+discussion in the new year with some custom graphics

If NIST NICE desires to maximize promotion of 800-181 to Commercial/Enterprise leaders (increase acceptance and public-private sector collaboration):

1. Fix the policy/vocabulary and operational gaps between ‘Risk’ and ‘Threat’ first? (see PNG attached)
    a. Example, even NIST definitions show the difference between ‘IT risk’ (technical) and ‘Business risk’ (strategic), but we (including NIST) are not executing/pitching 800-181 in this?
2. Pitch less ‘Event’/Incident Threat’ ‘SOC’ ‘reactive’ using ‘DHS NPPD/CISA’ alone (start using NPPD/CISA and I&A jointly? More ‘proactive’ ‘predictive’ ‘preventative’?)
3. Pitch more ‘Fusion Operations’ ‘Risk (Management)’ ‘CRISC’ ‘OpenFAIR’ ‘Carnegie Mellon’ ‘USNA’ and ‘External/Internal/Other data class of Threat (Capability, Intent, Controls)’?
    a. If you want to be most relevant to ‘C-Suite’ executives who make the decision to keep/apply 800-181, not the lower level practitioners?

/r

NISTIR 7298 v3

RISK

- Has (28) separate definitions
- Mentions Likelihood (19) and Impact (33) times
- Abbreviation(s) and Synonym(s):
  - Capability, Manage and Assess Risk

https://csrc.nist.gov/glossary/term/risk

NISTIR 7298 v3

THREAT

- Has (21) separate definitions
- Mentions Capability (0), Intent (0), and Control (0) times
- Abbreviation(s) and Synonym(s):
  - Cyber Threat

https://csrc.nist.gov/glossary/term/threat

NISTIR 7298 v3

VULNERABILITY

- Has (17) separate definitions
- Mentions Controls (12) and Weakness (15) times
- Abbreviation(s) and Synonym(s):
  - None

https://csrc.nist.gov/glossary/term/vulnerability

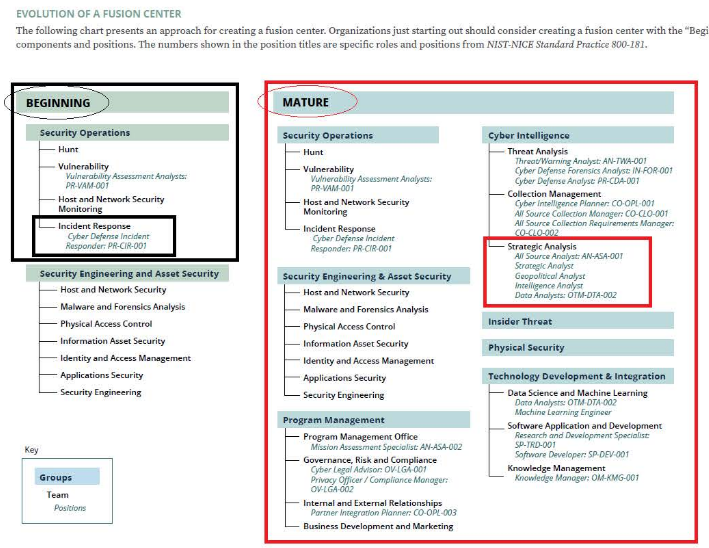
Definition Context:

Risk Management (14) definitions mentions Likelihood (0) Impact (1) times
Mentions *Risk (39 times in context)

- managing risks to agency operations
- risk management process
- risk assessment
- risk to mission/business
- acceptable level or risk
- risk mitigation strategy
- risk-related activities
- responding to risk
- monitoring risk
- information technology related risks
- information security risk

- event or condition
- circumstance or event
- “threat source”
- potential cause of an unwanted incident
- possible danger to a computer system
- an activity
- potential source of an adverse event
- likelihood or frequency of a harmful event

- “in the weeds” …



EVOLUTION OF A FUSION CENTER

The following chart presents an approach for creating a fusion center. Organizations just starting out should consider creating a fusion center with the "Beginning" components and positions. The numbers shown in the position titles are specific roles and positions from *NIST-NICE Standard Practice 800-181*.

BEGINNING

Security Operations

- Hunt
- Vulnerability
  - *Vulnerability Assessment Analysts: PR-VAM-001*
- Host and Network Security Monitoring
- Incident Response
  - *Cyber Defense Incident Responder: PR-CIR-001*

Security Engineering and Asset Security

- Host and Network Security
- Malware and Forensics Analysis
- Physical Access Control
- Information Asset Security
- Identity and Access Management
- Applications Security
- Security Engineering

Key

Groups

Team

Positions

MATURE

Security Operations

- Hunt
- Vulnerability
  - *Vulnerability Assessment Analysts: PR-VAM-001*
- Host and Network Security Monitoring
- Incident Response
  - *Cyber Defense Incident Responder: PR-CIR-001*

Security Engineering & Asset Security

- Host and Network Security
- Malware and Forensics Analysis
- Physical Access Control
- Information Asset Security
- Identity and Access Management
- Applications Security
- Security Engineering

Program Management

- Program Management Office
  - *Mission Assessment Specialist: AN-ASA-002*
- Governance, Risk and Compliance
  - *Cyber Legal Advisor: OV-LGA-001*
  - *Privacy Officer / Compliance Manager: OV-LGA-002*
- Internal and External Relationships
  - *Partner Integration Planner: CO-OPL-003*
- Business Development and Marketing

Cyber Intelligence

- Threat Analysis
  - *Threat/Warning Analyst: AN-TWA-001*
  - *Cyber Defense Forensics Analyst: IN-FOR-001*
  - *Cyber Defense Analyst: PR-CDA-001*
- Collection Management
  - *Cyber Intelligence Planner: CO-OPL-001*
  - *All Source Collection Manager: CO-CLO-001*
  - *All Source Collection Requirements Manager: CO-CLO-002*
- Strategic Analysis
  - *All Source Analyst: AN-ASA-001*
  - *Strategic Analyst*
  - *Geopolitical Analyst*
  - *Intelligence Analyst*
  - *Data Analysts: OTM-DTA-002*

Insider Threat

Physical Security

Technology Development & Integration

- Data Science and Machine Learning
  - *Data Analysts: OTM-DTA-002*
  - *Machine Learning Engineer*
- Software Application and Development
  - *Research and Development Specialist: SP-TRD-001*
  - *Software Developer: SP-DEV-001*
- Knowledge Management
  - *Knowledge Manager: OM-KMG-001*

Fig 1. **Carnegie Mellon SEI 'Cyber Intelligence Tradecraft Report' for ODNI, 2019**

Cyber Operations (All Disciplines/Roles) 'Mature'

Common Lexicon/Language of the **Operational Environment**:

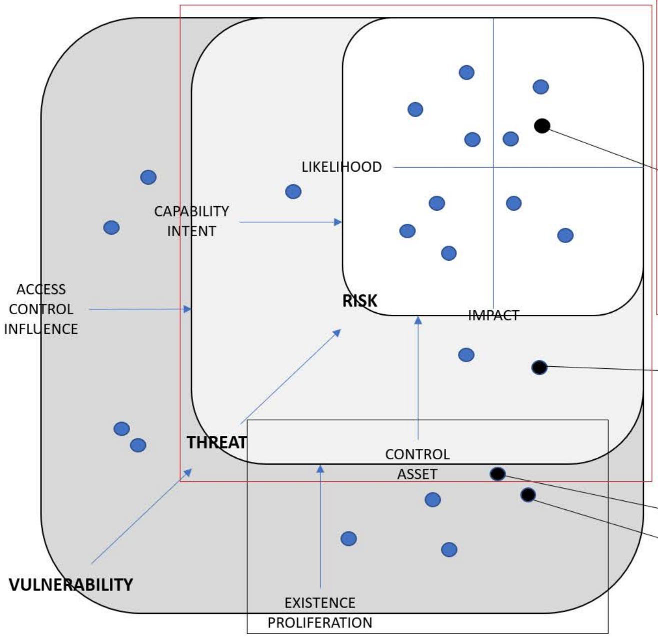
Risk is the **exposure to consequence** (loss); calculated as **likelihood x impact** of an incident or event triggered by a threat. Risk technical and non-technical examples include compliance, privacy, fraud, geopolitical (country-nexus), cyber attacks, etc.

Threat is the **trigger to consequence** (loss); resulting from a **person, group, or thing** with capability and intent to inflict consequence. Threat technical and non-technical examples include artificial intelligence, Advanced Persistent Threat (APTs), insiders, nature, etc.

Vulnerability is the **path to consequence** (loss); as an avenue of access, control, or influence that can inflict consequence. Vulnerability technical and non-technical examples include unpatched systems, poor coding practices, employees with no cybersecurity awareness,

DAILY STOP

Cybersecurity/CISSP/Incident Responder



RISK

- Regulatory
- Compliance
- Privacy
- Fraud
- Safety
- Business Continuity
- Economic Conditions
- **Geopolitical**
- Conduct
- Resistance to Change
- Succession and Talent
- IT Failure
- Disruptive Innovations
- **Cyber Attacks**

THREAT

- AI
- **APT**
- Nation State
- Individual
- Insider
- Nature

VULNERABILITY

- DDoS
- **Phishing**
- Patching
- **Malware**
- VPN
- IoT
- Data
- Flooding

DAILY STOP