INL/CON-23-74142-Revision-0

Addressing Consequence within Operational Risk

October 2023

Ollie Gagnon

Changing the World's Energy Future

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

INL/CON-23-74142-Revision-0

Addressing Consequence within Operational Risk

Ollie Gagnon

October 2023

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Addressing Consequence within Operational Risk: An Approach for Understanding an Organization's Unique Infrastructure Environment

O.T. Gagnon III (Ollie), CISSP, CPP, PSP
Strategic Advisor, Critical Infrastructure Security and Resilience
National & Homeland Security, Idaho National Laboratory

Risk Defined

The potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences.

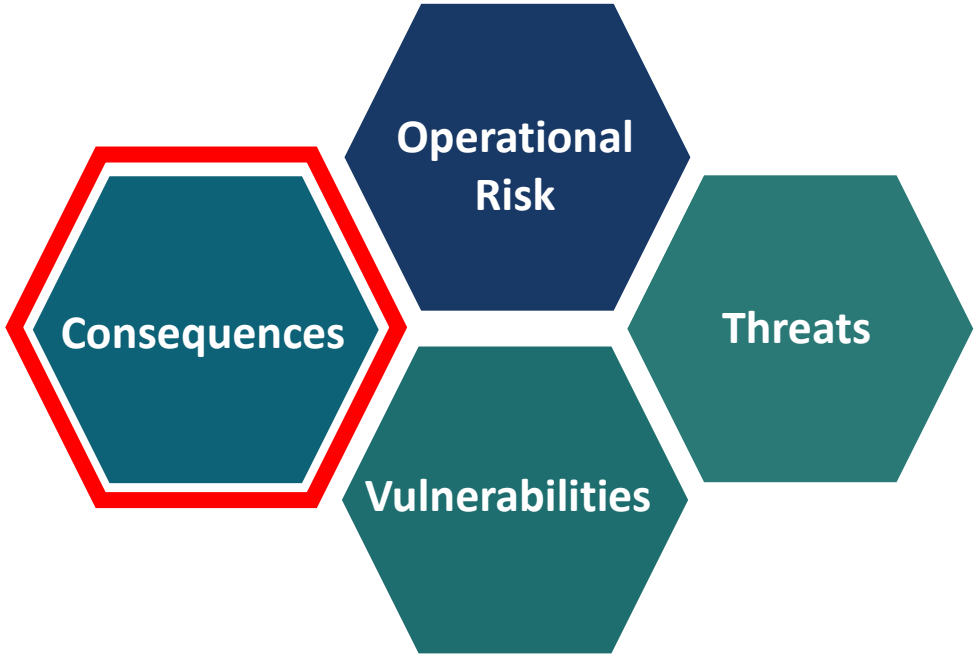
Sources: 2013 National Infrastructure Protection Plans (NIPP) & DHS Lexicon

How well do you know your operational risks?

Can your team list three critical systems, including their priorities, cyber and physical dependencies (internal/external), degree of IT/OT convergence, key stakeholders (internal/external), and incident response and recovery plans?

Operational Risk

- Captures “the uncertainties and hazards a company faces when it attempts to do its day-to-day activities.”
- Results from “breakdowns in internal procedures, people, and systems,” and focuses on “how things are accomplished within an organization.”
- Determined by analyzing the **consequences**, vulnerabilities, and threats within its procedures, workforce, and systems.



Before an organization can consider vulnerabilities within and threats to its operations, it must first have a solid understanding of the **consequences** existing inside it’s infrastructure environment.

Source: www.investopedia.com

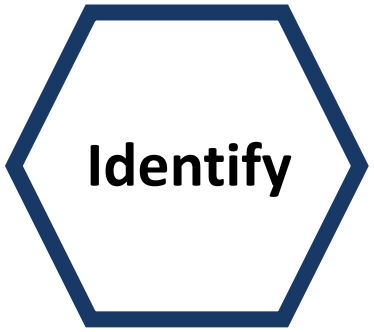
Understanding your infrastructure environment

Considerations:

- Infrastructure vs. Critical Infrastructure
- Security vs. Resilience
- Dependency vs. Interdependency

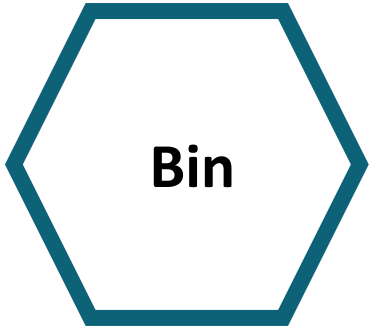
Approach

Where can an entity focus their efforts to gain a foundational understanding of the infrastructure environment to better understand risk with a focus on **consequence**?



Gather internal and external stakeholders and subject matter experts

Identify cyber and physical components



Group like things together

Analyze physical and cyber dependencies and interdependencies

Identify points of convergence

Thoughts on Operational Risk

Reality	Challenge
Most entities know all the components to be binned, their connections, their complexities, and their potential **consequences**.	Knowledge is fractured into **operational silos** within the entity and/or all the **right people** needed to contribute to understanding the infrastructure environment are not part of the process.

- **Facility Engineer/Maintenance** and **Security Manager** have as much to contribute to understanding the cyber and physical infrastructure environment as the **Operations Manager/Director and Chief Information Officer**.
- **People (internal/external)** involved in directing, operating, maintaining, and supporting the cyber and physical infrastructure environment are essential to understanding and ultimately enhancing security and resilience.

Thoughts on Operational Risk (cont.)

Different challenges for each individual organization	Future complications	Significant benefits and significant vulnerabilities	Potential consequences posed by identified points of convergence as part of risk
Explosive growth of Internet of Things (IoT) and Industrial Internet of Things (IIoT) including **potential attack surfaces**	Evolution of **wireless technology** such as 5G over the next several years and eventually 6G in the future	5G technology brings **significant benefits** to critical infrastructure stakeholders but also **potential vulnerabilities**	Influenced by **technology advancements** and **adaption factors** now and foreseeable future

FUNCTIONAL DEPENDENCY EXAMPLE: AIRPORTS

Internal Dependencies for Airport Operations

Airside Operations
- Passenger Ticketing
- Gate Operations
- Air Operations Center
- Ramp Operations & Cargo
- Runways
- Taxiways
- Apron Areas
- Deicing
- Aircraft Parking/Pushing

Communications
- Radio Equipment
- Cable TV
- Satellite Systems
- IT Servers

Landside Operations
- Terminal Facility
- Aircraft Hangars
- Cargo Terminals
- Maintenance Tunnels/Facilities
- Fueling Areas
- Mechanical/Equipment
- Pedestrian Access Tunnels
- Aircraft Fueling Equipment
- Deicing Equip & Facilities
- Food Services Area
- Fuel Storage Area

Landside Operations (cont.)
- Security Screening Area
- Inspection Areas
- Passenger Drop Off/Pick Up
- Rental Car Areas
- Baggage Handling

Safety & Security
- Security Ops Ctr
- Law Enforcement
- Fire
- EMS
- Emergency Mgmt
- EOC
- Contracted Security

Transportation
- Parking Garages
- Parking Lots
- EV Charging Areas
- Terminal Buses & Trams
- People Movers/Tram
- Helicopter Pad
- Roads/Highways

Workforce
- Airside Ops Personnel
- Landside Ops Personnel

Dependencies are relationships of reliance within and among infrastructure assets and systems that must be maintained for those systems to operate and provide services*

Types of Dependencies
- Physical
- Cyber
- Logical
- Geographic

External Dependencies for Airport Operations

Airlines

Aircraft

Air Traffic Control
- Control Facility
- Control Towers

Communications
- Fiber Optic
- Wireless
- Comms. Towers
- Cable TV
- Satellite Systems

Retail
- Food
- Shops
- Services

Safety & Security
- TSA
- Federal Air Security
- Customs & Immigration
- Local Law Enforcement
- Local Fire/EMS

Transportation
- Rideshare
- Rental Cars
- Public Transit
- Roads/Highways

Utilities
- Water
- Wastewater
- Electricity
- Garbage
- Recycling
- Petroleum
- Gas

Workforce
- Air Marshals
- TSA Agents
- FAA ATC Personnel
- Customs Personnel
- USDA Inspections Personnel
- Air Crews (Pilots & FA)
- Airline Personnel
- Airport Personnel
- Retail Personnel

*Source: https://www.cisa.gov/what-are-dependencies

Image source: INL.gov

Infrastructure Environment Complexities

- Infrastructure
- Critical Infrastructure
- Security
- Resilience
- Information Technology
- Operational Technology
- IT-OT Convergence

- Physical Dependencies
- Physical Interdependencies
- Cyber Dependencies
- Cyber Interdependencies
- Physical Element
- Cyber Element
- Human Element

Operational Risk

- Consequence
- Vulnerability
- Threat

Questions