Risk Management and Assessment

Chris Hankin

Types of Risk

- Financial
- Equipment failure
- Safety

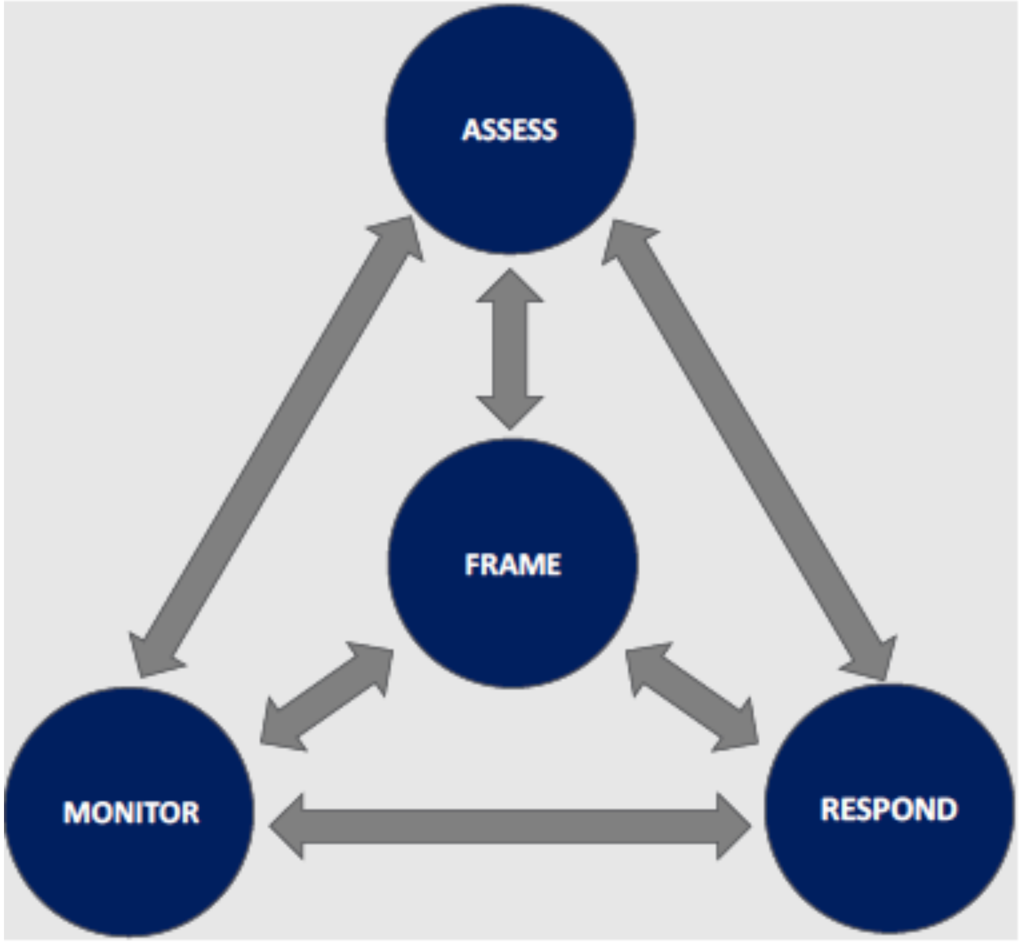
ALARP

- Information security

Risk Management Process

- Frame – framework for risk decisions; risk tolerance; safety and security; availability; and physical operating environment.
- Assess – identify threats and vulnerabilities; harm and likelihood; effect on physical process, dependent systems, and physical environment; and safety.
- Respond – to identification of risk (acceptance, avoidance, mitigation, sharing, transfer).
- Monitor – implementation; changes in environment; effectiveness and efficiency.

Risk Management Process

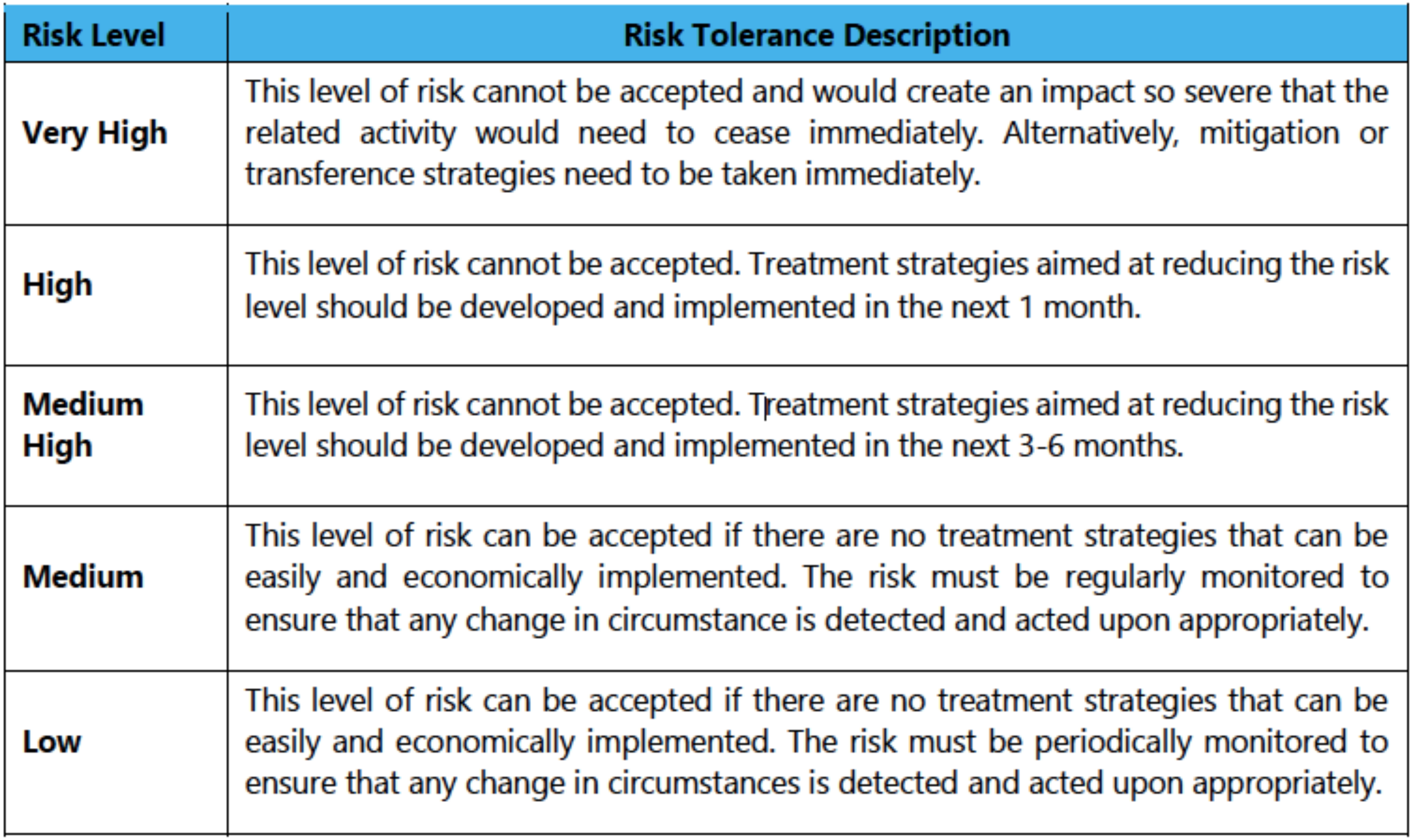


From NIST sp 800-82 (r3): Guide to Industrial Control Systems (ICS) Security

Framing Risk

- Risk assumptions – threat, vulnerabilities, impact and likelihood
- Risk constraints
- Risk tolerance
- Priorities and trade-offs
- Safety is likely to be a major consideration

Risk Tolerance



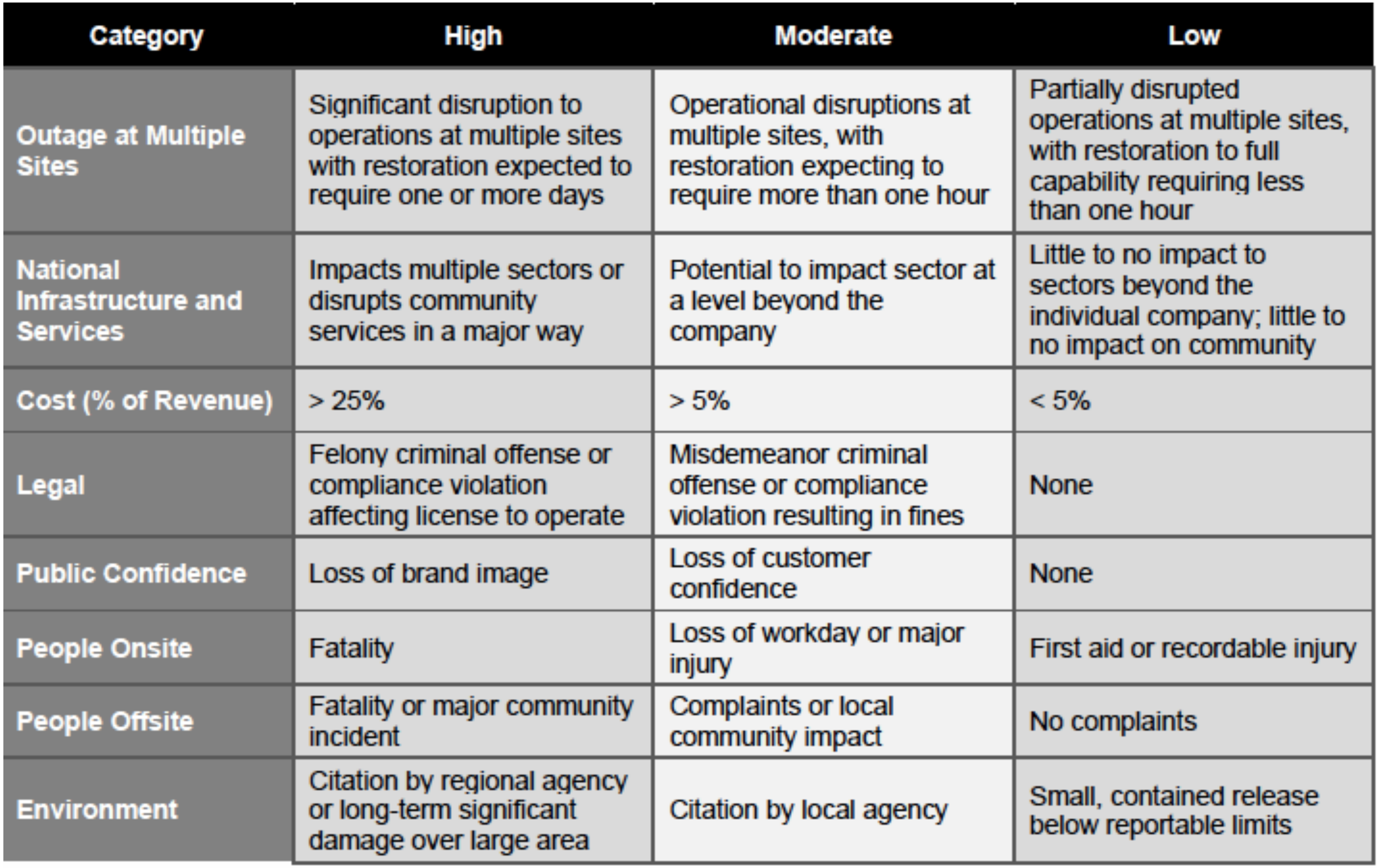
Risk Level	Risk Tolerance Description
Very High	This level of risk cannot be accepted and would create an impact so severe that the related activity would need to cease immediately. Alternatively, mitigation or transference strategies need to be taken immediately.
High	This level of risk cannot be accepted. Treatment strategies aimed at reducing the risk level should be developed and implemented in the next 1 month.
Medium High	This level of risk cannot be accepted. Treatment strategies aimed at reducing the risk level should be developed and implemented in the next 3-6 months.
Medium	This level of risk can be accepted if there are no treatment strategies that can be easily and economically implemented. The risk must be regularly monitored to ensure that any change in circumstance is detected and acted upon appropriately.
Low	This level of risk can be accepted if there are no treatment strategies that can be easily and economically implemented. The risk must be periodically monitored to ensure that any change in circumstances is detected and acted upon appropriately.

From CSA Singapore Guide to Conducting Risk Assessment for CII

Some OT Specific issues

- Legacy systems and organizational tolerance levels
- Availability requirements
- Inter-dependent systems
- Logical and Physical impact on inter-connected OT, for example by worm propagation (logical) or physical hazard

Possible OT Impact Levels



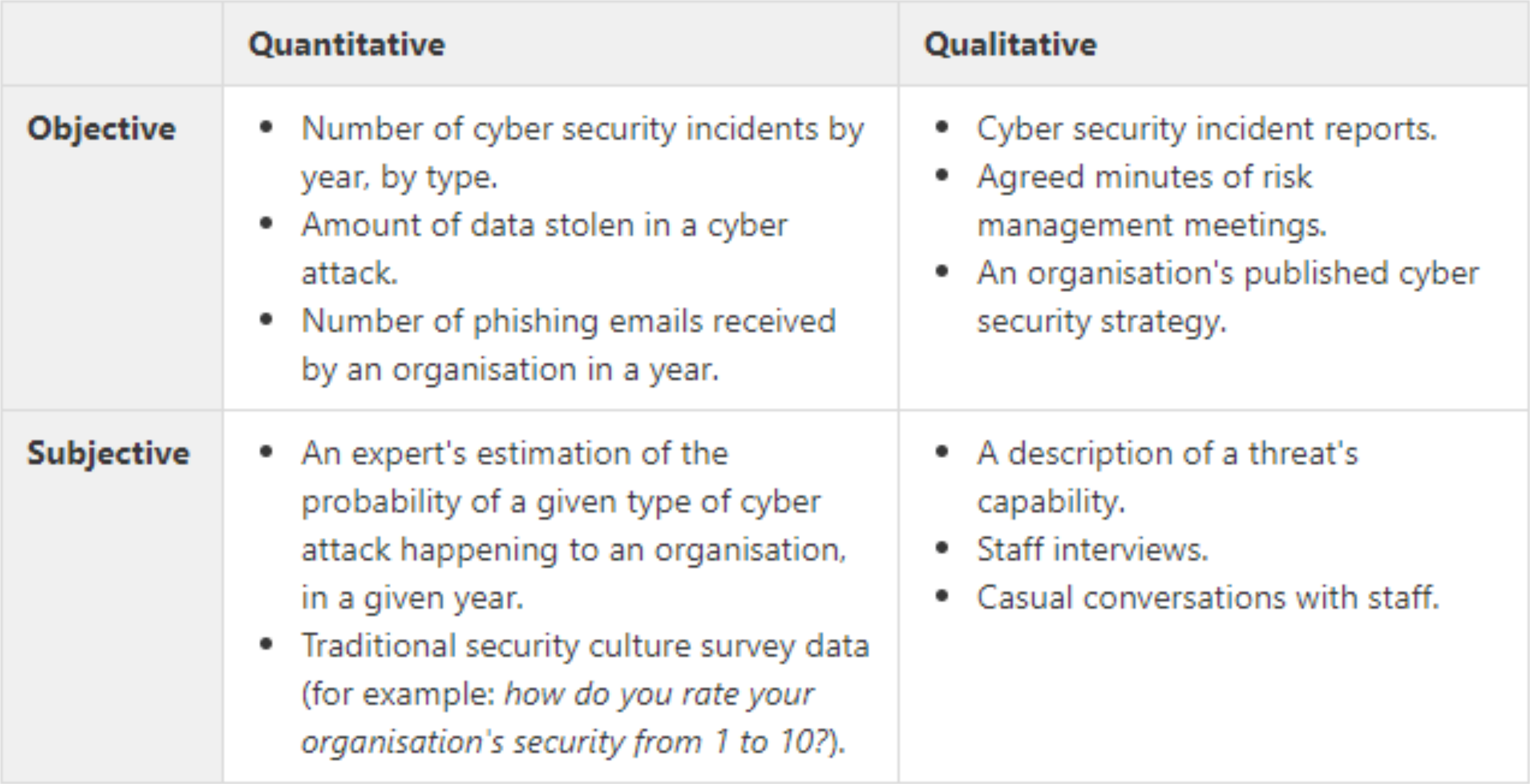
Category	High	Moderate	Low
Outage at Multiple Sites	Significant disruption to operations at multiple sites with restoration expected to require one or more days	Operational disruptions at multiple sites, with restoration expecting to require more than one hour	Partially disrupted operations at multiple sites, with restoration to full capability requiring less than one hour
National Infrastructure and Services	Impacts multiple sectors or disrupts community services in a major way	Potential to impact sector at a level beyond the company	Little to no impact to sectors beyond the individual company; little to no impact on community
Cost (% of Revenue)	> 25%	> 5%	< 5%
Legal	Felony criminal offense or compliance violation affecting license to operate	Misdemeanor criminal offense or compliance violation resulting in fines	None
Public Confidence	Loss of brand image	Loss of customer confidence	None
People Onsite	Fatality	Loss of workday or major injury	First aid or recordable injury
People Offsite	Fatality or major community incident	Complaints or local community impact	No complaints
Environment	Citation by regional agency or long-term significant damage over large area	Citation by local agency	Small, contained release below reportable limits

From NIST sp 800-82 (r3): Guide to Industrial Control Systems (ICS) Security

Risk Assessment

- Tools, techniques and methodologies
- Roles and responsibilities
- Collection, processing and communication of risk assessment information
- Conduct of risk assessment
- Frequency
- Obtaining threat intelligence

Different Information Sources

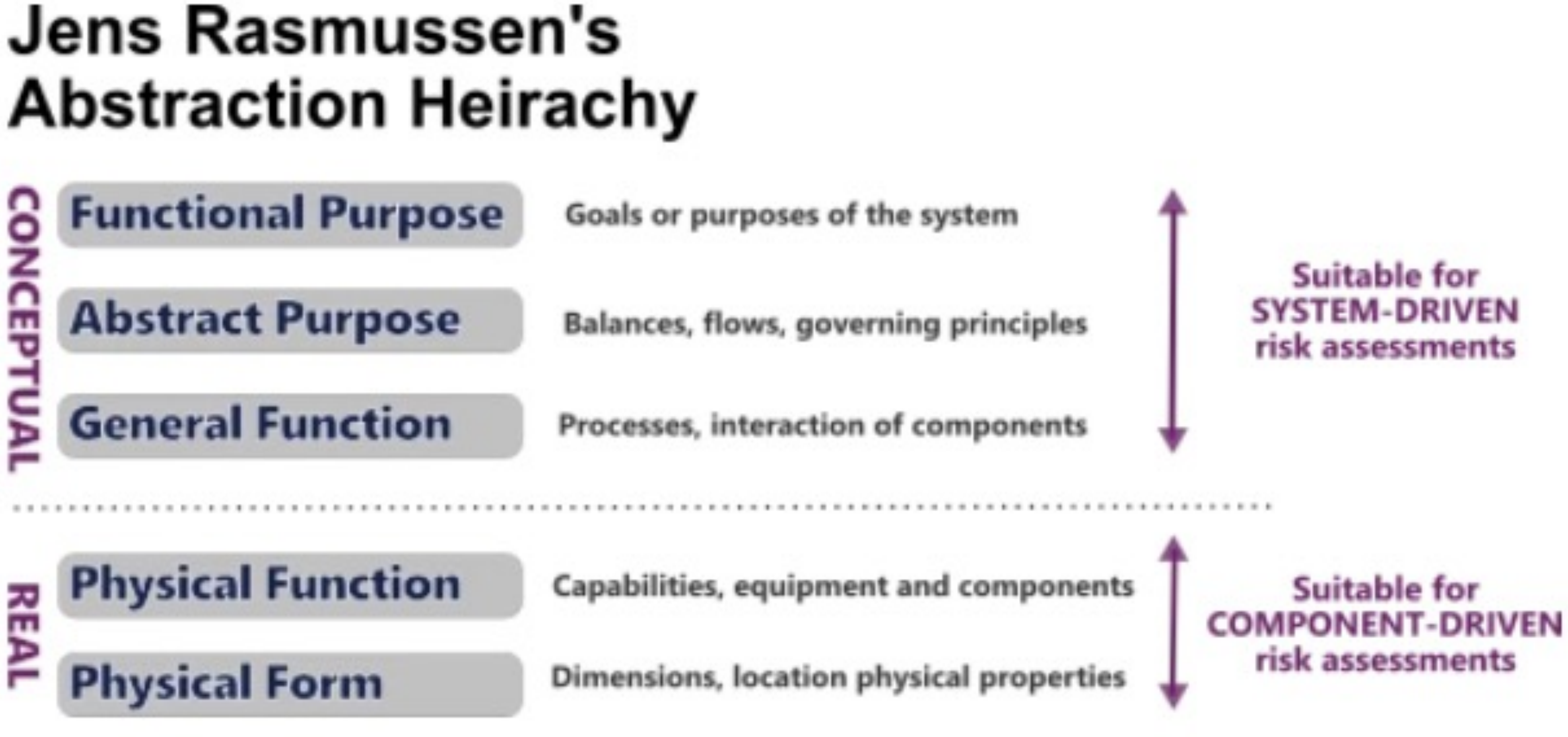


	Quantitative	Qualitative
Objective	• Number of cyber security incidents by year, by type. • Amount of data stolen in a cyber attack. • Number of phishing emails received by an organisation in a year.	• Cyber security incident reports. • Agreed minutes of risk management meetings. • An organisation's published cyber security strategy.
Subjective	• An expert's estimation of the probability of a given type of cyber attack happening to an organisation, in a given year. • Traditional security culture survey data (for example: *how do you rate your organisation's security from 1 to 10?*).	• A description of a threat's capability. • Staff interviews. • Casual conversations with staff.

From https://www.ncsc.gov.uk/collection/risk-management-collection/

Approaches to Risk Assessment

- Component-driven – bottom-up
- System-driven – top-down



Jens Rasmussen's Abstraction Heirachy

CONCEPTUAL

Functional Purpose	Goals or purposes of the system
Abstract Purpose	Balances, flows, governing principles
General Function	Processes, interaction of components

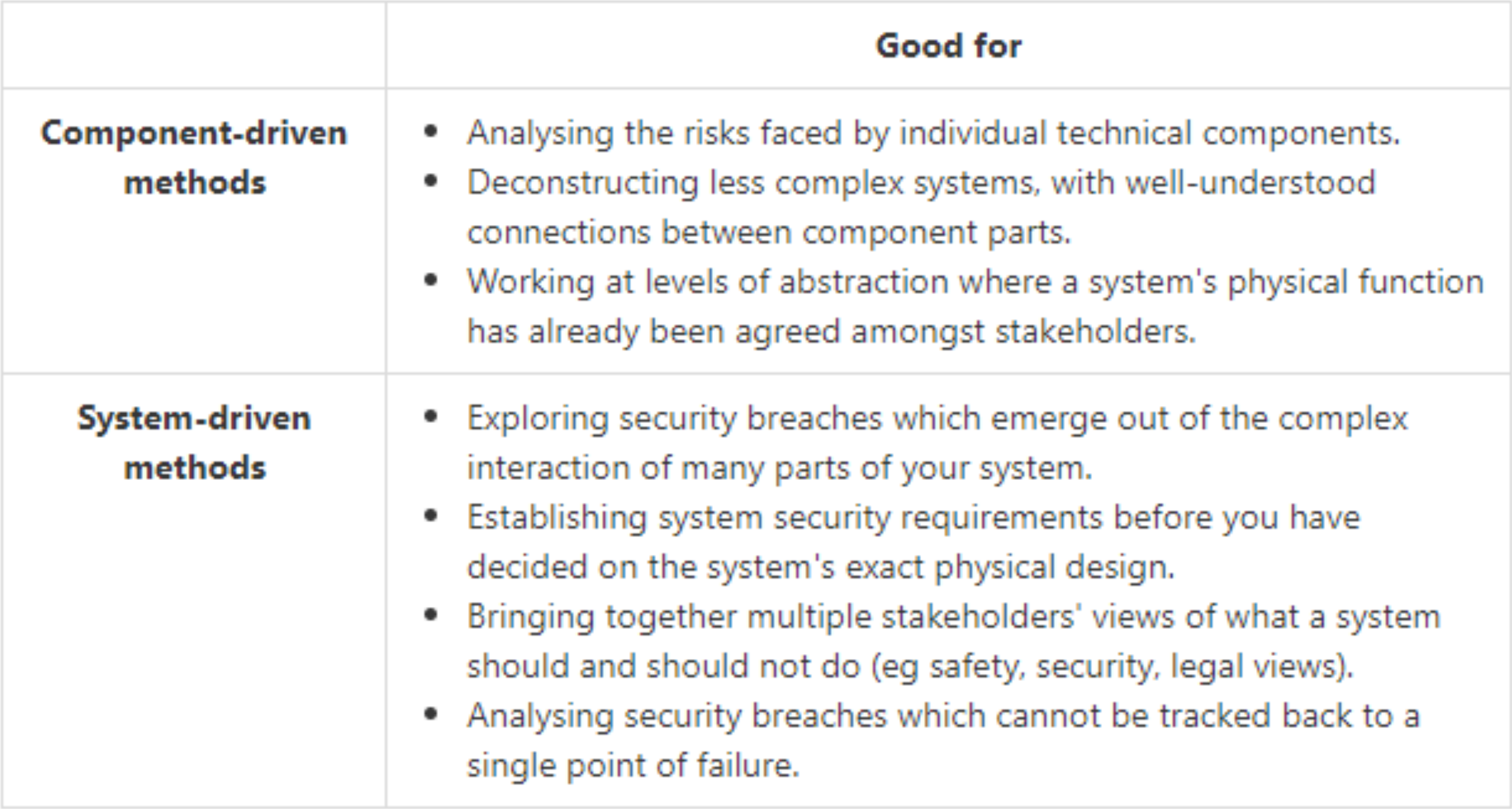
Suitable for SYSTEM-DRIVEN risk assessments

REAL

Physical Function	Capabilities, equipment and components
Physical Form	Dimensions, location physical properties

Suitable for COMPONENT-DRIVEN risk assessments

From https://www.ncsc.gov.uk/collection/risk-management-collection/



	Good for
Component-driven methods	• Analysing the risks faced by individual technical components. • Deconstructing less complex systems, with well-understood connections between component parts. • Working at levels of abstraction where a system's physical function has already been agreed amongst stakeholders.
System-driven methods	• Exploring security breaches which emerge out of the complex interaction of many parts of your system. • Establishing system security requirements before you have decided on the system's exact physical design. • Bringing together multiple stakeholders' views of what a system should and should not do (eg safety, security, legal views). • Analysing security breaches which cannot be tracked back to a single point of failure.

From https://www.ncsc.gov.uk/collection/risk-management-collection/

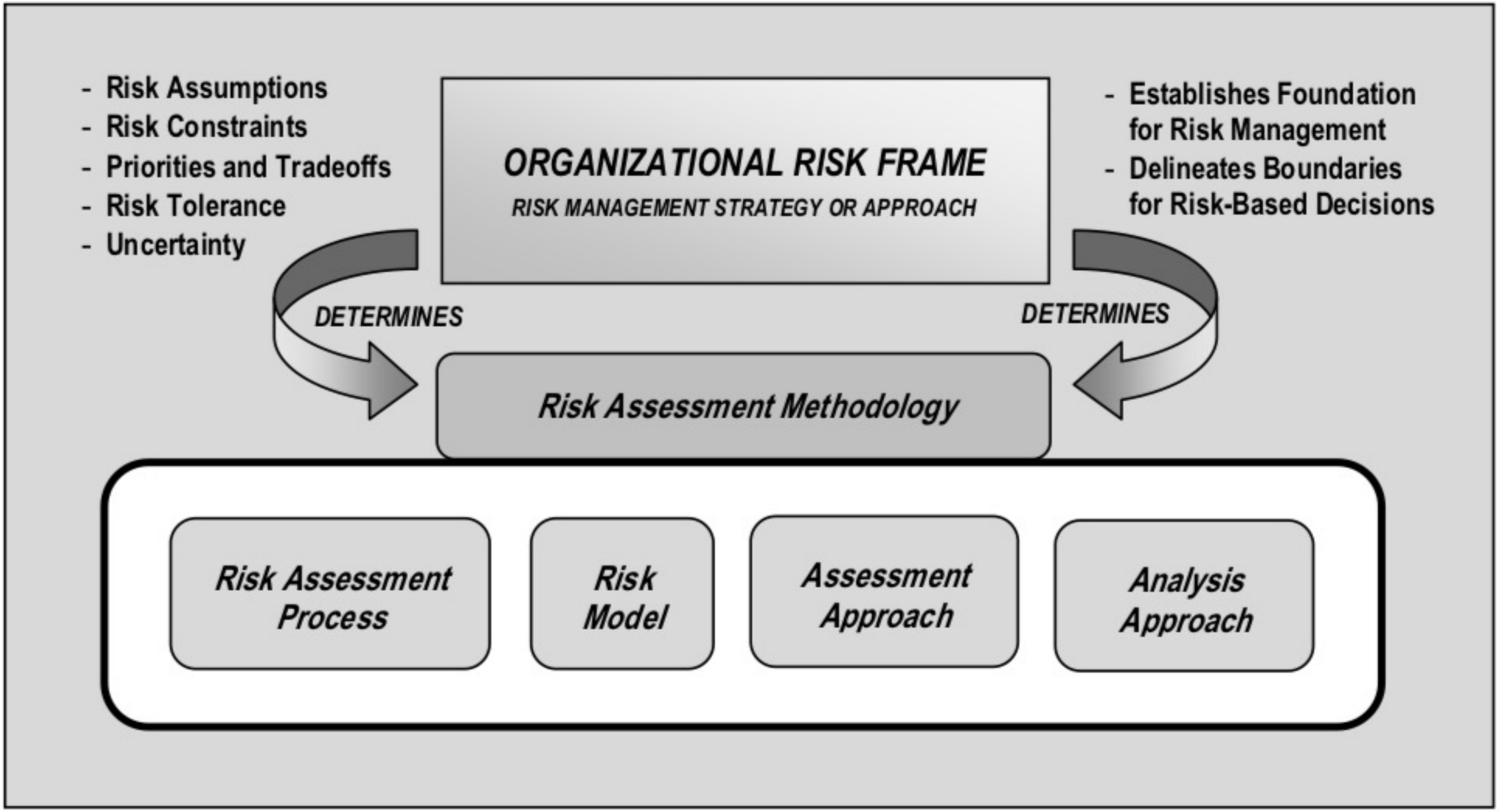
Risk Assessment

- Sources: CISA, NIST NVD, MITRE ATT&CK for ICS

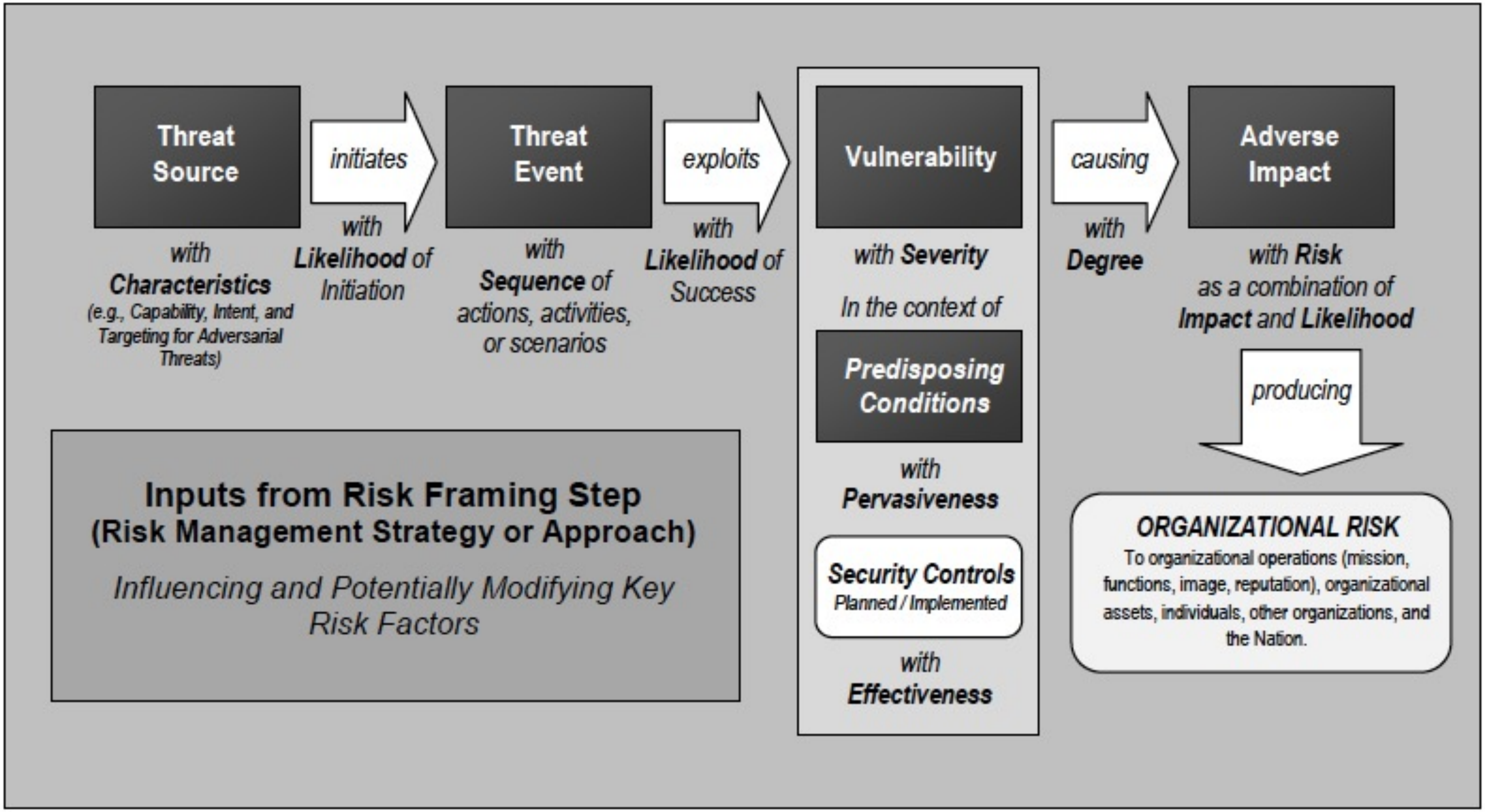
- Poor coding practices, network designs or device configurations
- Vulnerable network services and protocols
- Weak authentication
- Excessive privileges
- Information disclosure

- Risk = Function (Likelihood, Impact)

- Safety


- 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

From: NIST sp 800-30(r1) – Guide for conducting risk assessments

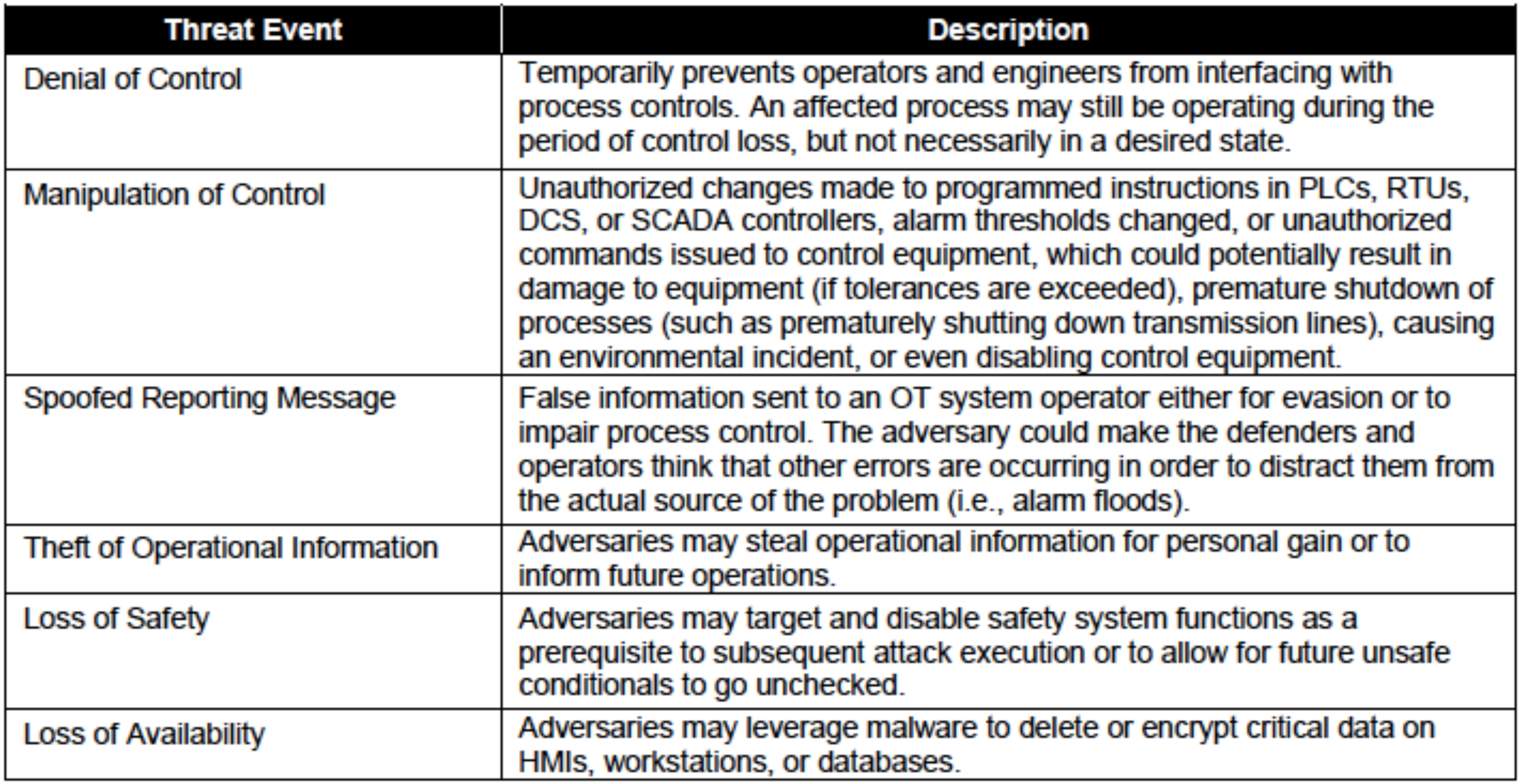

Threat Source
initiates
with Likelihood of Initiation
with Characteristics
(e.g., Capability, Intent, and Targeting for Adversarial Threats)
Threat Event
exploits
with Likelihood of Success
with Sequence of actions, activities, or scenarios
Vulnerability
with Severity
In the context of
Predisposing Conditions
with Pervasiveness
Security Controls
Planned / Implemented
with Effectiveness
causing
with Degree
Adverse Impact
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

From: NIST sp 800-30(r1) – Guide for conducting risk assessments

Threat Sources

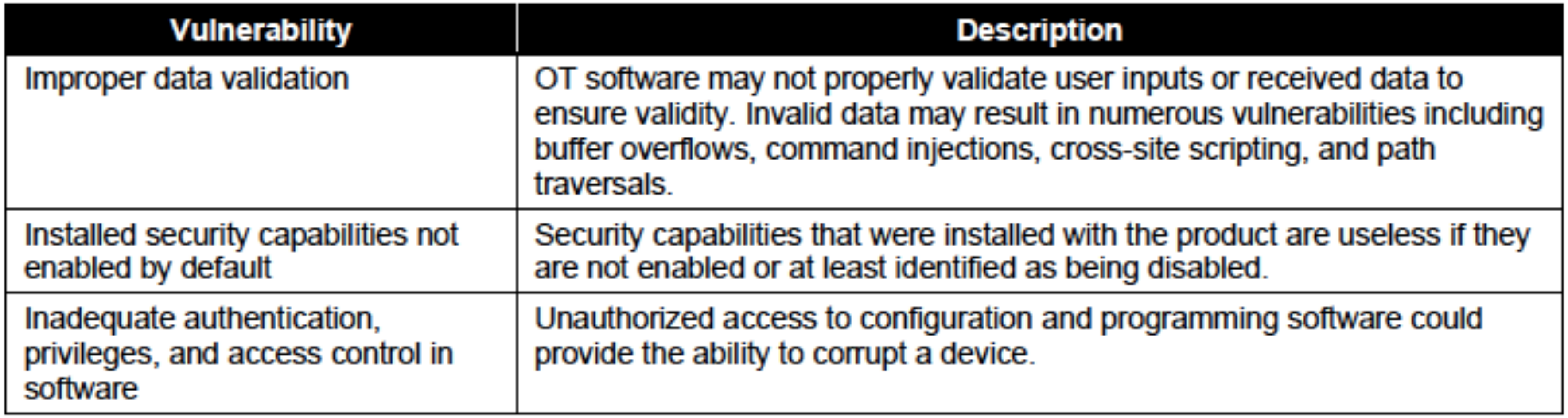
- Adversarial – Capability, Intent, Targeting: Colonial Pipeline (2021)
- Accidental – NASA Fire – patch and reboot cause oven to stop running; 3.5 hours to detect
- Structural – Browns Ferry-3 PLC Failure – dual redundancy connected to same network (2006)
- Environmental – Fukushima (2011)

Threat Events



Threat Event	Description
Denial of Control	Temporarily prevents operators and engineers from interfacing with process controls. An affected process may still be operating during the period of control loss, but not necessarily in a desired state.
Manipulation of Control	Unauthorized changes made to programmed instructions in PLCs, RTUs, DCS, or SCADA controllers, alarm thresholds changed, or unauthorized commands issued to control equipment, which could potentially result in damage to equipment (if tolerances are exceeded), premature shutdown of processes (such as prematurely shutting down transmission lines), causing an environmental incident, or even disabling control equipment.
Spoofed Reporting Message	False information sent to an OT system operator either for evasion or to impair process control. The adversary could make the defenders and operators think that other errors are occurring in order to distract them from the actual source of the problem (i.e., alarm floods).
Theft of Operational Information	Adversaries may steal operational information for personal gain or to inform future operations.
Loss of Safety	Adversaries may target and disable safety system functions as a prerequisite to subsequent attack execution or to allow for future unsafe conditionals to go unchecked.
Loss of Availability	Adversaries may leverage malware to delete or encrypt critical data on HMIs, workstations, or databases.

Example of Predisposing conditions - Software



Vulnerability	Description
Improper data validation	OT software may not properly validate user inputs or received data to ensure validity. Invalid data may result in numerous vulnerabilities including buffer overflows, command injections, cross-site scripting, and path traversals.
Installed security capabilities not enabled by default	Security capabilities that were installed with the product are useless if they are not enabled or at least identified as being disabled.
Inadequate authentication, privileges, and access control in software	Unauthorized access to configuration and programming software could provide the ability to corrupt a device.

Responding

- Alternative courses of action
- Evaluation of alternative courses
- Courses of action consistent with risk tolerance
- Implementation

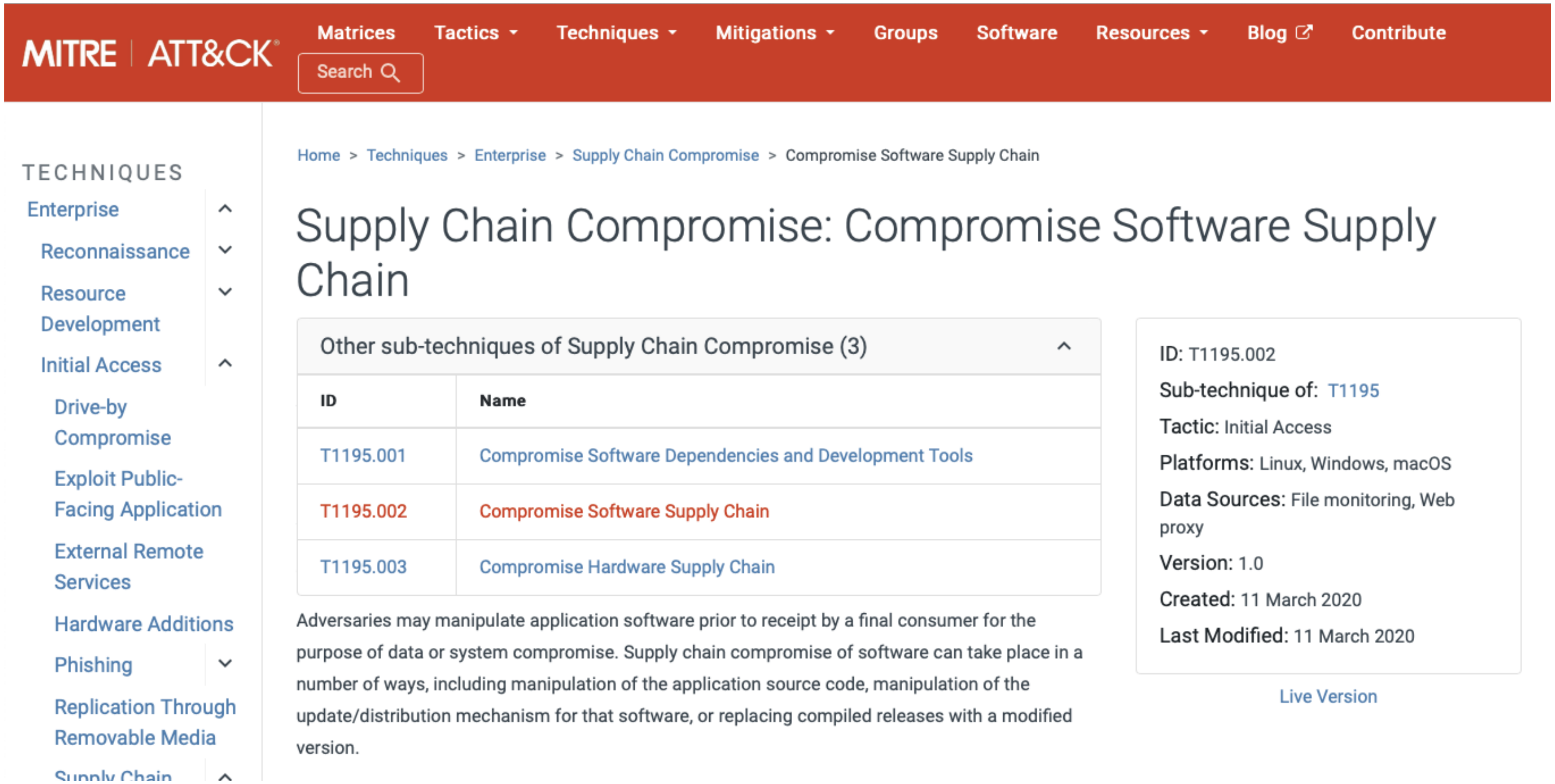
- Accept; Avoid; Mitigate; Share; Transfer

Monitoring

- Verification that planned risk response is implemented and compliant with any legal requirements
- Determining on-going effectiveness
- Identify risk-impacting changes to organizational information systems.

Special Areas

- Supply Chains
- Safety Systems



Home > Techniques > Enterprise > Supply Chain Compromise > Compromise Software Supply Chain

Supply Chain Compromise: Compromise Software Supply Chain

Other sub-techniques of Supply Chain Compromise (3)

ID	Name
T1195.001	Compromise Software Dependencies and Development Tools
T1195.002	Compromise Software Supply Chain
T1195.003	Compromise Hardware Supply Chain

Adversaries may manipulate application software prior to receipt by a final consumer for the purpose of data or system compromise. Supply chain compromise of software can take place in a number of ways, including manipulation of the application source code, manipulation of the update/distribution mechanism for that software, or replacing compiled releases with a modified version.

ID: T1195.002

Sub-technique of: T1195

Tactic: Initial Access

Platforms: Linux, Windows, macOS

Data Sources: File monitoring, Web proxy

Version: 1.0

Created: 11 March 2020

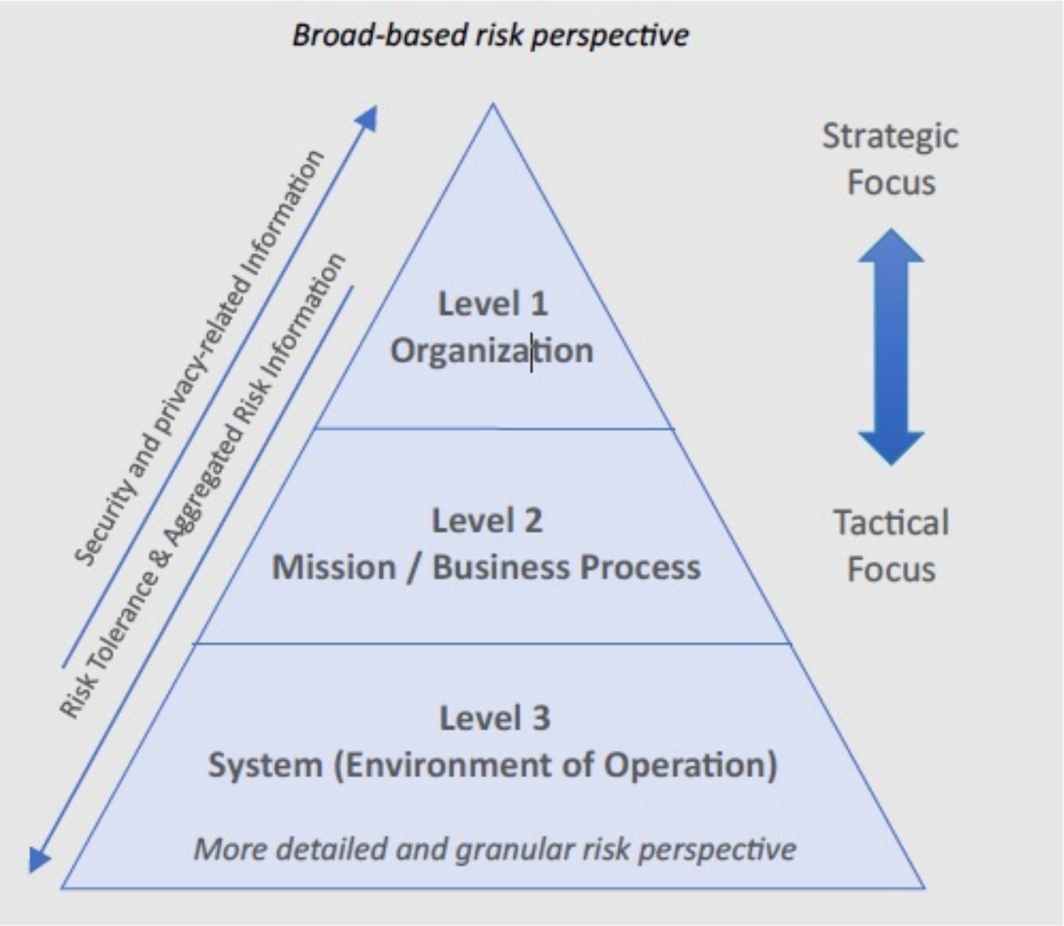
Last Modified: 11 March 2020

Live Version

Three Tiers

- Organization
- Mission/Business Process
- Information System (IT and ICS)

Risk Management Process


Broad-based risk perspective
Security and privacy-related Information
Risk Tolerance & Aggregated Risk Information
Level 1
Organization
Level 2
Mission / Business Process
Level 3
System (Environment of Operation)
More detailed and granular risk perspective
Strategic Focus
Tactical Focus

From NIST sp 800-82 (r3): Guide to Industrial Control Systems (ICS) Security

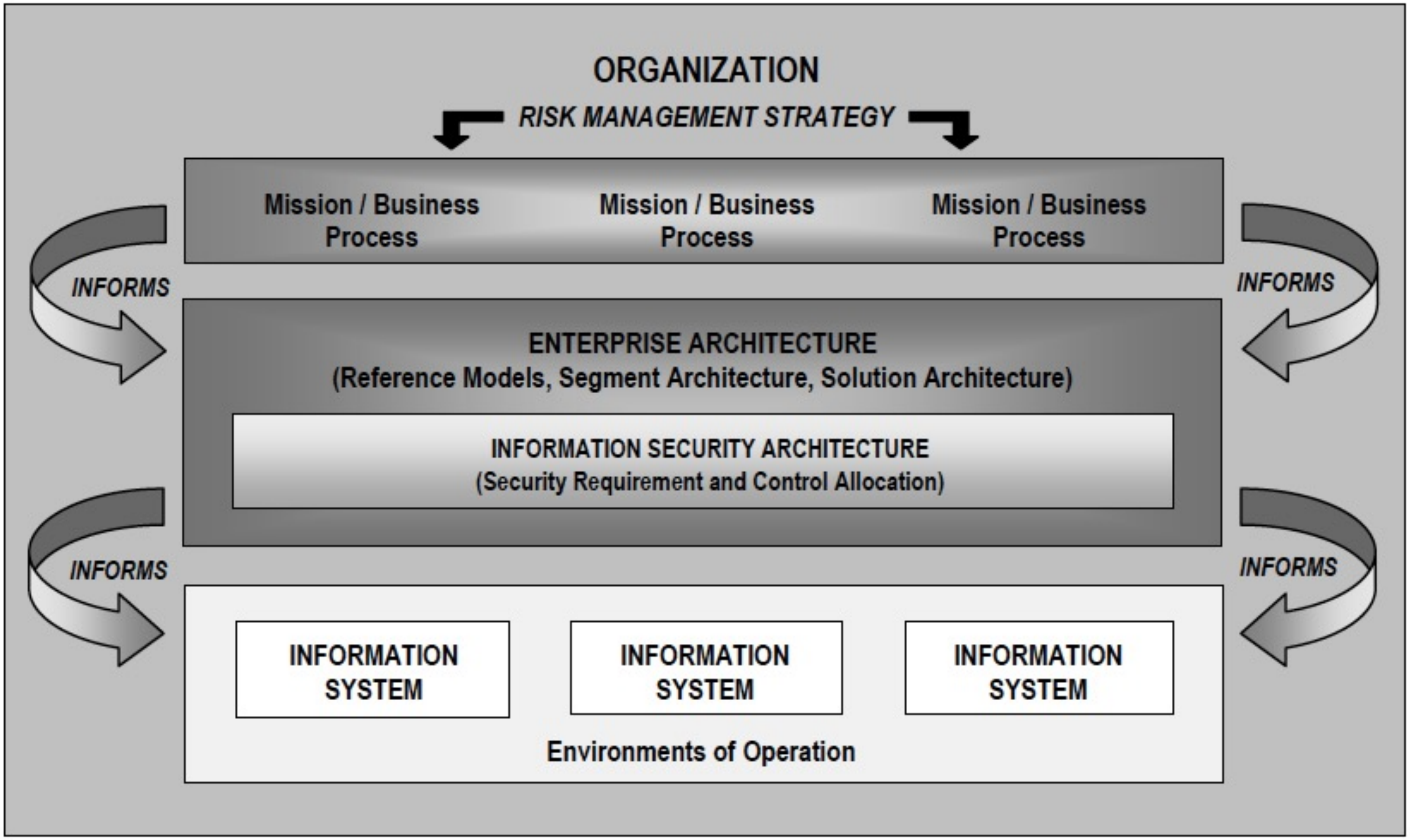
Organization

- Governance – strategic alignment; execution of risk management processes; effective and efficient allocation of resources; performance-based outcomes; and delivered value by optimized risk management investments.
- Risk Executive – individual or group
- Risk Management Strategy
- Investment strategy

Mission/Business Process

- Risk-aware mission/business processes
- Enterprise architecture – segmentation, redundancy and elimination of single points of failure
- Information Security Architecture – people, processes and technology

Mission/Business Process


ORGANIZATION
RISK MANAGEMENT STRATEGY
Mission / Business Process
Mission / Business Process
Mission / Business Process
INFORMS
INFORMS
ENTERPRISE ARCHITECTURE
(Reference Models, Segment Architecture, Solution Architecture)
INFORMATION SECURITY ARCHITECTURE
(Security Requirement and Control Allocation)
INFORMS
INFORMS
INFORMATION SYSTEM
INFORMATION SYSTEM
INFORMATION SYSTEM
Environments of Operation

From: NIST sp 800-39 – Managing Information Security Risk

Information Systems

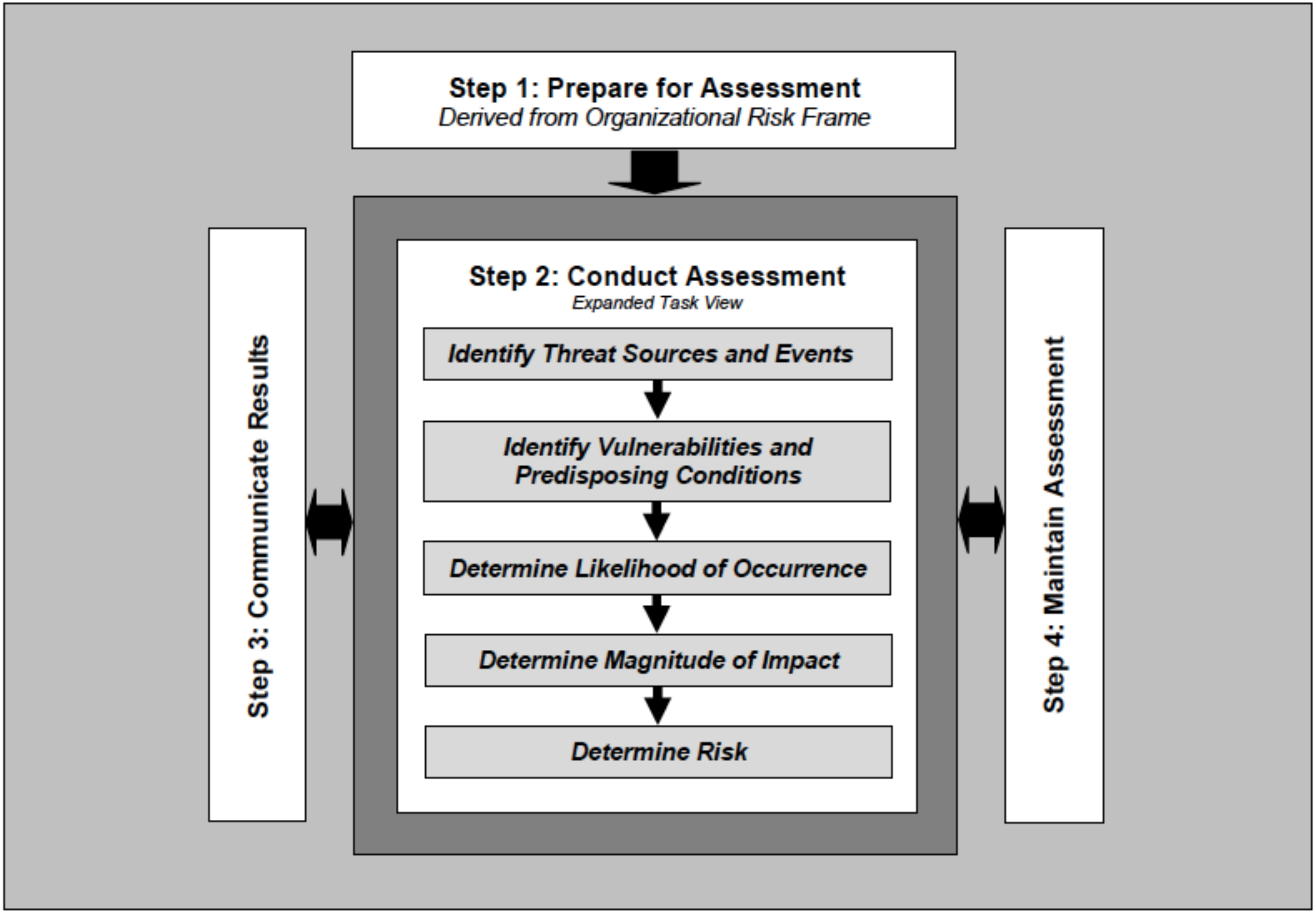
- Initiation - requirements
- Development/acquisition
- Implementation
- Operation/maintenance
- Disposal

Trust and Trustworthiness

- Trust: the belief that an entity will behave in a predictable manner in specified circumstances.
- Trustworthiness is an attribute of an entity.
- Trustworthiness of Information Systems:
  - Security functionality
  - Security Assurance

Organizational Culture

- Values, beliefs and norms
- Willingness to adopt new and leading edge technologies
- Inter-organization culture dis-connect can be the cause of problems.


Step 1: Prepare for Assessment
Derived from Organizational Risk Frame
Step 2: Conduct Assessment
Expanded Task View
Identify Threat Sources and Events
Identify Vulnerabilities and Predisposing Conditions
Determine Likelihood of Occurrence
Determine Magnitude of Impact
Determine Risk
Step 3: Communicate Results
Step 4: Maintain Assessment

From: NIST sp 800-30(r1) – Guide for conducting risk assessments

TABLE D-3: ASSESSMENT SCALE – CHARACTERISTICS OF ADVERSARY CAPABILITY

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The adversary has a very sophisticated level of expertise, is well-resourced, and can generate opportunities to support multiple successful, continuous, and coordinated attacks.
High	80-95	8	The adversary has a sophisticated level of expertise, with significant resources and opportunities to support multiple successful coordinated attacks.
Moderate	21-79	5	The adversary has moderate resources, expertise, and opportunities to support multiple successful attacks.
Low	5-20	2	The adversary has limited resources, expertise, and opportunities to support a successful attack.
Very Low	0-4	0	The adversary has very limited resources, expertise, and opportunities to support a successful attack.

TABLE D-4: ASSESSMENT SCALE – CHARACTERISTICS OF ADVERSARY INTENT

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The adversary seeks to undermine, severely impede, or destroy a core mission or business function, program, or enterprise by exploiting a presence in the organization's information systems or infrastructure. The adversary is concerned about disclosure of tradecraft only to the extent that it would impede its ability to complete stated goals.
High	80-95	8	The adversary seeks to undermine/impede critical aspects of a core mission or business function, program, or enterprise, or place itself in a position to do so in the future, by maintaining a presence in the organization's information systems or infrastructure. The adversary is very concerned about minimizing attack detection/disclosure of tradecraft, particularly while preparing for future attacks.
Moderate	21-79	5	The adversary seeks to obtain or modify specific critical or sensitive information or usurp/disrupt the organization's cyber resources by establishing a foothold in the organization's information systems or infrastructure. The adversary is concerned about minimizing attack detection/disclosure of tradecraft, particularly when carrying out attacks over long time periods. The adversary is willing to impede aspects of the organization's missions/business functions to achieve these ends.
Low	5-20	2	The adversary actively seeks to obtain critical or sensitive information or to usurp/disrupt the organization's cyber resources, and does so without concern about attack detection/disclosure of tradecraft.
Very Low	0-4	0	The adversary seeks to usurp, disrupt, or deface the organization's cyber resources, and does so without concern about attack detection/disclosure of tradecraft.

TABLE D-5: ASSESSMENT SCALE – CHARACTERISTICS OF ADVERSARY TARGETING

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The adversary analyzes information obtained via reconnaissance and attacks to target persistently a specific organization, enterprise, program, mission or business function, focusing on specific high-value or mission-critical information, resources, supply flows, or functions; specific employees or positions; supporting infrastructure providers/suppliers; or partnering organizations.
High	80-95	8	The adversary analyzes information obtained via reconnaissance to target persistently a specific organization, enterprise, program, mission or business function, focusing on specific high-value or mission-critical information, resources, supply flows, or functions, specific employees supporting those functions, or key positions.
Moderate	21-79	5	The adversary analyzes publicly available information to target persistently specific high-value organizations (and key positions, such as Chief Information Officer), programs, or information.
Low	5-20	2	The adversary uses publicly available information to target a class of high-value organizations or information, and seeks targets of opportunity within that class.
Very Low	0-4	0	The adversary may or may not target any specific organizations or classes of organizations.

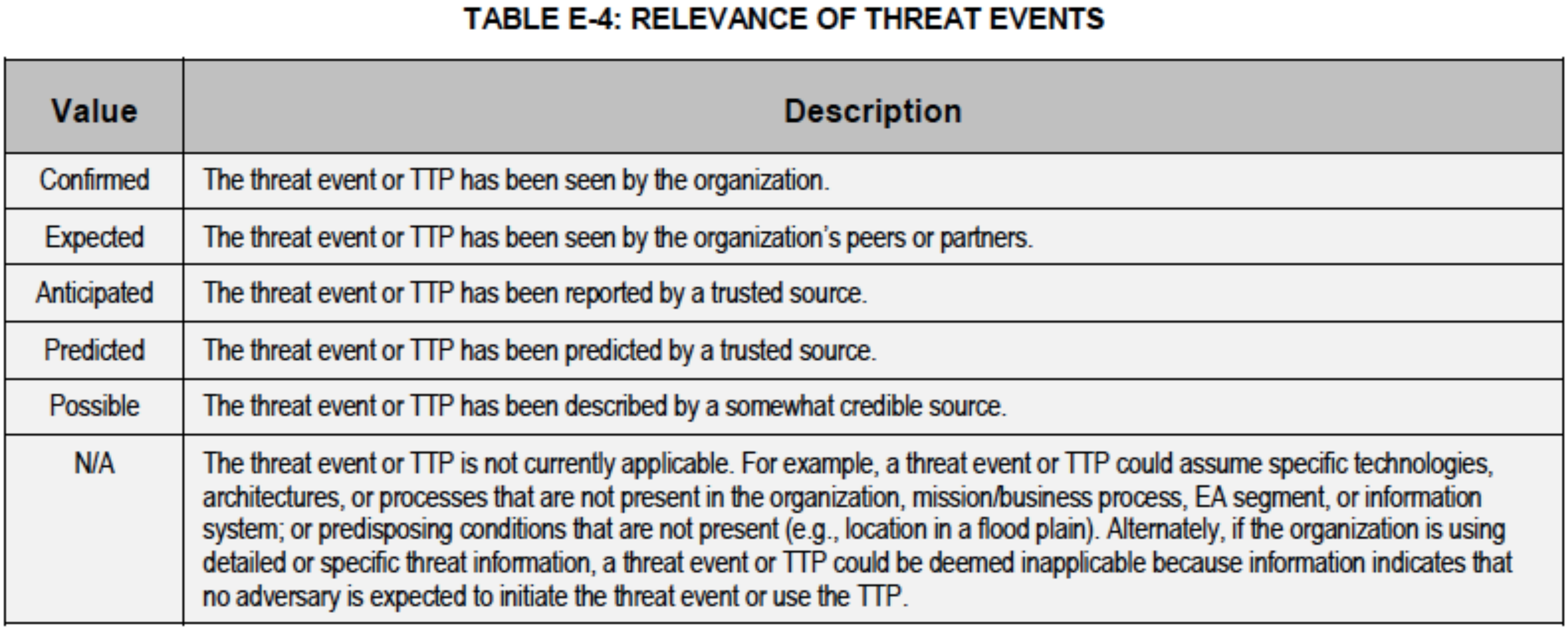


TABLE E-4: RELEVANCE OF THREAT EVENTS

Value	Description
Confirmed	The threat event or TTP has been seen by the organization.
Expected	The threat event or TTP has been seen by the organization's peers or partners.
Anticipated	The threat event or TTP has been reported by a trusted source.
Predicted	The threat event or TTP has been predicted by a trusted source.
Possible	The threat event or TTP has been described by a somewhat credible source.
N/A	The threat event or TTP is not currently applicable. For example, a threat event or TTP could assume specific technologies, architectures, or processes that are not present in the organization, mission/business process, EA segment, or information system; or predisposing conditions that are not present (e.g., location in a flood plain). Alternately, if the organization is using detailed or specific threat information, a threat event or TTP could be deemed inapplicable because information indicates that no adversary is expected to initiate the threat event or use the TTP.

TTP = Tactics, techniques and procedures

TABLE F-2: ASSESSMENT SCALE – VULNERABILITY SEVERITY

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The vulnerability is exposed and exploitable, and its exploitation could result in severe impacts. Relevant security control or other remediation is not implemented and not planned; or no security measure can be identified to remediate the vulnerability.
High	80-95	8	The vulnerability is of high concern, based on the exposure of the vulnerability and ease of exploitation and/or on the severity of impacts that could result from its exploitation. Relevant security control or other remediation is planned but not implemented; compensating controls are in place and at least minimally effective.
Moderate	21-79	5	The vulnerability is of moderate concern, based on the exposure of the vulnerability and ease of exploitation and/or on the severity of impacts that could result from its exploitation. Relevant security control or other remediation is partially implemented and somewhat effective.
Low	5-20	2	The vulnerability is of minor concern, but effectiveness of remediation could be improved. Relevant security control or other remediation is fully implemented and somewhat effective.
Very Low	0-4	0	The vulnerability is not of concern. Relevant security control or other remediation is fully implemented, assessed, and effective.

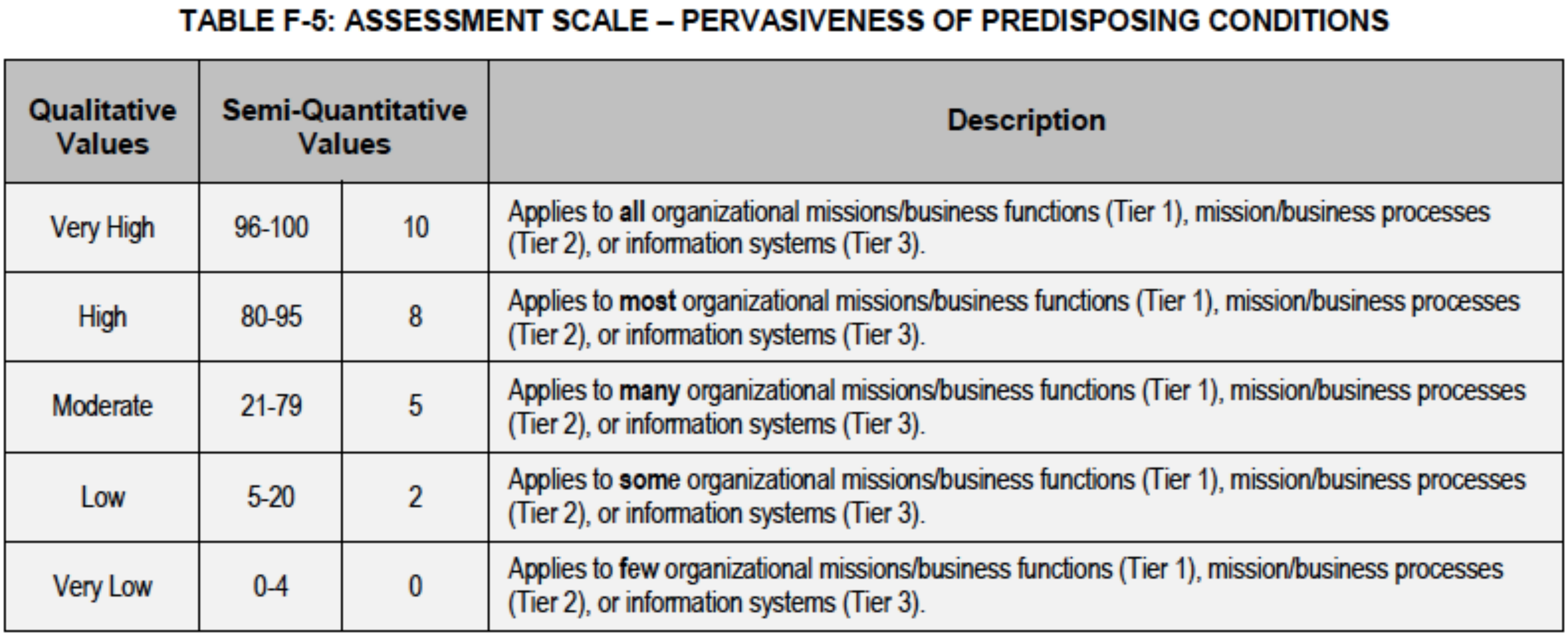
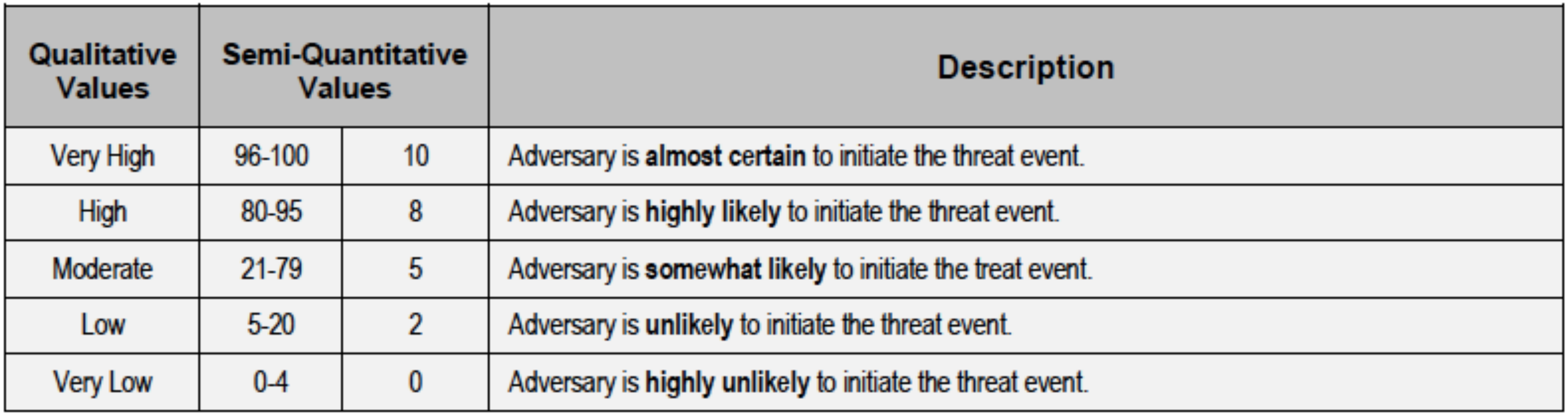


TABLE F-5: ASSESSMENT SCALE – PERVASIVENESS OF PREDISPOSING CONDITIONS

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Applies to **all** organizational missions/business functions (Tier 1), mission/business processes (Tier 2), or information systems (Tier 3).
High	80-95	8	Applies to **most** organizational missions/business functions (Tier 1), mission/business processes (Tier 2), or information systems (Tier 3).
Moderate	21-79	5	Applies to **many** organizational missions/business functions (Tier 1), mission/business processes (Tier 2), or information systems (Tier 3).
Low	5-20	2	Applies to **some** organizational missions/business functions (Tier 1), mission/business processes (Tier 2), or information systems (Tier 3).
Very Low	0-4	0	Applies to **few** organizational missions/business functions (Tier 1), mission/business processes (Tier 2), or information systems (Tier 3).

TABLE G-2: ASSESSMENT SCALE – LIKELIHOOD OF THREAT EVENT INITIATION (ADVERSARIAL)



Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Adversary is **almost certain** to initiate the threat event.
High	80-95	8	Adversary is **highly likely** to initiate the threat event.
Moderate	21-79	5	Adversary is **somewhat likely** to initiate the treat event.
Low	5-20	2	Adversary is **unlikely** to initiate the threat event.
Very Low	0-4	0	Adversary is **highly unlikely** to initiate the threat event.

TABLE G-3: ASSESSMENT SCALE – LIKELIHOOD OF THREAT EVENT OCCURRENCE (NON-ADVERSARIAL)

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Error, accident, or act of nature is **almost certain** to occur; or occurs **more than 100 times a year**.
High	80-95	8	Error, accident, or act of nature is **highly likely** to occur; or occurs **between 10-100 times a year**.
Moderate	21-79	5	Error, accident, or act of nature is **somewhat likely** to occur; or occurs **between 1-10 times a year**.
Low	5-20	2	Error, accident, or act of nature is **unlikely** to occur; or occurs **less than once a year**, but **more than once every 10 years**.
Very Low	0-4	0	Error, accident, or act of nature is **highly unlikely** to occur; or occurs **less than once** every **10 years**.

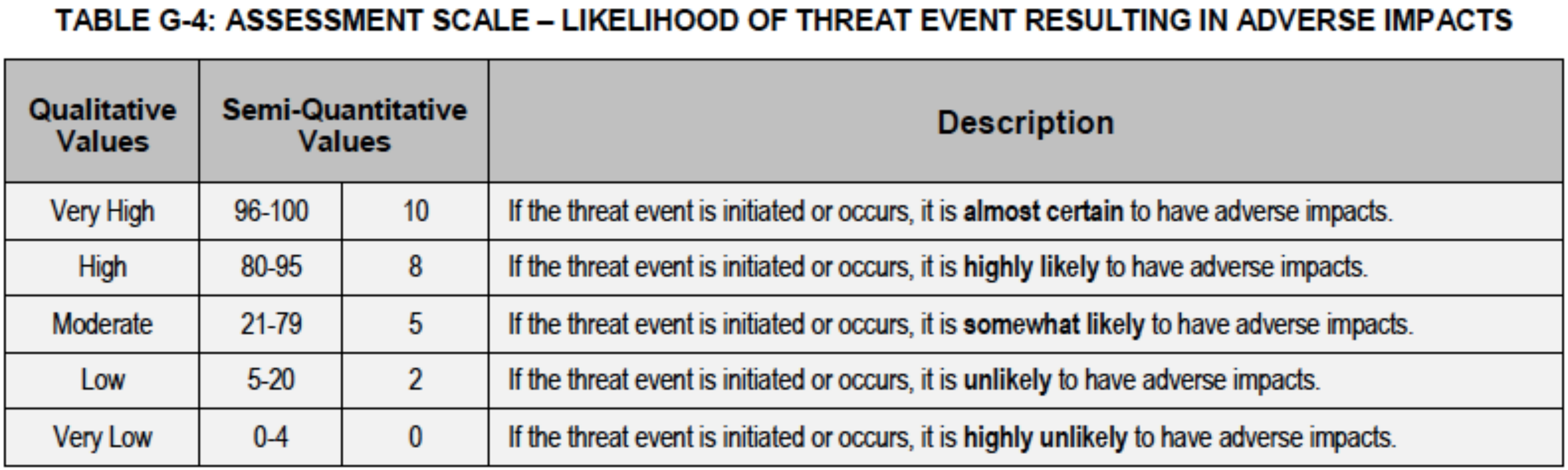
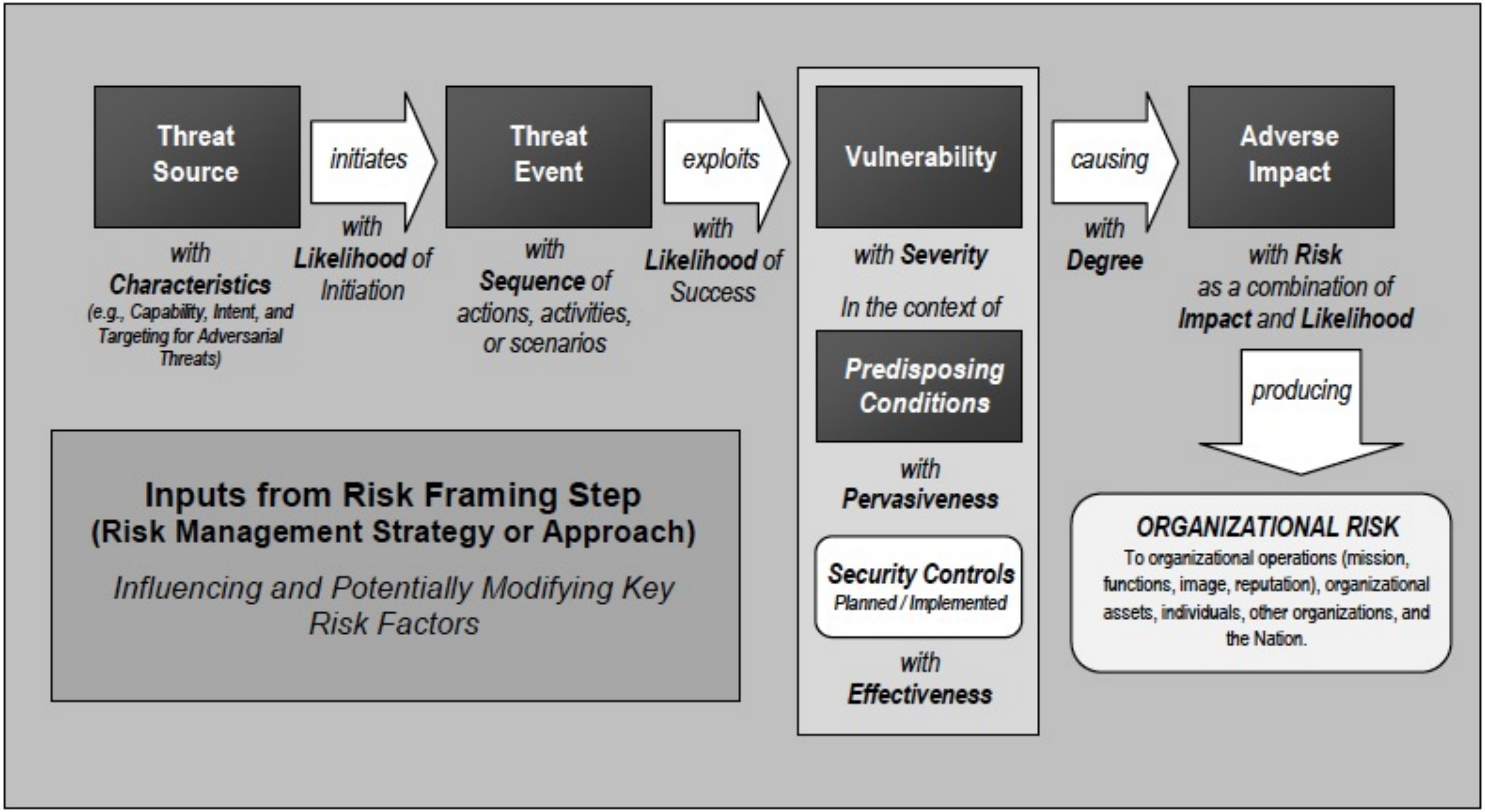


TABLE G-4: ASSESSMENT SCALE – LIKELIHOOD OF THREAT EVENT RESULTING IN ADVERSE IMPACTS

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	If the threat event is initiated or occurs, it is **almost certain** to have adverse impacts.
High	80-95	8	If the threat event is initiated or occurs, it is **highly likely** to have adverse impacts.
Moderate	21-79	5	If the threat event is initiated or occurs, it is **somewhat likely** to have adverse impacts.
Low	5-20	2	If the threat event is initiated or occurs, it is **unlikely** to have adverse impacts.
Very Low	0-4	0	If the threat event is initiated or occurs, it is **highly unlikely** to have adverse impacts.



Threat Source

initiates

with **Likelihood** *of Initiation*

with **Characteristics** *(e.g., Capability, Intent, and Targeting for Adversarial Threats)*

Threat Event

exploits

with **Likelihood** *of Success*

with **Sequence** *of actions, activities, or scenarios*

Vulnerability

with **Severity**

In the context of

Predisposing Conditions

with **Pervasiveness**

Security Controls
Planned / Implemented

with **Effectiveness**

causing

with **Degree**

Adverse Impact

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

From: NIST sp 800-30(r1) – Guide for conducting risk assessments

Table 4: Event Likelihood Evaluation

Likelihood of Threat Event Initiation or Occurrence	Likelihood Threat Events Result in Adverse Impacts				
	Very Low	Low	Moderate	High	Very High
Very High	Low	Moderate	High	Very High	Very High
High	Low	Moderate	Moderate	High	Very High
Moderate	Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Moderate	Moderate
Very Low	Very Low	Very Low	Low	Low	Low

TABLE H-3: ASSESSMENT SCALE – IMPACT OF THREAT EVENTS

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The threat event could be expected to have **multiple severe or catastrophic** adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.
High	80-95	8	The threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. A severe or catastrophic adverse effect means that, for example, the threat event might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.
Moderate	21-79	5	The threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A serious adverse effect means that, for example, the threat event might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries.
Low	5-20	2	The threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A limited adverse effect means that, for example, the threat event might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
Very Low	0-4	0	The threat event could be expected to have a **negligible** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation.

TABLE I-2: ASSESSMENT SCALE – LEVEL OF RISK (COMBINATION OF LIKELIHOOD AND IMPACT)

Likelihood (Threat Event Occurs and Results in Adverse Impact)	**Level of Impact**				
	Very Low	**Low**	**Moderate**	**High**	**Very High**
Very High	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low

TABLE I-3: ASSESSMENT SCALE – LEVEL OF RISK

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	**Very high risk** means that a threat event could be expected to have **multiple severe or catastrophic** adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.
High	80-95	8	**High risk** means that a threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Moderate	21-79	5	**Moderate risk** means that a threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Low	5-20	2	**Low risk** means that a threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Very Low	0-4	0	**Very low risk** means that a threat event could be expected to have a **negligible** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.

Worked Example (Hacking Exposed)

- **Potential Threat Source(s)** Nation-state; insider; malware
- **Attack** Stack-based buffer overflow
- **Threat Vector** Web interface; local network
- **Vulnerability** CVE-2016-0868
- **Target** Allen-Bradley MicroLogix 1100

Worked Example (Hacking Exposed)

- **Potential Threat Source(s)** Nation-state; insider; malware
- **Attack** Stack-based buffer overflow
- **Threat Vector** Web interface; local network
- **Vulnerability** CVE-2016-0868
- **Target** Allen-Bradley MicroLogix 1100
- **Abuse case/objective** Execute code; gain control; modify configuration
- **Potential consequences** Loss of control/vision; data corruption; damage

Worked Example (Hacking Exposed) – connected device

- **Potential Threat Source(s)** Nation-state; insider; malware
- **Attack** Memory corruption via kernel-mode driver
- **Threat Vector** Malicious file opened in a web browser
- **Vulnerability** CVE-2016-0005 (0008, 0009)
- **Target** Workstation running Windows 7 SP1 and IE
- **Abuse case/objective** Execute code; gain control; pivot
- **Potential consequences** damage; pivoting

Worked Example (Hacking Exposed) - correlated

- **Potential Threat Source(s)** Nation-state; insider; malware
- **Attack** Stack-based buffer overflow
- **Threat Vector** Web interface; local network; engineering workstation
- **Vulnerability** CVE-2016-0868
- **Target** Allen-Bradley MicroLogix 1100
- **Abuse case/objective** Execute code; gain control; modify configuration
- **Potential consequences** Loss of control/vision; data corruption; damage

Worked Example (Hacking Exposed)

- Risk = F(Severity, Criticality, Likelihood, Impact)
- F(s,c,l,i) = (s + 2c + 2l + 2i)/4
- Even weighting
- Vulnerability severity: 9.8
- Asset criticality: 3.0
- Attack Likelihood: 2.5
- Impact: 3.0
- Risk: 6.7

Risk Management Process

- Frame – framework for risk decisions; risk tolerance; safety and security; availability; and physical operating environment.
- Assess – identify threats and vulnerabilities; harm and likelihood; effect on physical process, dependent systems, and physical environment; and safety.
- Respond – to identification of risk (acceptance, avoidance, mitigation, sharing, transfer).
- Monitor – implementation; changes in environment; effectiveness and efficiency.

Response

- Analyse different courses of action
- Conduct cost-benefit analyses
- Address scalability issues for large scale implementations
- Examine interactions/dependencies amongst risk mitigation approaches
- Assess any other factors

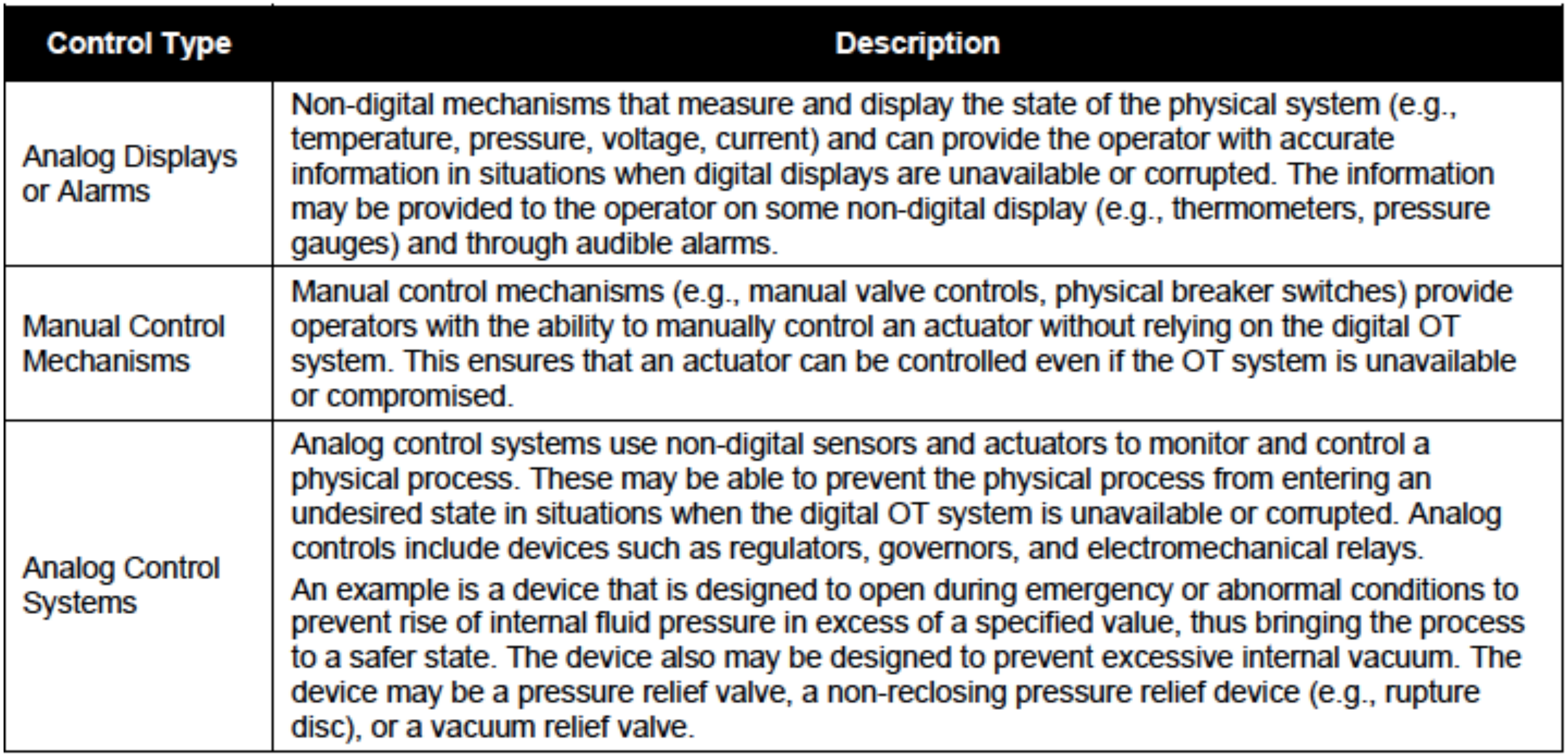
ICS Risk Assessment

- Impacts on safety and the use of safety assessments.

- Physical impact of a cyber incident on an ICS.

- The consequence of risk assessments of non-digital control components.

Non-digital OT Control Components



Control Type	Description
Analog Displays or Alarms	Non-digital mechanisms that measure and display the state of the physical system (e.g., temperature, pressure, voltage, current) and can provide the operator with accurate information in situations when digital displays are unavailable or corrupted. The information may be provided to the operator on some non-digital display (e.g., thermometers, pressure gauges) and through audible alarms.
Manual Control Mechanisms	Manual control mechanisms (e.g., manual valve controls, physical breaker switches) provide operators with the ability to manually control an actuator without relying on the digital OT system. This ensures that an actuator can be controlled even if the OT system is unavailable or compromised.
Analog Control Systems	Analog control systems use non-digital sensors and actuators to monitor and control a physical process. These may be able to prevent the physical process from entering an undesired state in situations when the digital OT system is unavailable or corrupted. Analog controls include devices such as regulators, governors, and electromechanical relays. An example is a device that is designed to open during emergency or abnormal conditions to prevent rise of internal fluid pressure in excess of a specified value, thus bringing the process to a safer state. The device also may be designed to prevent excessive internal vacuum. The device may be a pressure relief valve, a non-reclosing pressure relief device (e.g., rupture disc), or a vacuum relief valve.

From NIST sp 800-82 (r3): Guide to Industrial Control Systems (ICS) Security

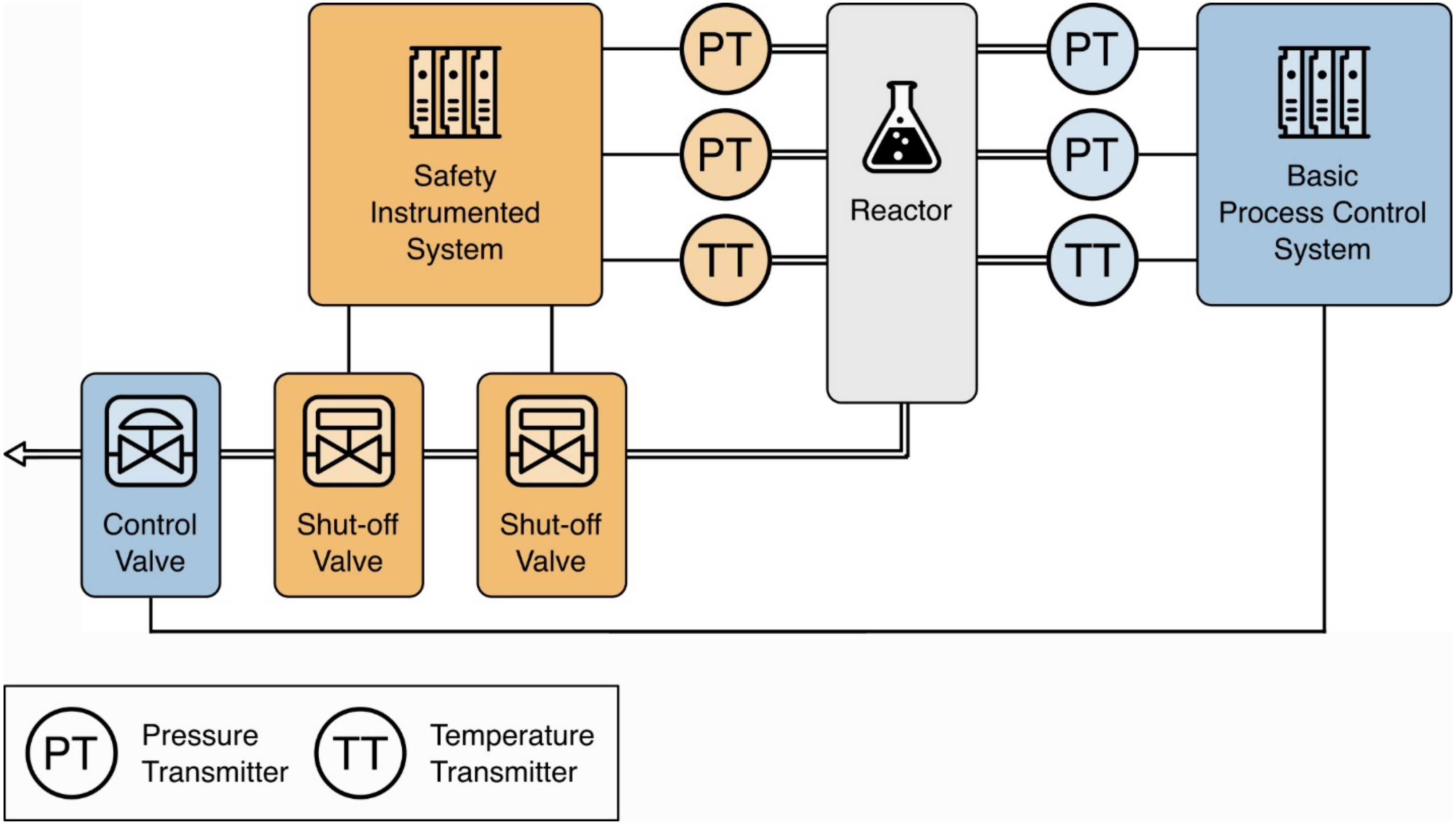
Safety

- UK HSE Guidance to Safety Inspectors – Major Accidents and Loss of Essential Services
- Protect, Detect and Respond
- Defence in Depth
    - Organizational counter-measures
    - Protective counter-measures
    - Detect and Respond counter-measures
- Inspectors assessing:
    - Adequacy of a cyber security management system
    - Adequacy of cyber security counter-measures

Physical Impacts

- How manipulation of sensors and actuators could create an impact
- What redundant controls exist to prevent an impact
- How a physical impact could emerge based on these conditions: for example, release of hazardous materials, explosions, …
- Focus on human safety, damage to the environment and damage to other critical infrastructures
- Cascading failure and short- or long-term outages

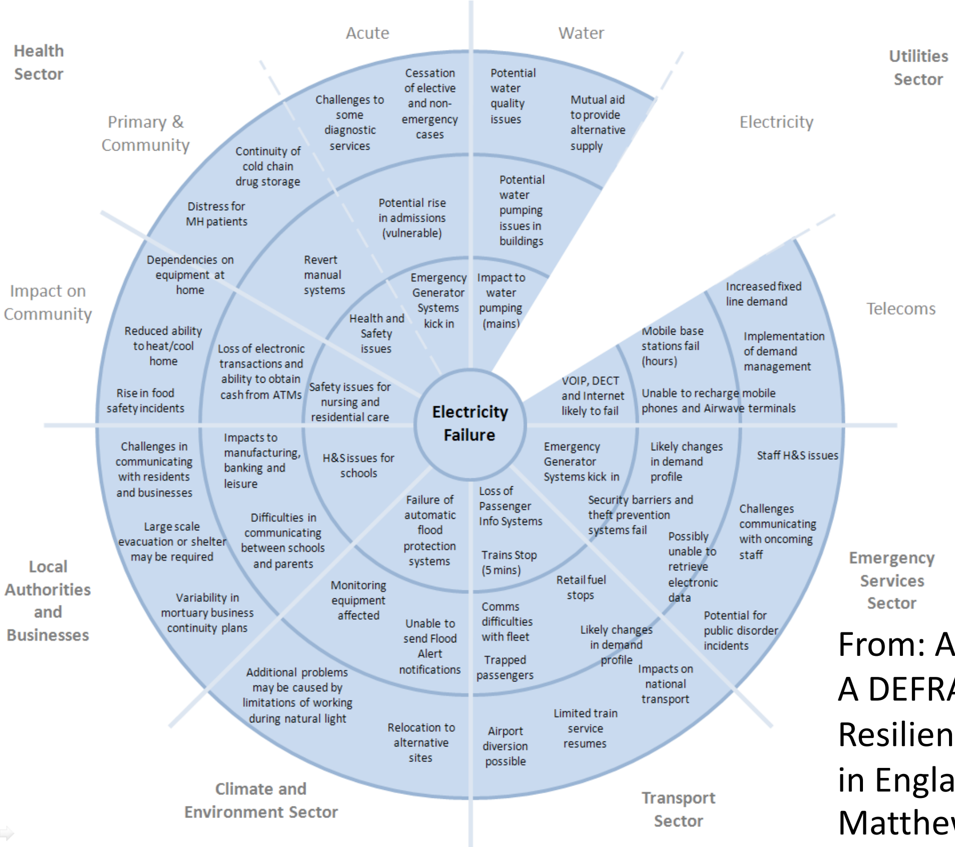
Safety Instrumented Systems



From NIST sp 800-82 (r3): Guide to Industrial Control Systems (ICS) Security

Connected Systems

- Physical or Logical Dependencies



Electricity Failure

Health Sector

Acute

Cessation of elective and non-emergency cases

Challenges to some diagnostic services

Potential rise in admissions (vulnerable)

Emergency Generator Systems kick in

Health and Safety issues

Primary & Community

Continuity of cold chain drug storage

Distress for MH patients

Revert manual systems

Impact on Community

Dependencies on equipment at home

Reduced ability to heat/cool home

Rise in food safety incidents

Loss of electronic transactions and ability to obtain cash from ATMs

Safety issues for nursing and residential care

Local Authorities and Businesses

Challenges in communicating with residents and businesses

Large scale evacuation or shelter may be required

Variability in mortuary business continuity plans

Impacts to manufacturing, banking and leisure

Difficulties in communicating between schools and parents

H&S issues for schools

Climate and Environment Sector

Additional problems may be caused by limitations of working during natural light

Monitoring equipment affected

Relocation to alternative sites

Unable to send Flood Alert notifications

Failure of automatic flood protection systems

Transport Sector

Loss of Passenger Info Systems

Trains Stop (5 mins)

Comms difficulties with fleet

Trapped passengers

Airport diversion possible

Retail fuel stops

Likely changes in demand profile

Limited train service resumes

Impacts on national transport

Emergency Services Sector

Emergency Generator Systems kick in

Security barriers and theft prevention systems fail

Likely changes in demand profile

Possibly unable to retrieve electronic data

Potential for public disorder incidents

Staff H&S issues

Challenges communicating with oncoming staff

Utilities Sector

Water

Potential water quality issues

Mutual aid to provide alternative supply

Potential water pumping issues in buildings

Impact to water pumping (mains)

Electricity

Telecoms

Increased fixed line demand

Implementation of demand management

Mobile base stations fail (hours)

VOIP, DECT and Internet likely to fail

Unable to recharge mobile phones and Airwave terminals

From: Anytown: Final Report
A DEFRA funded project - Community Resilience Funding for Local Resilience Forums in England
Matthew Hogan, London Resilience Team