Enterprise Risk
PERA Addendum 2025-1

The PERA Master Planning Handbook, and the Purdue Reference Model for CIM did not fully address Risk Identification, Analysis, and Mitigation. Since these PERA documents were issued, however, several major developments have raised the importance of Risk Management, including:

- **Project Management Book of Knowledge** (PMBOK Guide) was re-issued in 2000 to dramatically expand the treatment of Project Risk.
- **HAZOP (Hazard and Operability),** and other standards such as HACCP, and SIS/SIL have been issued to better address Facility Risks.
- **OSHA and Environmental** Standards have been issued to reduce Human Risk
- **NIST 800, ISA-62443** and other Cybersecurity standards have been issued to reduce the risks associated with cyber-attacks.

A "Risk Management Topic" has therefore been added to the PERA.NET website. Several new documents have been added to the website, including:

- MLMs and discussion papers to address Identification, Analysis, and Mitigation of Risks
- a Risk Management Section was added to the ACS, IT and OT sections of each PERA Master Planning Guide.
- a Risk Management Summary is being added for each PERA Enterprise Class as an example for use in Master Planning for Enterprises in that Industry.

A. Enterprise Risks may be classified as:

1. **General** (applies to many or all Enterprises such as corporate cybersecurity risks).
2. **Industry-specific** (e.g. oil and gas pipeline projects run the risk that a single faulty weld could cause a costly, dangerous and environmentally damaging pipeline failure).
3. **Project-specific** (unique to a particular project, e.g., a project to build a facility in a swampy area or severe climate will face risks specific to that project.

The following is a checklist of Risks that an Enterprise might encounter. Only risks with a credible probability of exceeding the risk tolerance of that Enterprise should be considered further.

Risks should be quantified on a common basis as defined by the Risk Management Policies of the Enterprise.

1) Generic Risks:

Generic Risks include those that are encountered by any Enterprise such as::

- **Financial** – risks from failure of related businesses (e.g. suppliers, partners, etc.), stock market variations, sudden interest rate changes, currency risks, etc.
- **Human** – Injury or death of employees or public, risks from hostile people or organizations (e.g. vandalism, or terrorism), or errors by inadequately trained staff. It may also include illness or death of key personnel and failure to establish succession plans.
- **Operational** – disruption to supplies (supply chain) and, loss of access to essential raw materials, failures in distribution of finished products, sudden changes in government policy, tax regimes, public opinion, foreign influence, etc.
- **Cybersecurity Attacks on Generic Applications** – such as accounting, Human Resources, Email and other common corporate applications.

2) Industry-Specific Risks:

Industry-specific Risks are addressed in the PERA Master Planning Guides for Owner/Operators, Vendors and EPCs for that industry. These risks are addressed during the Master Planning/Conceptual Engineering Phase, the EPC (Engineer, Procure, Construct) Phase, and during the Operations Phase.

A Risk Summary Report may be available for that industry to serve as a resource during Master Planning.

3) Project Risks:

Project-specific risks may include:

- **Schedule** - insufficient or late delivery of raw materials or services, etc.
- **Location** – a facility being built in a remote location, the arctic, or a flood-plain may experience unique risks.
- **Procedural** – failure of procedures, accountability, internal records, checks and balances, project audits, etc.

- **Suppliers** – Failure of contractors including bankruptcy, or product suppliers who do not meet quality requirements (e.g., boiler tubes might rupture or cement might disintegrate).

B. Risk Analysis

Once risks are identified various tools are available for analysis of these risks including:

- simple “heat tables” (high-medium-low impact plotted against high-medium-low likelihood.
- Statistical analysis (see MLMs for statistical analysis concepts and tools).
- Sophisticated models of facility and/or enterprise operation including “digital twin analysis that predicts failures.

C. Risk Mitigation

Once Risks are identified and quantified, four alternatives are available:

- **Eliminate the Risk** – for example remove the equipment causing the risk or substitute a less hazardous product.
- **Moderate the Risk** – implement a backup system or automated protection system reducing risk to an acceptable level.
- **Assign the Risk** – require supplier to provide insurance, or subcontract with terms that assign risk to a third party.
- **Accept the Risk** – if none of the above are possible. The Enterprise may decide to accept the risk (even if it exceeds the acceptable risk criteria for the Enterprise). Alternatively, the facility or project might be cancelled.

See MLMs 018, 19, 36, and 60, and Learning Map 18 – Cybersecurity Risk and Mitigation.