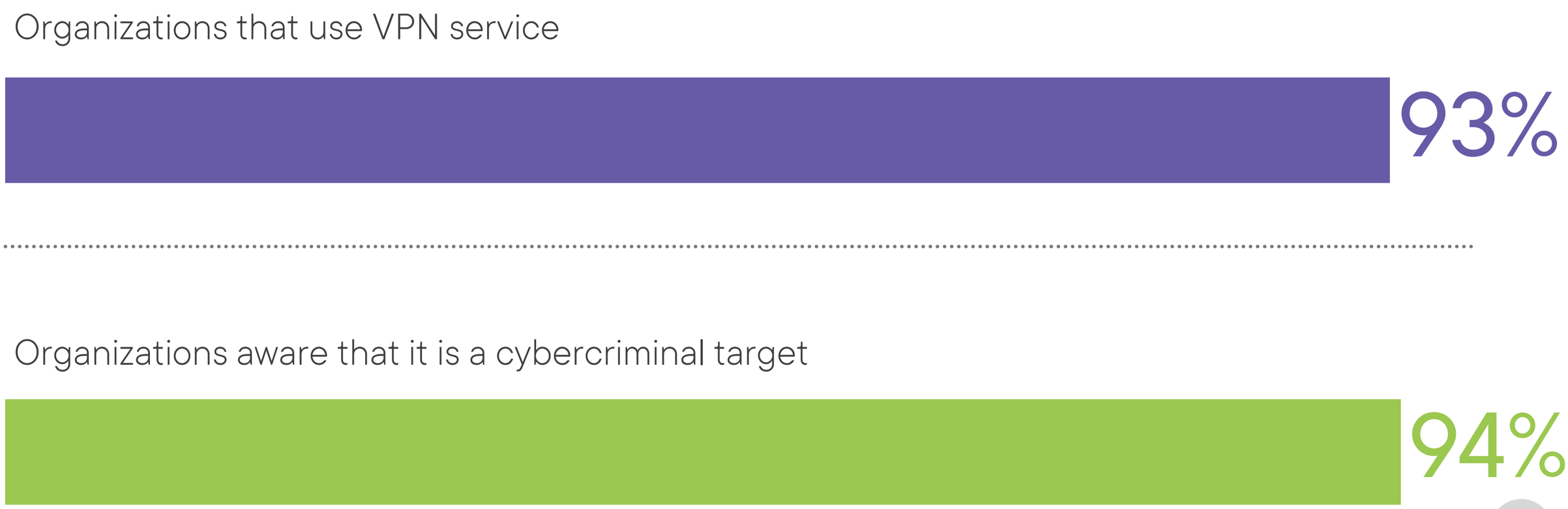
Vulnerability

Name the primary vulnerability

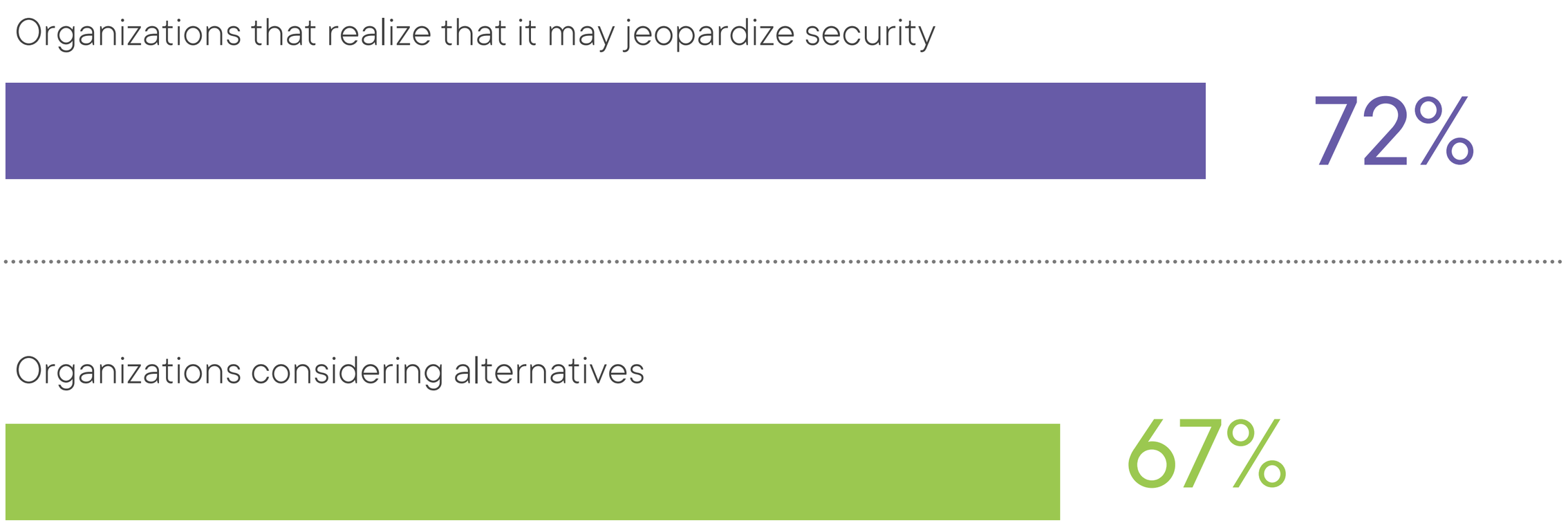
- The fence

Wait! How is a safeguard a vulnerability?

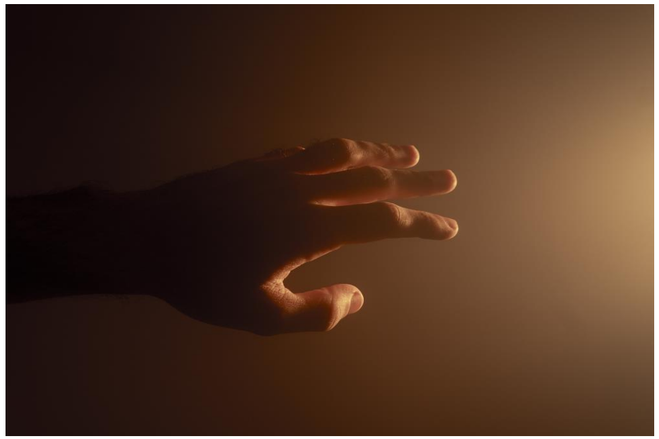
VPN as Safeguard and Vulnerability



VPN as Safeguard and Vulnerability



Assets



Name an asset

- The ball
- My brothers hand

NIST and ISO Frameworks for Risk Management

ISO 31000:2018 Risk Management - Guidelines

Not certifiable

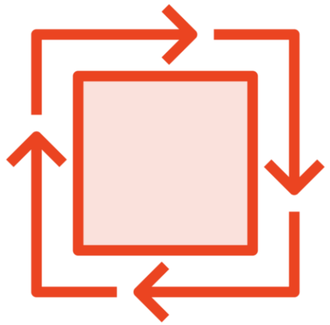
Addresses approach

Considers cloud

Five elements

Top management

ISO 27005 Information Security Risk Management



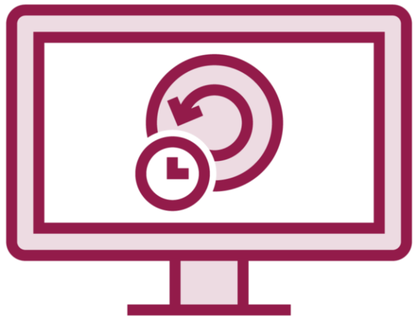
Context establishment

Risk assessment

Risk treatment

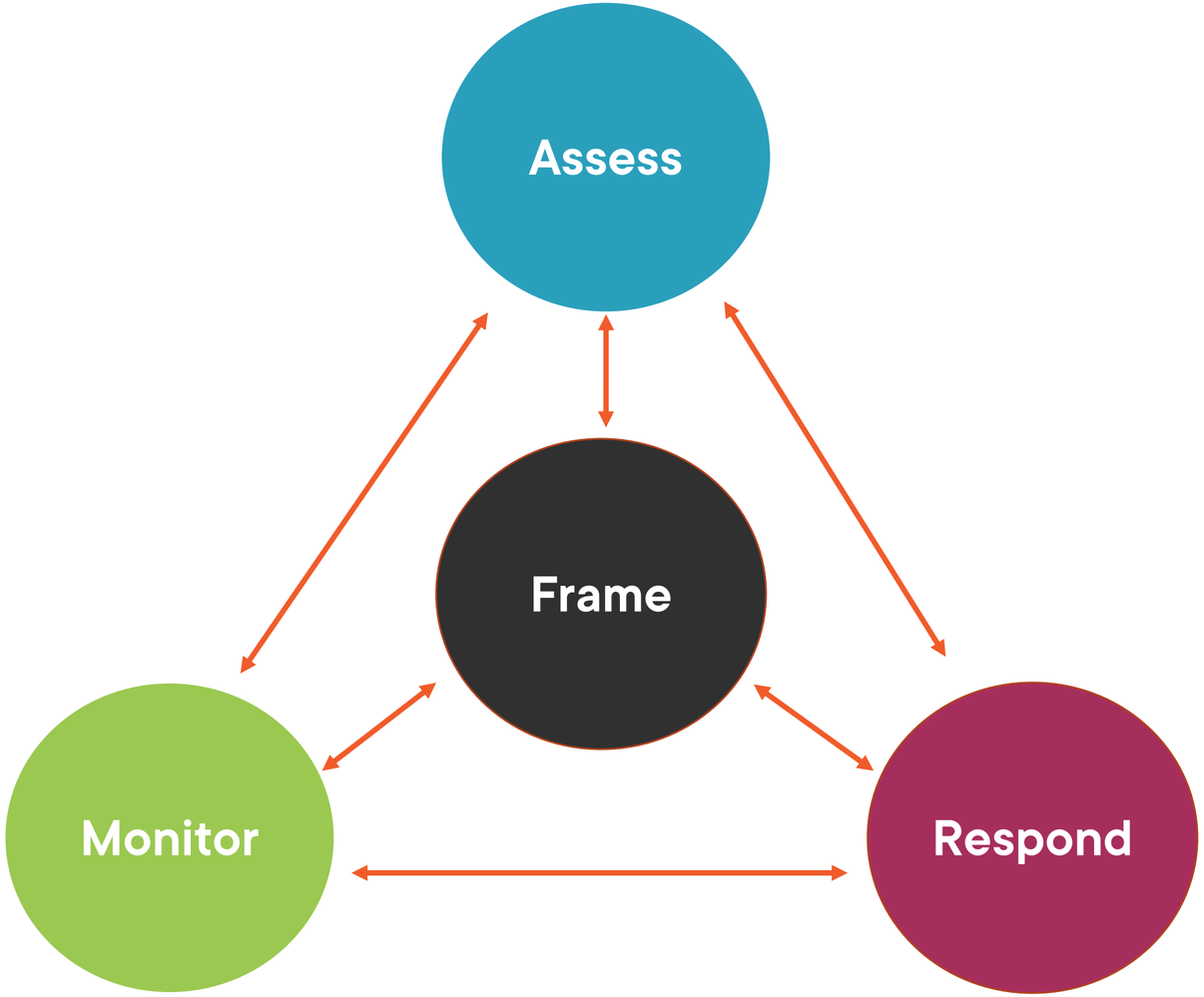
Risk acceptance

Risk communication



Risk monitoring

NIST SP 800-39 Managing IS Security Risk



Risk Management Framework (RMF)

Categorize system

Baseline selection

Controls implementation

Controls assessment

System authorization

Deployment Management

NIST Framework for Improving Critical Infrastructure Cybersecurity

Framework core

Framework tiers

Framework profile

Establishing Qualitative and Quantitative Analysis

Side-by-side Comparison

Qualitative	Quantitative
Subjective	Objective
Operational Impact	Financial Impact
Relatively easy	Quite involved

Qualitative Analysis Considering a Threat

Likelihood

If likely, then consider frequency

Impact

If it occurs what is the operational impact

Quantitative Analysis Considering a Threat

Single Loss Expectancy
$15,000

Asset Value **$150,000** x **Exposure Factor** **10%**

Annual Rate of Occurrence
.2

Frequency 1 ÷ **Years** 5

Annual Loss Expectancy
$3,000

SLE x ARO = ALE

Privacy Impact Assessment

Demonstrate
Proof of protection effectiveness

Communicate
Constituents have published statement

Application
Various industries and implementations

Risk Treatment Response

ISO/IEC 27005:2018: Information Security Risk Management

Modification

Retention

Avoidance

Sharing

Modification

Implements controls

Formerly called mitigation

Apply to previous case

Takes no extraordinary action

Formerly called acceptance

Apply to previous case

Retention

Same term used before

Expanded connotation

Apply to previous case

Avoidance

Sharing

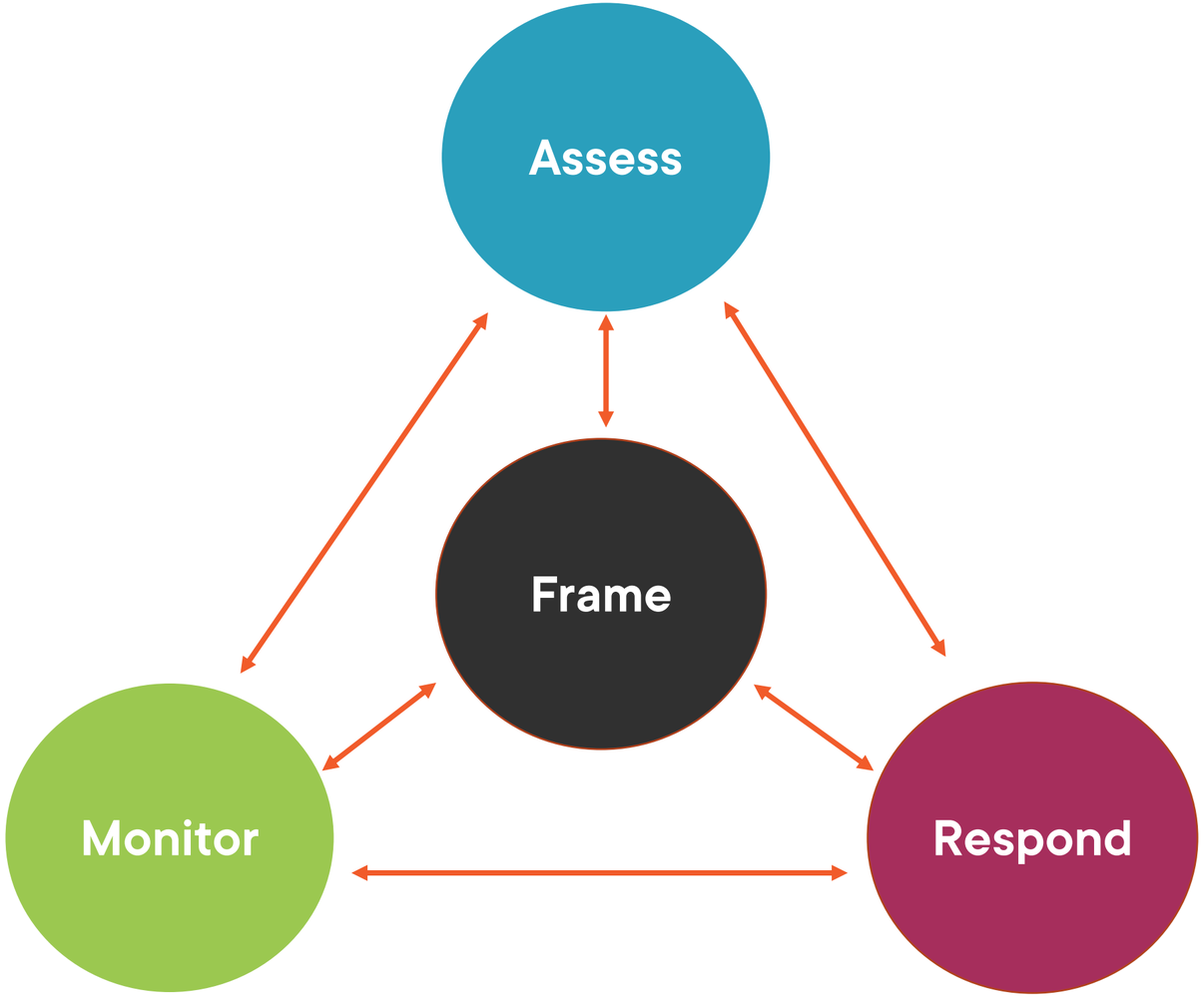
Risk shared with another party

Formerly called transfer

Apply to previous case

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

Monitor Risk

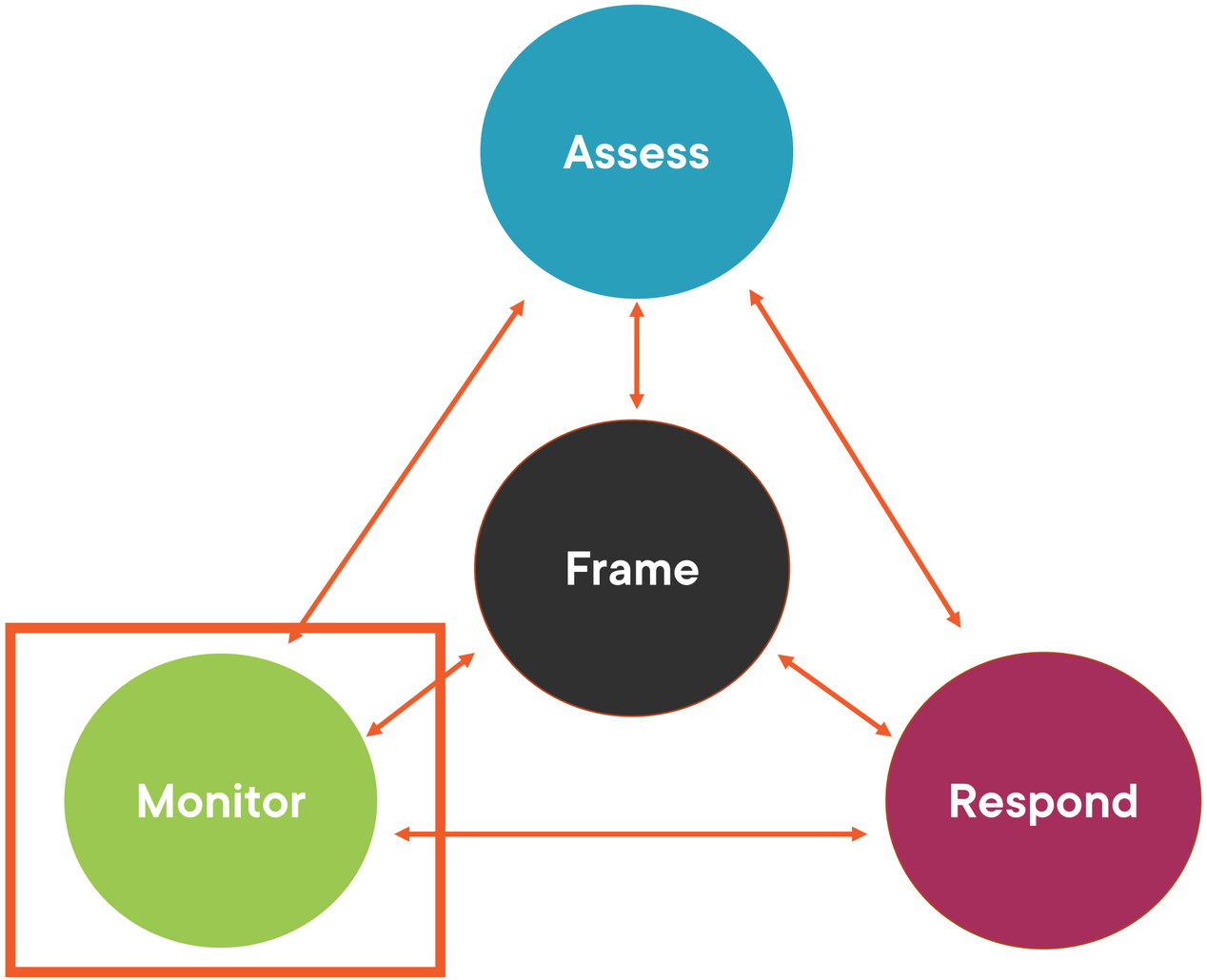
New vulnerabilities and threats

Change in asset value

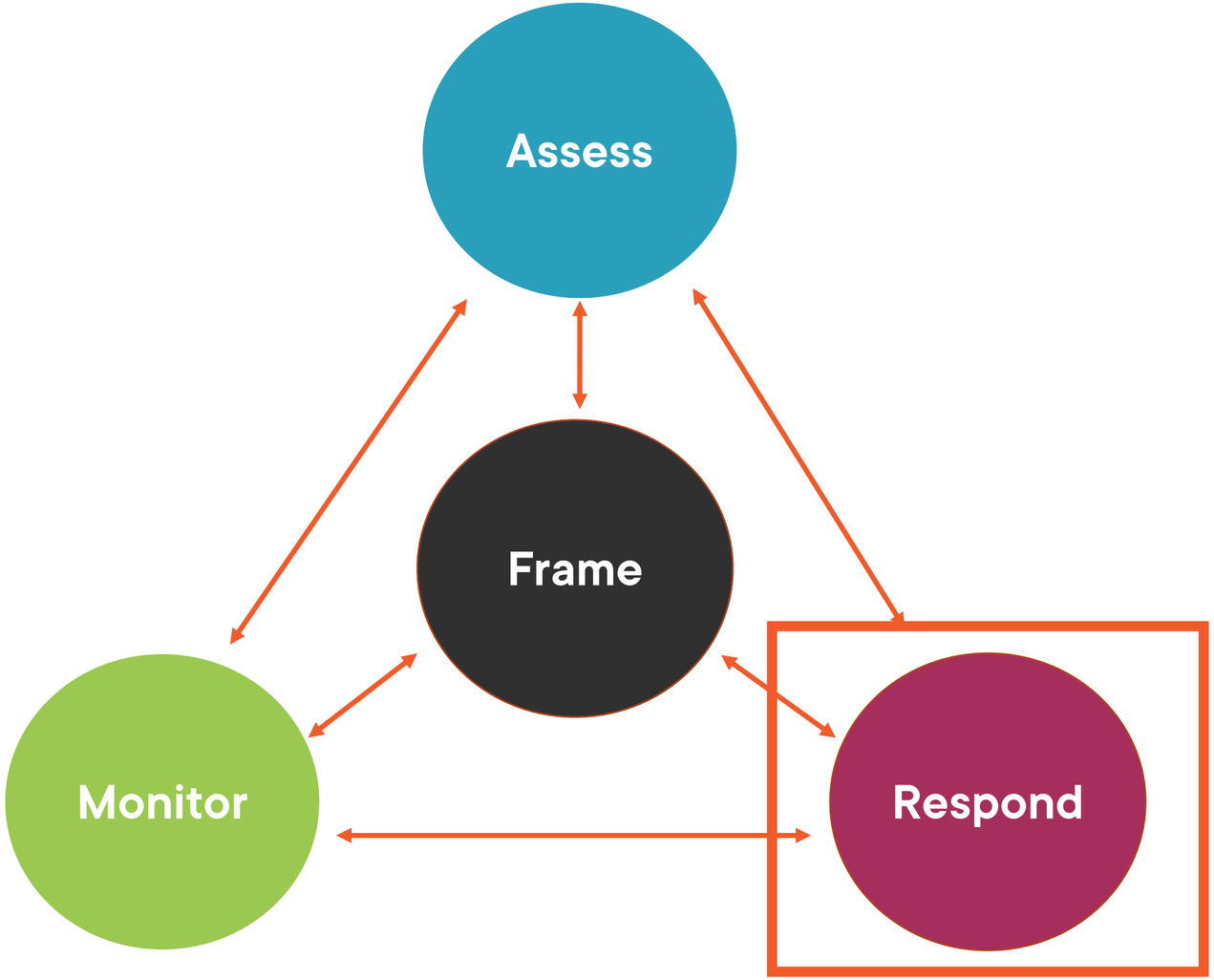
Legal and regulatory modifications

Organizational posture changes

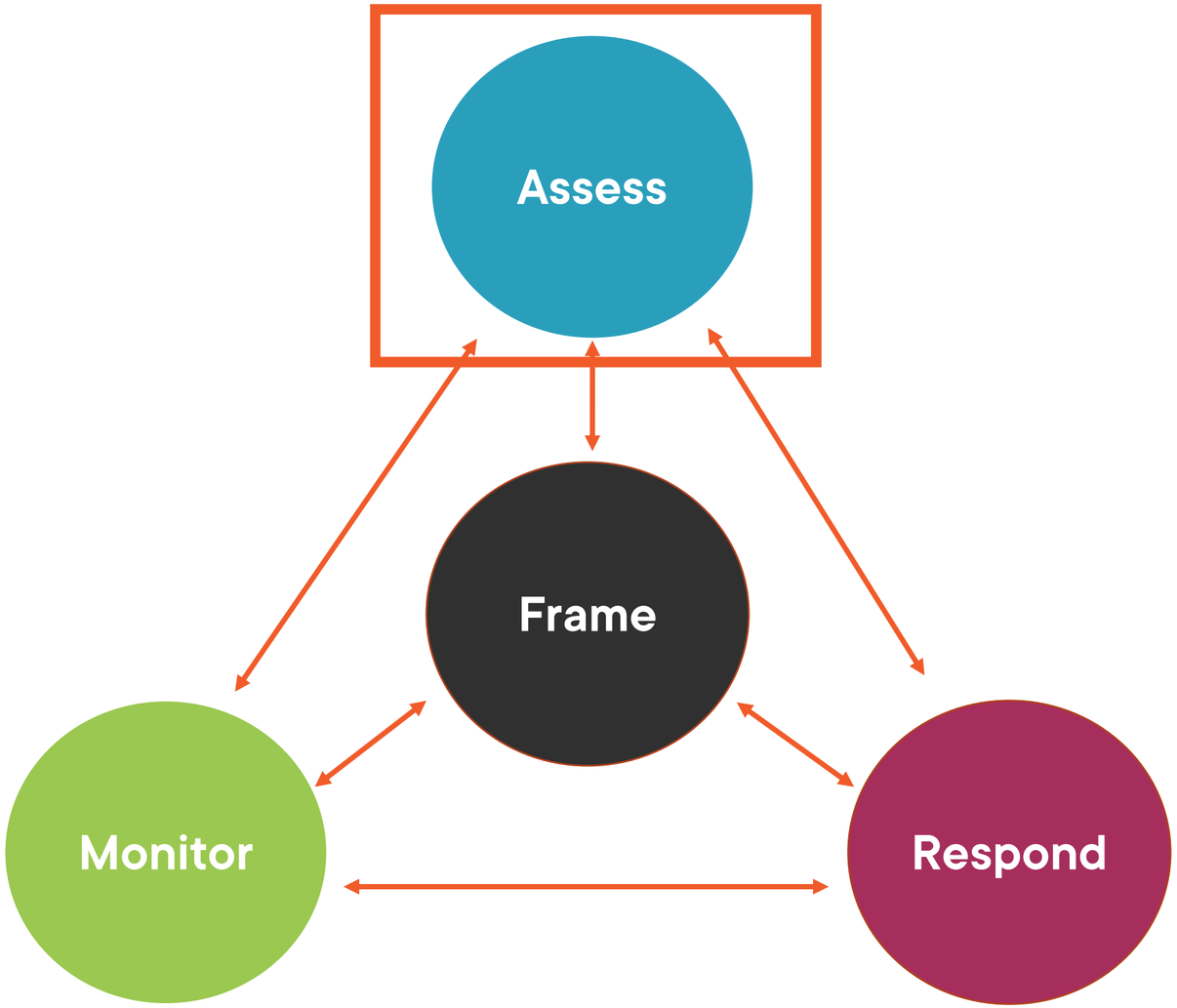
Risk Process Not Linear



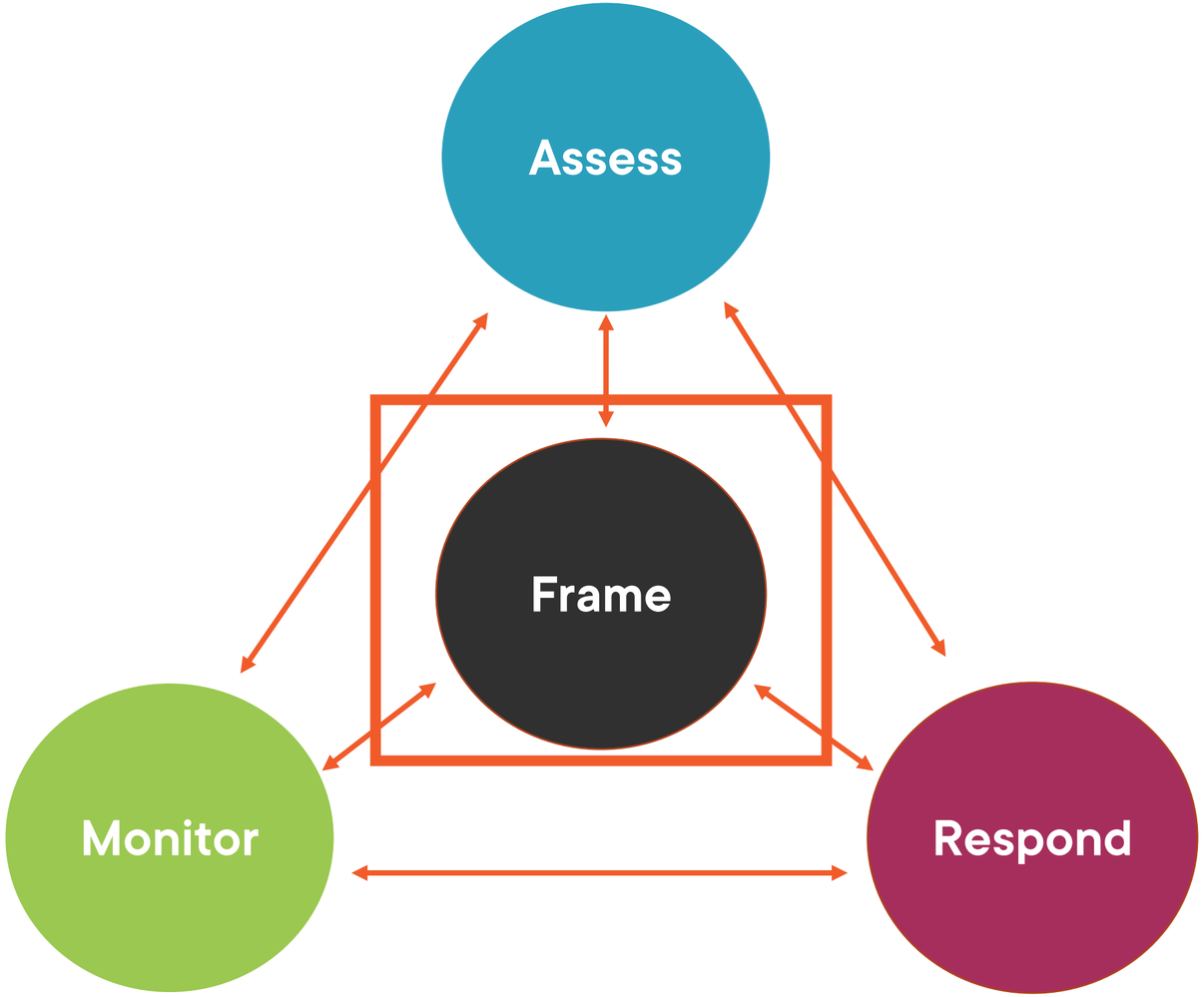
Risk Process Not Linear



Risk Process Not Linear



Risk Process Not Linear



Summary

What qualitative and quantitative risk analyses are realistic for your environment?

What steps to modify the environment are aligned with your business outcomes?

Up Next:
Cloud Audit and Assurance