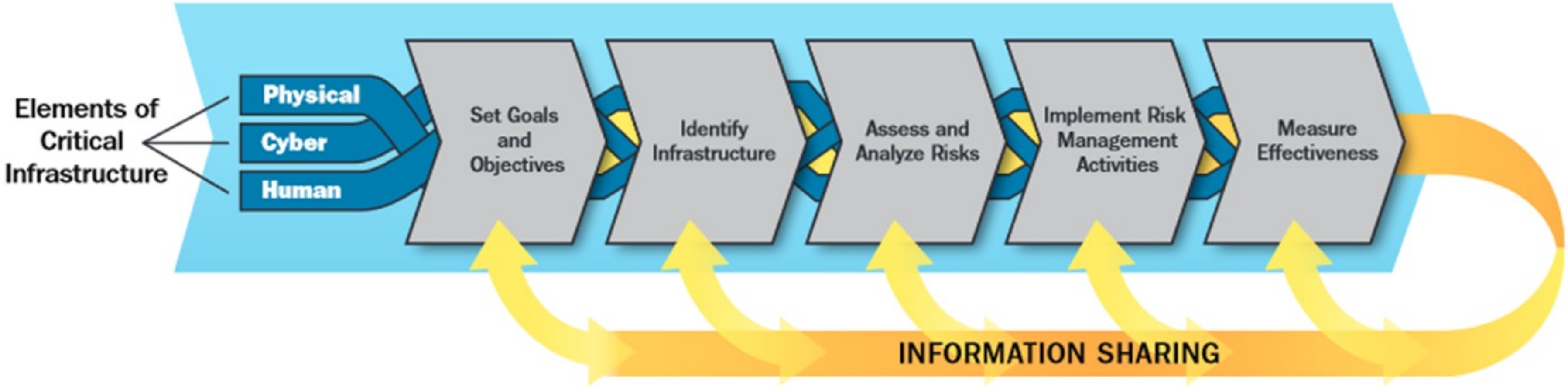
Health and Public Health Sector Specific Plan for Risk Management

John Petrozzelli

Director, MassCyberCenter

National Infrastructure Protection Plan Risk Management Framework

- Identifying and prioritizing each sector’s critical components and key internal and external dependencies and interdependencies;
- Defining the threats and hazards most likely to cause harm or disruption of services; and employing prioritized approaches to prevent, protect against, and/or mitigate
- The effects of those threats and hazards. It also increases security and strengthens resilience by
- Identifying and prioritizing actions to ensure continuity of essential functions and services and support enhanced response and restoration in the context of incidents in progress.



Source: NIPP Supplemental Tool: Executing A Critical Infrastructure Risk Management Approach

Step 1 Set Goals and Objectives: Define specific outcomes, conditions, end points, or performance targets that collectively describe an effective and desired risk management posture.

- Assess and analyze threats to, vulnerabilities of, and consequences to your organization:
  - Secure assets against human, physical, and cyber threats through sustainable efforts to reduce risk, while accounting for the costs and benefits of security investments;
  - Minimizing the adverse consequences of incidents through advance planning and mitigation efforts, as well as effective responses to save lives and ensure the rapid recovery of essential services;
  - Share actionable and relevant information across the critical infrastructure community to build awareness and enable risk-informed decision making; and
  - Promote learning and adaptation during and after exercises and incidents

Source: NIPP Supplemental Tool: Executing A Critical Infrastructure Risk Management Approach

Step 1 Set Goals and Objectives: Define specific outcomes, conditions, end points, or performance targets that collectively describe an effective and desired risk management posture. (Con’t)

- Consider distinct assets, systems, networks, functions, operational processes, business environments, and risk management approaches;
- Define the risk management posture that critical infrastructure partners seek to attain individually or collectively; and
- Express this posture in terms of the objectives and outcomes sought

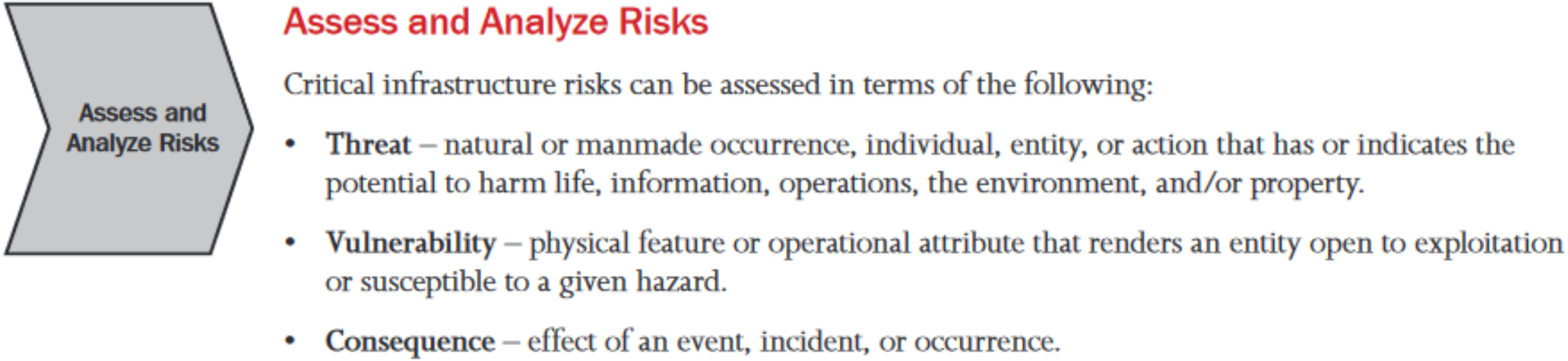
Source: NIPP Supplemental Tool: Executing A Critical Infrastructure Risk Management Approach

Step 2 Identify Infrastructure: Identify assets, systems, and networks that contribute to critical functionality and collect information pertinent to risk management, including analysis of dependencies and interdependencies.

- Consider distinct assets, systems, networks, functions, operational processes, business environments, and risk management approaches:
  - People
  - Data (proprietary, customer)
  - Reputation
  - Equipment
  - Labs and other facilities
  - IT Equipment
  - Medical Devices
  - Vehicles
  - Policies
  - Standard operating procedures
  - Cloud resources

Source: NIPP Supplemental Tool: Executing A Critical Infrastructure Risk Management Approach

Step 3 Assess and Analyze Risks: Evaluate the risk, taking into consideration the potential direct and indirect consequences of an incident, known vulnerabilities to various potential threats or hazards, and general or specific threat information.



Assess and Analyze Risks

Assess and Analyze Risks

Critical infrastructure risks can be assessed in terms of the following:

- **Threat** – natural or manmade occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property.
- **Vulnerability** – physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard.
- **Consequence** – effect of an event, incident, or occurrence.

Source: NIPP Supplemental Tool: Executing A Critical Infrastructure Risk Management Approach

Assess and Analyze Risks (Con’t)

Threat: A natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property. For the purpose of calculating risk, the threat of an unintentional hazard is generally estimated as the likelihood that a hazard will manifest itself. Intentional hazard is generally estimated as the likelihood of an attack being attempted by an adversary. In the case of intentionally adversarial actors and actions, for both physical and cyber effects, the threat likelihood is estimated based on the intent and capability of the adversary.

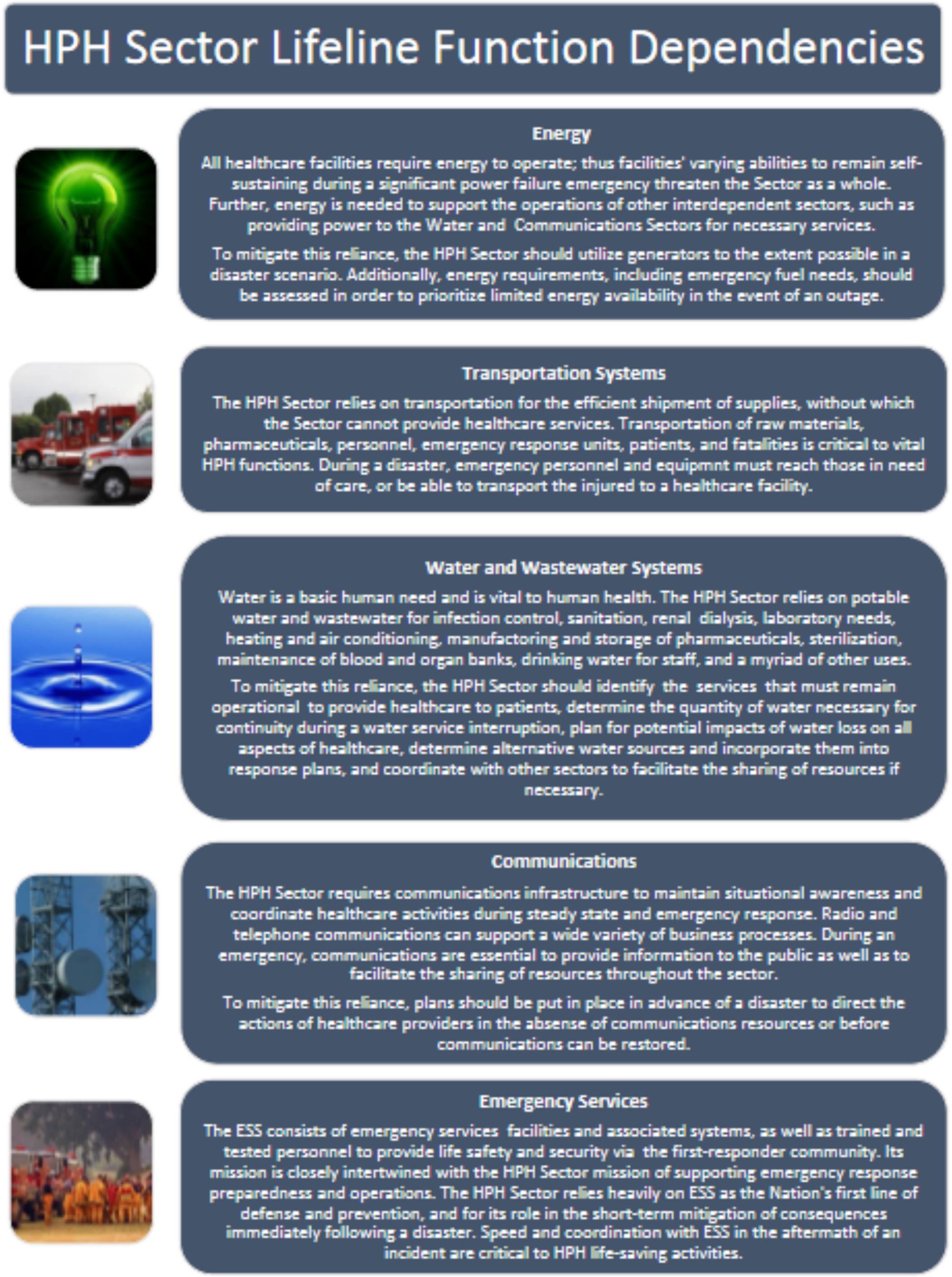
- Pandemics and Health Crises
- Cyber Attacks
- Malicious Human Acts
- Supply Chain Disruption and Corruption
- Space Weather and Electromagnetic Pulse (EMP) Risks
- Internal HPH Sector Dependencies and Interdependencies
- Cross-Sector Dependency and Interdependency Risks
- Natural Disasters, Extreme Weather, and Climate Change

Source: NIPP Supplemental Tool: Executing A Critical Infrastructure Risk Management Approach

Assess and Analyze Risks (Con’t)

Vulnerability: A physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given threat or hazard. In calculating the risk of an intentional threat, a common measure of vulnerability is the likelihood that an attack is successful, given that it is attempted.

Source: NIPP Supplemental Tool: Executing A Critical Infrastructure Risk Management Approach



HPH Sector Lifeline Function Dependencies

Energy

All healthcare facilities require energy to operate; thus facilities' varying abilities to remain self-sustaining during a significant power failure emergency threaten the Sector as a whole. Further, energy is needed to support the operations of other interdependent sectors, such as providing power to the Water and Communications Sectors for necessary services.

To mitigate this reliance, the HPH Sector should utilize generators to the extent possible in a disaster scenario. Additionally, energy requirements, including emergency fuel needs, should be assessed in order to prioritize limited energy availability in the event of an outage.

Transportation Systems

The HPH Sector relies on transportation for the efficient shipment of supplies, without which the Sector cannot provide healthcare services. Transportation of raw materials, pharmaceuticals, personnel, emergency response units, patients, and fatalities is critical to vital HPH functions. During a disaster, emergency personnel and equipmnt must reach those in need of care, or be able to transport the injured to a healthcare facility.

Water and Wastewater Systems

Water is a basic human need and is vital to human health. The HPH Sector relies on potable water and wastewater for infection control, sanitation, renal dialysis, laboratory needs, heating and air conditioning, manufactoring and storage of pharmaceuticals, sterilization, maintenance of blood and organ banks, drinking water for staff, and a myriad of other uses.

To mitigate this reliance, the HPH Sector should identify the services that must remain operational to provide healthcare to patients, determine the quantity of water necessary for continuity during a water service interruption, plan for potential impacts of water loss on all aspects of healthcare, determine alternative water sources and incorporate them into response plans, and coordinate with other sectors to facilitate the sharing of resources if necessary.

Communications

The HPH Sector requires communications infrastructure to maintain situational awareness and coordinate healthcare activities during steady state and emergency response. Radio and telephone communications can support a wide variety of business processes. During an emergency, communications are essential to provide information to the public as well as to facilitate the sharing of resources throughout the sector.

To mitigate this reliance, plans should be put in place in advance of a disaster to direct the actions of healthcare providers in the absense of communications resources or before communications can be restored.

Emergency Services

The ESS consists of emergency services facilities and associated systems, as well as trained and tested personnel to provide life safety and security via the first-responder community. Its mission is closely intertwined with the HPH Sector mission of supporting emergency response preparedness and operations. The HPH Sector relies heavily on ESS as the Nation's first line of defense and prevention, and for its role in the short-term mitigation of consequences immediately following a disaster. Speed and coordination with ESS in the aftermath of an incident are critical to HPH life-saving activities.

Assess and Analyze Risks (Con’t)

Consequence: The effect of an event, incident, or occurrence. It reflects the level, duration, and nature of the loss resulting from the incident. Potential consequences may include public health and safety (i.e., loss of life and illness), economic (direct and indirect), psychological, and governance/mission impacts

Exercising Scenarios to inform risk assessments: A scenario is a hypothetical situation consisting of an identified threat or hazard, an entity impacted by that hazard, and associated conditions including consequences, when appropriate.

Source: NIPP Supplemental Tool: Executing A Critical Infrastructure Risk Management Approach

Step 4 Implement Risk Management Activities: Make decisions and implement risk management approaches to control, accept, transfer, or avoid risks. Approaches can include prevention, protection, mitigation, response, and recovery activities.

- Risk management activities also may include the means for reducing the consequences of an attack or incident. These actions are focused on mitigation, response, and/or recovery. Often it is more cost-effective to build security and resilience into assets, systems, and networks than to retrofit them after initial development and deployment.

Step 5 Measure: Use metrics and other evaluation procedures to measure progress and assess the effectiveness of efforts to secure and strengthen the resilience of critical infrastructure

- Performance metrics allow partners to track progress against priorities and against their goals and objectives. The metrics provide a basis for the critical infrastructure community to establish accountability, document actual performance, promote effective management, and provide a feedback mechanism to inform decision making.

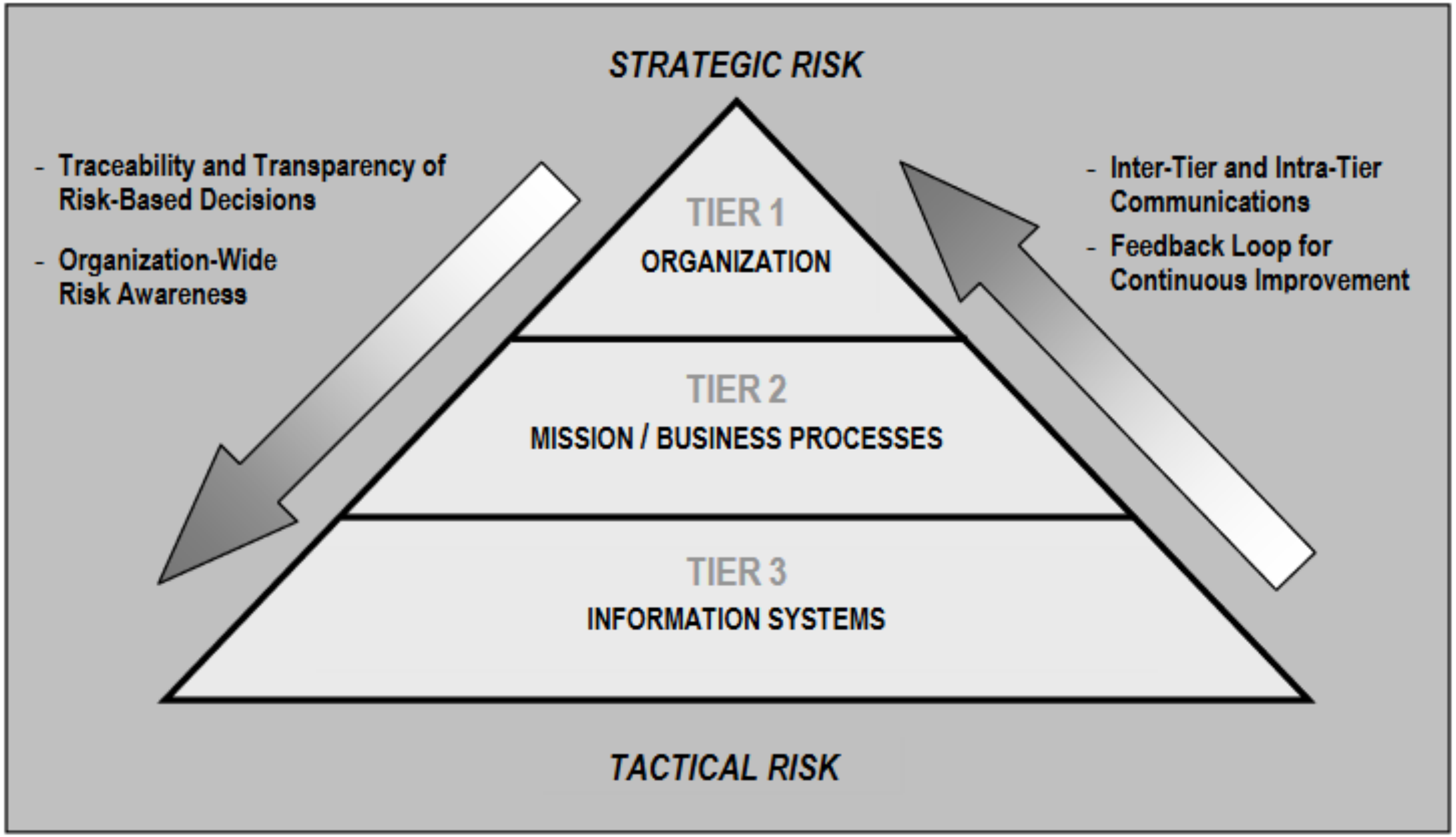
- Metrics are used to focus attention on areas of security and resilience that warrant additional resources or other changes through an analysis of challenges and priorities at the national, sector, and owner/operator levels

Conducting Risk Assessments

NIST Special Publication 800-30R1 Guide for Conducting Risk Assessments

- *Risk* is a measure of the extent to which an entity is threatened by a potential circumstance or event, and is typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

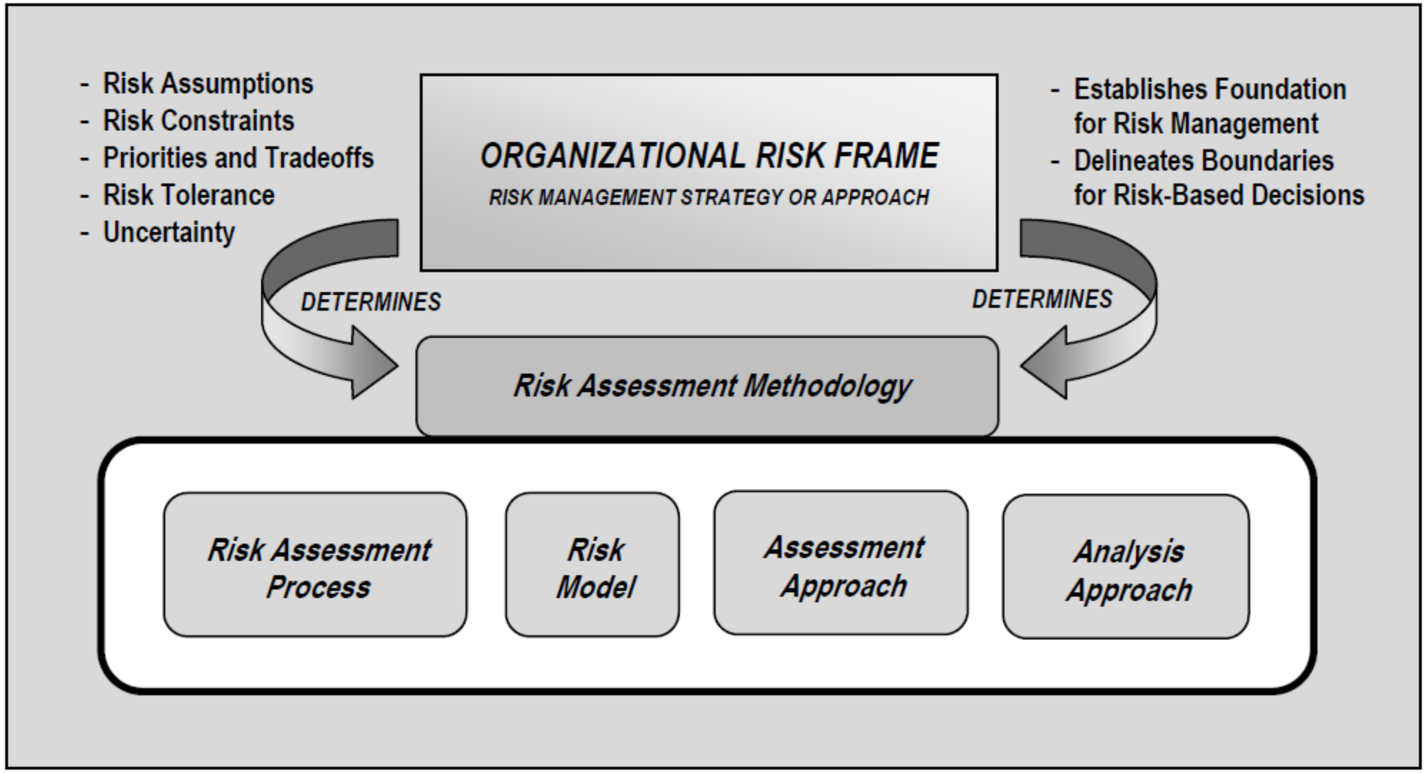
- An organization may conduct a risk assessment at one or more tiers


STRATEGIC RISK
- Traceability and Transparency of Risk-Based Decisions
- Organization-Wide Risk Awareness
TIER 1
ORGANIZATION
TIER 2
MISSION / BUSINESS PROCESSES
TIER 3
INFORMATION SYSTEMS
- Inter-Tier and Intra-Tier Communications
- Feedback Loop for Continuous Improvement
TACTICAL RISK

Risk Assessment Methodology

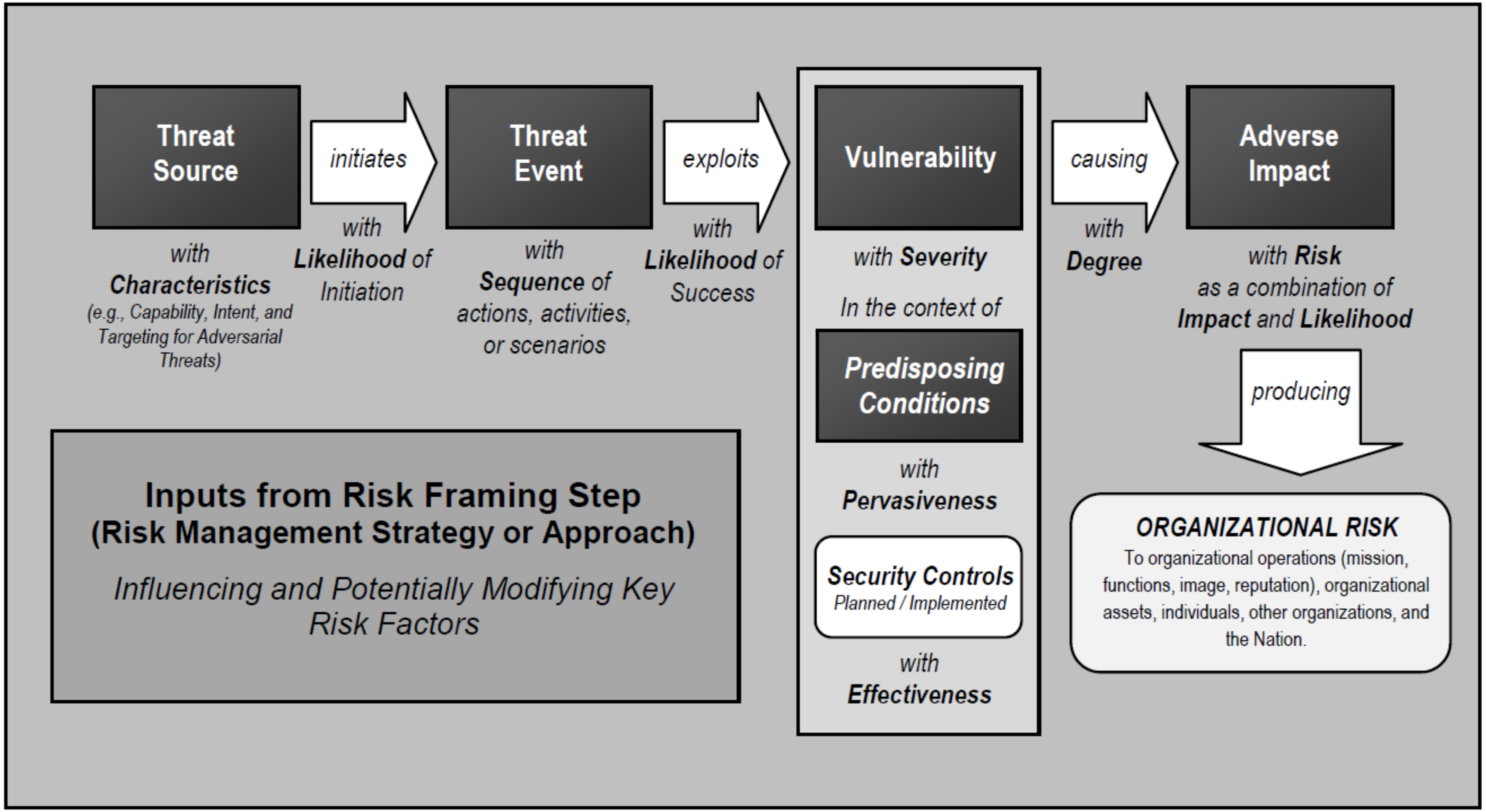
Risk Assessment Methodology

1. Risk Assessment Process
2. Risk Model
3. Assessment Approach
   a) Quantitative
   b) Qualitative
   c) Semi-Qualitative
4. Analysis Approach
   a) threat-oriented
   b) asset/impact-oriented
   c) vulnerability-oriented


- Risk Assumptions
- Risk Constraints
- Priorities and Tradeoffs
- Risk Tolerance
- Uncertainty
ORGANIZATIONAL RISK FRAME
RISK MANAGEMENT STRATEGY OR APPROACH
- Establishes Foundation for Risk Management
- Delineates Boundaries for Risk-Based Decisions
DETERMINES
DETERMINES
Risk Assessment Methodology
Risk Assessment Process
Risk Model
Assessment Approach
Analysis Approach

Source: NIST Special Publication 800-30R1

Risk Management Workflow


Threat Source
initiates
with Likelihood of Initiation
Threat Event
exploits
with Likelihood of Success
Vulnerability
causing
with Degree
Adverse Impact
with Characteristics (e.g., Capability, Intent, and Targeting for Adversarial Threats)
with Sequence of actions, activities, or scenarios
with Severity
In the context of
Predisposing Conditions
with Pervasiveness
Security Controls Planned / Implemented
with Effectiveness
with Risk as a combination of Impact and Likelihood
producing
ORGANIZATIONAL RISK
To organizational operations (mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation.
Inputs from Risk Framing Step (Risk Management Strategy or Approach)
Influencing and Potentially Modifying Key Risk Factors

Source: NIST Special Publication 800-30R1

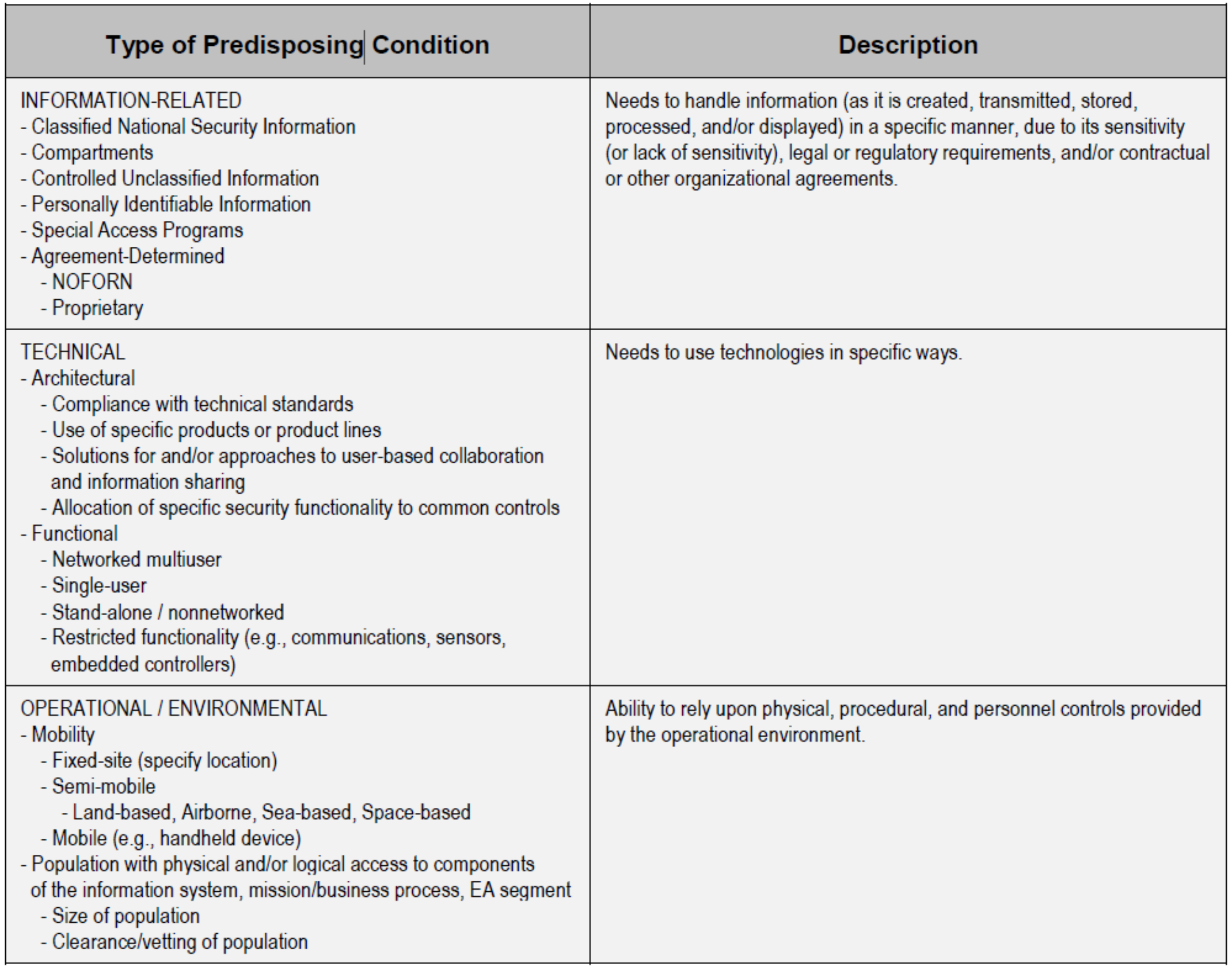
Threat: any circumstance or event with the potential to adversely impact organizational operations and assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service

- A *threat source* is characterized as:
  - (i) the intent and method targeted at the exploitation of a vulnerability; or
  - (ii) a situation and method that may accidentally exploit a vulnerability.
- Types of threat sources include:
  - hostile cyber or physical attacks;
  - human errors of omission or commission;
  - structural failures of organization-controlled resources natural and man-made disasters, accidents, and failures beyond the control of the organization

Source: NIST Special Publication 800-30R1

Vulnerabilities: a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source

A *predisposing condition* is a condition that exists within an organization, a mission or business process, enterprise architecture, information system, or environment of operation, which affects (i.e., increases or decreases) the likelihood that threat events, once initiated, result in adverse impacts to organizational operations and assets, individuals, other organizations, or the Nation



Type of Predisposing Condition	Description
INFORMATION-RELATED - Classified National Security Information - Compartments - Controlled Unclassified Information - Personally Identifiable Information - Special Access Programs - Agreement-Determined - NOFORN - Proprietary	Needs to handle information (as it is created, transmitted, stored, processed, and/or displayed) in a specific manner, due to its sensitivity (or lack of sensitivity), legal or regulatory requirements, and/or contractual or other organizational agreements.
TECHNICAL - Architectural - Compliance with technical standards - Use of specific products or product lines - Solutions for and/or approaches to user-based collaboration and information sharing - Allocation of specific security functionality to common controls - Functional - Networked multiuser - Single-user - Stand-alone / nonnetworked - Restricted functionality (e.g., communications, sensors, embedded controllers)	Needs to use technologies in specific ways.
OPERATIONAL / ENVIRONMENTAL - Mobility - Fixed-site (specify location) - Semi-mobile - Land-based, Airborne, Sea-based, Space-based - Mobile (e.g., handheld device) - Population with physical and/or logical access to components of the information system, mission/business process, EA segment - Size of population - Clearance/vetting of population	Ability to rely upon physical, procedural, and personnel controls provided by the operational environment.

Source: NIST Special Publication 800-30R1

Likelihood: a weighted risk factor based on an analysis of the probability that a given threat is capable of exploiting a given vulnerability (or set of vulnerabilities)

- The likelihood risk factor combines an estimate of the likelihood that the threat event will be initiated with an estimate of the likelihood of impact (i.e., the likelihood that the threat event results in adverse impacts).

- For adversarial threats, an assessment of likelihood of occurrence is typically based on:
  - Adversary *intent*;
  - Adversary *capability*;
  - Adversary *targeting*.

- For other than adversarial threat events, the likelihood of occurrence is estimated using historical evidence, empirical data, or other factors. Note that the likelihood that a threat event will be initiated or will occur is assessed with respect to a specific time frame (e.g., the next six months, the next year, or the period until a specified milestone is reached).

Source: NIST Special Publication 800-30R1

Impact: magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability

- Input that affects the impact assessment:
  - The process used to conduct impact determinations;
  - Assumptions related to impact determinations;
  - Sources and methods for obtaining impact information; and
  - The rationale for conclusions reached with regard to impact determinations.

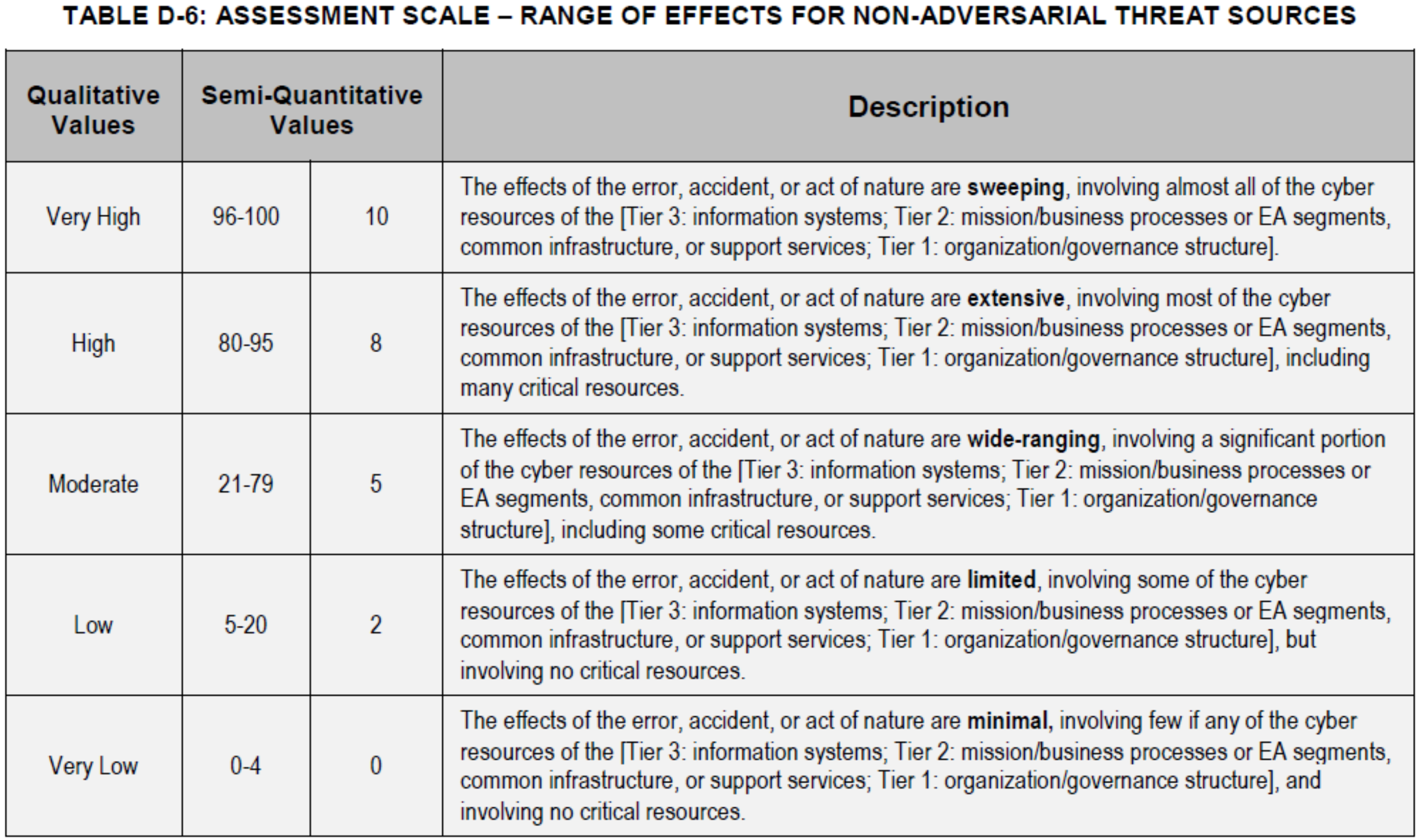


TABLE D-6: ASSESSMENT SCALE – RANGE OF EFFECTS FOR NON-ADVERSARIAL THREAT SOURCES

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The effects of the error, accident, or act of nature are **sweeping**, involving almost all of the cyber resources of the [Tier 3: information systems; Tier 2: mission/business processes or EA segments, common infrastructure, or support services; Tier 1: organization/governance structure].
High	80-95	8	The effects of the error, accident, or act of nature are **extensive**, involving most of the cyber resources of the [Tier 3: information systems; Tier 2: mission/business processes or EA segments, common infrastructure, or support services; Tier 1: organization/governance structure], including many critical resources.
Moderate	21-79	5	The effects of the error, accident, or act of nature are **wide-ranging**, involving a significant portion of the cyber resources of the [Tier 3: information systems; Tier 2: mission/business processes or EA segments, common infrastructure, or support services; Tier 1: organization/governance structure], including some critical resources.
Low	5-20	2	The effects of the error, accident, or act of nature are **limited**, involving some of the cyber resources of the [Tier 3: information systems; Tier 2: mission/business processes or EA segments, common infrastructure, or support services; Tier 1: organization/governance structure], but involving no critical resources.
Very Low	0-4	0	The effects of the error, accident, or act of nature are **minimal**, involving few if any of the cyber resources of the [Tier 3: information systems; Tier 2: mission/business processes or EA segments, common infrastructure, or support services; Tier 1: organization/governance structure], and involving no critical resources.

Source: NIST Special Publication 800-30R1

Example, for illustration purposes, of a simplistic, notional hospital threat assessment

Threat/Event	Vulnerability (1 lowest:10 highest)	Likelihood (1 lowest:10 highest)	Impact (Can Be aggregated)	Score
Active Directory Server Down	5	7	4	140
Electromagnetic Pulse damages Equipment	6	1	10	60
Physical assault on staff	8	9	3 (depends on incident)	216
Blood Supply disruption	5	7	8	280