FILED
07/31/26
04:59 PM
R2604016

BEFORE THE PUBLIC UTILITIES COMMISSION OF THE

STATE OF CALIFORNIA

Order Instituting Rulemaking to Refine the Risk-Based Decision-Making Framework for Electric and Gas Utilities.	R.26-04-016

<u>SUBMISSION OF SOUTHERN CALIFORNIA EDISON COMPANY'S (U 338-E), PACIFIC GAS AND ELECTRIC COMPANY'S (U 39-E), SOUTHERN CALIFORNIA GAS COMPANY'S (U 904-G), AND SAN DIEGO GAS & ELECTRIC COMPANY'S (U 902-M) JOINT SURVEY REPORT REGARDING RISK TOLERANCE APPROACHES</u>

WIILLIAM K. BRIGGS
KRIS G. VYAS
Attorneys for
SOUTHERN CALIFORNIA EDISON COMPANY
2244 Walnut Grove Avenue
Post Office Box 800
Rosemead, California 91770
Telephone: (626) 302-6613
E-mail: Kris.Vyas@sce.com

WALKER MATTHEWS
PETER OUBORG
Attorneys for
PACIFIC GAS AND ELECTRIC COMPANY
300 Lakeside, Suite 210
Oakland, CA 94612
Telephone: (415) 238-7987
Email: peter.ouborg@pge.com

SIOBHÁN E. MURILLO
Attorney for
SAN DIEGO GAS AND ELECTRIC COMPANY
8330 Century Park Court, CP32D
San Diego, California 92123
Telephone: (619) 616-0624
Email: smurill1@sdge.com

HOLLY A. JONES
Attorney for
SOUTHERN CALIFORNIA GAS COMPANY
555 West Fifth Street, Suite 1400
Los Angeles, California 90013
Telephone: (626) 681-6377
Email: HAJones@SoCalGas.com

Dated: **July 31, 2026**

BEFORE THE PUBLIC UTILITIES COMMISSION OF THE

STATE OF CALIFORNIA

Order Instituting Rulemaking to Refine the Risk-Based Decision-Making Framework for Electric and Gas Utilities.	R.26-04-016

Pursuant to the July 20, 2026 Assigned Commissioner's Scoping Memo and Ruling (Scoping Memo and Ruling (Scoping Memo) issued in this proceeding, Southern California Edison Company (SCE), Pacific Gas and Electric Company (PG&E), Southern California Gas Company (SoCalGas), and San Diego Gas and Electric Company (SDG&E) respectfully file the attached joint survey report regarding risk tolerance approaches.[1] The Scoping Memo stated the following: "The utilities conducted a joint utility survey on approaches to risk tolerance pursuant to D.25-08-032, ordering paragraph 4. To aid in the Commission's consideration of risk tolerance, the utilities shall file and serve that survey in this proceeding no later than July 31, 2026."[2] The attached survey report is hereby incorporated into this pleading by reference.

Respectfully submitted,

WILLIAM K. BRIGGS
KRIS G. VYAS

/s/ Kris G. Vyas
By: Kris G. Vyas

Attorneys for
SOUTHERN CALIFORNIA EDISON COMPANY

2244 Walnut Grove Avenue
Post Office Box 800
Rosemead, California 91770
Telephone: (626) 302-6613
E-mail: Kris.Vyas@sce.com

Dated: July 31, 2026

---

1 Pursuant to Rule 1.8(d) SCE has been fully authorized by PG&E, SoCalGas, and SDG&E to sign and tender the Joint Survey Report and make the representations stated herein.

2 Scoping Memo, p. 6. *See also* Scoping Memo at p. 13, Ordering Paragraph 6.

<u>ATTACHMENT</u>

SOUTHERN CALIFORNIA EDISON COMPANY'S, PACIFIC GAS AND ELECTRIC COMPANY'S, SOUTHERN CALIFORNIA GAS COMPANY'S, AND SAN DIEGO ELECTRIC COMPANY'S SURVEY REPORT

RDF Phase IV Joint IOU Risk Tolerance Survey

Executive Summary

Pursuant to Decision (D.) 25-08-032 (Phase IV Decision) in the Risk-Based Decision-Making Framework (RDF) Rulemaking (R.) 20-07-013, the joint investor-owned utilities (IOUs)[1] submit the corresponding Risk Tolerance (RT) survey report. The survey report shall include the following information: whether a regulator sets the baseline risk tolerance, or, if not or if only partially, how industries or private companies set, implement, and modify risk tolerance thresholds.[2] The survey report shall include, but is not limited to, the following industries: aviation, chemical, mining, oil and gas, nuclear, autonomous vehicles, spaceflight, investor-owned utilities in other jurisdictions, and large California investor-owned electric and/or gas utilities.[3] For the section on large California investor-owned electric and/or gas utilities, the utilities shall include a description of the status quo, explaining the internal process of how each company currently sets the amount of risk they accept in safety, operations, and decision-making.[4]

The findings reveal that regulatory bodies often set baseline risk tolerance thresholds, based on specific criteria. The processes for establishing those risk tolerance thresholds can vary by industry and jurisdiction. Typically, the regulator first establishes baseline risk tolerance thresholds, and individual companies within those industries define additional risk tolerance metrics based on the company's role and responsibilities and specific regulatory and/or legal requirements and considerations. Based on the survey efforts and results, the industry demonstrates a clear preference for proactively managing catastrophic-type (e.g., tail risk) events. While this approach aligns with the broader risk management landscape, specific risk tolerance frameworks can vary across countries and regions and are shaped by local regulatory requirements.

Additionally, the evidence set forth in this white paper demonstrates that regulators, as well as individual entities, in each of these industries that have historically experienced significant risk outcomes detrimental to public and worker safety have substantially embedded important principles of risk aversion into their risk-based decision-making regulatory framework. In fact, the industries that are most analogous to electric utilities regarding potential public exposure to risk outcomes (*i.e.,* commercial aviation, nuclear) do not have regulatory requirements that prescribe regulated entities to manage to "expected value," without consideration of the

---

[1] Pacific Gas and Electric Company (PG&E), Southern California Edison Company (SCE), and San Diego Gas & Electric Company (SDG&E). Please note that while Southern California Gas Company (SoCalGas) was not specifically identified in the order directing the survey (see D.25-08-032 at page 129), SoCalGas is considered an IOU and participated in this survey.

[2] D.25-08-032 at Ordering Paragraph (OP) 4.

[3] *Id.*

[4] *Id.*

uncertainty or variability of potential risk outcomes. Rather, regulators of such industries (e.g., FAA, NRC) have adopted requirements specifically intended to avoid catastrophic (*i.e.,* tail-risk) events.

I. Introduction[5]

D.25-08-032 directs the Joint IOUs to draft a survey report on approaches to risk tolerance in related industries within 80 days of the issuance date of the Decision.[6]

This survey report should address:
- Whether a regulator sets the baseline risk tolerance [thresholds]?, or, if not, or if only partially,
- How do industries or private companies set, implement, and modify risk tolerance thresholds?

It should include, but is not limited to the following industries:

- Aviation
- Chemical
- Mining
- Oil and gas
- Nuclear
- Autonomous vehicles
- Spaceflight
- Investor-owned utilities in other jurisdictions
- Large California investor-owned electric and/or gas utilities.

For the section on large California investor-owned electric and/or gas utilities, the utilities shall include a description of:

- The status quo, and;
- An explanation of the internal process of how each company currently sets the amount of risk they accept in safety, operations, and decision-making.

Based on this guidance, as well as the timeline allocated to submit a report of their findings to the service list for this proceeding, the Joint IOUs have developed a structured survey of relevant and available literature to comply with this Commission directive. This structured survey was designed to systematically evaluate how risk tolerance is defined, established, and operationalized across each of the sectors identified, with particular attention paid to the

[5] For ease, all references, used herein, are included at the end of each respective section.
[6] D.25-08-032 was approved by the Commission at the Commission's Business Meeting on August 28, 2025, and the issuance date is August 29, 2025.

dynamics between industry regulators, individual entities (*e.g.*, companies) within each industry, as well as other stakeholders.

II. Background

Following the 2010 San Bruno pipeline rupture and explosion, the Commission issued Rulemaking (R.) 13-11-006, formally initiated the Safety Model Assessment Proceeding (S-MAP).[7] Through the S-MAP, the CPUC set out to establish a more structured approach to risk-informed decision-making, particularly as it relates to investment planning processes within utility General Rate Cases (GRCs). Over the years, the Commission has made notable progress in developing formalized methodologies for risk assessment. These efforts have resulted in the creation of detailed risk models and frameworks designed to enhance transparency, comparability, and consistency across the State.

Although significant advancements have been made, an explicit risk tolerance standard has not yet been adopted in California. While the Commission has acknowledged the importance of such standards, most notably in a 2016 Safety Policy Division (SPD) white paper,[8] substantive steps have not yet occurred toward the formal development and adoption of such a standard for the State. While the Commission initially included Risk Tolerance within the scope of Phase IV of the RDF Proceeding, it ultimately decided to postpone its determination of this issue and instead initiate a separate new proceeding to address Risk Tolerance.

To further this effort, and in compliance with the direction in D.25-08-032, the Joint IOUs have undertaken a focused effort through this risk tolerance survey to examine the dynamic between regulators and stakeholders in shaping and operationalizing these types of risk tolerance standards, while stressing the importance of not only the expected value of these risks, but also defined metrics regarding what may constitute intolerable tail risk events.

III. Risk Tolerance Concepts

Prior to delving into the complexities of how risk tolerances are developed and established, it is important to clarify several foundational themes implicit in the Commission's inquiry, which involve questions that have yet to be fully addressed, specifically:

- Whose perspective is being represented in the articulation of risk tolerance? In other words, *whose* risk tolerance, is it?
- How are these tolerances influenced by each stakeholder involved in the process (*e.g.*, the regulator, the entities responsible for implementing the measures to ensure those tolerances are met, investors, the public)?
- Who is accepting the risk, including what is their risk appetite and ability to absorb the risk (risk capacity)?

---

[7] See Report of the Independent Review Panel San Bruno Explosion, prepared for the California Public Utilities Commission, at 100-101 (June 24, 2011).

[8] California Public Utilities Commission, Safety and Enforcement Division. (2016). *Safety and Enforcement Division evaluation report on the risk evaluation models and risk-based decision frameworks in A.15-05-002, et al.* https://www.cpuc.ca.gov/industries-and-topics/electrical-energy/risk-assessment/risk-assessment-mitigation-phase

These questions are central to understanding how risk is perceived, managed, and ultimately accepted across various stakeholder groups. Their answers have broad implications in terms of mitigation strategies, funding authorization, and cost recovery across utility planning and operations. In order to provide those answers, it is important to distinguish between the types of perspectives in which risk tolerance is often represented (*e.g.*, societal, individual) as well as the role those perspectives play in shaping risk tolerance levels within each of these industries.

Societal risk tolerance refers to the collective level of risk the public is willing to accept in exchange for the benefits of essential services, (*e.g.*, the provisioning of electricity and natural gas).[9] These tolerances are typically reflected in the standards promulgated by regulatory authorities and are shaped by public perceptions of risk and the resilience of service providers including their financial capacity to absorb adverse events. In this context, regulators serve as proxies for societal preferences, translating public expectations into enforceable thresholds to guide utility operations.

Individual risk tolerance varies significantly across individual stakeholder groups including companies, their employees, their customers, their investors, as well as members of the general public.[10] For individual companies, their risk tolerances are influenced by regulatory compliance obligations, workforce and resource dynamics, duty to provide service, public scrutiny, and financial constraints such as creditworthiness and access to capital. Similarly, employees and contractors assess risk through the lens of workplace safety, compensation, or alternative employment opportunities. Meanwhile, customer and public risk tolerance standards are shaped by their own exposure to risk, socioeconomic status, and general awareness of potential hazards.

In each of these cases, risk tolerances of each type are governed by three interrelated concepts that underpin risk management frameworks: risk appetite, risk capacity, and risk attitude.

Risk Appetite describes the degree and nature of risk an entity is willing to pursue or retain in order to achieve its objectives. It reflects strategic preferences and is shaped by industry norms, regulatory expectations, and stakeholder priorities (IRM, 2011).[11] In safety-critical domains such as nuclear energy, aviation, or dam operators, risk appetite defines the boundaries of acceptable risk and informs long-term planning.

Risk Capacity represents an organization's ability to absorb adverse effects from risks. For a commercial firm, capacity might be specified in terms of maximum level of risk an entity can

---

[9] Frewer, L. (1999). *Risk perception, social trust, and public participation in strategic decision making: Implications for emerging technologies.* Retrieved from https://www.jstor.org/stable/4314956

[10] Power, M. (2015). *Risk, social theories, and organizations.* In The Oxford Handbook of Sociology, Social Theory, and Organization Studies (pp. 370–392). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199671083.013.0016

[11] Institute of Risk Management. (2011). *Risk appetite and tolerance guidance paper*. Institute of Risk Management. https://www.theirm.org/media/8633/irm-risk-appetite-exec-summary-web.pdf

absorb without compromising its viability.[12] Unlike risk appetite, which is discretionary, risk capacity is a hard constraint determined by financial resources, operational resilience, and legal obligations. It describes the upper limit of acceptable risk, from the perspective of each individual entity particularly in domains with high-impact consequences, such as cybersecurity, environmental compliance, and/or financial solvency.

Based on the Joint IOUs' review of industry literature, risk tolerances across these industries are shaped by both societal expectations reflected by regulatory agencies as well as the capacities of individual entities within those industries to respond to and/or accept those risks. These layers include:

- **Regulatory Standards**: In all industries surveyed, regulatory bodies put forth a risk framework, comprised of a set of minimally acceptable thresholds based on the collective ability of entities. These standards are informed by societal expectations, legal precedent, as well as industry best practices. While in some cases these risk tolerance levels take the form of specific thresholds, in other cases, they are described only through overarching principles.

- **Organizational Interpretation**: Individual entities, typically through their Boards of Directors, interpret these regulatory standards in the context of long-term viability (e.g., risk capacity) of their organizations. This includes considerations such as operational capability, capital attraction, workforce retention, and alignment with broader policy objectives and ability to obtain needed capital. In some cases, these individual risk capacities are reflected either explicitly or implicitly by their risk attitude, which may differ across companies within an industry.

In addition to regulators and individual entities, other **entities, including employees, contractors, customers, as well as the general public,** exert additional influence through advocacy, consumer behavior, direct engagement, or any combination thereof, to further shape and define risk tolerance standards based on their own risk appetites, capacities, and attitudes. Divergent risk tolerance standards as well as incentives among stakeholders further complicate this alignment and navigate these competing priorities that often require trade-offs and negotiation across these stakeholder groups.

General References

- International Organization for Standardization. (2018). *Risk management – Guidelines* (ISO Standard No. 31000:2018). https://www.iso.org/standard/65694.html

[12] International Electrotechnical Commission. (2019). IEC 31010:2019 Risk management — Risk assessment techniques. Geneva, Switzerland: IEC.

Committee of Sponsoring Organizations of the Treadway Commission. (2017). *Enterprise Risk Management—Integrating with Strategy and Performance*. https://www.scribd.com/document/854173331/Coso-Erm-Standard-2017

IV. Industry-Specific Risk Tolerance Case Studies

A. Aviation

Does the industry have a risk tolerance threshold?
There is no single, explicit risk tolerance threshold that is universally applied across all operators within the aviation industry. Instead, regulatory bodies such as the Federal Aviation Administration (FAA),the International Civil Aviation Organization (ICAO), and European Union Aviation Safety Agency (EASA) require aviation organizations to implement Safety Management Systems (SMS), which include risk assessment processes, but they do not prescribe fixed numerical thresholds for acceptable risk.[13] Acceptable levels of safety risk are defined contextually and operationally by each organization, and are then monitored by the relevant regulatory authority (*e.g.*, FAA). Ensuring safety and compliance with regulatory processes tend to be reactive and require that incidents be investigated and processes that allowed the incidents be scrutinized and corrected.[14]

Is it set by the applicable regulatory body?

Partially. The FAA sets baseline expectations through regulations such as 14 CFR Part 5, which mandates the implementation of SMS.[15] These regulations establish the framework and process for risk management but stop short of defining specific risk tolerance thresholds. However, the FAA also provides guidance through documents like Advisory Circular 120-92D and FAA Order 8040.4B, which outline how safety risk should be assessed and managed. Given the catastrophic potential of aviation failures, and the exposure of this risk to the public, the FAA also mandates comprehensive SMSs so that risk is continuously assessed and controlled. These requirements promote a culture in the aviation industry where even low-probability hazards are treated with rigorous scrutiny to prevent high-impact outcomes, such as mid-air collisions or systemic failures. These risks are assessed using probabilistic safety models and stress testing for extreme scenarios. ICAO similarly requires member states to define acceptable levels of safety risk but allows flexibility in how these are implemented.

If not, what is the internal process by which each company (within the industry) establishes a risk tolerance level?

Individual airlines and airports develop their own risk tolerance thresholds within the regulatory framework. These thresholds are typically established through internal risk committees, operational data analysis, and cross-functional collaboration. Companies use tools such as risk

---

[13] 14CFR5.71, 5.73 prescribes the need for "assurance of the overall safety performance of aviation organizations".
[14] AC 120-92D G-9; AC 120-92D further elaborates that "Investigations should focus on what went wrong rather than who caused the error and emphasize improvement of safety performance.
[15] AC 120-92D; National Archives and Records Administration. (2025, September 29). *14 CFR Part 5 – Safety Management Systems*. Electronic Code of Federal Regulations. https://www.ecfr.gov/current/title-14/chapter-I/subchapter-A/part-5

matrices, predictive analytics, and incident trend analysis to tailor risk thresholds to their specific operations, fleet, and customer base. These thresholds are embedded in operational manuals, pilot training programs, maintenance schedules, and emergency procedures.

How are they implemented?

Risk tolerance thresholds for individual organizations (e.g. airlines, air carriers, and airport operators) in the aviation industry are operationalized through the Safety Risk Management (SRM) process, a structured methodology used to identify, assess, and control safety risks. This process begins with system analysis, which involves understanding the operational environment and its components. It is followed by hazard identification, where potential sources of risk are recognized. Next, risk analysis evaluates the likelihood and severity of those hazards, and risk assessment determines whether the identified risks are acceptable or require mitigation. Finally, risk control involves implementing measures to reduce or eliminate unacceptable risks. The effectiveness of this process is verified through FAA certification, which requires compliance with SMS standards. Once certified, airlines incorporate these thresholds into their daily operations, training programs, and safety protocols to promote consistent and proactive risk management.

How are they modified/updated?

Risk tolerance thresholds for individual organizations in the aviation industry are regularly reviewed and updated to remain aligned with evolving safety standards and operational realities. This process is informed by a combination of incident and accident data, such as reports from the National Transportation Safety Board (NTSB), as well as technological advancements, regulatory updates, and stakeholder feedback. Oversight bodies like the FAA's SMS committee, along with international organizations such as the ICAO, and EASA, periodically assess safety performance and make recommendations for updates to risk management practices. In parallel, airlines conduct internal audits and benchmarking exercises to refine their own risk thresholds, so that their safety protocols remain effective, responsive, and compliant with both domestic and international standards.

Other Applicable Considerations

- Aversion to Tail Risk Events – Based on the survey efforts and results, the industry demonstrates a clear preference for proactive management of catastrophic-type (e.g., tail risk) events. While this approach aligns with the broader risk management landscape, specific risk tolerance frameworks vary across countries and regions and are shaped by local regulatory requirements.
- Public perception - High-profile incidents and media coverage can influence both regulatory and organizational risk tolerance levels. The FAA was established in response

to early aviation safety concerns, and its current approach reflects decades of evolution in safety oversight.[16]

- Performance data – The aviation industry relies heavily on the use of performance data. According to NTSB data, the average likelihood of accidents per million flight hours decreased from 0.126 (2004–2008) to 0.033 (2019–2023), demonstrating the effectiveness of SMS-based approaches.[17]

References

- Civil Aviation Organization. (2013). *Safety management manual (SMM)* (Doc 9859, 3rd ed.). https://www.icao.int/sites/default/files/EURNAT/Documents/EUR%20and%20Nat%20Docs/EUR%20Documents/RASGEUR%20Reports/RASG%20EUR05_SOD_Appendices/RASG-EUR05_SoD-Appendix-A-SMM-provisional-table-of-content.pdf

- European Union Aviation Safety Agency. (n.d.). *Safety Risk Management*. Retrieved from https://www.easa.europa.eu/en/domains/safety-management/safety-risk-management

- Federal Aviation Administration. (2016). *Safety risk management guidance for system acquisitions*. FAA Order 8040.4B. https://www.faa.gov/documentLibrary/media/Order/FAA_Order_8040.4B.pdf

- Federal Aviation Administration. (2022). *Risk management handbook* (FAA-H-8083-2A). U.S. Department of Transportation. https://www.faa.gov/sites/faa.gov/files/2022-06/risk_management_handbook_2A.pdf

B. Chemical

Does the industry have a risk tolerance threshold?

Partially. The chemical industry incorporates risk tolerance thresholds as a foundational component of its safety and risk management systems. However, these thresholds are not standardized across the industry but are instead shaped by a combination of regulatory mandates, international standards, and company-specific policies. As such, these thresholds often vary by jurisdiction, company, and risk type, and are typically differentiated between

---

[16] The FAA provides its history on its website stating that it was borne out of a need to reduce the frequent crashes and fatalities in the early days the rise of flight in America. Federal Aviation Administration. (n.d.). *A brief history of the FAA*. U.S. Department of Transportation. https://www.faa.gov/about/history/brief_history

[17] The FAA supports its current approach of requiring license holders to have a certified SMS with data from the NTSB demonstrating the reduction in likelihood of a fatal airline incident along with the global trend of safer flights. From the 5-year period of 2004-2008, the average likelihood of accidents per million flight hours is reported as 0.126. The most recent 5-year period analyzed by the NTSB of 2019-2023 shows an average likelihood of accidents per million flight hours as 0.033. https://www.ntsb.gov/safety/data/Documents/AviationAccidentStatistics_2004-2023_20241217.xlsx

societal risk (*e.g.*, group exposure to catastrophic events) and individual risk (*e.g.*, worker or public exposure).

Is it set by the applicable regulatory body?

Partially. In some jurisdictions, regulatory agencies establish explicit quantitative risk tolerance criteria, while others provide general safety requirements without fixed thresholds. In the United States, agencies such as the Environmental Protection Agency (EPA) and the Occupational Safety and Health Administration (OSHA) require companies to conduct risk management planning and hazard assessments, but they do not mandate universal quantitative thresholds across all hazards. However, specialized agencies like the National Institute for Occupational Safety and Health (NIOSH) may define specific limits for certain risks, such as exposure to carcinogens. [18] In contrast, the United Kingdom's Health and Safety Executive (HSE) and several European Union member states require companies to demonstrate that risks fall below defined thresholds, such as an annual fatality risk to the public of 1 in 10,000 or 1 in 1,000,000.[19] These thresholds are continually evaluated to determine acceptable levels of both individual and societal risk. Additionally, the EU's Seveso III Directive mandates the establishment of tolerable risk criteria for major accident hazards.

If not, what is the internal process by which each company (within the industry) establishes a risk tolerance level?

In cases where regulators do not define explicit risk tolerance thresholds, chemical companies can establish their own risk tolerance levels. Commonly adopted approaches include the COSO Enterprise Risk Management (ERM) framework, Center for Chemical Process Safety (CCPS) guidelines, and ISO 31000, which provide principles for identifying, assessing, and managing risk. Companies also rely on Quantitative Risk Assessment (QRA) to estimate the likelihood and consequences of hazardous events, and apply tools such as risk matrices, frequency-number (F-N) curves, and the "As Low As Reasonably Practicable" (ALARP) principle to guide decision-making. A typical internal process begins with the adoption of a formal risk management framework, followed by QRA and hazard identification. Companies then set internal criteria for safety, environmental, and financial risks, which are overseen by a dedicated risk management committee. These criteria are documented in corporate risk policies and, in many cases, disclosed in annual reports to promote transparency and accountability.

How are they implemented?

Risk tolerance thresholds in the chemical industry are embedded within operational systems that support continuous monitoring and control of safety risks. These systems include Hazard Identification and Risk Assessment (HIRA), which systematically identifies potential hazards and

[18] AIHA, "The Safety Threshold," n.d.

[19] Dunjó et al., "An Overview of Worldwide Risk Tolerability Criteria for Chemical Process Industries," 2016, p. 18.

evaluates their likelihood and severity; Layer of Protection Analysis (LOPA), which assesses the effectiveness of existing safeguards and determines whether additional layers of protection are needed; and Process Safety Management (PSM), a regulatory framework for the safe design, operation, and maintenance of hazardous processes.

How are they modified/updated?

Risk tolerance thresholds in the chemical industry are not static. They are regularly updated to reflect new insights and changing conditions, which are driven by several key factors, including new scientific data and technological advancements. Additionally, incident investigations and the lessons learned from past events play a critical role in refining risk thresholds. Regulatory changes and public pressure also influence adjustments. Internally, companies conduct audits and performance reviews to assess the effectiveness of existing risk controls and identify areas for improvement.

Other Applicable Considerations

- Aversion to Tail Risk Events – Based on the survey efforts and results, the industry demonstrates a clear preference for proactive management of catastrophic-type (e.g. tail risk) events. While this approach aligns with the broader risk management landscape, specific risk tolerance frameworks vary across countries and regions and are shaped by local regulatory requirements.
- Public Perception - Public engagement and consultation influence risk tolerance standards. Involuntary risks (*e.g.*, public exposure) often lead to stricter thresholds than voluntary risks (*e.g.*, worker exposure).[20]
- Individual vs. Societal Risk - Companies and regulators distinguish between risks to individuals and risks to groups and generally implement higher risk thresholds for risk that may cause multiple casualties.
- Regulatory vs. Company-Driven Thresholds - Regulatory thresholds focus on public and environmental safety, while company-initiated risk thresholds reflect their individual risk appetites and operating environments.

References

- Center for Chemical Process Safety. (2009). *Guidelines for Developing Quantitative Safety Risk Criteria*. John Wiley & Sons. https://onlinelibrary.wiley.com/doi/pdf/10.1002/9780470552940.app3

- Chemical Institute of Canada. (2019). *Risk – How to measure it and evaluate it.* https://www.cheminst.ca/wp-content/uploads/2019/04/Public20Risk20How20to20Measure-1.pdf

[20] HSE, Reducing Risks, Protecting People, p. 12.

- Dunjó, J., Ph.D., Prophet, N., & Amorós, M. (2016, October 25). *An Overview of Worldwide Risk Tolerability Criteria for Chemical Process Industries.* The Oak Trust Digital Repository. Retrieved September 22, 2025, from https://oaktrust.library.tamu.edu/server/api/core/bitstreams/e74383ae-d8fc-4bab-9da0-845e52218353/content

- Korchevskiy, A. (2023, January). *The safety threshold: Understanding risk tolerances.* The Synergist. American Industrial Hygiene Association. https://publications.aiha.org/202301-safety-threshold

- ioMosaic. (2021). *Risk-Based Approach Risk Tolerability Criteria.* https://iomosaic.com/docs/default-source/papers/risk-based-approach-risk-tolerability-criteria.pdf

- Price, P. S. (2021). Application of Cost Effectiveness and Value of Information Analyses in Evaluating Toxicity Testing. U.S. EPA. https://www.epa.gov/system/files/documents/2021-11/session2_price.pdf

- Primatech Inc. (2012). *Understanding risk tolerance criteria.* https://www.primatech.com/images/docs/understanding-risk-tolerance-criteria.pdf

- PTT Global Chemical Public Company Limited. (2023). *Risk Appetite and Tolerance* Levels. https://sustainability.pttgcgroup.com/storage/document/risk-governance/risk-appetite-and-tolerance-levels-en.pdf

- U.K. Health and Safety Executive. (2022). *Reducing Risks, Protecting People (R2P2): HSE's Decision-Making Process.* https://www.cambridgesafety.co.uk/wp-content/uploads/2018/02/r2p2-reducing-risks-protecting-people.pdf

- Zhang, Y., Wang, Y., & Li, G. (2024). *A risk-based approach for the optimal scheduling of maintenance in power systems.* Engineering Applications of Artificial Intelligence, 130, 106983. https://www.sciencedirect.com/science/article/pii/S0950423024000329

C. Mining

Does the industry have a risk tolerance threshold?

Partially. The mining industry does utilize risk tolerance thresholds, but they are not standardized across the sector or across all mining related risks. These thresholds are typically defined at the company or project level, reflecting each operation's unique context, risk appetite, and stakeholder expectations. While some regulatory bodies set minimum safety and environmental standards, the specific definition of "tolerable risk" is usually determined internally by mining companies themselves that these meets or exceeds the applicable regulatory requirements.

Is it set by the applicable regulatory body?

Partially. Regulatory agencies such as the Mine Safety and Health Administration (MSHA) in the U.S. as well as international bodies like the International Council on Mining and Metals (ICMM) establish baseline standards for occupational safety, environmental protection, and emergency preparedness. These agencies require companies to manage risks to a level that is "As Low As Reasonably Practicable" (ALARP), but rarely prescribe a single, quantitative risk tolerance threshold for all mining related risks.

If not, what is the internal process by which each company (within the industry) establishes a risk tolerance level?

Mining companies establish their own risk tolerance thresholds through structured internal processes. These processes typically begin with the adoption of Enterprise Risk Management (ERM) frameworks, such as ISO 31000 or COSO ERM. Companies then conduct risk assessment workshops involving multidisciplinary teams that utilize tools like risk matrices, bow-tie analysis, and quantitative risk assessments (QRA) to evaluate potential hazards and their consequences. Based on these evaluations, internal risk criteria are set for various categories, including safety, environmental impact, and financial exposure, often distinguishing between risks to employees, contractors, the public, and the environment. Oversight and approval of these thresholds are typically managed by risk committees or senior leadership. Finally, the established criteria are documented in risk registers, internal policies, and sustainability reports, providing transparency and a basis for continuous improvement.

How are they implemented?

Risk tolerance thresholds in the mining industry are implemented through a combination of site-specific assessments, control measures, and monitoring systems. These include Hazard Identification and Risk Assessment (HIRA), which identifies and evaluates potential hazards; Job Safety Analysis (JSA), which breaks down tasks to assess risks associated with each step; and Failure Modes and Effects Analysis (FMEA), which systematically examines potential failure points and their consequences. To manage these risks, mining companies apply hierarchy of controls such as engineering solutions, administrative procedures, and the use of personal protective equipment (PPE). Ongoing monitoring and reporting are performed through audits, inspections, and incident tracking so that operations remain within defined risk tolerance thresholds. Additionally, companies rely on operational guidance from resources like the *Australian Risk Management Handbook for the Mining Industry*,[21] which provides best practices for identifying, assessing, and mitigating risks in mining environments.

How are they modified/updated?

Risk tolerance levels in the mining industry are regularly updated to reflect new insights, changing conditions, and evolving operational demands. These updates are driven by a variety of factors, including incident investigations and the lessons learned from past events, which help identify vulnerabilities and areas for improvement. Technological advancements also play a key role, introducing new tools and methods that can enhance safety and efficiency. Additionally, regulatory changes and stakeholder feedback from employees, communities, and oversight bodies inform adjustments so that risk thresholds remain relevant and responsive. Once proposed, updates to risk tolerance levels are reviewed and approved by risk committees or senior leadership and are then communicated throughout the organization via revised policies, training programs, and operational procedures.

Other Applicable Considerations

- Aversion to Tail Risk Events – Based on the survey efforts and results, the industry demonstrates a clear preference for proactive management of catastrophic-type (e.g. tail risk) events. While this approach aligns with the broader risk management landscape, specific risk tolerance frameworks vary across countries and regions and are shaped by local regulatory requirements.
- Public Perception - Community concerns about environmental impacts, Indigenous rights, and catastrophic events (*e.g.*, tailings dam failures) can influence risk tolerance. Companies must maintain a social license to operate through transparent communication and stakeholder engagement.
- Individual vs. Societal Risk - Mining frameworks distinguish between individual risk (*e.g.*, workers or residents) and societal risk (*e.g.*, events causing multiple fatalities or environmental harm). Societal risk thresholds are generally more stringent, especially for involuntary harms, such as contamination.
- Regulatory vs. Company-Driven Thresholds - Regulatory thresholds define minimum standards, while company-driven thresholds reflect internal risk appetite and may be more conservative. Companies use both qualitative and quantitative methods to define and manage these thresholds.

---

[21] Australian Department of Mineral Resources. (1997). *Risk management handbook for the mining industry: How to conduct a risk assessment of mine operations and equipment and how to manage the risks* (MDG 1010). Mineral Resources. https://nswdpe.intersearch.com.au/nswdpejspui/handle/1/2075

References

- Australian Government Department of Industry, Innovation and Science. (2016). *Risk management: Leading practice sustainable development program for the mining industry.* https://www.industry.gov.au/sites/default/files/2019-04/lpsdp-risk-management-handbook-english.pdf

- Department of Mineral Resources. (1997). *Risk management handbook for the mining industry: How to conduct a risk assessment of mine operations and equipment and how to manage the risks (MDG 1010).* Mineral Resources. https://nswdpe.intersearch.com.au/nswdpejspui/handle/1/2075

- Marsh. (2016). *Mining risk reporting: Emerging trends in an evolving risk landscape* [PDF]. https://www.marsh.com/content/dam/marsh/Documents/PDF/UK-en/Mining%20Risk%20Report%20Emerging%20Trends%20in%20an%20Evolving%20Risk%20Landscape.pdf

- National Mining Association. (2016). *CORE Safety handbook.* https://nma.org/wp-content/uploads/2016/09/CORESafety-Handbook.pdf

- Oboni, C., & Oboni, F. (2021, June). *Tolerable risk thresholds.* SRK Consulting. https://www.srk.com/en/publications/tolerable-risk-thresholds-oboni

- United Nations Mine Action Service. (2019). *IMAS 07.14: Risk management in mine action.* https://www.mineactionstandards.org/standards/07-14/

D. Oil and Gas

Does the industry have a risk tolerance threshold?

Partially. The global oil and gas industry, inclusive of pipeline operators, considers risk tolerance and, in some cases, operates within defined risk tolerance thresholds. However, these thresholds are not standardized across the industry. They vary by jurisdiction and are typically established either externally, through regulatory frameworks, or internally, by company leadership. In some regions, such as the UK and parts of Europe, regulators define explicit, quantitative risk tolerability criteria (*e.g.*, individual or societal risk limits). In other jurisdictions, including the U.S., regulators generally set minimum safety and environmental standards rather than formal risk thresholds, leaving companies to adopt their own criteria. Where thresholds exist, they may be quantitative or qualitative/semi-quantitative (*e.g.*, risk matrices). A 2016 PHMSA study found that nearly half of surveyed pipeline operators had internally defined unacceptable or intolerable risk levels.[22]

Is it set by the applicable regulatory body?

No. U.S. regulatory agencies such as PHMSA, OSHA, EPA, and BSEE establish minimum safety and environmental standards for the oil and gas industry rather than explicit risk tolerance thresholds. These standards are typically prescriptive or performance-based and informed by incident data, stakeholder input, and technical reviews. Companies typically implement them through safety cases, operational protocols, and emergency response plans. While agencies periodically update regulations to reflect technological and societal changes, formal quantitative risk tolerability criteria (*e.g.*, individual or societal risk thresholds) are generally not mandated in U.S. regulations; such thresholds are more common in international frameworks. However, individual companies do pay particular attention to certain failure modes, such as blowouts or pipeline ruptures.

In other jurisdictions:

- UK Health and Safety Executive (HSE) – Defines IR/SR criteria and ALARP zones.[23]
- Netherlands – Employ F-N curves and differentiates IR for vulnerable vs. less vulnerable populations.[24]
- Canada (CSA Z662:23 Annex B)[25] – Formalizes IR/SR criteria and QRA requirements.

---

[22] Kiefner, J. F. (2016). *Study on Risk Tolerance*. PHMSA. https://primis.phmsa.dot.gov/rd/FileGet/10733/0339-1501_Final_Report_Paper_Study_on_Risk_Tolerance.pdf

[23] Health and Safety Executive. (2001). *Reducing risks, protecting people: HSE's decision-making process*. https://webarchive.nationalarchives.gov.uk/ukgwa/20230703113731/https://www.hse.gov.uk/enforce/expert/r2p2.htm

[24] Ministry of Infrastructure and Water Management (Netherlands). *Risk assessment guidelines for hazardous installations*.

[25] CSA Group. (2023). CSA Z662:23 – Oil and gas pipeline systems. https://www.csagroup.org/store/product/2430394/

- Ireland (CRU): Mandates quantified IR/SR in safety cases aligned with ALARP.[26]
- China (GB 36894-2018, GB/T 37243-2019)[27] – Defines IR/SR thresholds and safety distances for hazardous facilities.

If not, what is the internal process by which each company (within the industry) establishes a risk tolerance level?

Individual companies within the oil and gas industry establish their own internal risk tolerance thresholds through structured processes that combine technical analysis and organizational oversight. These processes typically involve multidisciplinary risk committees that guide the development and approval of risk criteria. Companies use tools such as Frequency-Number (F-N) curves, Quantitative Risk Analysis (QRA), risk matrices, and scenario analysis to evaluate potential hazards and determine acceptable levels of risk. Once established, these thresholds are not static. They are regularly updated based on incident investigations, regulatory changes, technological advancements, and stakeholder feedback. Updates are typically reviewed and approved by senior leadership and are communicated throughout the organization via revised procedures, training programs, and operational protocols to promote consistent application and alignment with evolving safety and performance expectations.

How are they implemented?

Implementation of risk tolerance thresholds in the oil and gas industry occurs through structured risk management frameworks that translate tolerability criteria into operational decisions. Companies first define acceptable and unacceptable risk levels, often using qualitative matrices or quantitative criteria, and then integrate these into processes such as Hazard Identification and Risk Assessment (HIRA), and Layer of Protection Analysis (LOPA). These tools enable evaluation of identified hazards against defined thresholds and so that additional safeguards can be added when risk exceeds tolerable limits. Safety Integrity Levels (SILs) further operationalize thresholds by specifying reliability requirements for safety systems based on risk severity and likelihood. Supporting systems such as permit-to-work systems, Job Safety Analysis (JSA), and Management of Change (MOC) help maintain compliance with these thresholds during day-to-day operations and changes. Together, these mechanisms promote consistent application and maintenance of risk tolerance thresholds across operations.[28]

---

[26] Commission for Regulation of Utilities. (2022). *Gas safety framework*. https://www.cru.ie/regulations-policy/safety/gas-safety-framework/

[27] China National Standardization Administration. (2018). GB 36894-2018: *Risk criteria for hazardous chemicals production unit and storage installations*. https://www.codeofchina.com/standard/GB36894-2018.htm ; China National Standardization Administration. (2019). *GB/T 37243-2019: Determination method of external safety distance for hazardous chemicals production units and storage installations*. https://openstd.samr.gov.cn/bzgk/std/newGbInfo?hcno=562DEE9A4FEB5EF7CE2DEF8A0345AE00

[28] Olsen, J. E. (2021). *Hazard Identification and Risk Assessment for Smaller Changes: Tips and Tools for Avoiding Misses and Improving Quality*. Institution of Chemical Engineers. Retrieved from https://www.icheme.org/media/27734/hazards-31-paper-38-olsen.pdf

How are they modified/updated?

Changes to risk tolerance thresholds are typically reviewed and approved by executive leadership and then communicated throughout the organization via updated procedures, training programs, and operational protocols. Through this process, personnel are informed of the revised standards to drive consistent implementation across departments and functions.

Other Applicable Considerations

- Aversion to Tail Risk Events – Based on the survey efforts and results, the industry demonstrates a clear preference for proactive management of catastrophic-type (e.g. tail risk) events. While this approach aligns with the broader risk management landscape, specific risk tolerance frameworks vary across countries and regions and are shaped by local regulatory requirements.
- Public Perception – Public perception, particularly as in relation to zoning and land-use planning, plays a critical role in shaping acceptable levels of risk (*e.g.*, Keystone Pipeline)
- Risk Aversion - Societal risk criteria often reflect public attitudes toward the oil and gas industry and are often reflected within these risk tolerance thresholds.

References

- American Petroleum Institute. (2021). *API recommended practice 754: Process safety performance indicators for the refining and petrochemical industries (3rd ed.).* https://www.api.org/-/media/files/oil-and-natural-gas/refining/process%20safety/rp-754-fact-sheet.pdf

- Center for Offshore Safety. (2017). *Risk management and safety culture in offshore oil and gas operations.* https://www.bsee.gov/sites/bsee.gov/files/research-reports/5009aa.pdf

- Commission for Regulation of Utilities. (n.d.). *Petroleum safety framework.* https://www.cru.ie/regulations-policy/safety/gas-safety-framework/

- CSA Group. (2023). *CSA Z662: Oil and gas pipeline systems – Annex B*. https://www.csagroup.org/store/product/2430394/

- GB 36894-2018. (2018). *Safety regulations for hazardous chemical production units and storage facilities.* China National Standardization Administration. https://www.codeofchina.com/standard/GB36894-2018.html

- Health and Safety Executive. (2022.) *Risk criteria and ALARP guidance.* United Kingdom. https://www.hse.gov.uk/offshore/index.htm

- Kiefner, J. F. (2016). *Study on Risk Tolerance*. PHMSA. https://primis.phmsa.dot.gov/rd/FileGet/10733/0339-1501_Final_Report_Paper_Study_on_Risk_Tolerance.pdf

- Tomic, B., & Kariyawasam, S. (2016). *Application of individual and societal risk criteria in pipeline risk assessments.* International Pipeline Conference, IPC2016-64356

E. Nuclear

Does the industry have a risk tolerance threshold?

Yes. The nuclear industry has clearly defined risk tolerance thresholds. These are established by national and international regulatory bodies and are primarily reflective of tolerances related to public exposure to radiological harm.[29] For instance, the U.S. Nuclear Regulatory Commission (NRC) explicitly states in 10 CFR 50 that while no death from nuclear power plant operation is considered "acceptable," certain risk levels are deemed acceptable.[30] These thresholds are operationalized through standards such as Regulatory Guide 1.174, which defines acceptable limits for Core Damage Frequency (CDF) and Large Early Release Frequency (LERF).

The U.S. Nuclear Regulatory Commission's risk tolerance is defined by its 1986 "Policy Statement on Safety Goals for the Operation of Nuclear Power Plants," which includes two qualitative safety goals supported by two quantitative objectives.[31]

The qualitative safety goals are:

1. Individual Risk: No significant added risk to life and health for the public from nuclear power plant operations.
2. Societal Risk: Societal risks should be comparable to or less than those from competing electricity generation technologies.

The quantitative objectives are numerical targets:

- Prompt Fatalities: Risk to an average individual near a plant should not exceed 0.1% of the risk from other accidents to which the U.S. population is exposed.
- Cancer Fatalities: Risk to the population near a plant from operations should not exceed 0.1% of the risk from all other causes.

Is it set by the applicable regulatory body?

Yes. In the U.S., the NRC sets baseline risk tolerances, while in other countries, the International Atomic Energy Agency (IAEA) provides guidance and standards. Because nuclear operations involve the potential for widespread and long-lasting harm, the NRC mandates risk tolerance thresholds through a combination of technical and regulatory methodologies designed so that

[29] The U.S. Nuclear Safety Policy was established in response to "recommendations of the President's Commission on the Accident at Three Mile Island, the [NRC] stated that it was 'prepared to move forward with an explicit policy statement on safety philosophy and the role of safety-cost tradeoffs in the NRC safety decisions." U.S. Nuclear Regulatory Commission. (2016). *Three Mile Island accident of 1979: Knowledge management digest* (NUREG/KM-0001, Rev. 1). Office of Nuclear Regulatory Research. https://www.nrc.gov/reading-rm/doc-collections/nuregs/knowledge/km0001/r1/index

[30] 10 CFR Part 50. The prompt fatality risk to an average individual near a nuclear plant must not exceed 0.1% of the risk from other accidents; The cancer fatality risk from plant operation must also not exceed 0.1% of the risk from all other causes.

[31] 10 CFR Part 50, Safety Goals for the Operations of Nuclear Power Plants; Policy Statements; Republication (1986) https://www.nrc.gov/reading-rm/doc-collections/commission/policy/51fr30028.pdf

even low-probability events (i.e., tail risks) are rigorously controlled. A foundational approach is the use of defense-in-depth strategies, which layer multiple safety barriers to prevent and mitigate accidents. These strategies are supported by Probabilistic Risk Assessment (PRA), a quantitative method that evaluates the likelihood and consequences of potential nuclear events. Additionally, radiological dose limits are set for both workers and the public so that exposure remains within acceptable bounds. Risk modeling also includes the analysis of Design Basis Accidents (DBAs) and Beyond Design Basis Events (BDBEs) to account for both expected and extreme scenarios. To integrate safety and security considerations, the Potential Facility Risk Index (PFRI) is used, leveraging PRA techniques to guide decision-making and prioritize risk mitigation efforts across nuclear facilities.

If not, what is the internal process by which each company (within the industry) establishes a risk tolerance level?

Although regulators set the baseline for risk tolerance in the nuclear industry, individual nuclear operators often establish internal thresholds that exceed these regulatory requirements. To do so, they rely on structured processes that incorporate input from multidisciplinary safety committees, which oversee the development and approval of risk criteria. Operators use risk-informed tools such as risk monitors, maintenance rule compliance, and configuration risk management to evaluate and manage operational risks. These thresholds are integrated directly into reactor design, operational limits, and emergency planning zones, so that safety considerations are embedded throughout the facility's lifecycle. The safety margins are formally documented in Safety Analysis Reports (SARs) and technical specifications, providing a clear and traceable framework for decision-making and regulatory compliance.

How are they implemented?

Risk tolerance thresholds in the nuclear industry are implemented through a suite of technical tools and operational systems that provide safety is maintained across all phases of plant operation. These tools include risk monitors, which track real-time safety metrics; maintenance rule compliance, so that equipment and systems meet regulatory and performance standards; and configuration risk management, which evaluates the safety implications of changes to plant systems or operations. Risk tolerances are embedded directly into design specifications, operational procedures, and safety systems, as well as emergency response protocols, so that safety is proactively managed. To support risk evaluation and mitigation, nuclear operators analyze both Design Basis Accidents (DBAs) anticipated events accounted for in the plant's design and Beyond Design Basis Events (BDBEs), which represent more extreme or unexpected scenarios. The outcomes of these analyses are documented in Safety Analysis Reports (SARs) and technical specifications, which define the plant's operating limits and serve as a foundation for regulatory compliance and internal decision-making.

How are they modified/updated?

Risk thresholds in the nuclear industry are subject to ongoing oversight and refinement through a combination of internal and external review processes. Internally, safety committees, audits, and performance reviews are used to evaluate the effectiveness of current risk tolerance levels and identify areas for improvement. When changes to these thresholds are proposed, they undergo regulatory review, are evaluated by independent safety boards, and are often subject to public consultation to provide transparency and alignment with societal expectations. This multi-layered approach helps maintain the integrity of safety standards while allowing for continuous improvement in response to evolving risks and operational conditions.

Other Applicable Considerations

- Aversion to Tail Risk Events – Based on the survey efforts and results, the industry demonstrates a very clear and defined preference for proactive management of catastrophic-type (e.g. tail risk) events. While this approach aligns with the broader risk management landscape, specific risk tolerance frameworks vary across countries and regions and are shaped by local regulatory requirements.
- Public Perception – Risk tolerance thresholds regarding the nuclear industry are highly sensitive to public opinion, especially following major incidents (e.g., Fukushima, Chernobyl).
- Scientific Rigor – Thresholds in the nuclear industry are based on extensive modeling, historical data, as well as peer-reviewed research.
- Regulatory Oversight – Changes to risk tolerance require sometimes several rounds of formal review by regulators, and independent safety boards, followed by public consultation.

References

- Institute of Nuclear Power Operations. (2013). *Principles for excellence in nuclear safety risk management*. https://www.nrc.gov/docs/ML0534/ML053410342.pdf

- U.S. Nuclear Regulatory Commission. (2016). *Risk-informed decision-making for nuclear power plants*. NUREG-2150. https://www.nrc.gov/about-nrc/regulatory/risk-informed/rpp

F. Autonomous Vehicles

Does the industry have a risk tolerance threshold?

Partially, but there is no single, universally fixed threshold. Risk tolerance for autonomous vehicles (AVs) is shaped by both federal (*e.g.*, National Highway Transportation Safety Administration (NHTSA)) and individual state departments of transportation (DOTs), as well as internal company processes. These risk tolerances are typically expressed in terms of acceptable failure rates, response times, and decision accuracy under various driving scenarios. These are generally informed by simulation data, real-world testing, as well as the validation of machine learning models.

Is it set by the applicable regulatory body?

Partially. Regulators, such as the NHTSA, set minimum safety standards, as well as acceptable failure rates for automation-related technologies, such as Intelligent Speed Assistance (ISA). In addition to federal oversight, state-level Departments of Transportation (DOTs) may impose additional requirements that reflect regional priorities or local perceptions of risk. While NHTSA and state DOTs establish baseline safety expectations, they do not prescribe universal quantitative thresholds for all autonomous vehicle technologies. Instead, regulatory thresholds are typically informed by accident data, disengagement reports, and public consultation, which are all used to inform evolving standards for safety and performance. Safety (e.g., collision risk), reliability (*e.g.*, sensor failure), and public trust are the primary metrics used to inform evolving standards such as ISO 26262 and NHTSA guidelines.

If not, what is the internal process by which each company (within the industry) establishes a risk tolerance level?

Companies such as Tesla, Waymo, and Cruise establish internal risk tolerance thresholds based on system performance metrics and stakeholder expectations. To demonstrate compliance with these thresholds, they develop detailed safety cases that are submitted to regulators, outlining how their autonomous vehicle systems meet or exceed defined safety benchmarks. These benchmarks often include Operational Design Domain (ODD) thresholds, which specify the environmental and operational conditions, such as weather, road type, and traffic scenarios, under which the vehicle can safely operate. Risk tolerance is further quantified using both qualitative and quantitative metrics, including acceptable failure rates, decision accuracy, and response times tailored to specific use cases, such as urban versus highway driving.

How are they implemented?

Risk tolerance thresholds for autonomous vehicles are implemented through a combination of structured safety documentation and real-time operational oversight. Safety cases, which detail how a vehicle's systems meet or exceed defined safety benchmarks, are submitted to regulators as part of the assurance process. These are complemented by Operational Design Domain

(ODD) definitions, which specify the exact conditions, such as road types, weather, and traffic environments, under which the vehicle can safely operate. For ongoing compliance with these thresholds, manufacturers employ continuous monitoring systems that rely on real-time data collection and analysis, allowing them to track performance, detect anomalies, and make timely adjustments to maintain safe operation within acceptable risk bounds.

How are they modified/updated?

Risk tolerance thresholds in the autonomous vehicle industry are regularly reviewed and updated so that they remain aligned with technological progress and evolving safety expectations. Regulatory bodies periodically revise standards based on technological advancements, incident data, and stakeholder feedback, so that safety benchmarks reflect current capabilities and public concerns. Similarly, manufacturers update their internal risk thresholds through incident investigations, regulatory reviews, and the integration of new technologies, allowing for continuous improvement in system performance and risk mitigation strategies.

Other Applicable Considerations

- <u>Aversion to Tail Risk Events</u> – Based on the survey efforts and results, the industry demonstrates a clear preference for proactive management of catastrophic-type (e.g. tail risk) events. While this approach aligns with the broader risk management landscape, specific risk tolerance frameworks vary across countries and regions and are shaped by local regulatory requirements.
- <u>Evolution of Safety Standards</u> - New methods such as adaptive stress testing, reinforcement learning, and scenario-based simulation are used to identify rare but critical failure modes within the autonomous vehicle industry.
- <u>Individual vs. Societal Risk</u> - Frameworks are being developed to distinguish between risks threshold for individual users versus risks to the general public (*e.g.*, multi-fatality events). Societal risk tolerance thresholds are generally more stringent due to the involuntary nature of public exposure.

References

- Beedham, M. (2025, January 6). *Risk tolerance and ADAS regulation: EU and USA.* TomTom Newsroom. https://www.tomtom.com/newsroom/explainers-and-insights/risk-tolerance-and-adas-regulation-eu-and-usa/

- Blumenthal, M. S., Fraade-Blanar, L., Best, R., & Irwin, J. L. (2020). *Safe Enough: Approaches to Assessing Acceptable Safety for Automated Vehicles*. RAND Corporation. https://www.rand.org/pubs/research_reports/RRA569-1.html

- Koopman, P., Ferrell, U., Fratrik, F., & Wagner, M. (2019). *A safety standard approach for fully autonomous vehicles.* WAISE 2019 Preprint. Edge Case Research and The MITRE Corporation. https://users.ece.cmu.edu/~koopman/pubs/Koopman19_WAISE_UL4600.pdf

- Moss, R. J., Gupta, S., Dyro, R., Leung, K., Kochenderfer, M. J., Gao, G. X., Pavone, M., Schmerling, E., & Corso, A. (2021). *Autonomous Vehicle Risk Assessment.* Stanford University. https://web.stanford.edu/~mossr/pdf/Autonomous_Vehicle_Risk_Assessment.pdf

- National Highway Traffic Safety Administration. (2020). *Automated driving systems 2.0: A vision for safety*. https://www.nhtsa.gov/sites/nhtsa.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf

- ROHM Semiconductor. (n.d.). *ISO 26262 functional safety standard for automotive electronic systems [White paper].* https://fscdn.rohm.com/en/products/databook/white_paper/iso26262_wp-e.pdf

G. Spaceflight

Does the industry have a risk tolerance threshold?

Yes. The spaceflight industry operates with well-defined risk tolerance thresholds, particularly due to the high-stakes nature of its operations. These thresholds are shaped by both regulatory agencies (e.g., NASA, FAA, ESA)[32] as well as individual spaceflight operators (e.g., SpaceX, Boeing, Blue Origin). Risk tolerances vary by mission type, especially between manned and unmanned missions, and are expressed through metrics such as damage probability, loss of crew probability, and mission assurance criteria.

Is it set by the applicable regulatory body?

Partially. Regulatory standards for spaceflight risk tolerance are partially defined by agencies such as NASA, the European Space Agency (ESA), and the FAA Office of Commercial Space Transportation. These organizations establish baseline thresholds based on mission objectives and public safety imperatives, particularly distinguishing between manned and unmanned missions. To operationalize these thresholds, spaceflight entities apply structured methodologies including Risk-Informed Decision Making (RIDM), Probabilistic Risk Assessment (PRA), and Safety and Mission Assurance (SMA). These frameworks are embedded into launch protocols, system design specifications, and operational procedures for consistent application across mission types. NASA's *Risk Informed Decision-Making Handbook* (NASA/SP-2011-3422)[33] provides detailed guidance on how risk tolerances are defined based on mission-critical failure thresholds and applied across mission alternatives, enabling comparative assessments on a risk-normalized basis. In spaceflight, tail risk encompasses launch failures, re-entry accidents, and loss of crew or mission. These are modeled using worst-case scenario planning and probabilistic mission assurance frameworks. Safety (crew survival – manned missions), mission reliability (launch failure), as well as financial losses (unmanned missions) are key metrics.

If not, what is the internal process by which each company (within the industry) establishes a risk tolerance level?

While agencies such as NASA, ESA, and the FAA define baseline safety expectations, private spaceflight operators, such as SpaceX, Boeing, and Virgin Galactic, have the discretion to set more stringent internal thresholds tailored to their specific mission profiles. These companies develop mission-specific risk tolerances through internal risk assessments, the development of safety cases, and ongoing review processes. The thresholds they establish are aligned with internal performance goals and are implemented through Safety and Mission Assurance (SMA)

---

[32] National Aeronautics and Space Administration (NASA), the Federal Aviation Administration (FAA) Office of Commercial Space Transportation, and the European Space Agency (ESA).

[33] Dezfuli, H., Stamatelatos, M., Maggio, G., Everett, C., & Youngblood, R. (2010). *NASA Risk-Informed Decision-Making Handbook* [NASA/SP-2010-576]. NASA Office of Safety and Mission Assurance. https://ntrs.nasa.gov/api/citations/20100021361/downloads/20100021361.pdf

protocols, launch procedures, and engineering design standards, so that safety is embedded throughout the mission lifecycle.

How are they implemented?

Risk tolerance thresholds are implemented through a combination of design standards, launch procedures, and mission assurance protocols. These elements work together so that safety expectations are embedded throughout the lifecycle of a mission. By incorporating risk thresholds into the engineering design, operational planning, and procedural safeguards, spaceflight operators maintain alignment with both internal performance goals and regulatory requirements, helping to mitigate risks and for mission success.

How are they modified/updated?

Risk tolerance thresholds in the spaceflight industry are not static; they are continuously refined to reflect evolving conditions and insights. Updates are driven by technological advancements, which introduce new capabilities and safety measures, as well as regulatory updates that adjust compliance expectations. Additionally, operational experience, including lessons learned from past missions, plays a critical role in shaping and improving risk thresholds over time. This dynamic approach provide that safety standards remain relevant and responsive to the complexities of modern spaceflight.

Other Applicable Considerations

- Assumption of Risk – Given the emphasis on innovation in the industry, there is a material assumption of risk that drives individual entities.[34]
- Jurisdictional Dependence – Within an overall construct of assumption of risk, specific risk tolerance frameworks for the spaceflight industry vary across national boundaries. They are influenced by local regulatory agencies, as well as geopolitical priorities.
- Public Perception – Public sentiment, especially regarding manned missions, the environmental impacts of spacecraft launch and decommissioning, as well as national prestige, can significantly influence both regulatory and organizational risk tolerance decisions.
- Dynamic Nature of Risk – Risk tolerance is not static within the spaceflight industry. It has evolved with technological capabilities, mission complexity, as well as societal and stakeholder expectations for private and public spaceflight.
- High Visibility and Consequence – Due to the catastrophic potential of failure, risk tolerance-related decision making is at the forefront of the spaceflight industry.

---

[34] For example, in 1962, President John F. Kennedy stated: "We choose to go to the Moon ... in this decade and do the other things not because they are easy, but because they are hard. ... And therefore, as we set sail, we ask God's blessing on the most hazardous and dangerous and greatest adventure that man has ever gone." As another example, in 1986, following the catastrophic event of the space shuttle Challenger loss, President Ronald Reagan stated: "The future doesn't belong to the fainthearted; it belongs to the brave... The crew of the space shuttle Challenger honored us by the manner in which they lived their lives."

References

- Dezfuli, H., Guarro, S., Everett, C., Benjamin, A., & Skow, M. C. (2024). *NASA risk management handbook* (Version 2.0) [NASA/SP-20240014019]. National Aeronautics and Space Administration. https://ntrs.nasa.gov/api/citations/20240014019/downloads/SP-20240014019.pdf

- Federal Aviation Administration. (2015). *Commercial space transportation safety management system manual* (Version 2.0). FAA Office of Commercial Space Transportation. https://www.faa.gov/sites/faa.gov/files/about/initiatives/sms/reference_library/AST_SMS_Manual_V2.0.pdf

- Go, S., Mathias, D., Mattenberger, C., Lawrence, S., & Gee, K. (2019). An Integrated Reliability and Physics-Based Risk Modeling Approach for Human Spaceflight Systems. NASA Technical Reports Server. https://ntrs.nasa.gov/api/citations/20190001060/downloads/20190001060.pdf

- Langston, S. M. (2016). *Space travel: Risk, ethics, and governance in commercial human spaceflight*. *New Space, 4*(2), 83–97. https://doi.org/10.1089/space.2015.0015

- Ligor, D. C., Miller, B. M., McCollester, M., Phillips, B., Kirkwood, G., Becker, J., Mazzotta, G., McClintock, B., & Bicksler, B. (2023). *Assessing the readiness for human commercial spaceflight safety regulations: Charting a trajectory from revolutionary to routine travel*. RAND Corporation. https://www.rand.org/pubs/research_reports/RRA2466-1.html

- NASA. (2011). *Probabilistic risk assessment procedures guide for NASA managers and practitioners* (2nd ed.) [NASA/SP-2011-3421]. NASA Office of Safety and Mission Assurance. https://ntrs.nasa.gov/api/citations/20120001369/downloads/20120001369.pdf

- NASA. (2011). *NASA risk management handbook* [NASA/SP-2011-3422]. NASA Office of Safety and Mission Assurance. https://ntrs.nasa.gov/api/citations/20120000033/downloads/20120000033.pdf

- NASA. (2021). *Modernizing NASA's space flight safety and mission success assurance framework*. NASA Office of Safety and Mission Assurance. https://ntrs.nasa.gov/api/citations/20220003490/downloads/SMS%20Assurance%20Framework%20White%20Paper%20STI.pdf

H. Electric Industry

The electric industry operates within a complex and interdependent infrastructure environment, where reliability, safety, and affordability are paramount. The systemic nature of electric grid operations means that even localized disruptions have the potential to cause widespread outages and other cascading impacts. Accordingly, the establishment and management of risk tolerance thresholds in this sector are governed by a layered framework that reflects both regulatory mandates and organizational discretion and shaped by the diverse roles of these entities across the electric sector.

In order to adequately address each of these unique entities, the Joint IOUs have addressed each of the entities separately, including:

- Independent System Operators and Regional Transmission Operators
- Investor-Owned Utilities
- Public Utilities, including Municipal Utilities and Electric Cooperatives

a. Independent System Operators (ISOs) and Regional Transmission Organizations (RTOs)

Does the industry have a risk tolerance threshold?

Yes. ISOs and RTOs operate under a layered risk tolerance framework that reflects both regulatory mandates and internal governance. These thresholds are essential for maintaining grid reliability, market integrity, and operational security across large geographic regions.

Is it set by the applicable regulatory body?

Partially. Baseline risk tolerance thresholds are primarily established by federal regulatory authorities, including the Federal Energy Regulatory Commission (FERC),[35] the North American Electric Reliability Corporation (NERC),[36] as well as regional reliability councils (e.g., Western Electricity Coordinating Council). These agencies define minimum standards for system reliability, cybersecurity, and market operations. Thresholds are developed through formal rulemaking, stakeholder consultation, and analysis of system performance data. They are periodically reviewed and updated to reflect technological advancements, incident experience, and evolving policy objectives such as decarbonization and resilience. Utilities actively assess and manage tail risk events, particularly those impacting system reliability, such as grid failures, cyberattacks, and extreme weather through scenario analysis, and tracked through reliability

---

[35] Federal Energy Regulatory Commission. (2023). *Reliability Primer*. https://www.ferc.gov/sites/default/files/2023-03/reliability-primer.pdf; Electronic Code of Federal Regulations. (2025). *18 CFR Part 40 – Mandatory Reliability Standards for the Bulk-Power System*. https://www.ecfr.gov/current/title-18/chapter-I/subchapter-B/part-40

[36] North American Electric Reliability Corporation. (2023). *Risk-Based Compliance Monitoring and Enforcement Program*. https://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/RAIProgramOverview.pdf

metrics (e.g. System Average Interruption Duration (SAID) and System Average Frequency Index (SAIFI)).

If not, what is the internal process by which each company (within the industry) establishes a risk tolerance level?

ISOs and RTOs build upon federal regulatory standards by developing internal risk management frameworks tailored to their regional context and strategic priorities. These frameworks define risk tolerance across multiple dimensions, including grid reliability, financial exposure, market operations, and system security. Governance is overseen by executive leadership, risk committees, and boards of directors, who establish formal risk appetite statements, monitor key risk indicators, and adjust thresholds in response to changing conditions. The process includes regular risk assessments, scenario analysis, and performance monitoring for alignment with regulatory expectations and stakeholder needs.

How are they implemented?

Risk tolerance thresholds are embedded into operational protocols and decision-making systems. ISOs and RTOs incorporate these thresholds into daily operations through structured procedures, system controls, and monitoring tools. Internal audits and compliance reviews help ensure that risk management practices are consistently applied and effective.

How are they modified/updated?

Risk tolerance thresholds are refined based on input from internal audits, external regulatory reviews, and changes in market conditions such as fuel price volatility, resource adequacy concerns (due to DER integration), as well as emerging cyber threats. These updates are reviewed by governance bodies and implemented through revised operational protocols to maintain system resilience and reliability.

Other Applicable Considerations

- <u>Aversion to Tail Risk Events</u> – Based on the survey efforts and results, the industry demonstrates a clear preference for proactive management of catastrophic-type (e.g. tail risk) events. The survey efforts and results did not uncover a single public utilities commission that dictated a risk-neutral approach to such catastrophic-type (e.g. tail risk events). The general approach aligns with the broader risk management landscape, while specific risk tolerance frameworks may vary across countries and regions and are shaped by local regulatory requirements.
- <u>Integration of distributed energy resources (DERs)</u> **–** Increasing DER penetration has required ISO/RTOs to dynamically adjust their risk thresholds, particularly as it relates to reliability risk.
- <u>Cybersecurity threats</u> – Growing digitalization of grid operations necessitates continuous updates to risk management strategies for cybersecurity threats.

- Stakeholder engagement – Transparent communication with market participants and regulators is essential for maintaining trust and compliance.
- Climate-related risks – Extreme weather events and long-term climate shifts are influencing reliability planning and have required recalibration of risk tolerance levels.

b. Investor-Owned Utilities (IOUs)

Does the industry have a risk tolerance threshold?

Partially. IOUs operate under a layered risk tolerance framework that integrates regulatory mandates with internal Enterprise Risk Management (ERM) practices. These thresholds are essential for managing risks related to grid reliability, operational safety, financial exposure, as well as customer and shareholder expectations across often large and complex utility systems.

Is it set by the applicable regulatory body?

Partially. Baseline risk tolerance thresholds are implicitly or explicitly established by federal and state regulatory authorities, including the Federal Energy Regulatory Commission (FERC), the North American Electric Reliability Corporation (NERC), as well as individual state Public Utility Commissions (PUCs). These agencies define minimum standards for reliability, environmental compliance, financial transparency, and safety. Risk thresholds are developed through formal regulatory proceedings, industry benchmarking, and analysis of system performance data. Regulators also consult with stakeholders, including industry experts, consumer advocates, and public interest groups, so that thresholds reflect both technical feasibility and societal expectations. These standards are periodically updated to address emerging risks such as cybersecurity threats, climate change, as well as evolving regulatory objectives.

If not, what is the internal process by which each company (within the industry) establishes a risk tolerance level?

Investor-Owned Utilities (IOUs) build upon regulatory requirements by developing internal risk tolerance guidance through comprehensive Enterprise Risk Management (ERM) frameworks. These frameworks define acceptable levels of risk across key domains, such as grid reliability, financial exposure, operational safety, and customer satisfaction, and are tailored to each utility's business model, strategic objectives, and regional operating environment. The process typically involves oversight by executive leadership, risk committees, and boards of directors, who guide the development of formal risk appetite statements. Investor-owned utilities also employ scenario analysis, performance monitoring, and stress testing to evaluate potential exposures. Additionally, stakeholder feedback and lessons learned from operational experience are integrated into the process to refine risk criteria. This structured approach provides that internal risk tolerances are aligned with both shareholder expectations and regulatory obligations, supporting informed decision-making and long-term resilience.

How are they implemented?

Risk tolerance principles are embedded into the operational systems and decision-making processes of individual IOUs to promote consistent and proactive risk management within the IOU and maintain safe and reliable service. These principles guide key activities such as investment planning and prioritization, where capital is allocated based on risk exposure and mitigation needs; maintenance and asset management programs, which promote infrastructure reliability and safety; emergency response protocols, which are designed to address high-impact events within regulatorily established safety and reliability performance limits. The implementation of these principles is supported by internal controls, staff training, and compliance monitoring, all of which help provide that risk management practices are consistently applied across departments and aligned with organizational objectives.

How are they modified/updated?

Risk tolerance principles employed by IOUs are not static. They are continuously refined to reflect changing operational, regulatory, and environmental conditions. This refinement process is driven by inputs such as internal audits, which assess the effectiveness of current risk controls, and regulatory reviews, which promote compliance with evolving standards. Additionally, changes in their operating environment, including the approval or denial of risk mitigation funding requests play a critical role in shaping risk tolerance guidance. Once proposed, updates are reviewed by governance bodies, such as risk committees and executive leadership, and are communicated throughout the organization via revised policies, operational procedures, and training programs. This adaptive approach enables IOUs to maintain operational resilience, respond effectively to emerging threats, and align long-term planning with public policy goals and stakeholder expectations.

Other Applicable Considerations

- Aversion to Tail Risk Events – Based on the survey efforts and results, the industry demonstrates a clear preference for proactive management of catastrophic-type (e.g., tail risk) events. Survey results and efforts did not uncover a single public utilities commission that dictated that IOUs follow a risk-neutral approach to such catastrophic-type risks or risk events. The general approach aligns with the broader risk management landscape, while the details of specific risk tolerance frameworks may vary across countries and regions and are shaped by local regulatory requirements.
- Ratepayer and shareholder balance – IOUs must manage risk in a way that satisfies both their obligations to serve the public consistent with their franchise obligations, as well as their ability to attract needed capital from investors to maintain safe and reliable service and meet public policy goals.
- Infrastructure modernization – Aging assets and the transition to clean energy technologies require dynamic risk tolerance thresholds, particularly to promote reliability within specified metrics.

- Regulatory scrutiny – IOUs face intense oversight, particularly in high-consequence areas, such as cybersecurity, wildfire prevention, and grid reliability.
- Public trust and transparency – Risk-based decisions are increasingly subject to public review and scrutiny, and mitigation decisions require clear communication and justification.
- Climate adaptation – Utilities must increasingly account for future long-term climate risks, including drought, heatwaves, and severe storms, within their operational and investment decision-making processes.

In addition to the previous questions, the Large California IOUs were required to provide responses to the following questions:

What is the Status Quo?

The implicit or explicit risk tolerance used by Large California IOUs is meaningfully shaped by the CPUC's Risk-Based Decision-Making Framework (RDF),[37] long-term viability and effectiveness of utility operations and service to customers, and the IOUs' ability to meet applicable state policy objectives (*e.g.*, SB901) and compliance obligations.

The most recent guidance is outlined in the RDF Phase IV Decision (D.25-08-032, adopted August 28, 2025),[38] which acknowledges the importance of formalizing risk tolerance thresholds. The Commission has not mandated specific risk tolerance thresholds for individual risks, or for utility operations as a whole. Instead, the CPUC has directed utilities to present and explain their internal approaches to risk tolerance through their individual Risk Assessment and Mitigation Phase (RAMP) filings and corresponding General Rate Case showings.

Each of California's major IOUs SCE, PG&E, SDG&E, and SoCalGas - have submitted RAMP filings during the course of different phases of the evolving RDF proceedings. In each of these filings, the IOUs have reflected the CPUC's evolving expectations and requirements, advancements in risk analysis and modeling, and changing circumstances and operational conditions.

These filings demonstrate that while the CPUC has provided overarching guidance regarding risk analysis, they have deferred defining and applying risk tolerance thresholds within the specific IOU operational and strategic contexts. Some representative examples of IOU submissions regarding risk tolerance are as follows:

---

[37] California Public Utilities Commission. *Risk-Based Decision-Making Framework (RDF):* R.20-07-013. https://www.cpuc.ca.gov/about-cpuc/divisions/safety-policy-division/risk-assessment-and-safety-analytics/r-20-07-013

[38] California Public Utilities Commission. (August 28, 2025). *Decision 25-08-032: Phase 4 decision in Rulemaking 20-07-013 – Risk-Based Decision-Making Framework for Electric and Gas Utilities.* https://docs.cpuc.ca.gov/PublishedDocs/Published/G000/M578/K198/578198350.PDF

- SCE's 2022 RAMP filing – (subject to RDF, Phase I) discusses risk tolerance in the context of Hydro Dam Failure (Chapter 12, pg. 6) and Wildfire and Public Safety Power Shutoff (PSPS) (Chapter 4, pg. 107).[39]
- PG&E's 2024 RAMP filing – (subject to RDF, Phase II) includes a dedicated section on Risk Tolerance (PG&E-1, Section A, pp. 1–13) and Risk Management Approach (PG&E-2, Section B), with additional insights embedded in individual risk chapters.[40]
- SoCalGas's and SDG&E's 2025 RAMP filing – (Subject to RDF, Phase III) outlines its approach in Risk Quantification, detailing how risk tolerance is integrated into decision-making.[41]

Additionally, in the area of price risk management of the IOUs' Bundled Electric Portfolio, the Commission adopted a To-Expiration Value at Risk (TeVaR) metric and an associated Customer Risk Tolerance (CRT) value. Per D.07-12-052, "(t)he TEVaR represents an estimate, at a given confidence level, of the amount of electric rate increase that could occur due to changes in market conditions such as nuclear outage risk, hydro-power availability risk, electricity spot market price volatility, credit risk, and gas price volatility (which represents the single greatest historical source of price volatility). For example, TEVaR 95% measures the maximum rate increase over the expected value with 95% confidence level (in other words, it is the 1-in-20 worst case scenario)"[42]. The CRT is used in conjunction with the TeVaR to establish a risk tolerance level for the Bundled Electric Portfolio. For example, the CRT for PG&E was set by the Commission to 10% of PG&E's system average rate and tied to TeVaR 95%[43]. Therefore, this means that the 1-in-20 worst case outcome that is tolerable results in a system average rate increase of no more than 10% over the forecasted (expected) value. Furthermore, CA IOUs have flexibility to implement their own methodologies to measure the TeVaR[44], and develop mitigations (which in the context of price risk, are known as hedging plans) in consultation with their Procurement Review Group, an advisory group[45].

[39] California Public Utilities Commission. *Southern California Edison Risk Assessment and Mitigation Phase (RAMP)*. https://www.cpuc.ca.gov/about-cpuc/divisions/safety-policy-division/risk-assessment-and-safety-analytics/risk-assessment-mitigation-phase/sce-ramp
[40] California Public Utilities Commission. *PG&E Risk Assessment and Mitigation Phase (RAMP).* https://www.cpuc.ca.gov/about-cpuc/divisions/safety-policy-division/risk-assessment-and-safety-analytics/risk-assessment-mitigation-phase/pg-and-e-ramp PG&E's risk evaluation approach is explained further in PG&E's 2027 General Rate Case testimony (A.25-05-009), Exhibit 2, Chapter 1.
[41] California Public Utilities Commission. *Sempra Risk Assessment and Mitigation Phase (RAMP)*. https://www.cpuc.ca.gov/about-cpuc/divisions/safety-policy-division/risk-assessment-and-safety-analytics/risk-assessment-mitigation-phase/sempra-ramp
[42] D.07-12-052, p. 173.
[43] D.15-10-031, p. 205.
[44] D.15-10-031, pp. 211-213.
[45] D.07-12-052, p0. 119-125.

What is the Internal Process for Setting Risk Tolerance?

With the context of the Commission's RDF, each utility has employed a structured internal process to determine the amount of risk it can accept in light of operational considerations, authorized funding levels, resource constraints, and regulatory and legal requirements.

These internal processes typically incorporate the following:

- Enterprise Risk Management (ERM) Frameworks – Utilities have adopted broadly-accepted ERM models (*e.g.*, COSO ERM, ISO 31000) to identify, assess, and prioritize risks across domains such as safety, reliability, financial exposure, and regulatory compliance.
- Risk Committees – Utilities make decisions through formal risk committees, which are often composed of executives, engineers, financial analysts, and regulatory experts, overseeing the development of risk tolerance thresholds and promoting alignment with corporate objectives and stakeholder expectations.
- Quantitative and Qualitative Risk Tools – Utilities use tools such as risk matrices, probabilistic modeling, scenario analysis, failure modes and effects analysis, as well as likelihood and consequence scoring to evaluate risk levels and determine acceptable thresholds.
- Integration into Decision-Making – Risk tolerance thresholds are embedded into capital planning, operational protocols, emergency response strategies, and mitigation prioritization. For example, wildfire risk scores may influence grid hardening investments or PSPS activation and de-energization criteria.
- Continuous Review and Adjustment – Risk tolerance levels are updated based on incident investigations, regulatory feedback, technological advancements, and changes in environmental or regulatory policy conditions. These updates are reviewed by senior leadership and communicated through revised procedures, training, and stakeholder engagement.

c. Public Utilities

Does the industry have a risk tolerance threshold?

Partially. Public electric utilities, including municipal utilities and electric cooperatives throughout the U.S. operate under a layered risk tolerance framework. This framework integrates federal and state regulatory requirements with locally tailored governance and operational practices. Risk tolerance thresholds for these entities are essential for system reliability, operational safety, and environmental compliance while fulfilling their public service mandates.

Is it set by the applicable regulatory body?

Partially. Public utilities are subject to baseline risk tolerance thresholds established by several regulatory bodies, including the Federal Energy Regulatory Commission (FERC), the North

American Electric Reliability Corporation (NERC), and state Public Utility Commissions (PUCs). In certain cases, the Federal Communications Commission (FCC) and the Environmental Protection Agency (EPA),[46] may also play a role, particularly for electric cooperatives that provide broadband services. These agencies define minimum standards for reliability, safety, cybersecurity, and environmental performance. Risk thresholds are developed through formal rulemaking processes, stakeholder consultation, and analysis of historical reliability and safety data. To remain effective and relevant, these standards are periodically reviewed and updated in response to technological advancements, incident experience, as well as local policy objectives.

If not, what is the internal process by which each company (within the industry) establishes a risk tolerance level?

Individual public utilities establish internal risk tolerance thresholds based on their unique governance structures, operating environment, as well as the needs of the communities they serve. Municipal utilities, which are governed by city councils or local boards, set risk tolerance levels for areas such as system reliability, financial exposure, operational safety, and customer service. These thresholds are shaped by local priorities, budgetary constraints, and political oversight. In contrast, electric cooperatives are member-owned utilities and define risk tolerance in alignment with member expectations and their longer-term goals. Cooperatives often adopt Enterprise Risk Management (ERM) frameworks to assess and manage strategic, financial, operational, and hazard-related risks. In both types of public utilities, risk committees and governing boards play a central role in overseeing the development of risk appetite statements, monitoring exposures, and adjusting thresholds as needed to maintain alignment with organizational objectives and stakeholder expectations.

How are they implemented?

Risk tolerance thresholds in public utilities are implemented through a combination of operational systems, performance monitoring, and organizational controls. These include maintenance protocols, outage response plans, and safety procedures, so that day-to-day operations align with defined risk limits. Utilities also use performance monitoring tools to track key metrics related to reliability and safety, enabling timely identification of deviations or emerging risks. To provide consistent application across departments, staff training and internal controls are essential components of the implementation process. Additionally, public utilities often rely on guidance from industry associations, such as the American Public Power Association, which provide resources like risk registers, scoring criteria, and enterprise risk management (ERM) toolkits to support structured and transparent implementation of risk management activities.

---

[46] U.S. Environmental Protection Agency. (2010). *An overview of public utility commissions for state environment and energy officials*. https://www.epa.gov/sites/default/files/2016-03/documents/background_paper.pdf

How are they modified/updated?

Risk tolerance thresholds in public utilities are regularly updated so that they remain aligned with evolving operational conditions and stakeholder expectations. These updates are informed by a variety of inputs, including internal audits, which assess the effectiveness of current risk controls; regulatory reviews, which evaluate compliance with external standards; and scenario analysis, which tests the utility's response to potential risk events; Additionally, changes in market conditions and stakeholder feedback, from customers, governing boards, and community representatives, play a critical role in shaping adjustments to risk thresholds. Once proposed, updates are reviewed and approved by utility boards or risk committees and are then communicated throughout the organization via revised policies, operational procedures, and training programs for consistent implementation and alignment.

Other Applicable Considerations

- Aversion to Tail Risk Events – Based on the survey efforts and results, the industry demonstrates a clear preference for proactive management of catastrophic-type (e.g. tail risk events). Survey results and efforts did not uncover a single public utilities commission that dictated a risk-neutral approach to such catastrophic-type (e.g. tail risk) events. The general approach aligns with the broader risk management landscape, while specific risk tolerance frameworks can vary across countries and regions and are shaped by local regulatory requirements.
- Local Accountability – Public utilities are directly accountable to their individual local governments or cooperative members. These stakeholders influence how risk decisions are made and communicated.
- Resource Constraints – Smaller utilities may face limitations in technical capacity or funding, affecting the scope of risk analysis and mitigation.
- Community Engagement – Risk tolerance decisions often reflect community values and priorities, especially in areas with high public involvement.
- Infrastructure Age and Investment – Many public utilities manage aging infrastructure, requiring careful risk prioritization and long-term planning.
- Climate and Environmental Risks – Increasing exposure to extreme weather events and environmental regulations necessitates adaptive risk management strategies.

References

- American Public Power Association. (2024–2025). *Risk management toolkit for public power utilities (Volumes I–III).* https://www.publicpower.org/resource/risk-management-toolkit-public-power-utilities

- Ayyub, B. M., Sawaya, R., Butry, D. T., Helgeson, J., Oum, Y., & Loh, V. (2023). *Risk tolerance, aversion, and economics of energy utilities in community resilience to* *wildfires.* ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems, Part A: Civil Engineering. https://doi.org/10.1061/AJRUA6.RUENG-1254

- California Independent System Operator. (2023). *ISO planning standards.* https://www.caiso.com/Documents/ISO-Planning-Standards-Effective-Feb22023.pdf

- California Independent System Operator. (2025). *2024–2025 transmission planning process overview.* https://stakeholdercenter.caiso.com/RecurringStakeholderProcesses/2024-2025-Transmission-planning-process

- California Independent System Operator. (2025, May 30). *2024–2025 transmission plan* [Board-approved report]. https://www.caiso.com/documents/iso-board-approved-2024-2025-transmission-plan.pdf

- California Public Utilities Commission, Safety and Enforcement Division. (2016*). Safety and Enforcement Division evaluation report on the risk evaluation models and risk-based decision frameworks in A.15-05-002, et al.* https://webtest.cpuc.ca.gov/-/media/cpuc-website/divisions/safety-policy-division/reports/sed-smap-evaluation-report-final-032116.pdf

- Federal Energy Regulatory Commission. (2023). *Reliability primer*. https://www.ferc.gov/media/reliability-primer

- Ferran, R., & Schmidt, J. (2025, September 9). *Risk assessment for electric cooperative organizations*. BPM. https://www.bpm.com/insights/risk-assessment-electric-cooperatives/

- Midcontinent Independent System Operator. (2024). *Risk management*. https://www.misoenergy.org/about/miso-risk-management/

- National Rural Electric Cooperative Association. (2023). *NRECA resource guide: Strategic and operational support for electric cooperatives.* https://www.cooperative.com/value-of-membership/Documents/NRECA_ResourceGuide.pdf

- National Rural Electric Cooperative Association. (2023). *NRECA safety resources and enterprise risk guidance.* https://www.cooperative.com/topics/safety/Pages/default.aspx

- Park, J. L., & Siebert, J. (2010). *Rebuilding cooperative leadership: The case of Pedernales Electric Cooperative*. Journal of Cooperatives, 24, 64–79. https://ageconsearch.umn.edu/record/164699

- U.S. Environmental Protection Agency. (2010). *An overview of public utility commissions for state environment and energy officials.* https://www.epa.gov/sites/default/files/2016-03/documents/background_paper.pdf

I. Other Industries – Dam Operators

Does the industry have a risk tolerance threshold?

Yes. Risk tolerance thresholds in dam operations are clearly defined by federal, state, and international regulatory bodies due to the high-consequence nature of dam failure. Given the potential for catastrophic failure and widespread downstream impacts, the establishment and management of risk tolerance thresholds in this sector are governed by a layered framework that integrates federal regulatory mandates with project-specific operational discretion. These thresholds are expressed in terms of probability of failure, life loss, economic disruption, and environmental damage.

Is it set by the applicable regulatory body?

Yes. Risk tolerance thresholds for dam operations are primarily defined by federal agencies such as the Federal Energy Regulatory Commission (FERC),[47] the U.S. Army Corps of Engineers (USACE),[48] the Bureau of Reclamation,[49] the Federal Emergency Management Agency (FEMA),[50] and internationally by the International Commission on Large Dams (ICOLD).[51] These agencies establish minimum safety standards and risk management guidelines, including requirements for risk analysis, assessment, and mitigation. Key regulatory documents, such as the Federal Guidelines for Dam Safety Risk Management and FERC's Engineering Guidelines, require dam owners to evaluate potential failure modes, structural performance, and consequences such as life loss, environmental damage, and economic disruption. The USACE, which manages a vast portfolio of dams and levees, anchors its risk tolerance framework in federal guidelines, internal governance, and project-specific considerations. Its tolerable risk thresholds reflect a balance between societal expectations and technical constraints, particularly in the context of flood risk reduction and infrastructure benefits.

Regulatory thresholds are established through a combination of historical incident analysis, scientific modeling, and stakeholder consultation. Agencies employ both quantitative and

---

[47] Federal Energy Regulatory Commission (FERC). 2016. Risk-Informed Decision Making (RIDM). Chapter 3 - Risk Assessment. Accessed online at: RIDM Guidelines Chapter 3 Risk Assessment Ver 4.1
[48] U.S. Army Corps of Engineers. (2014). *Safety of Dams – Policy and Procedures* (ER 1110-2-1156). https://www.publications.usace.army.mil/Portals/76/Users/182/86/2486/ER_1110-2-1156.pdf
[49] Bureau of Reclamation. (2022). *Reclamation public protection guidelines*. U.S. Department of the Interior. https://www.usbr.gov/damsafety/documents/ReclamationPublicProtectionGuidelines2022.pdf; Bureau of Reclamation. (2025). *Risk Management in Dam Safety.* https://www.usbr.gov/damsafety/risk/index.html
Note: USBR is moving away from USBR has been moving away from claiming that their guidelines reflect societal "tolerability" but, in practice their guidelines are consistent with the tolerable risk frameworks used by the other federal agencies.
[50] • Federal Energy Regulatory Commission. (2020). Federal Guidelines for Dam Safety Risk Management. https://www.ferc.gov/media/2326
[51] International Commission on Large Dams. (2020). *General Principles and Framework for Dam Safety* [Draft Bulletin]. https://www.itcold.it/wp-content/uploads/2020/10/DRAFT-ICOLD-Bulletin-General-Principles-for-DS-FINAL-2020-02-14.pdf

qualitative measures such as probability of failure and consequence severity, to define acceptable risk limits (e.g., Failure Modes and Effects Analysis (FMEA). These standards are subject to periodic review and revision, incorporating lessons learned from incidents (e.g., Oroville Dam[52]), technological advancements, and evolving policy goals. Dam operators define tail risk as dam breaches caused by seismic or hydrologic events. These risks are assessed by evaluating the likelihood of a load (e.g., flood), the structural response to that load, as well as the consequences.

If not, what is the internal process by which each company (within the industry) establishes a risk tolerance level?

Individual dam operators translate federal standards into project-specific risk management protocols through a structured, multi-tiered process. Each dam is managed by a Project Delivery Team (PDT), responsible for identifying, assessing, and documenting risks using tools such as risk registers and contingency analyses. Risk thresholds for each of these dams are tailored through Change Management Plans (CMPs), which define specific acceptance criteria and mitigation strategies.[53] These CMPs are reviewed and approved by Change Control Boards (CCBs) at the district division (Major Subordinate Commands in the case of USACE), for consistency and compliance across all organizational layers. Other dam owners, including public utilities, private companies, and municipalities, also implement risk management programs grounded in federal standards. These entities conduct site-specific risk analyses, maintain risk registers, and develop emergency action plans. In these cases, risk tolerance thresholds are similarly customized to each dam's design, geographic location, and operational context, and are embedded in surveillance, monitoring, and maintenance protocols.

How are they implemented?

Risk tolerance thresholds for dam operations are implemented and continuously refined through a combination of embedded systems and structured oversight. These thresholds are operationalized using tools such as risk registers, contingency analyses, and real-time monitoring platforms, which enable dam operators to proactively visualize, prioritize, and manage risks. These thresholds are further embedded into monitoring systems, maintenance schedules, and operational protocols, and are tailored to reflect each dam's unique characteristics and stakeholder expectations. The USACE's risk tolerance levels, for instance, are subject to ongoing review and recalibration, informed by project delivery experience, updates to federal guidelines, and the evolving risk landscape. For effectiveness and relevance, regular

[52] Friends of the River, California Sportfishing Protection Alliance, & American Whitewater. (2017). *The Oroville Dam 2017 Spillway Incident: Lessons from the Feather River Basin*. https://www.friendsoftheriver.org/wp-content/uploads/2017/09/The-Oroville-Dam-2017-Spillway-Incident-Lessons-from-the-Feather-River-Basin-Final.pdf ; Hollins, L. X., Eisenberg, D. A., & Seager, T. P. (2018). *Risk and resilience at the Oroville Dam*. Infrastructures, 3(4), 49. https://www.mdpi.com/2412-3811/3/4/49

[53] U.S. Army Corps of Engineers. (2022). *Project Delivery Business Process Manual* (EM 5-1-11). https://www.publications.usace.army.mil/Portals/76/EM%205-1-11_Admin%20revision%202024%2003%2027.pdf

audits, self-assessments, and event analyses are conducted, contributing to the refinement of risk management practices and helping maintain dam safety protocols that are current, responsive, and aligned with emerging challenges.

How are they modified/updated?

Risk tolerance thresholds for dam operations are regularly reviewed and updated so that they remain aligned with evolving safety standards and operational realities. These updates are driven by a variety of factors, including incident investigations, technological advancements, policy changes, as well as lessons learned from dam safety events. Additionally, inspections, stakeholder feedback, and regulatory updates contribute to the refinement of these thresholds. The process of continuous improvement is supported by audits, self-assessments, and event analyses, which help identify gaps and opportunities for enhancement. Proposed changes to risk tolerance levels are typically reviewed by risk committees or senior leadership, and once approved, are communicated throughout the organization via revised policies, training programs, and updated operational procedures.

Other Applicable Considerations

- Aversion to Tail Risk Events– Based on the survey efforts and results, the industry demonstrates a clear preference for proactive management of catastrophic-type (e.g., tail risk) events. While this approach aligns with the broader risk management landscape, specific risk tolerance frameworks vary across countries and regions and are shaped by local regulatory requirements.
- Aging Infrastructure – Many dams in the U.S. are several decades old. Aging components at these facilities can significantly affect their structural integrity, thereby influencing their associated risk tolerance thresholds.
- Downstream Population Exposure – Risk tolerance for dams must account for the number of people and critical infrastructure located downstream, especially in high-hazard zones. These populations may increase over time.
- Climate Change and Hydrologic Variability – Increasing frequency of extreme weather events and changing precipitation patterns can alter flood risk profiles and challenge existing design assumptions particularly over longer time horizons.
- Emergency Action Planning and Community Engagement – Effective risk management includes clear communication with downstream communities and robust emergency response protocols.
- Interagency Coordination and Regulatory Overlap – Dam safety often involves multiple agencies (e.g., FERC, USACE, FEMA), requiring alignment of risk tolerance standards and coordinated oversight across agencies.

References

- Bureau of Reclamation. (2025). *Risk management in dam safety*. https://www.usbr.gov/damsafety/risk/index.html

Bureau of Reclamation. (2022). *Reclamation public protection guidelines*. U.S. Department of the Interior. https://www.usbr.gov/damsafety/documents/ReclamationPublicProtectionGuidelines2022.pdf

- California Department of Water Resources, Division of Safety of Dams. (2019). *Inspection and reevaluation protocols*. California Natural Resources Agency. https://water.ca.gov/-/media/DWR-Website/Web-Pages/Programs/All-Programs/Division-of-Safety-of-Dams/Files/Publications/DSOD-Inspection-and-Reevaluation-Protocols_a_y19.pdf

Bureau of Reclamation. (2025). Risk Management in Dam Safety. https://www.usbr.gov/damsafety/risk/index.html

- Federal Energy Regulatory Commission. (2020). Federal Guidelines for Dam Safety Risk Management. https://www.ferc.gov/media/2326

- Friends of the River, California Sportfishing Protection Alliance, & American Whitewater. (2017). *The Oroville Dam 2017 spillway incident: Lessons from the Feather River Basin*. https://www.friendsoftheriver.org/wp-content/uploads/2017/09/The-Oroville-Dam-2017-Spillway-Incident-Lessons-from-the-Feather-River-Basin-Final.pdf

- Hollins, L. X., Eisenberg, D. A., & Seager, T. P. (2018). Risk and resilience at the Oroville Dam. *Infrastructures, 3*(4), 49. https://www.mdpi.com/2412-3811/3/4/49

- International Commission on Large Dams (ICOLD). (2016). *Bulletin 189: Current state-of-practice in risk-informed decision-making for the safety of dams and levees*. ICOLD-CIGB. https://www.icold-cigb.org/GB/publications/bulletins.asp

- International Commission on Large Dams. (2020). *General principles and framework for dam safety* [Draft Bulletin]. https://www.itcold.it/wp-content/uploads/2020/10/DRAFT-ICOLD-Bulletin-General-Principles-for-DS-FINAL-2020-02-14.pdf

- U.S. Army Corps of Engineers. (2014). *Safety of dams: Policy and procedures* (Engineer Regulation ER 1110-2-1156). https://www.publications.usace.army.mil/Portals/76/Users/182/86/2486/ER_1110-2-1156.pdf

- U.S. Army Corps of Engineers. (2022). *Project delivery business process manual* (Engineer Manual EM 5-1-11). https://www.publications.usace.army.mil/Portals/76/EM%205-1-11_Admin%20revision%202024%2003%2027.pdf

V. Conclusion

The Joint IOUs' survey highlights that while regulators frequently establish baseline risk tolerance thresholds, approaches can vary significantly across industries and jurisdictions. Companies typically build upon these regulatory foundations to define and operationalize risk tolerance in alignment with their roles, responsibilities, and legal obligations. This report provides a structured overview of these practices and describes how California's large investor-owned utilities currently determine and manage acceptable levels of risk in safety, operations, and decision-making.

Based on the survey efforts and results, the industries demonstrate a clear preference for proactively managing catastrophic-type events (e.g., tail risk events). While this approach aligns with the broader risk management landscape, specific risk tolerance frameworks can vary across countries and regions and are shaped by local regulatory requirements.

The Joint IOUs also respectfully note that the evidence set forth in this white paper clearly demonstrates that regulators, as well as individual entities, in each of these industries that have historically experienced significant risk outcomes detrimental to public and worker safety have substantially embedded important principles of risk aversion into their risk-based decision-making regulatory framework. In fact, the industries that are most analogous to electric utilities regarding potential public exposure to risk outcomes (e.g., commercial aviation, nuclear) do not have regulatory requirements that merely manage to "expected value" without regard to the uncertainty or variability of the outcomes themselves. Rather, regulators of such industries (e.g., FAA, NRC) have appropriately imposed requirements that are specifically intended to avoid catastrophic-type (or tail risk) events.

The Joint IOUs appreciate the Commission's guidance and look forward to engaging with stakeholders in the upcoming Risk Tolerance proceeding to further refine and align risk management practices that promote safety, reliability, and transparency.