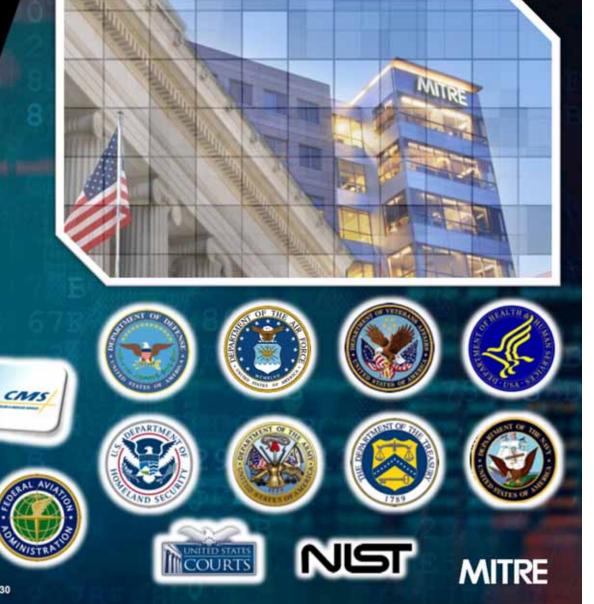
Risk Management Standards in Practice

Robert A. Martin 20 March 2018



CISQ Cyber Resilience Summit

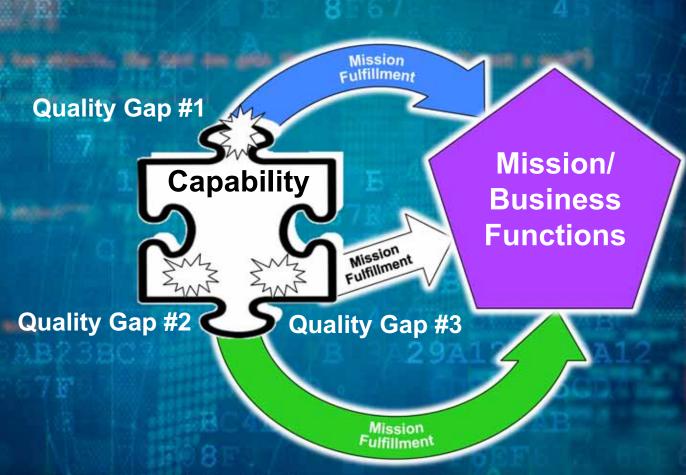






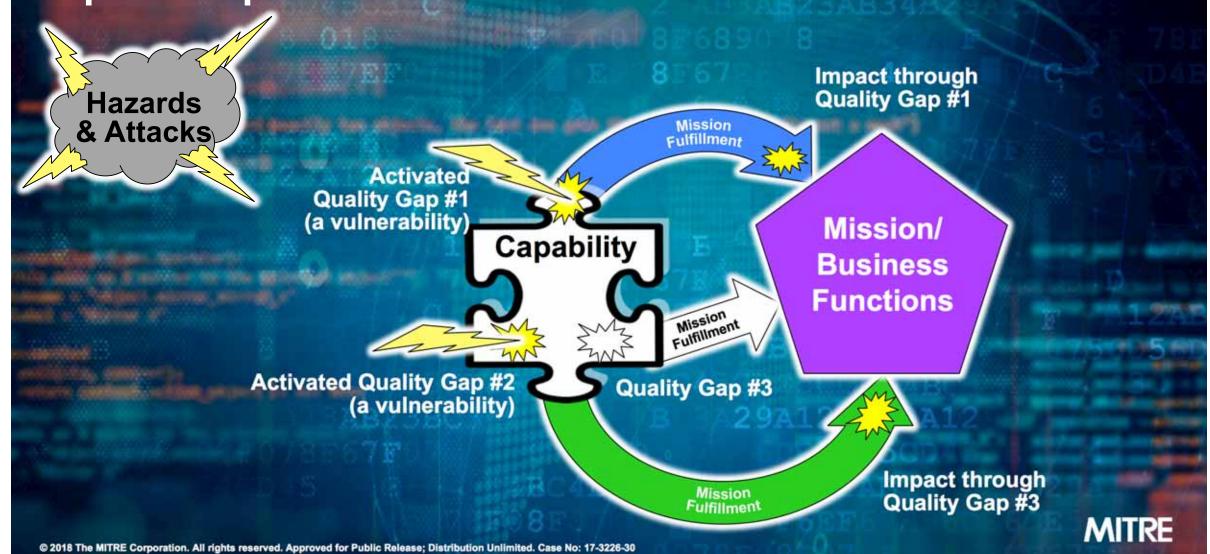
One element of Risk Management is Identifying Quality Gaps in Capabilities Critical to Mission/Business Functions

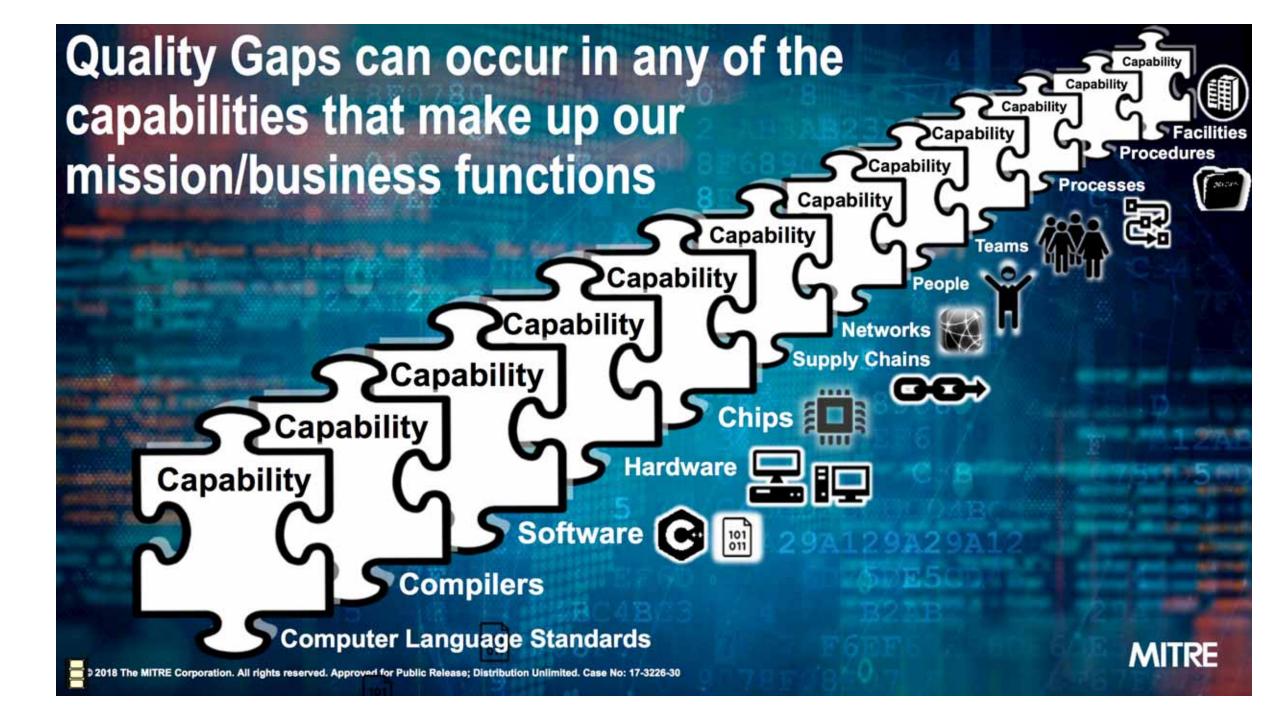




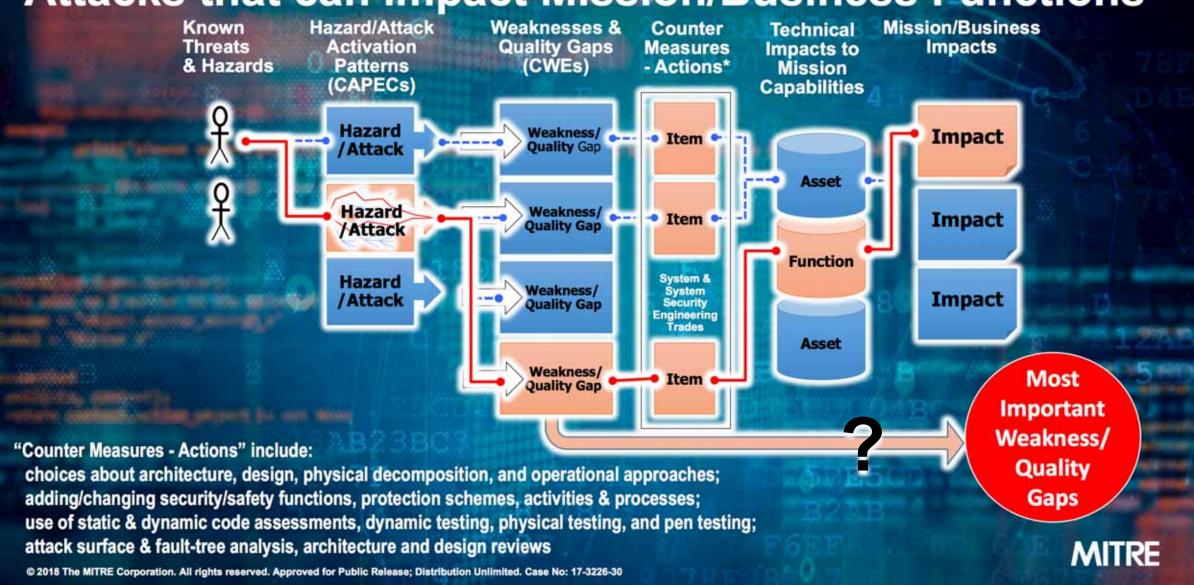
MITRE

One element of Risk Management is Identifying Quality Gaps in Capabilities Critical to Mission/Business Functions

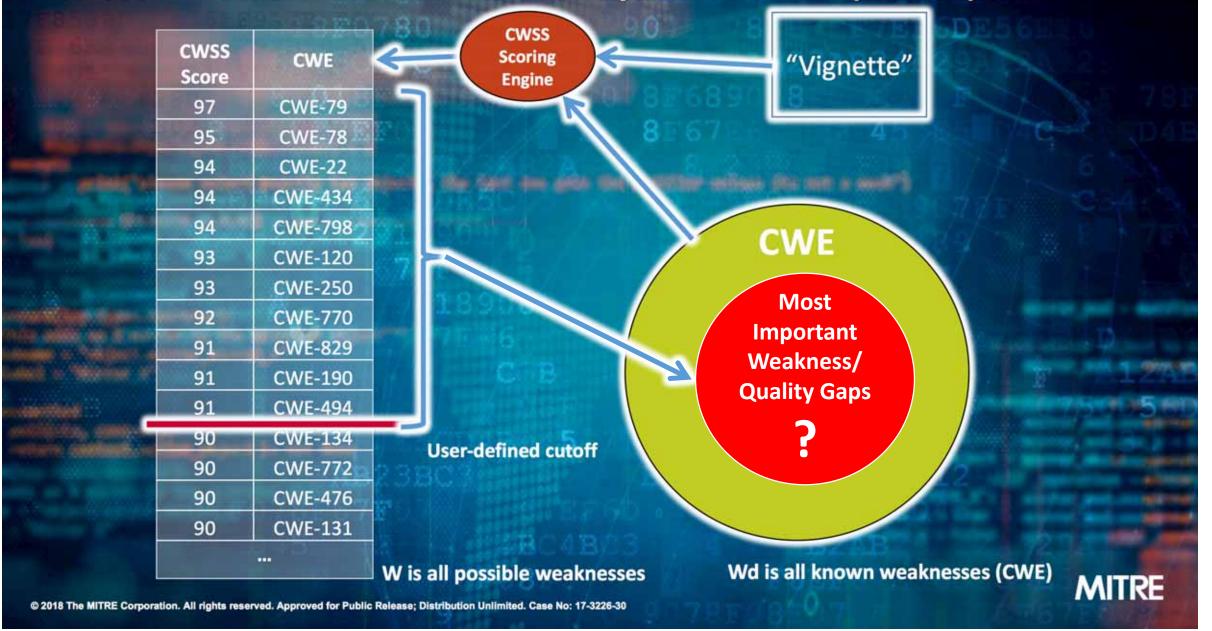




Risk Management is about addressing the Hazards & Attacks that can impact Mission/Business Functions



CWSS & the Common Weakness Risk Analysis Framework (CWRAF) in a Nutshell



Common Weakness Scoring System (5 Sep 2014)

Base Finding Group

- Technical Impact
- Acquired Privilege
- Acquired Privilege Layer
- Internal Control Effectiveness
- Finding Confidence

Attack Surface Group

- Required Privilege
- Required Privilege Layer
- Access Vector
- Authentication Strength
- · Level of Interaction
- Deployment Scope

CWSS

Environmental Group

Business Impact

na tilat kuningiliar salikasi (Pili tari) a sasait?

- Likelihood of Discovery
- Likelihood of Exploit
- External Control Effectiveness
- Prevalence

Common Weakness Risk Analysis Framework (CWRAF)

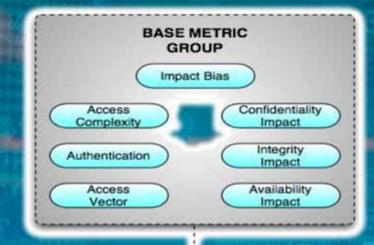
- Vignettes
- Technical Impact Scorecard

MITRE

© 2018 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 17-3226-30

Common Vulnerability Scoring System

- NVD provides CVSS scores for all CVE identifiers
- Payment Card Industry (PCI) using CVSS to determine compliance



Base Formula www.first.org/cvss/

Core aspects of the problem



Temp. Formula

Changes

over time

priorities

ENVIRONMENTAL
METRIC GROUP

Reflects your own

organizations

Formula

Collateral Damage Potential

> Target Distribution

> > **MITRE**

© 2018 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: 17-3226-30

Standards for Inputs and Calculating Risks...









2011 & 2016



ITU-T
TELECOMMUNICATION SECTOR

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY
Cybersecurity information exchange – Vulnerability/state exchange

Common weakness enumeration

Recommendation ITU-T X.1524

2012



ITU-T

**SLECTAMANICATION
BYTE:

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY
Cybersecurity information exchange – Vulnerability/state
exchange

Common weakness scoring system

Recommendation (TU-T X.1525

2015 MITRE

Cyber Risk is Expanding into Physical Risk

IT Risk

Operational Risk

Loss of information or service

Loss of reliability or safety

Loss of life or property

"Back office"

Production

© 2017 Gartner. All rights reserved.

MITRE

Who's risk is being managed?

