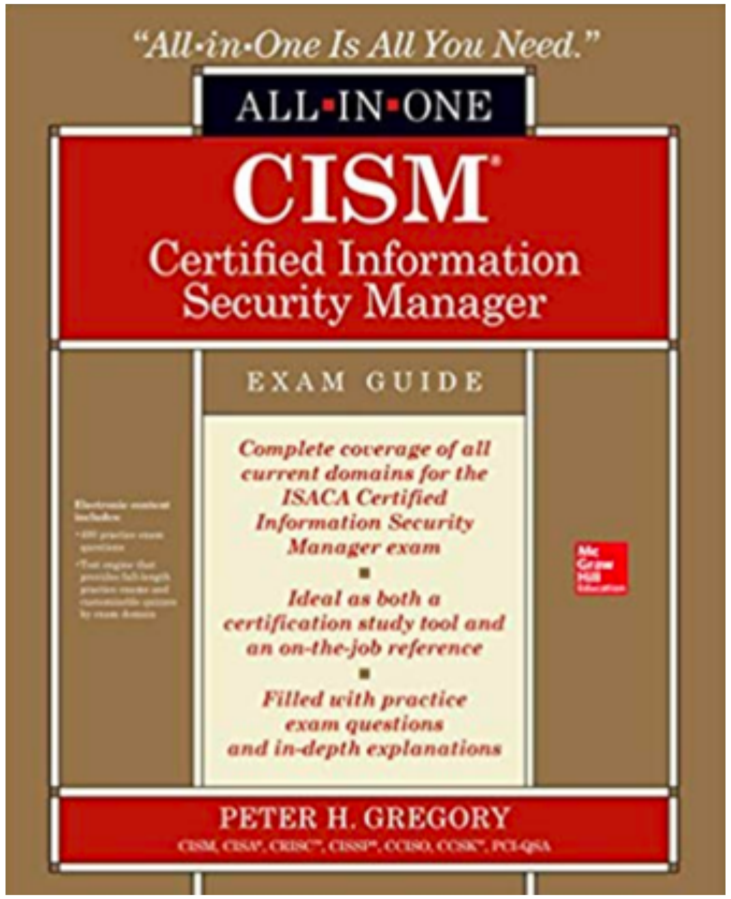
CNIT 160: Cybersecurity Responsibilities

3. Information Risk Management

Part 2

Pages 114 - 126



Updated 2-24-22

Topics

- Part 1 (p. 102 - 115)
  - Risk Management Concepts
  - Implementing a Risk Management Program
- Part 2 (p. 114 - 125)
  - The Risk Management Life Cycle
- Part 3 (p. 125 - 158)
  - The Risk Management Life Cycle
- Part 4 (p. 158 - 182)
  - Operational Risk Management

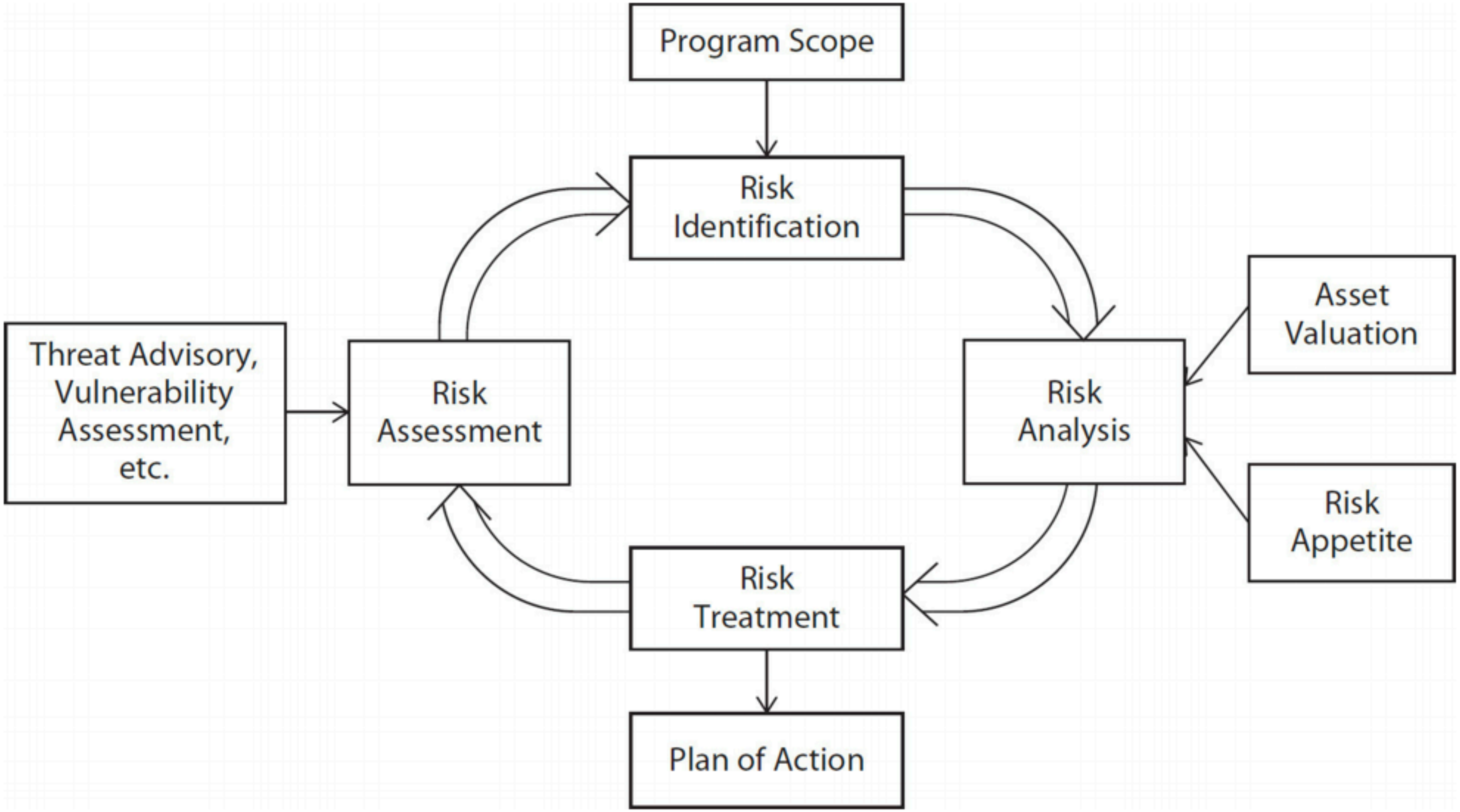
The Risk Management Life Cycle

- Cyclical, iterative process to
  - Acquire, analyze, and treat risks
- Formally defined in policy and process documents
  - Defining scope, roles and responsibilities, workflow, business rules, and business records

The Risk Management Life Cycle

- **Several frameworks and standards**
- **Risk assessments**

The Risk Management Life Cycle



The Risk Management Process

- **Scope definition**
- **Asset identification and valuation**
- **Risk appetite**
- **Risk identification**
  - **Risk assessment**
  - **Vulnerability assessment**
  - **Threat advisory**
  - **Risk analysis**

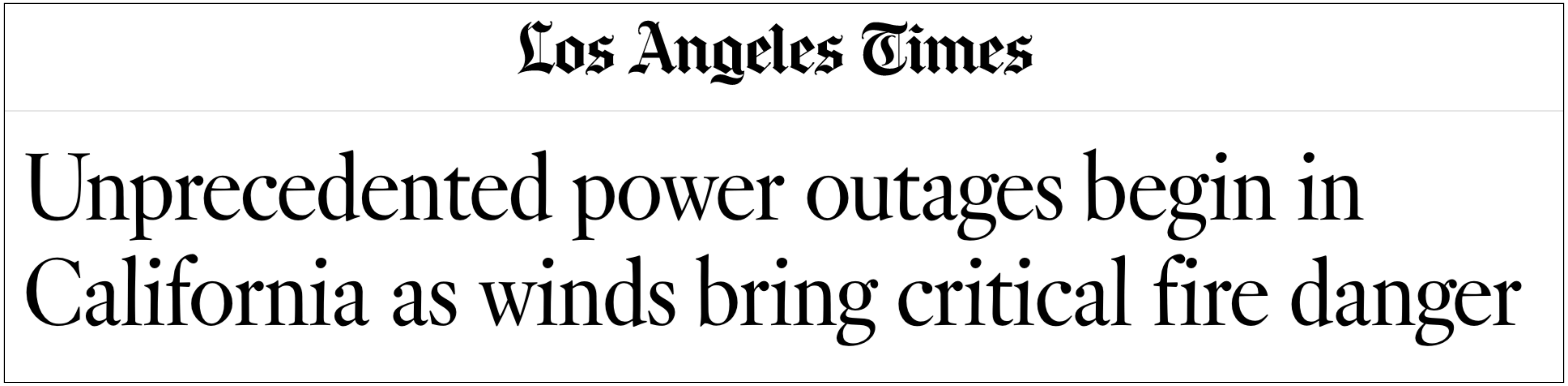
The Risk Management Process

- **Risk analysis**
  - **Probability of event occurrence**
  - **Impact of event occurrence**
  - **Mitigation**
  - **Recommendation**

The Risk Management Process

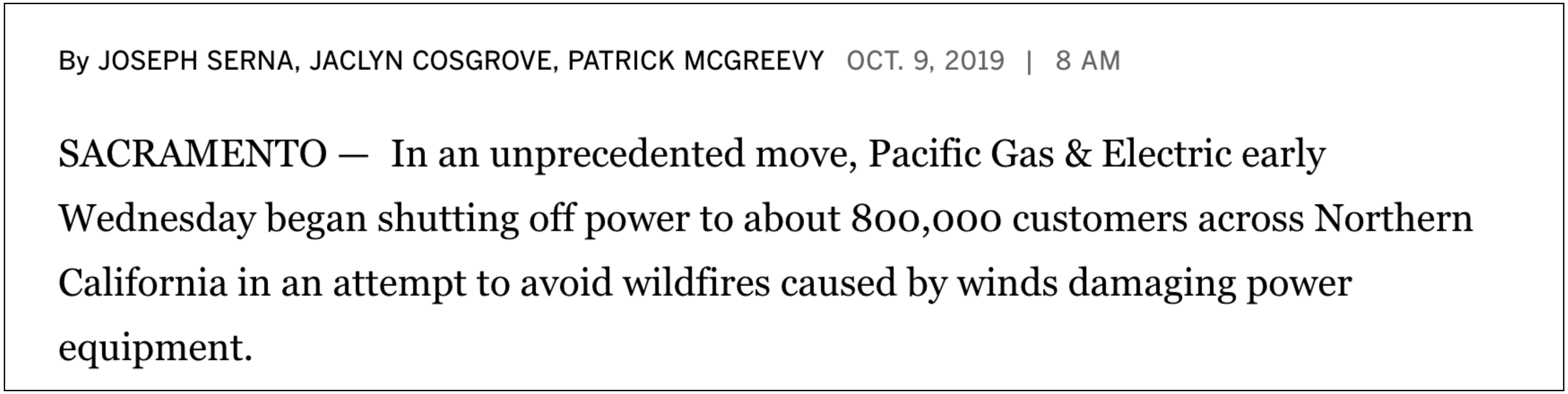
- Risk treatment
  - Accept
  - Mitigate
  - Transfer
  - Avoid
- Risk communication

Risk Avoidance



Los Angeles Times

Unprecedented power outages begin in California as winds bring critical fire danger



By JOSEPH SERNA, JACLYN COSGROVE, PATRICK MCGREEVY OCT. 9, 2019 | 8 AM

SACRAMENTO — In an unprecedented move, Pacific Gas & Electric early Wednesday began shutting off power to about 800,000 customers across Northern California in an attempt to avoid wildfires caused by winds damaging power equipment.

Risk Register

- **List of identified risks, with**
  - **Description**
  - **Level and type**
  - **Risk treatment decisions**
- **Also called a *risk ledger***

Kahoot!

Ch 3b-1

Risk Management Methodologies

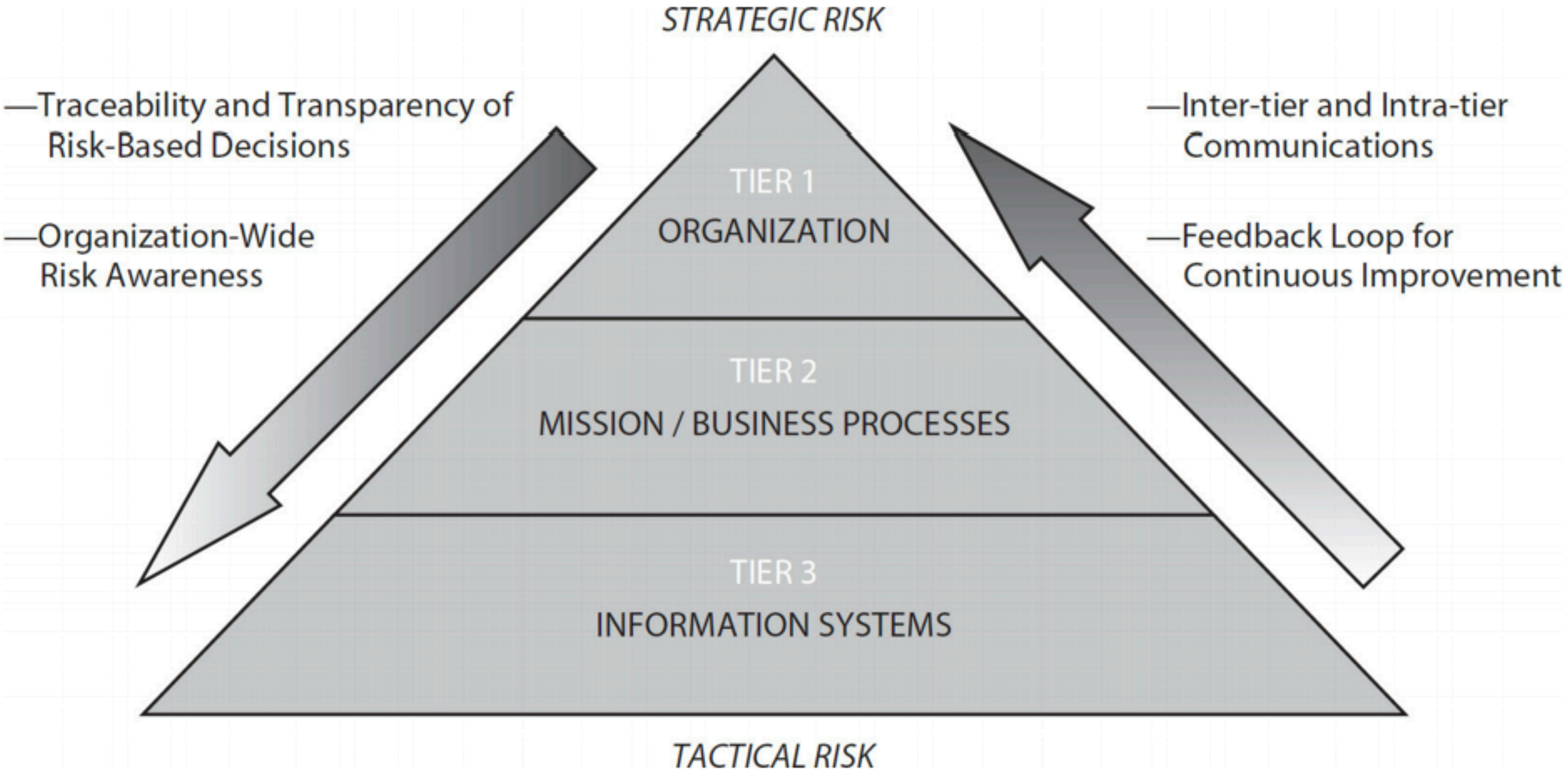
- **NIST SP 800-39 "Managing Information Security Risk: Organization, Mission, and Information, System View"**
- **NIST SP 800-30 "Guide for Conducting Risk Assessments"**
- **ISO/IEC 27005**
- **Factor Analysis of Information Risk (FAIR)**

NIST SP 800-39
"Managing Information Security Risk: Organization, Mission, and Information, System View"

NIST SP 800-39

- **Multilevel risk management**
  - **Information systems level**
  - **Mission/business process level**
  - **Overall organization level**
- **Risks are communicated upward**
- **Risk awareness and risk decisions are communicated downward**

NIST SP 800-39


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

NIST SP 800-39

- **Tier 1: Organization view** This level focuses on the role of governance, the activities performed by the risk executive, and the development of risk management and investment strategies.
- **Tier 2: Mission/business process view** This level is all about enterprise architecture, enterprise security architecture, and ensuring that business processes are risk aware.
- **Tier 3: Information systems view** This level concentrates on more tactical things such as system configuration and hardening specifications, vulnerability management, and the detailed steps in the systems development life cycle.

NIST SP 800-39

- Risk management process
  - Step 1: Risk framing
  - Step 2: Risk assessment
  - Step 3: Risk response
  - Step 4: Risk monitoring

NIST SP 800-30 "Guide for Conducting Risk Assessments"

NIST SP 800-30

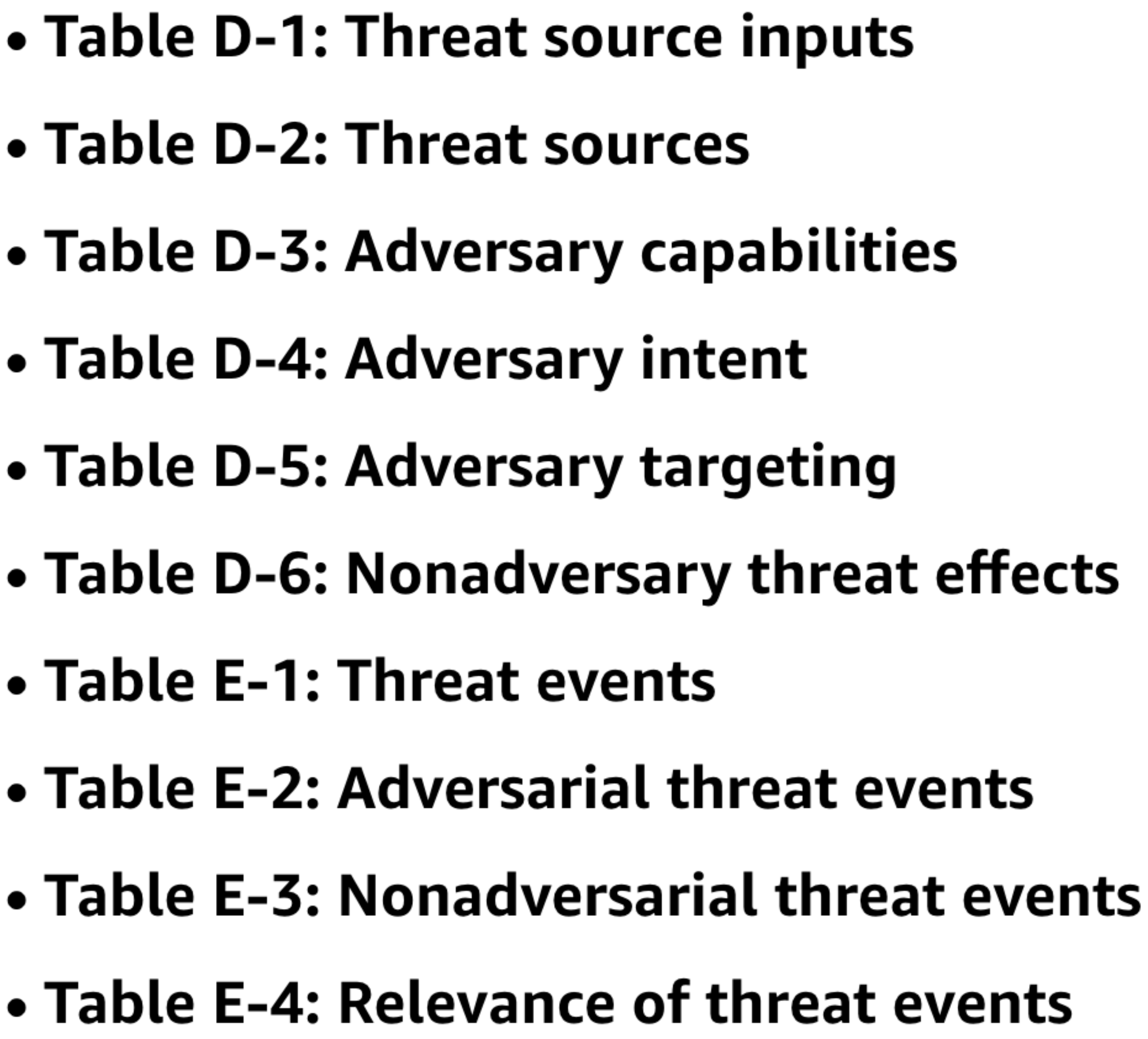
- Standard methodology for conducting a risk assessment
- Quite structured
- A number of worksheets recording
  - Threats and vulnerabilities
  - Probability of occurrence
  - Impact

NIST SP 800-30

- Steps for conducting a risk assessment
  - Step 1: Prepare for assessment
    - Determine purpose, scope, and
    - Source of threat, vulnerability, and impact information
    - NIST 800-30 has example lists

NIST SP 800-30

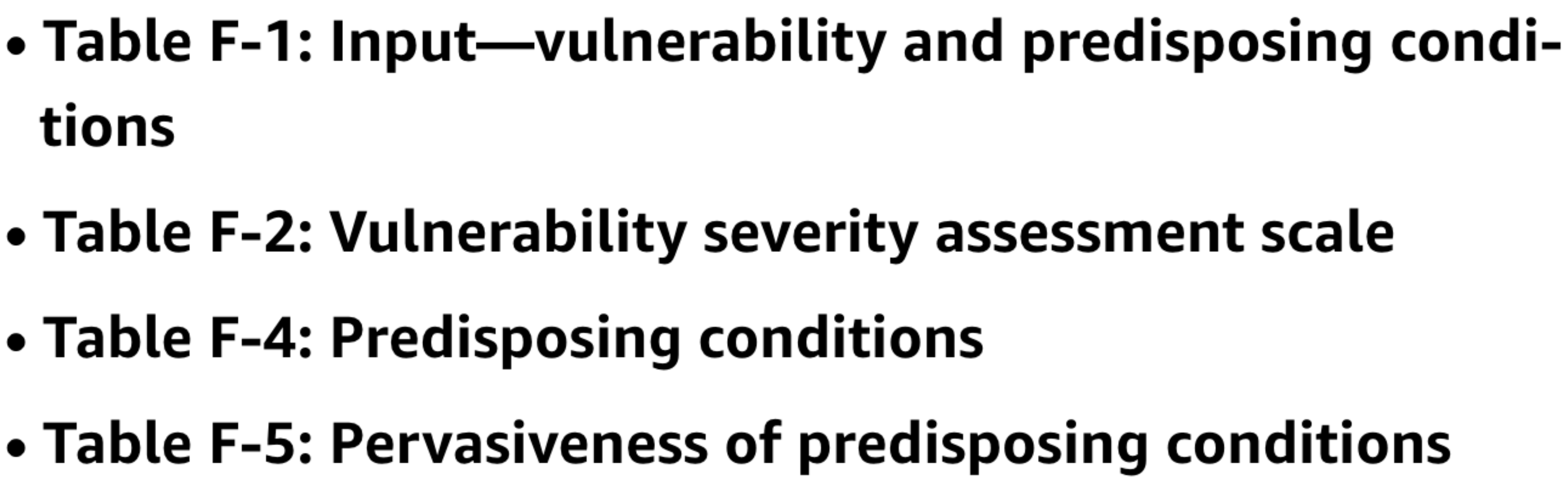
- Step 2: Conduct assessment
  - A. Identify threat sources and events



- Table D-1: Threat source inputs
- Table D-2: Threat sources
- Table D-3: Adversary capabilities
- Table D-4: Adversary intent
- Table D-5: Adversary targeting
- Table D-6: Nonadversary threat effects
- Table E-1: Threat events
- Table E-2: Adversarial threat events
- Table E-3: Nonadversarial threat events
- Table E-4: Relevance of threat events

NIST SP 800-30

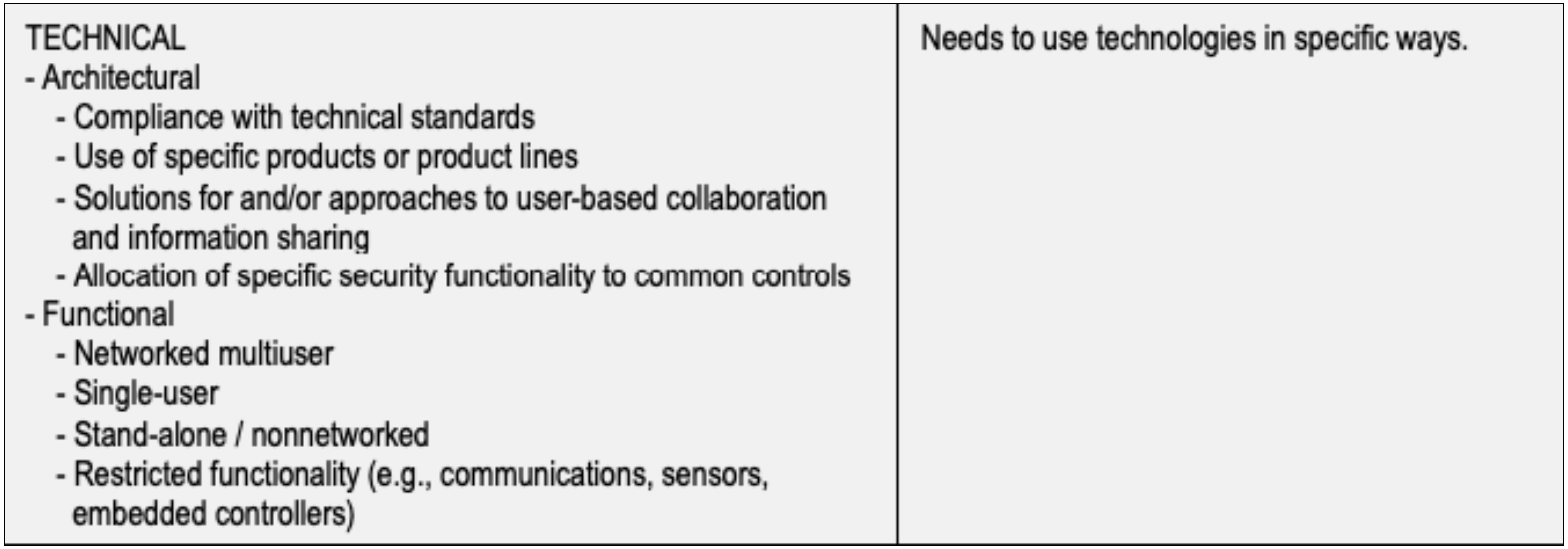
- **B. Identify vulnerabilities and predisposing conditions**



- **Table F-1: Input—vulnerability and predisposing conditions**
- **Table F-2: Vulnerability severity assessment scale**
- **Table F-4: Predisposing conditions**
- **Table F-5: Pervasiveness of predisposing conditions**

Table F-4

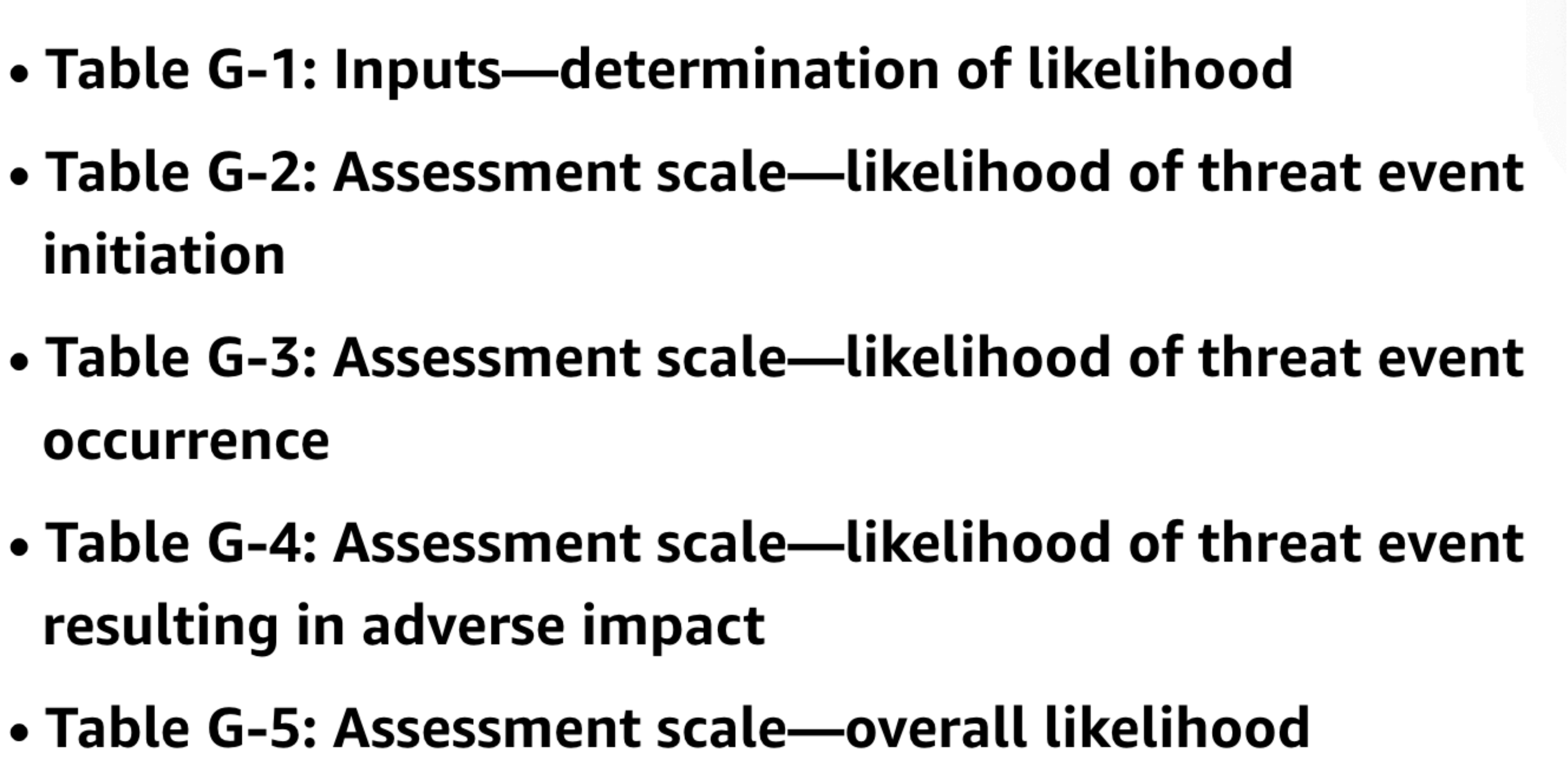
- **Examples of predisposing conditions**
  - **https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf**



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.

NIST SP 800-30

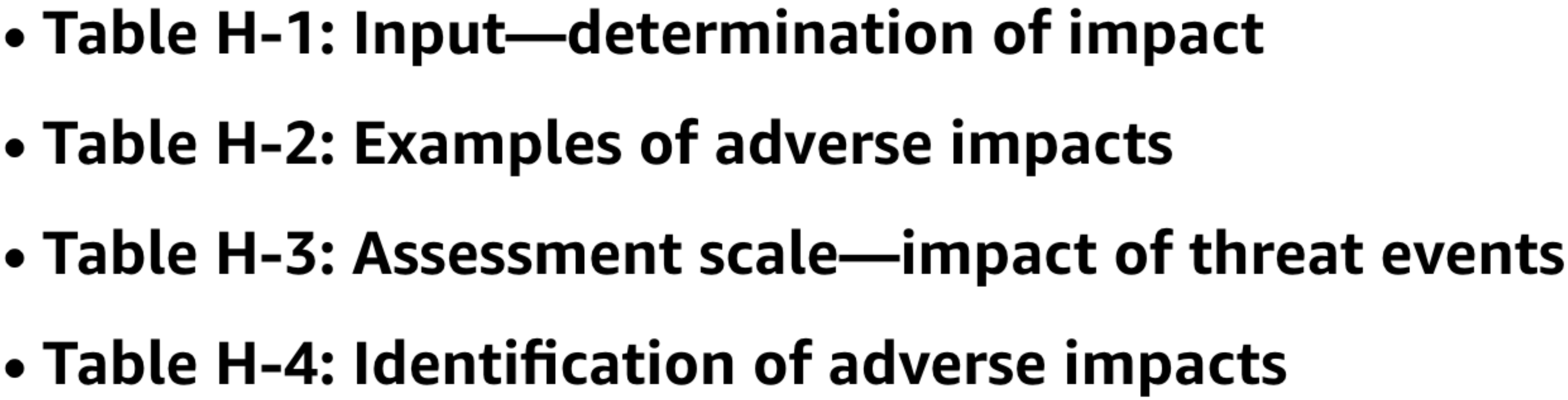
- C. Determine likelihood of occurrence



- Table G-1: Inputs—determination of likelihood
- Table G-2: Assessment scale—likelihood of threat event initiation
- Table G-3: Assessment scale—likelihood of threat event occurrence
- Table G-4: Assessment scale—likelihood of threat event resulting in adverse impact
- Table G-5: Assessment scale—overall likelihood

NIST SP 800-30

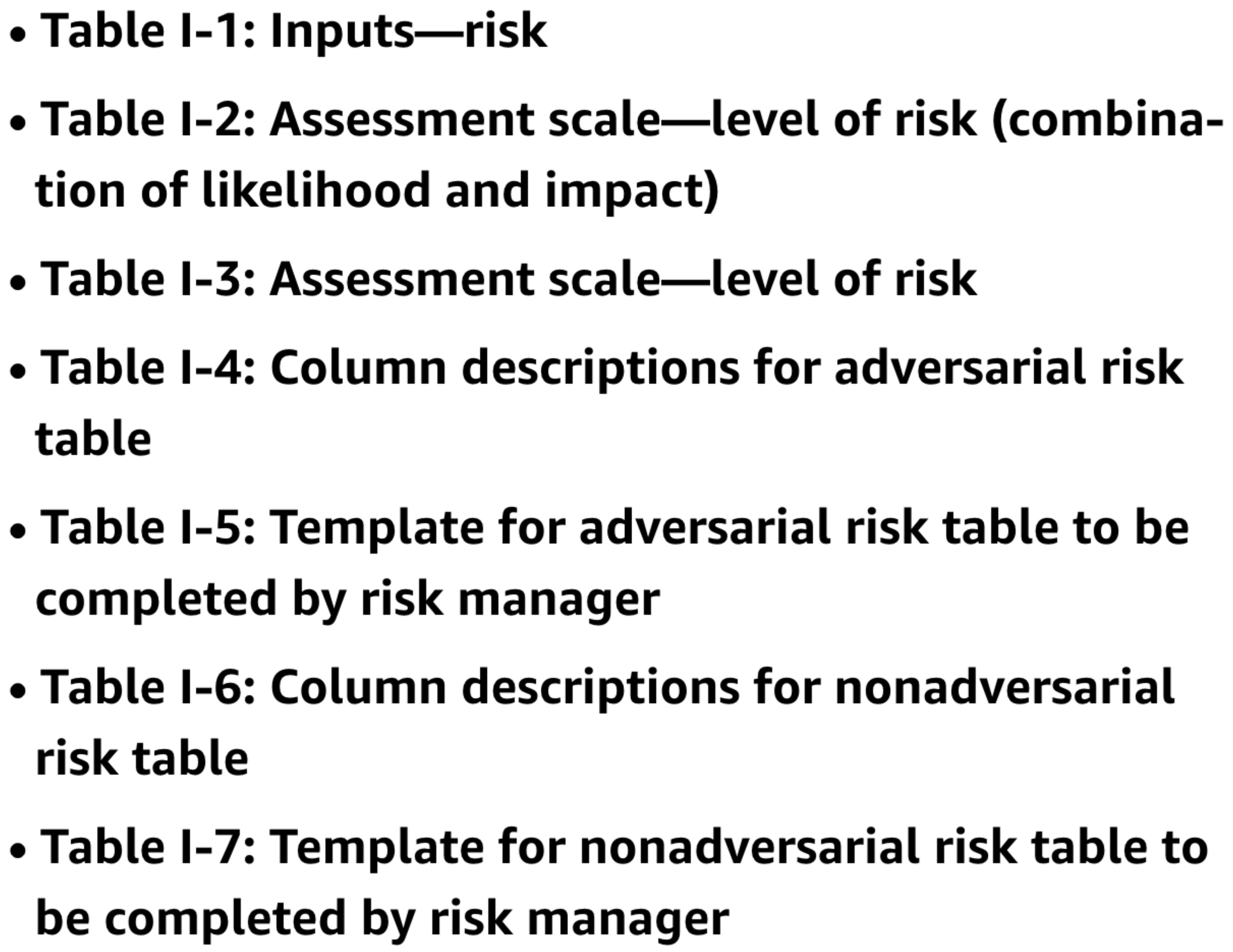
- **D. Determine magnitude of impact**



  - **Table H-1: Input—determination of impact**
  - **Table H-2: Examples of adverse impacts**
  - **Table H-3: Assessment scale—impact of threat events**
  - **Table H-4: Identification of adverse impacts**

NIST SP 800-30

- **E. Determine risk**



  - **Table I-1: Inputs—risk**
  - **Table I-2: Assessment scale—level of risk (combination of likelihood and impact)**
  - **Table I-3: Assessment scale—level of risk**
  - **Table I-4: Column descriptions for adversarial risk table**
  - **Table I-5: Template for adversarial risk table to be completed by risk manager**
  - **Table I-6: Column descriptions for nonadversarial risk table**
  - **Table I-7: Template for nonadversarial risk table to be completed by risk manager**

NIST SP 800-30

- Step 3: Communicate results
- Step 4: Maintain assessment
  - Monitor risk factors

ISO/IEC 27005

ISO/IEC 27005

- **International standard**
- **Defines a structured approach**
- **To risk assessments and risk management**

ISO/IEC 27005

- **Step 1: Establish context**
  - **Scope, purpose**
  - **Criteria for evaluating risk, impact**
  - **Risk acceptance criteria**
  - **Logistical plan**

ISO/IEC 27005

- **Step 2: Risk assessment**
  - **Asset identification**
  - **Threat identification**
  - **Control identification**
  - **Vulnerability identification**
  - **Consequences identification**

ISO/IEC 27005

- **Step 3: Risk evaluation**
- **Step 4: Risk treatment**
  - **Risk reduction (also called *mitigation*)**
  - **Risk retention (also called *acceptance*)**
  - **Risk avoidance**
  - **Risk transfer**
- ***Residual risk* remains**

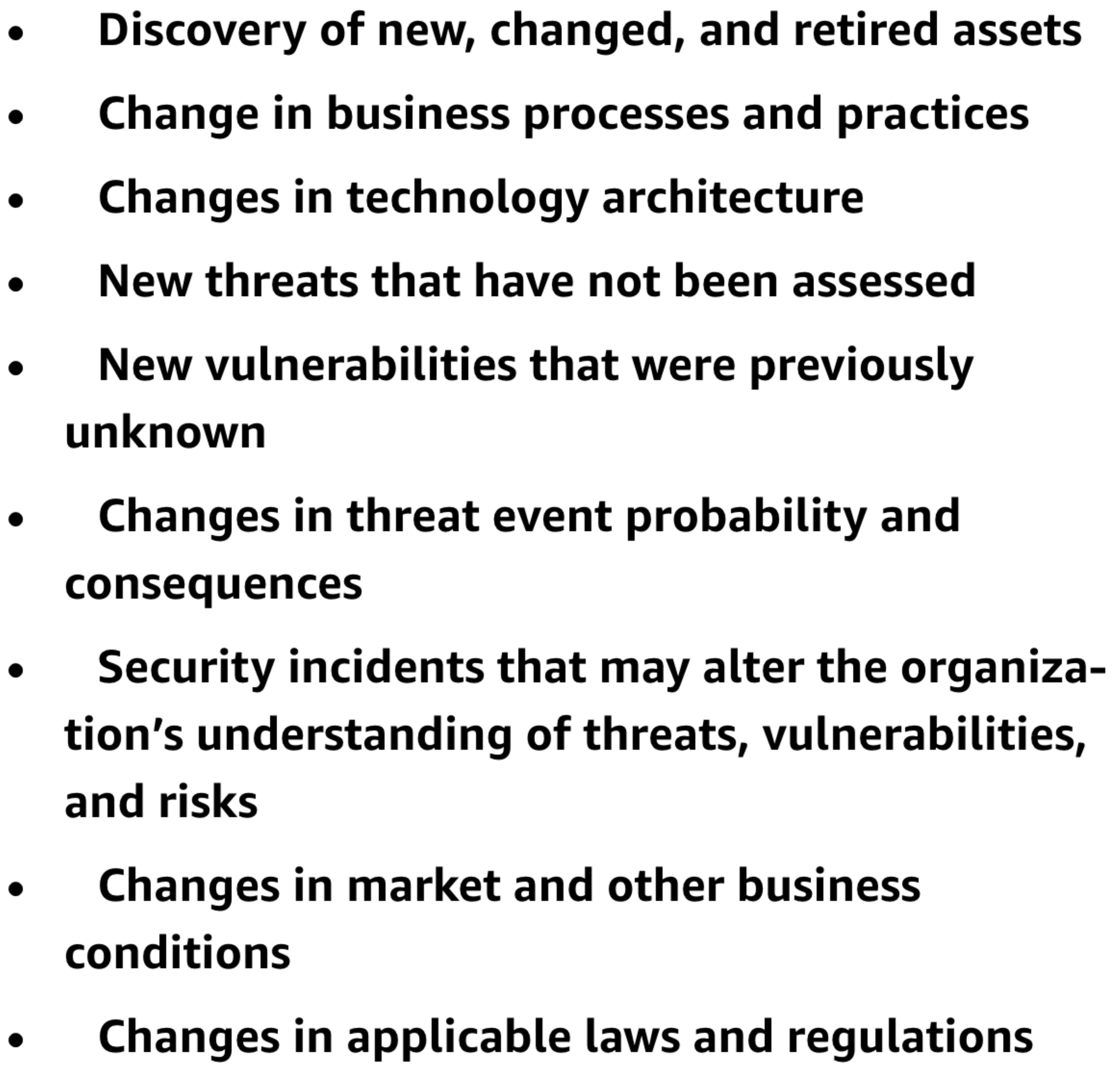
ISO/IEC 27005

Step 5: Risk communication

- Announcements and discussions of upcoming risk assessments
- Collection of risk information during risk assessments (and at other times)
- Proceedings and results from completed risk assessments
- Discussions of risk tolerance
- Proceedings from risk treatment discussions and risk treatment decisions and plans
- Educational information about security and risk
- Updates on the organization’s mission and strategic objectives
- Communication about security incidents to affected parties and stakeholders

ISO/IEC 27005

Step 6: Risk monitoring and review



- Discovery of new, changed, and retired assets
- Change in business processes and practices
- Changes in technology architecture
- New threats that have not been assessed
- New vulnerabilities that were previously unknown
- Changes in threat event probability and consequences
- Security incidents that may alter the organization's understanding of threats, vulnerabilities, and risks
- Changes in market and other business conditions
- Changes in applicable laws and regulations

Factor Analysis of Information Risk (FAIR)

FAIR

- **An analysis method for**
  - **Factors that contribute to risk**
  - **Probability of threat occurrence**
  - **Estimation of loss**

FAIR

- Six types of loss
  - Productivity
  - Response
  - Replacement
  - Fines and judgments
  - Competitive advantage
  - Reputation

FAIR

- **Ways a threat agent acts upon an asset**
  - **Access**
  - **Misuse**
  - **Disclose**
  - **Modify**
  - **Deny use**

Kahoot!

Ch 3b-2