Risk Assessment and Response

Dr. Lyron H. Andrews

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

@drlyronandrews | www.profabula.com

Overview

Overview

- Define risk appetite, profile, tolerance, and register
- Apply quantitative and qualitative analysis to a realistic use case
- Review security testing, vulnerability assessment, and remediation

Risk Profile, Appetite, and Tolerance

Risk appetite

Risk tolerance

Risk register

Risk profile

Tools of the Trade

Risk Tolerance

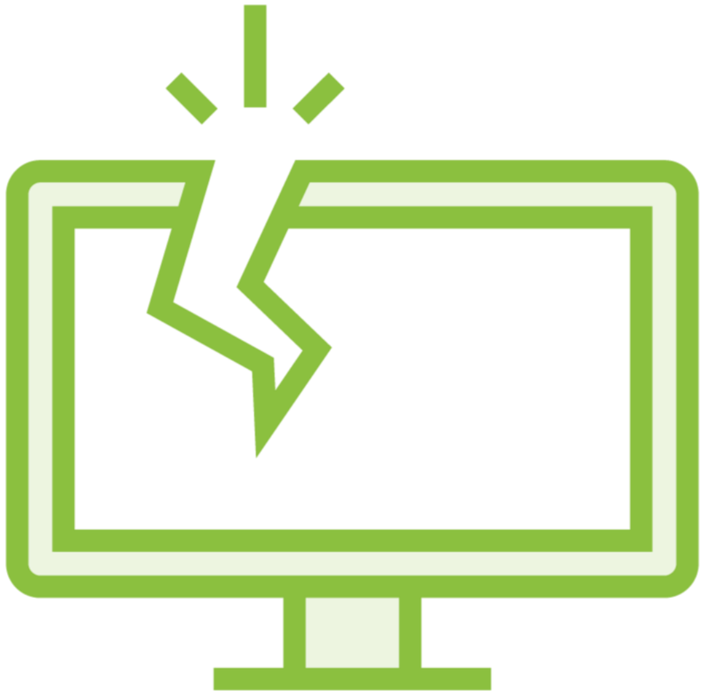
Behaviors and actions outside of the norm

Risk Visibility and Reporting

Contents of Sample Risk Register

Notional Risk Register											
ID	Priority	Risk Description	Risk Category	Current Assessment			Risk Response Type	Risk Response Cost	Risk Response Description	Risk Owner	Status
				Likelihood	Impact	Exposure Rating					
1											
2											
3											
4											
5											

NIST SP 800-221 Enterprise Impact of Information and Communications Technology Risk



Risk Profile

- Informed by risk register contents
- Overall effectiveness and maturity of risk program
- Describes the current state of risk program

Quantitative and Qualitative Analysis

Two Types of Risk Analysis

Qualitative

Subjective likelihood consideration of risk and the non-numeric impact

Quantitative

Objective empirical consideration of risk and corresponding cost if realized

Comparison: Quantitative and Qualitative

Qualitative	VS.	Quantitative
Subjective		Objective
Operational impact		Financial impact
Relatively easy		More complex
Derived faster		Longer duration

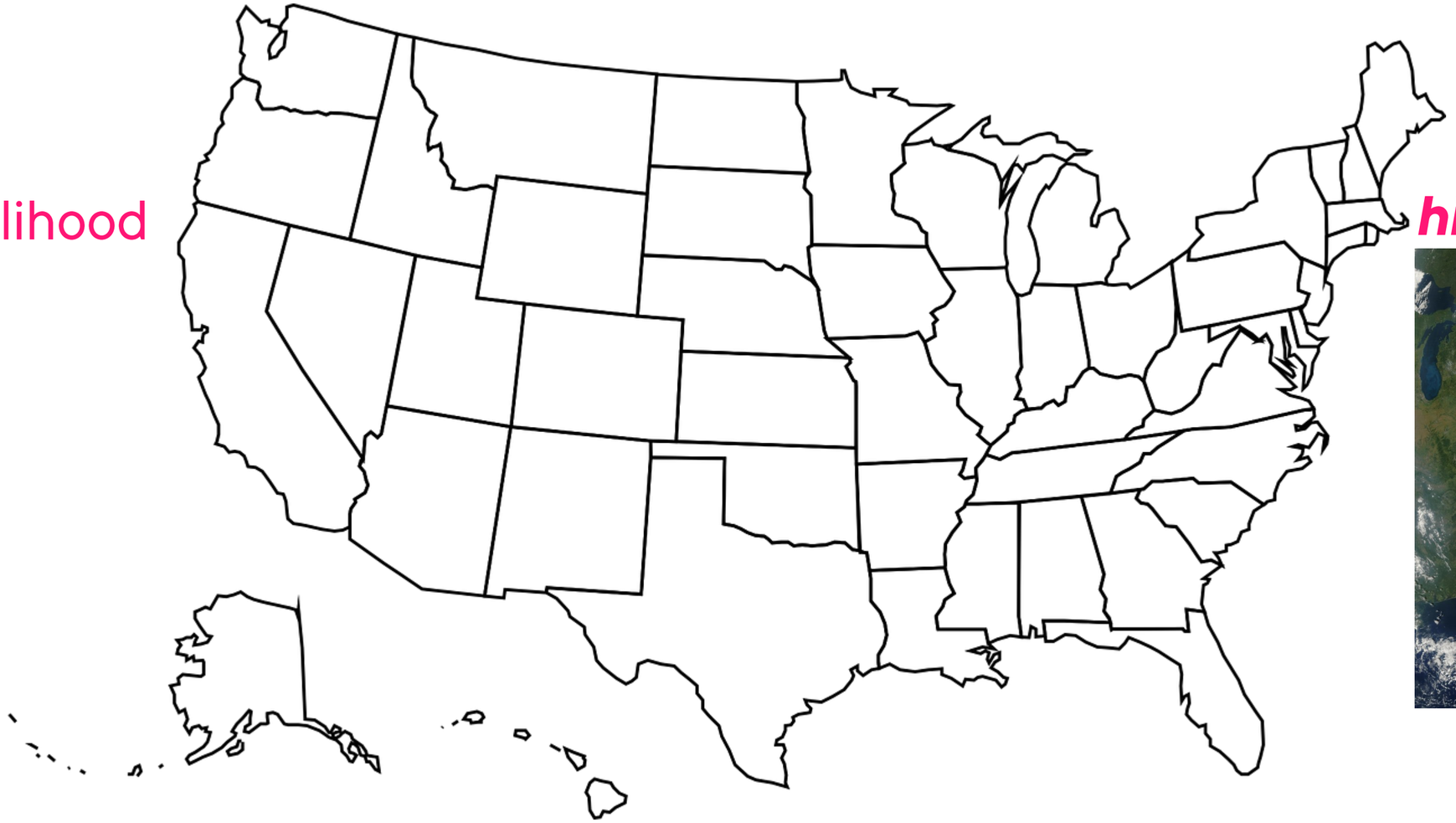
Qualitative Analysis - Likelihood and Impact

Category 5 Hurricane

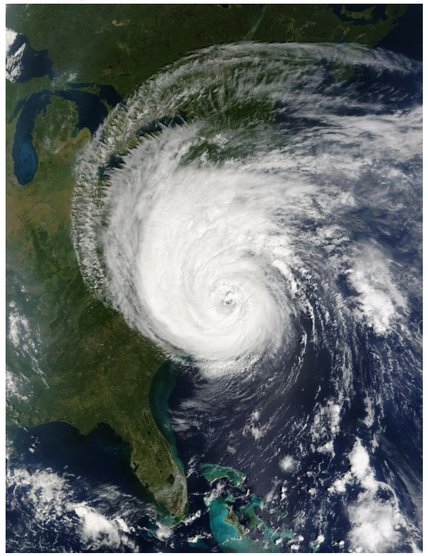
Qualitative Analysis - Likelihood and Impact

Category 5 Hurricane

low likelihood



high likelihood



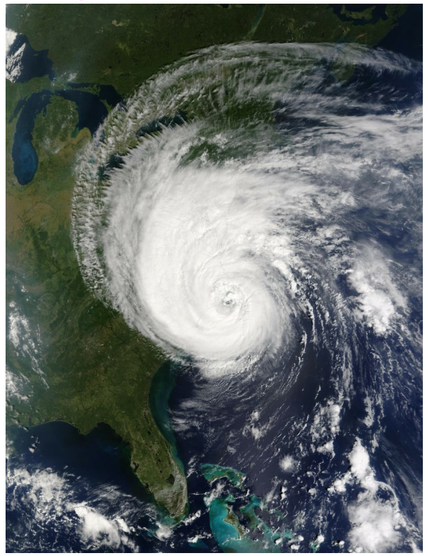
Qualitative Analysis - Likelihood and Impact

Category 5 Hurricane

Next focus on impact

low likelihood

high likelihood



Qualitative analyses are an excellent first step and foundation before doing a quantitative analysis.

Quantitative Analysis

Single Loss Expectancy (SLE)

Asset Value x Exposure Factor

Annual Rate of Occurrence (ARO)

Frequency / Years

Annual Loss Expectancy (ALE)

SLE x ARO = ALE

Quantitative Analysis

Single Loss Expectancy (SLE)

SLE = $4,800,000

Asset Value		Exposure Factor
$16,000,000	x	30%

Quantitative Analysis

Annual Rate of Occurrence (ARO)

ARO = .2

Frequency / Years

1 / 5

Quantitative Analysis

Annual Loss Expectancy (ALE)

ALE = $960,000

SLE x ARO

SLE = $4,800,000 X ARO = .2

Risk Response and Treatment

ISO/IEC 27005:2018: Information Security Risk Management

Modification

Retention

Avoidance

Sharing

Modification

Implements controls

Formerly called mitigation

Apply to flood threat in data center

Retention

Takes no extraordinary action

Formerly called acceptance

Apply to flood threat in data center

Sharing

Risk shared with another party

Formerly called transfer

Apply to flood threat in data center

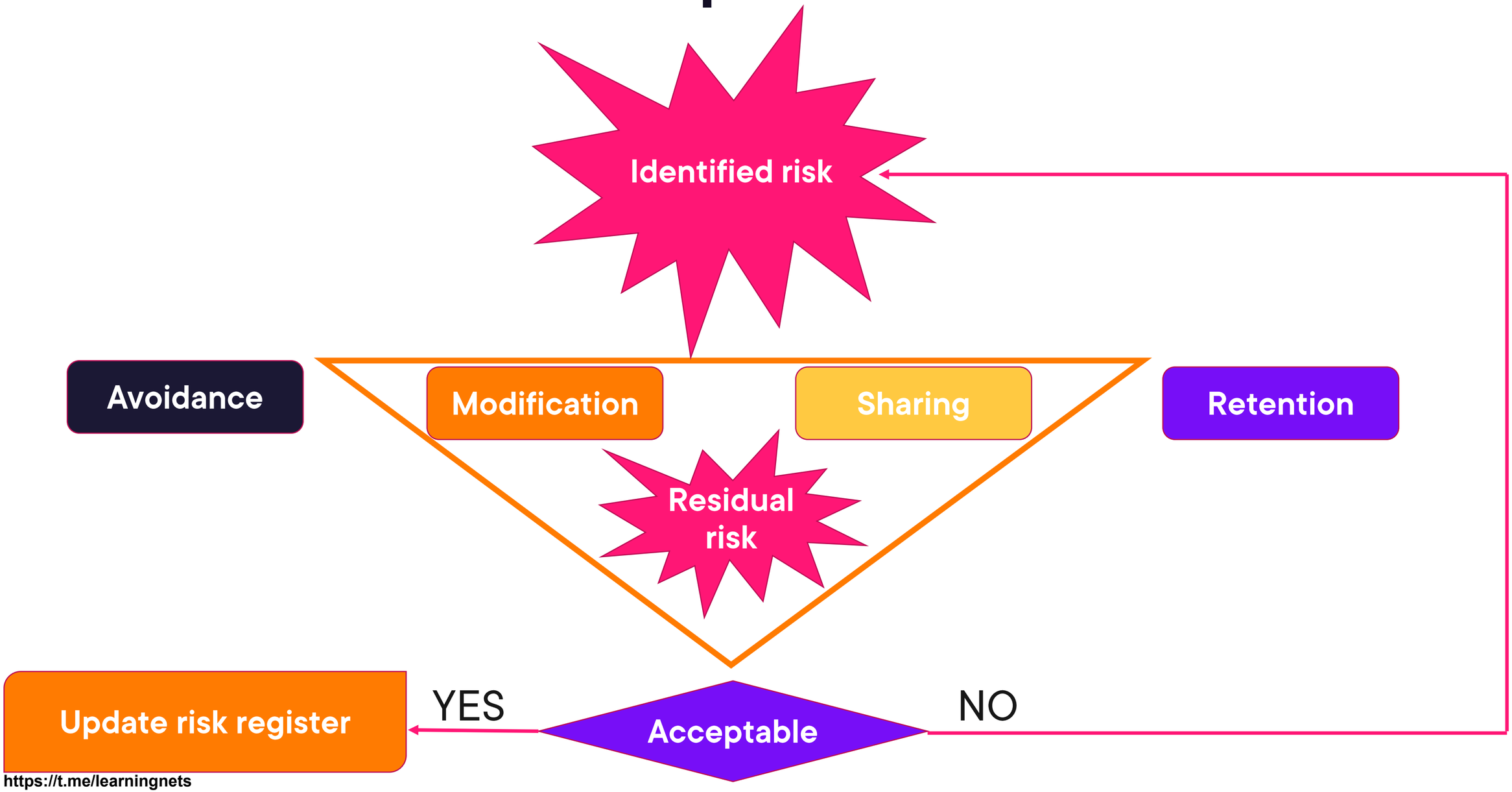
Avoidance

Same term used before

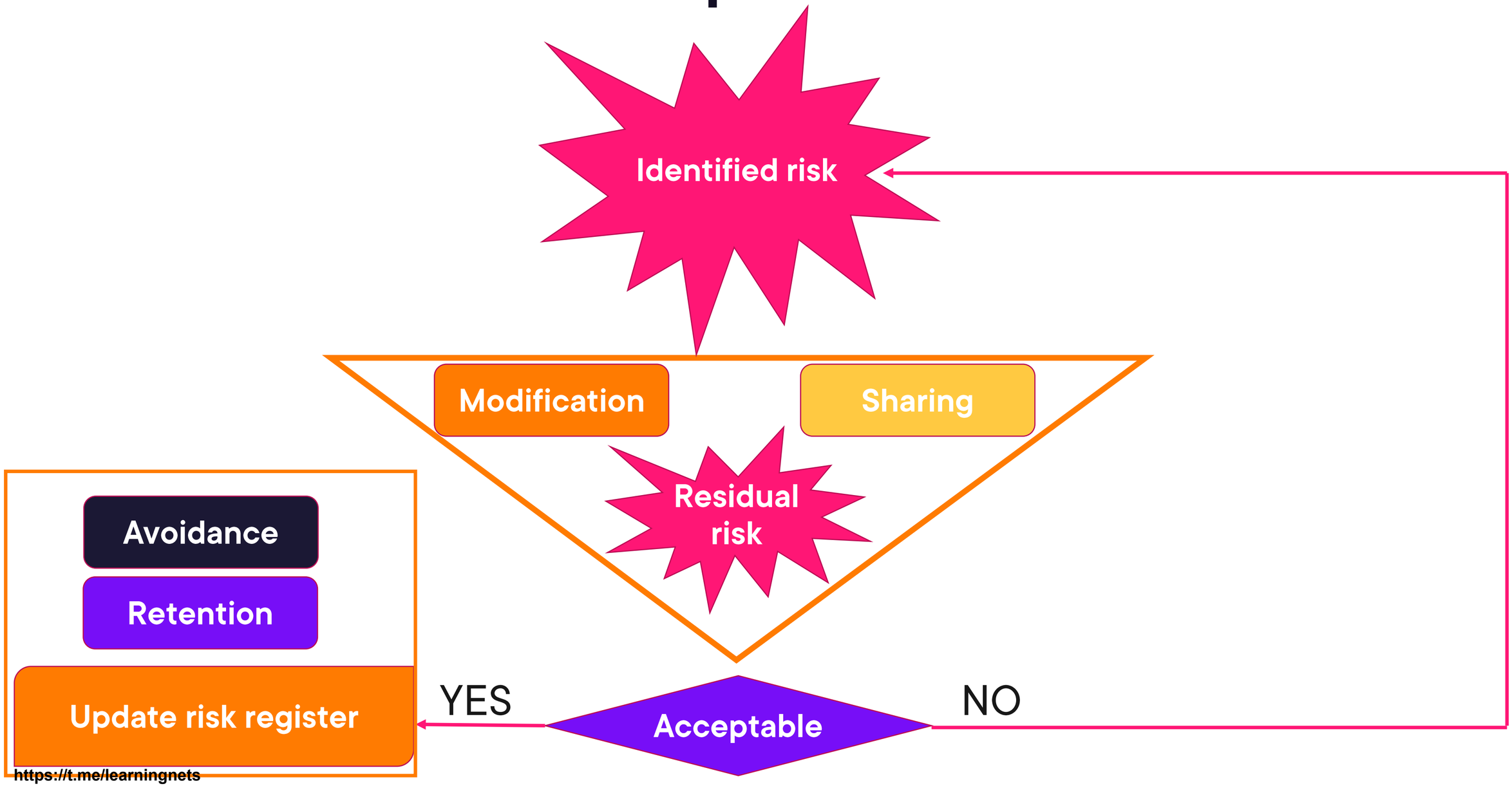
Expanded connotation

Apply to flood threat in data center

Risk Response Flow Cart



Risk Response Flow Cart



Quantifying and Qualifying Vulnerabilities

CVSS v4.0

Base: intrinsic qualities of a vulnerability

Threat: vulnerabilities that change over time

Environmental: vulnerability unique to a user's environment

Supplemental: used as additional insight into vulnerability

Base Metrics Composites

Exploitability

Ease of technical means of vulnerability

Impact

Direct consequence of successful exploit

Threat Metrics

Exploit maturity (E)

Not Defined (X)

Attacked (A)

Proof-of-Concept (P)

Unreported (U)

Environmental Metrics

Score dependent on importance of asset

Values related to loss possibility

Allows modification of earlier scoring

Supplemental Metrics

New to CVSS v4

Human safety focus

Not Defined (X), Present (P), or Negligible (N)

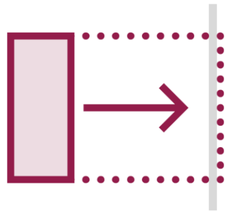
Vulnerability and Security Assessment

Vulnerability assessments address known issues that could be residing within a system.

Vulnerability Testing Capabilities

- OS fingerprinting
- Stimulus and response algorithms
- Privileged logon ability
- Cross-referencing
- Update capability
- Reporting capability

Potential Problems



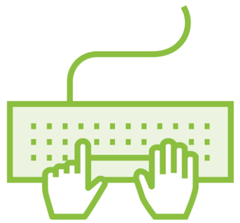
False positives

Filtering false positives

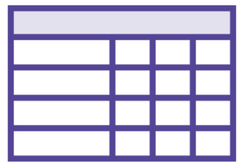
Crash exposure

Temporal information

Host Scanning



Encrypted authentication



Application weakness

Verify patch levels

Signed executables

Limited file permissions

Antimalware prevention

Firewall Testing

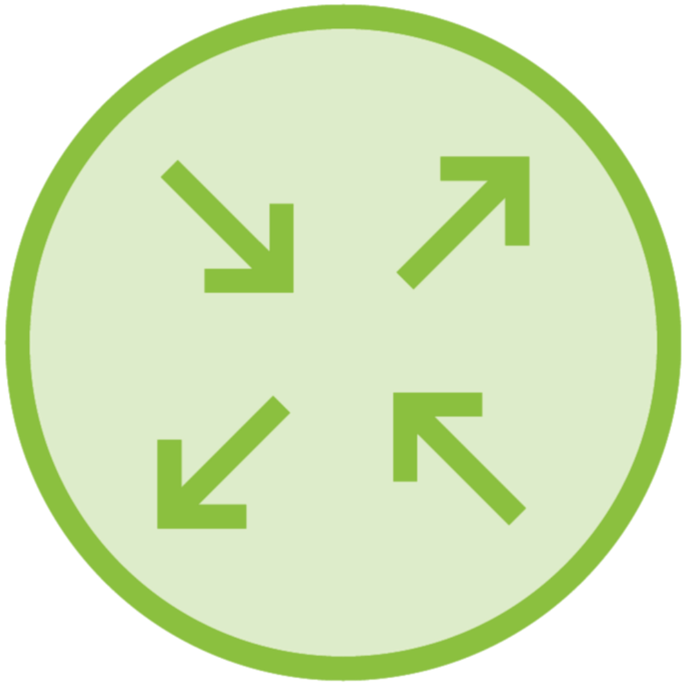
Limit TCP port scanning

Limit ICMP and UDP port scanning

Limit overlapping fragments

Limit half-open connections

Edge Router Testing



Telnet disabled

Authentication limits

Accounting system

Basic intrusion enunciation

Blocking RFC1918 from inbound and outbound

Penetration Testing

Vulnerability testing helps to expose the known-unknowns whereas penetration testing can expose the unknow-unknows.

Penetration Testing Modes

Zero knowledge

Partial knowledge

Full knowledge

Blind

Penetration Testing

Phase 1: Preparation

Establish approval and scope

Allow strategy to drive tool selection

Develop reporting format and plan

www.yourcompany.com + “for internal use only”

Penetration Testing

Phase 2: Reconnaissance

Collect public information

Map internal and external networks

Mixed methods can yield unexpected results

Perform risk analysis before active penetration

Phase 2 must be fully completed

Do not interrupt business

Penetration Testing

Phase 3: Enumeration

Web server may crash with ../../../../../../

Penetration Testing

Phase 4: Exploitation

Active penetration of agreed systems

Use vulnerability information

Weigh benefit of crashing system

Penetration Testing

Phase 5: Reporting

Provide documentation of test

Analyze the results

Review finding for remediation

Risk Review

MITRE ATT&CK Framework

Tactics

Techniques

Defenses

Course Summary

Summary

- Name the foundational designations that provide risk assessment capabilities
- When should quantitative and qualitative analysis be performed?
- What tools does your organization use for security assessments?

Up Next:

Continuous Risk Monitoring and Analysis