

Master Risk, Deliver Results: ISO 9001 Risk-Based Thinking

Course No: B01-007
Credit: 1 PDH

Brian Lisiewski, P.E.

CED CANADA engineering.ca
CPD FOR THE PROFESSIONAL

Continuing Education and Development, Inc.

P: (877) 322-5800
info@cedengineering.ca

Table of Contents

Module 1: Introduction to ISO 9001 and Risk-Based Thinking 1

Module 2: Risk Identification in Engineering Projects 3

2.1 Methods and Tools for Risk Identification 3

2.2 Cross-Discipline Risk Identification Examples 4

2.3 Documenting Identified Risks – The Risk Register 5

Module 3: Risk Analysis and Evaluation Tools 6

3.1 Qualitative Risk Analysis 6

3.2 Quantitative Risk Analysis 7

Module 4: Risk Mitigation Strategies and Planning 8

4.1 Strategy 1: Avoid the Risk 8

4.2 Strategy 2: Mitigate (Reduce) the Risk 8

4.3 Strategy 3: Transfer (or Share) the Risk 8

4.4 Strategy 4: Accept the Risk 9

4.5 Choosing the Right Strategy 9

4.6 Integrating Risk Mitigation into the Project Plan 9

Module 5: Applying Risk-Based Thinking Across the Project Lifecycle 10

5.1 Planning Phase (Project Initiation and Concept) 10

5.2 Design Phase 11

5.3 Procurement Phase 12

5.4 Construction and Manufacturing Phase 12

5.5 Commissioning and Testing Phase 13

5.6 Operations and Maintenance Phase 14

Module 6: Conclusion and Continuous Improvement 16

6.1 The PDCA Cycle and Risk Management 16

References 17

Module 1: Introduction to ISO 9001 and Risk-Based Thinking

In any engineering project, **risk** can be defined broadly as **"the effect of uncertainty on expected results or objectives"**, capturing the possibility that some event or condition may adversely or beneficially affect project outcomes. **Risk identification and mitigation** are critical because engineering projects often operate under constraints of **safety, quality, budget, and schedule** – and unforeseen problems in these areas can cause failures or inefficiencies. This is why modern standards like **ISO 9001:2015** require organizations to **embrace risk-based thinking** as an integral part of their Quality Management System (QMS).

ISO 9001:2015 explicitly emphasizes **risk-based thinking** to encourage a **preventive, proactive approach** in operations rather than reacting after problems occur. In earlier editions of ISO 9001, organizations had a separate "preventive action" clause; **the 2015 revision integrates prevention via risk management throughout the standard**. Practically, this means that at all levels – from planning processes to operations and monitoring – companies should **identify what could go wrong, evaluate potential impacts, and take appropriate actions** to manage those risks. Risk is inherent in all processes, and not all processes carry equal risk; ISO 9001 requires focusing more attention and controls on higher-risk processes or decisions. Moreover, risk-based thinking also addresses **opportunities** – beneficial possibilities – as the upside of uncertainty, since taking an opportunity also entails risk that should be carefully considered.

> **Key Principle:** Risk-based thinking in ISO 9001 is about integrating awareness of risks and opportunities into daily decision-making and planning. It is not a standalone task or a burdensome extra step – it is a mindset where everyone from top management to project teams consistently plans and acts with potential risks in mind. Organizations practicing this proactive mindset tend to have fewer surprises, fewer quality issues, and better alignment of project outcomes with objectives.

Example: Civil Engineering Bridge Project

Consider a civil engineering team planning a highway bridge project. A risk-based approach might involve early geotechnical studies to identify subsurface risks (such as unknown soil conditions or seismic faults) and then plan mitigation (e.g., deeper foundations) in the design phase. In ISO 9001 terms, the team is "addressing risks and opportunities" during planning, fulfilling QMS expectations by preventing a quality or safety issue (foundation failure) upfront rather than correcting it later. This kind of proactive risk identification is exactly what ISO 9001's risk-based thinking seeks to foster – doing things right the first time by foreseeing challenges.

ISO 9001 and Professional Engineering

Professional engineers have an ethical and professional duty to safeguard the public's health, safety, and welfare. By following a structured risk management approach, **engineers align with ISO 9001 and licensure obligations**: ensuring designs and projects meet requirements without unforeseen failures that could compromise safety or quality. In this course, we will explore practical ways to implement risk-based thinking in engineering projects, step by step through the project lifecycle.


PLAN
Identify risks & opportunities
Set objectives & plan actions
DO
Implement plans
and risk controls
in project activities
ACT
Take corrective actions
Improve processes
Update risk plans
CHECK
Monitor results
Measure quality metrics
Review risk outcomes

Module 2: Risk Identification in Engineering Projects

Risk identification is the foundational step of risk management. It involves systematically **examining all aspects of the project to uncover what could go wrong**, so that potential issues can be managed from the outset. The guiding question is: **"What could go wrong, and what uncertainties do we face?"**

2.1 Methods and Tools for Risk Identification

Brainstorming with Project Teams

Gathering engineers and stakeholders to think through possible problems in each project phase. Sessions often reveal risks such as supplier delays, design assumptions not holding true, or permit approvals taking longer than expected. These sessions utilize past experiences and expert judgment.

Historical Data and Lessons Learned

Reviewing previous similar projects or organizational databases for known issues. For instance, if past mechanical projects showed that a certain cooling system frequently had field installation issues, that risk should be identified upfront in a new project. Historical failure data and lessons learned are invaluable sources of risk information.

Checklists and Prompt Lists

Using standardized checklists of common risks, often categorized by risk type (technical, safety, regulatory, logistical, etc.), ensures no obvious category is overlooked. Many organizations and industries have developed lists of typical risks to consider.

Failure Mode and Effects Analysis (FMEA)

In mechanical and electrical engineering especially, teams use FMEA to identify how each component or process step could fail and what the effects would be. FMEA provides a systematic, detailed approach to highlighting technical failure risks in design and production. Each failure mode is scored for **Severity**, **Occurrence** (likelihood), and **Detection** (how easily the failure can be detected before causing harm). These three scores are multiplied to produce a **Risk Priority Number (RPN)**. Note that a higher Detection score indicates the failure is **harder to detect**, so a high RPN signals a failure mode requiring priority attention.

Note that a higher Detection score indicates the failure is harder to detect — unlike Severity and Occurrence, where a higher score also means worse outcomes, Detection is scored inversely: 1 means the failure is almost certain to be caught, while 10 means it is nearly impossible to detect before causing harm.

Hazard Identification (HAZID) Workshops

Common in environmental and civil projects, HAZID sessions focus on safety and environmental hazards. For example, an environmental engineer on a site remediation project would identify potential hazards such as chemical spills or exposure risks during excavation.

Risk Breakdown Structure (RBS)

An RBS is a hierarchical framework, similar to a Work Breakdown Structure, that breaks down risks by categories such as technical, financial, schedule, external, and environmental. An RBS guides identification by prompting consideration of each category in turn.

> **Important:** Risk identification is an ongoing process, not a one-time activity. New risks can emerge as conditions change or as the project progresses. Teams should revisit risk identification periodically – for example, at phase gates or major design reviews – to catch new issues early.

2.2 Cross-Discipline Risk Identification Examples

Electrical Engineering

An electrical project team designing a substation will identify risks such as equipment failure rates, short-circuit hazards, power demand changes, and cybersecurity threats to control systems. Supply chain risks (such as delayed transformer delivery) and safety hazards (such as arc-flash in switchgear operation) are also identified and entered into the risk register.

Mechanical Engineering

For a mechanical system design such as an HVAC system, engineers identify risks including excessive vibration or noise, component fatigue failure under peak loads, or inability to meet temperature control specifications. FMEA on major components (chillers, pumps) reveals failure modes. For example, a pump seal failure could result in a leak, leading the team to plan for a leak detector or redundant pump.

Civil Engineering

In a bridge construction project, civil engineers identify numerous planning-phase risks: geotechnical surprises (weak soil pockets), extreme weather events (flooding during construction), design errors, contractor performance issues, and public opposition to certain construction activities. These become entries in the project risk register.

Environmental Engineering

For an environmental remediation or water treatment project, risk identification highlights regulatory compliance risks (e.g., permits not granted on time), environmental impact risks (e.g., containment failure causing pollutant spread), and operational risks (e.g., treatment process not achieving required standards).

2.3 Documenting Identified Risks – The Risk Register

All identified risks should be recorded in a **Risk Register**, a living document or spreadsheet listing each risk along with: likelihood, impact, potential mitigation actions, risk owner, and current status.

> **Example Risk Register Entry:**
> Risk: Critical transformer delivery delayed
> Cause: Supplier production backlog
> Impact: 6-week project delay | Likelihood: Moderate
> Mitigation: Order well in advance; identify alternate supplier or temporary unit
> Owner: Project Procurement Lead | Status: Open



Module 3: Risk Analysis and Evaluation Tools

Once risks are identified, the next step is **analyzing and evaluating** them to prioritize action. Not all risks are equal – some are very unlikely or minor in effect, while others could be likely and catastrophic. Risk analysis answers: **"How likely is this event, and how severe would the consequences be?"**

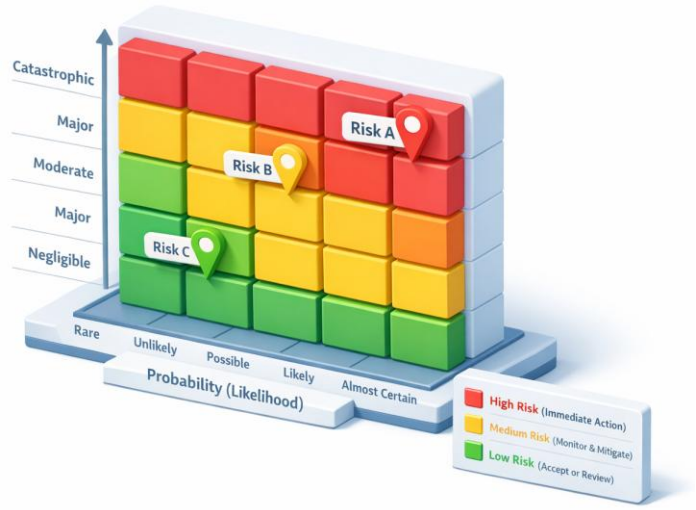
3.1 Qualitative Risk Analysis

Most engineering projects begin with a qualitative risk assessment. This involves estimating each risk's **probability (likelihood of occurrence)** and **impact (severity of consequence)** in relative terms (such as High/Medium/Low or on numerical scales). Teams typically use a **risk matrix** to rate and rank risks.

The Risk Matrix

A risk matrix is a grid (commonly 5×5 or 4×4) mapping **Likelihood** on one axis and **Impact** on the other. Each identified risk is placed into the matrix based on its estimated probability and impact levels. The matrix is color-coded – green cells for low risk, yellow for medium, red for high – to clearly show which risks need the most urgent attention.

- A risk with **low probability and low impact** falls in the green zone (acceptable; minimal oversight needed).
- A risk with **high probability and high impact** lands in the red zone (critical risk requiring immediate mitigation).
- Medium probability/high impact or vice versa typically indicates **moderate priority** requiring case-by-case judgment.



Risk Ranking and Scoring

Some teams assign numerical scores (1 to 5) for both probability and impact and calculate a **risk priority number** (Probability × Impact) for each risk. For example, if likelihood = 4 (out of 5) and impact = 5 (out of 5), then risk score = 20, which would be among the highest. While not a precise measurement, this approach helps sort risks from highest to lowest priority efficiently. As a practical rule of thumb: **high risks must be addressed**; **low risks can be accepted**; and **medium risks** require case-by-case judgment.

3.2 Quantitative Risk Analysis

For complex or critical risks, or when a more rigorous estimate is needed (particularly on large projects where data is available), a quantitative analysis may be performed.

Expected Value Calculations

Using probability × impact to estimate an **expected monetary value** for cost risks. For example, if a rare event (1% probability) could cost $500 million, the expected cost of that risk is calculated as $5 million. This gives insight into appropriate contingency budgets or insurance thresholds.

Monte Carlo Simulations

Running many iterations of a project model to see the distribution of outcomes, commonly used in schedule or cost risk analysis for large projects. For example, a simulation might determine that "there is an 80% probability the project will complete within a 6-month delay range." This is an advanced technique not required for every project.

FMEA Risk Priority Number (RPN)

In FMEA, each failure mode is scored for Severity, Occurrence, and Detection, and these are multiplied to give an RPN that prioritizes failure modes for mitigation. Application note, In practice, failure modes with high Severity and poor Detection scores should be prioritized even when Occurrence is low, because the consequences of a missed detection in those cases can be catastrophic.

> **ISO 9001 Connection – Clause 6.1:** ISO 9001's Clause 6.1 ("Actions to address risks and opportunities") expects organizations to evaluate their identified risks and determine which require action. Using risk matrices and qualitative analysis is a practical way to fulfill this requirement by demonstrating a clear rationale for which risks are "significant" and need to be controlled.

Module 4: Risk Mitigation Strategies and Planning

With a prioritized list of project risks in hand, engineers must decide **what to do about each risk**. Risk mitigation planning involves developing **strategies and actions to address identified risks** so that project objectives can still be met. There are **four classic risk response strategies** for negative risks (threats):

> **Note on Risk Response Frameworks:** Different frameworks use slightly different terminology for the four strategies. ISO 9001 and PMI use Avoid / Mitigate / Transfer / Accept. A comparable UK/ISO 31000-aligned framework uses Terminate / Treat / Transfer / Tolerate. These are equivalent in practice. This course uses the Avoid / Mitigate / Transfer / Accept terminology throughout. Specifically: Terminate = Avoid, Treat = Mitigate, Transfer = Transfer, Tolerate = Accept.

4.1 Strategy 1: Avoid the Risk

Change the plan to **eliminate the risk entirely**, or choose an alternative approach that bypasses the risk. This is ideal but not always possible. Risk avoidance means making a decision that removes the possibility of the risk occurring.

> **Example:** If building at a site on a floodplain poses too high a risk, a civil engineer might choose to relocate the project to higher ground. By altering the scope or approach, the risk of flooding during construction is eliminated. In another example, selecting a proven, established design approach instead of a novel unproven one – with many uncertainties – is also a form of risk avoidance.

4.2 Strategy 2: Mitigate (Reduce) the Risk

Take **proactive steps to reduce the likelihood or impact** (or both) of the risk. This often involves engineering controls or process changes. Mitigation is the most commonly applied strategy in engineering.

> **Examples:** An electrical team worried about power failure on a manufacturing line installs an uninterruptible power supply (UPS) or backup generator, reducing the impact of an outage without eliminating the possibility. A mechanical design team may redesign a component with a higher safety factor or add a redundant component after FMEA shows a fatigue risk. Other mitigation actions include strengthening designs, adding safety features, increasing inspection frequency to catch issues early, and building schedule buffers.

4.3 Strategy 3: Transfer (or Share) the Risk

Shift the risk or part of it to another party who is better placed to handle it, usually via contracts, insurance, or partnerships.

> **Examples:** A construction firm purchases insurance to transfer financial risk of property damage or worker accidents to an insurer. A project might outsource a risky element to a specialist subcontractor with applicable expertise, transferring that technical risk contractually. Vendor warranties and performance bonds also effectively transfer certain risks to the vendor.

4.4 Strategy 4: Accept the Risk

Acknowledge that the risk exists and take **no active preventive measures**, though monitoring continues and a contingency plan may be prepared. Acceptance is appropriate for low-level risks or where mitigation is not cost-effective or feasible. Acceptance does not mean ignoring the risk – the team should continue to **monitor** it in case circumstances change.

> **Example:** An environmental project identifies the risk of mild weather delays in excavation (a few days of rain). Judged as low impact and reasonably likely, the team decides to accept this minor schedule risk rather than spend money on expensive shelter structures or schedule acceleration. Small delays will simply be absorbed if they occur.

4.5 Choosing the Right Strategy

Deciding which strategy to use depends on risk priority and the cost-benefit of addressing it. **High risks typically demand avoidance or mitigation**, rarely just acceptance. Medium risks may be mitigated or accepted depending on judgment, and low risks are often accepted with periodic re-evaluation.

4.6 Integrating Risk Mitigation into the Project Plan

- **Project Plan Integration**: For each significant risk, chosen mitigation actions should be built into the project plan and schedule as tasks, with associated timeline and budget.
- **Risk Owners**: Assign an owner to each risk – a team member responsible for ensuring the mitigation is carried out and effective, and for tracking the risk's status on the risk register.
- **Contingency Reserves**: Allocate contingency reserves (time or budget buffers) specifically for risk response. Adding schedule float to accommodate possible delays, or maintaining budget contingency funds for unforeseen costs, is part of risk-adjusted planning.
- **Unknown Unknowns**: Even after thorough identification, some risks remain unforeseeable. Many project teams include a general contingency (typically 5–10% of budget and some schedule slack) to handle complete surprises.

Module 5: Applying Risk-Based Thinking Across the Project Lifecycle

Engineering projects move through distinct phases: Planning, Design, Procurement, Construction (or Manufacturing), Commissioning, and Operations/Maintenance. In each phase, the nature of risks and how we manage them differs. ISO 9001's risk-based thinking provides a **thread that runs through all phases**, ensuring continuous risk awareness and action.

5.1 Planning Phase (Project Initiation and Concept)

Overview: The planning or initiation phase is where the project's broad scope, objectives, feasibility, and constraints are defined. This is the earliest point to identify high-level project risks and incorporate them into the project strategy. Decisions made here will influence risk exposure significantly.

Risk Focus

- Strategic and scope-related risks: Is the project concept sound? Are objectives realistic?
- Resource and funding risks: Is the budget realistic? Are key resources available?
- Stakeholder risks: Are there stakeholders who might oppose or create obstacles?
- Regulatory and permitting risks: What approvals are required, and what is the risk of delay?

Key Risk Activities in Planning

- **Initial Risk Assessment Workshop**: Engage project stakeholders to produce an initial risk register.
- **Context Analysis (ISO 9001 Clause 4)**: Understand internal and external factors that present risk or opportunity, including regulatory context and market conditions.
- **Feasibility Studies**: Incorporate risk analysis such as SWOT analysis or scenario planning into feasibility assessments.

Discipline Examples – Planning Phase

Civil and Environmental: For a proposed new wastewater treatment plant, the planning team identifies big-picture risks such as community opposition, land acquisition problems, major environmental permit hurdles, and funding shortfalls. Preliminary soil borings can reduce geotechnical uncertainty, and early community engagement can mitigate opposition. Selecting a site with fewer environmental constraints is itself a risk avoidance decision.

Electrical: An electrical utility considering a substation upgrade identifies the risk of extended customer outage if the upgrade is mishandled. Scheduling work in shoulder seasons (low demand) and building temporary bypass circuits are planned upfront as risk mitigations. Long procurement lead times for large transformers are identified early, influencing procurement planning.

5.2 Design Phase

Overview: During design, detailed specifications, calculations, drawings, and simulations are developed. Technical risks are most pronounced here – design errors or omissions can lead to failures or costly changes later.

Risk Focus

- Technical/design risks: Calculation errors, design not meeting requirements or codes, unproven technologies.
- Interface risks: Misalignment between disciplines (e.g., mechanical designs not fitting civil structural provisions).
- Compliance risks: Does the design comply with all regulatory standards? Missing compliance issues in design are expensive to correct later.

Key Risk Activities in Design

- **Design Reviews and Hazard Analyses**: Multi-disciplinary reviews including HAZOP (Hazard and Operability) studies catch design flaws and hazards.
- **Simulations and Safety Factors**: Engineers incorporate safety factors and perform simulations (finite element analysis, circuit simulation) to validate designs against worst-case conditions.
- **FMEA in Design**: Performing FMEA on critical subsystems identifies failure modes to mitigate on paper, before construction or manufacture begins.

Discipline Examples – Design Phase

Mechanical: Designing a new HVAC system for a hospital, mechanical engineers identify the risk of HVAC failure in critical areas. They incorporate redundant chillers and robust control systems with alarms and backup power. Past project experience with vibration-induced piping fatigue leads to inclusion of flexible couplings and supports in the design. Seismic bracing for equipment and fail-safe controls are included to mitigate earthquake and control system risks respectively.

Civil: Structural engineers designing a high-rise consider risks such as wind load calculation errors and greater-than-expected soil settlement. They mitigate by applying conservative safety factors and planning additional soil investigations. Coordination with architects and other disciplines identifies interface risks such as heavy rooftop equipment requiring additional structural support.

Electrical: When designing an industrial power distribution system, the electrical engineer identifies risks including voltage drop in long cables, short-circuits, arc-flash hazards, and equipment incompatibilities. Mitigation includes power system studies (load flow, short-circuit analysis) and design of protection devices and arc-flash safety boundaries. Where unfamiliar relay technology is used, vendor support and pilot testing are planned as mitigation.

5.3 Procurement Phase

Overview: Procurement involves sourcing materials, equipment, and services needed for the project. Supply chain and supplier-related risks dominate this phase.

Risk Focus

- Supplier reliability risks: Late deliveries, poor quality, supplier financial failure, sole-source dependencies.
- Cost risks: Material price volatility, foreign exchange risk if using international suppliers.
- Contractual risks: Gaps or ambiguities in procurement contracts creating liabilities.

Key Risk Activities in Procurement

- **Supplier Risk Assessment**: Evaluate suppliers' track records and classify them by criticality. ISO 9001 Clause 8.4 requires control of externally provided processes and products. Risk-based thinking requires imposing stricter controls on high-risk suppliers and pursuing dual-source qualification for sole-source critical components.
- **Early Ordering and Time Buffers**: For long-lead or risky items, build time buffers into the procurement plan and order critical items early.
- **Factory Acceptance Testing (FAT)**: Include robust inspection and testing requirements for incoming materials and equipment. Witnessing FATs at the supplier facility catches quality issues before equipment ships, reducing impact on the project timeline.

Discipline Examples – Procurement Phase

Mechanical: A project requiring a custom-engineered compressor with an 8-month lead time qualifies two vendors and places orders to allow backup if one fails. Contractual penalties for delivery delays are included as a risk mitigation.

Electrical: When procuring switchgear for a power distribution project, the team arranges a pre-production design review with the vendor and witnesses a factory acceptance test. Parallel work is scheduled during the delivery window, and old equipment is not decommissioned until the new gear passes acceptance tests.

Environmental: Procuring water treatment equipment with performance guarantees and partial payment withheld until on-site performance tests pass. Pre-ordered spare materials (such as membrane filter elements) mitigate the risk of running out if a production batch fails.

5.4 Construction and Manufacturing Phase

Overview: This phase involves execution of the work – constructing the facility or manufacturing the product. Execution risks and safety risks are front and center.

Risk Focus

- Worksite safety hazards: Worker accidents, falls, equipment incidents.
- Quality control during execution: Deviations from design specifications, poor workmanship.
- Environmental risks on site: Spills, emissions, community disturbance (noise, dust).
- Logistics and coordination risks: Scheduling conflicts, equipment breakdowns, labor issues, weather disruptions.

Key Risk Activities in Construction and Manufacturing

- **Safety Risk Mitigation**: Rigorous safety plans, training, and Job Hazard Analyses (JHA) for each major task pre-plan hazard controls. Fall protection, equipment safety, and emergency response procedures are implemented.
- **Quality Control Plan**: Inspection checkpoints (hold points) and testing protocols ensure construction output meets specifications. Examples include concrete strength tests and nondestructive weld inspections. Detecting issues early allows correction before they become costly rework.
- **Change Management**: A controlled process to evaluate and approve changes reduces the risk of cost growth or quality compromise when site conditions differ from assumptions.
- **Continuous Monitoring**: The risk register is regularly updated. Certain risks may escalate or new ones may emerge (e.g., sudden material shortage). The project team adapts accordingly.

Discipline Examples – Construction and Manufacturing Phase

Civil: Building a bridge involves enforcing fall protection and maintaining a safety supervisor on site. The schedule includes extra buffer in winter months for likely weather downtime. A testing technician samples each concrete delivery truck, and a backup concrete supplier is pre-qualified in case a batch fails strength tests. A traffic management plan mitigates accident risk from construction activity over an active roadway.

Mechanical: When installing a large HVAC or mechanical system, engineers mitigate installation errors such as equipment misalignment or incorrect connections through thorough commissioning checklists and skilled supervision. Strict handling procedures and protective packaging reduce the risk of component damage during installation.

Environmental: During contaminated soil remediation, dust suppression systems, containment berms, and on-site monitoring mitigate the risk of spreading contamination. An on-site environmental compliance officer checks daily that all permit requirements (such as erosion controls) are met.

5.5 Commissioning and Testing Phase

Overview: Commissioning is where the constructed system or product is verified to meet requirements before full operation or delivery. This phase confirms that mitigations implemented earlier were effective.

Risk Focus

- Performance risks: The facility or product may not meet performance criteria (throughput, capacity, quality specifications).
- Integration risks: Subsystems may not integrate as expected (e.g., electrical system tripping when mechanical load peaks).
- Safety and compliance test failures: Failing a required safety test causes delays and rework.

Key Risk Activities in Commissioning

- **Comprehensive Test Plans**: Commissioning test plans capture both normal and worst-case operating scenarios to surface any lingering issues.
- **Issue Resolution Resources**: If something fails a test, an issue resolution process and the necessary resources (designers for redesign, spare parts for replacement) must be readily available.
- **Phased Startup**: Mitigate risk by starting up a plant at partial capacity to monitor performance, then ramping to full capacity. Issues encountered at lower loads are safer and cheaper to resolve.

Discipline Examples – Commissioning Phase

Electrical: Commissioning a new substation, the team performs pre-energization simulations and checks, then energizes sections stepwise. Vendor support is on site to troubleshoot problems such as misconfigured relays. Any unexpected protection trip is investigated, the cause identified, and settings corrected before proceeding.

Mechanical: During startup of a new industrial boiler, vendor specialists tune the control loop and conduct a trial run with water load to ensure safe operation. A safety valve is subjected to a controlled lift test to verify proper operation before the boiler is loaded.

Environmental: Testing a new wastewater treatment plant, a several-week trial operation closely monitors effluent quality. Filters not performing to specification are tuned or replaced. Chemical dosing is available as a contingency if the biological process is slow to reach steady state.

5.6 Operations and Maintenance Phase

Overview: Once the project is delivered, the operational phase begins. Risk-based thinking continues to apply to ensure long-term performance, safety, and improvement.

Risk Focus

- Operational reliability risks: Equipment breakdowns, maintenance needs, wear beyond expectations.
- Safety and environmental risks: Process safety hazards if operations deviate; environmental discharges if controls fail.
- Change management: Modifications to how a facility is used can introduce new risks if not formally assessed.

Key Risk Activities in Operations

- **Preventive Maintenance Programs**: Scheduling maintenance to fix or replace components before they fail catastrophically. Using reliability data to drive maintenance intervals is a direct application of risk-based planning.
- **Monitoring and Continuous Improvement**: Gathering performance data, incident reports, and near-miss reports to update risk assessments. Root cause analysis of any incident feeds lessons back into improved procedures, applying the ISO 9001 "Check" and "Act" phases.
- **Emergency Preparedness**: Maintaining emergency response plans for disasters (fire, major equipment failure) mitigates the impact of rare but severe events.

Discipline Examples – Operations Phase

Mechanical: Operating a large building HVAC system, a preventive maintenance schedule and remote monitoring catch anomalies before they cause chiller failure on a hot day. Service contracts ensure quick repair capability. If a particular pump shows a pattern of repeated failure, a risk-based approach triggers a design upgrade or equipment replacement (continual improvement).

Civil: A highway bridge in service is subject to periodic structural inspections, structural health monitoring, and timely maintenance (repainting steel, sealing cracks) to reduce the probability of deterioration leading to a major safety event. An emergency traffic rerouting plan is maintained as a readiness measure.

Environmental: A water treatment facility in continuous operation uses control system alarms to alert operators of abnormal conditions, maintains backup treatment capacity (a spare filter unit ready to come online), and keeps an on-call response team. Effluent test results trending toward regulatory limits trigger process adjustments before a violation occurs.

Module 6: Conclusion and Continuous Improvement

Risk management is not a one-off task; it is an **ongoing discipline** that should become part of an engineer's professional routine. ISO 9001's risk-based thinking means **embedding risk awareness** into everything – designing processes, making decisions, allocating resources – such that preventive thinking becomes second nature.

6.1 The PDCA Cycle and Risk Management

The **Plan-Do-Check-Act (PDCA)** cycle provides the continuous improvement framework within which risk management operates:

- **Plan**: Identify and assess risks; develop mitigation strategies and integrate them into project plans.
- **Do**: Implement mitigations, execute project work with risk controls in place.
- **Check**: Monitor outcomes, inspect work products, track risk status against the risk register, conduct commissioning tests.
- **Act**: Make adjustments based on what monitoring reveals; update risk register, revise procedures, incorporate lessons learned.

Key Principles for Effective Risk Management:

1. **Keep it practical and proportionate:** Focus effort where it matters most. Not every small risk needs extensive analysis, but significant risks definitely do.
2. **Ensure team engagement:** Everyone on the project team should understand the key risks and their role in mitigation. A culture that encourages raising concerns and discussing "what ifs" catches issues early.
3. **Review and update regularly:** As the project or operations evolve, so do risks. Integrate risk review into project status meetings so no new threat goes unnoticed.
4. **Learn from outcomes:** After project completion, review which risks occurred and how mitigations performed. Lessons learned – both successes and failures – should inform future projects, closing the PDCA loop.

By applying these principles, **professional engineers can deliver projects that not only meet technical specifications but also avoid the pitfalls that could otherwise lead to failures, delays, or accidents**. This risk-based approach demonstrates due diligence and adherence to the standard of care expected in engineering practice.

Risk management, when done well, does not stifle innovation or make projects overly conservative. Instead, it **enables** innovation by identifying challenges early and managing them, giving stakeholders confidence that even ambitious projects are under control. Embracing risk-based thinking as taught in this course will help you build more **resilient, successful engineering projects** that stand the test of time.

References

1. Gillespie, M. (n.d.). Risk-Based Thinking in ISO 9001: Practical Applications. https://www.linkedin.com/pulse/risk-based-thinking-iso-9001-practical-applications-matthew-gillespie-xmgfc
2. CED Engineering. Risk Management for Engineers (Course B02-013). https://www.cedengineering.com/userfiles/B02-013%20-%20Risk%20Management%20for%20Engineers%20-%20US.pdf
3. Quality.org. Managing Quality and Risk in Projects. https://www.quality.org/knowledge/managing-quality-and-risk-in-projects
4. ISO/TC 176/SC 2. ISO 9001:2015 and Risk — Implementation Guidance. https://committee.iso.org/files/live/sites/tc176sc2/files/documents/ISO%209001%202015%20-%20Implementation%20guidance%20docs/ISO9001_2015_and_Risk.docx
5. Eminent Design. Risk Management in Engineering Projects. https://eminent-design.com/17-risk-management-in-engineering-projects/
6. ISMS Online. ISO 9001 Clause 6 — Planning. https://www.isms.online/iso-9001/clause-6-planning/