Risk Management in Practice

Lecture Title:
Risk Management Standards and Frameworks

Lecturer: Chris Camilleri

Date: 19th January 2026

Undergraduate Diploma in
Occupational Health and Safety

Welcome and Objectives

This lecture explores internationally recognized standards and frameworks that guide risk management practices in occupational health and safety. It emphasizes ISO 31000, ISO 45001, and other relevant guidelines, explaining how these frameworks ensure consistency and compliance across industries.

Learning Objectives:

1. Understand the purpose and scope of major risk management standards (ISO 31000, ISO 45001).
2. Explain the principles and components of risk management frameworks.
3. Apply standards to develop systematic risk management processes.
4. Evaluate compliance requirements and their impact on organizational practices

What is Risk Management in OHS?

1. Identifying workplace hazards
2. Evaluating risks to workers and operations
3. Implementing controls to eliminate or minimise harm
4. Monitoring and reviewing risk controls for continuous improvement
5. Ensuring safe systems of work are embedded across the organization

Purpose: Prevent harm, ensure legal compliance, and strengthen organizational resilience.

Why Standards Matter

Why Global Standards Ensure Consistency and Compliance

1. Provide a structured, repeatable approach to risk management
2. Align organizations to international best practice
3. Facilitate legal and regulatory compliance across jurisdictions
4. Support continuous improvement and auditing
5. Enhance communication and clarity between stakeholders
6. Enable benchmarking with global industry peers

Setting the Scene for the Lecture

1. Key global risk management standards
2. How these standards interconnect and differ
3. How organisations apply these frameworks in high-risk industries
4. Practical examples of standards in action
5. How standards drive governance, accountability, and performance

Which standards do you use or know?

ISO 31000 – Principles & Framework
Purpose and Scope

1. ISO 31000 is the international standard for risk management.
2. It provides:

- A common language and approach to risk across all organisational levels.
- A universal, sector-agnostic framework applicable to all industries, including high-risk sectors like construction, manufacturing, energy, and healthcare.
- Guidance for integrating risk management into governance, leadership, culture, planning, and operations.

ISO 31000 – Principles & Framework Purpose and Scope

Key points

1. ISO 31000 is not a certification standard but a guideline.
2. It emphasizes maximizing value, not simply reducing risk.
3. It bridges strategy, operations, and decision-making.

Principles of ISO 31000 (Value Creation, Integration, Structured Approach) ISO 31000 outlines eight guiding principles.

A. Value Creation & Protection

Risk management should enhance organisational performance by enabling better decision-making and resilience.

Examples in high-risk industries:

1. Optimised maintenance scheduling based on risk.
2. Preventing major incidents that could disrupt business continuity.

Principles of ISO 31000 (Value Creation, Integration, Structured Approach) ISO 31000 outlines eight guiding principles.

B. Integration

Risk management must be part of all activities, not a standalone function.

It should be integrated into:

1. Strategic planning
2. Project design
3. Daily operations
4. Change management
5. Safety culture development

Principles of ISO 31000 (Value Creation, Integration, Structured Approach) ISO 31000 outlines eight guiding principles.

C. Structured Approach

A systematic and consistent approach ensures comparability and repeatability in risk assessments.

This resonates well in high-risk contexts, where structured processes increase oversight and improve hazard visibility.

ISO 31000 Framework & Process

A. Framework

The ISO 31000 framework consists of five interconnected components:

1. **Leadership & Commitment**

Senior management must drive expectations, allocate resources, and define accountability.

2. **Integration**

Embedding risk management into culture, processes, and decision pathways.

3. **Design**

Understanding external and internal context.

Establishing roles, responsibilities, tools, and communication channels

ISO 31000 Framework & Process
A. Framework

4. **Implementation**

Applying the risk management process throughout the organisation.

5. **Evaluation & Improvement**

Monitoring performance.

Learning from incidents, near-misses, and audits.

Continually refining the framework.

ISO 31000 Framework & Process
B. Risk Management Process

The ISO 31000 process includes:

1. **Communication & Consultation**

Engagement with stakeholders to ensure clarity and shared understanding.

2. **Scope, Context, Criteria**

Defining boundaries, understanding constraints, determining risk appetite and tolerance.

3. **Risk Assessment**

Risk Identification – What could happen? Why? How?

Risk Analysis – Likelihood, consequence, existing controls, level of risk.

Risk Evaluation – Prioritization based on risk criteria.

ISO 31000 Framework & Process
B. Risk Management Process

4. **Risk Treatment**

Selecting and implementing the best control strategies.

Aligns with the Hierarchy of Controls (engineering, substitution, etc.)

5. **Monitoring & Review**

Ensuring controls are effective and updated.

6. **Recording & Reporting**

Transparent documentation to support governance and continual improvement

Example 1 – Risk: Slips, Trips & Falls in a Warehouse

Value Creation

1. Reducing injuries decreases lost-time incidents and insurance costs.
2. Improved floor layout and housekeeping increase productivity and material flow efficiency.

Integration

1. Incorporated into daily housekeeping routines, supervisor walkthroughs, and onboarding training.
2. Included in procurement decisions (e.g., anti-slip flooring, spill kits).
3. Embedded into incident reporting and continuous improvement processes.

Example 1 – Risk: Slips, Trips & Falls in a Warehouse

Structured Approach

1. Risk identified during routine inspections → analysed by looking at likelihood (high traffic areas) and consequence (potential fractures).
2. Controls selected using a systematic method: floor resurfacing, improved drainage, visual cues, footwear policy.
3. Monitoring and review: weekly audits, reviewing near-miss reports.

Example 2 – Risk: Confined Space Entry in Manufacturing

Value Creation

1. Safer entry procedures reduce fatalities and severe injuries.
2. Consistent protocols minimise downtime and allow faster maintenance turnaround.

Integration

1. Integrated into permit-to-work system, maintenance planning, contractor management, and training programs.
2. Cross-functional involvement: safety, engineering, operations, maintenance.
3. Risk considerations included in equipment design and modification processes.

Example 2 – Risk: Confined Space Entry in Manufacturing

Structured Approach

1. Hazard identification: oxygen deficiency, toxic gases, engulfment, restricted movement.
2. Risk analysis using standard tools (gas monitoring, entry checklists, PPE assessment).
3. Treatment with engineering controls (forced ventilation), administrative controls (permits), rescue plans, and competency requirements.
4. Periodic review of entry logs and rescue drill outcomes..

Example 3 – Risk: Exposure to Hazardous Chemicals During Mixing/Decanting

Value Creation

1. Automated or controlled chemical handling reduces worker exposure, preventing chemical burns, respiratory issues, and long-term health effects.
2. Improved dosing accuracy enhances product quality and reduces waste, saving money and reducing environmental impact.
3. Fewer incidents mean less downtime and fewer disruptions to operations.

Integration

1. Integrated into procurement (closed-transfer systems, chemical-resistant containers), engineering design, and standard operating procedures.
2. Embedded into training, spill response plans, emergency preparedness, and PPE programs.
3. Included in contractor management and chemical inventory processes (SDS updating, chemical substitutions)..

Example 3 – Risk: Exposure to Hazardous Chemicals During Mixing/Decanting

Structured Approach

1. Hazard identification: splash potential, inhalation of vapours, incompatible mixing, drum over-pressurisation.
2. Analysis: reviewing SDS data, assessing ventilation, evaluating control effectiveness, estimating likelihood and severity.
3. Treatment: engineering controls (local exhaust ventilation, closed-loop transfer), administrative measures (SOPs, batch control), PPE (gloves, goggles, aprons).
4. Monitoring: routine inspections, exposure monitoring, periodic training refreshers, and incident trend analysis.

ISO 31000 – Principles & Framework: Key Takeaways

1. ISO 31000 provides a universal, structured approach for managing risk across any industry.
2. The standard focuses on value creation and protection — risk management supports better decisions and stronger organisational resilience.
3. Effective risk management must be integrated into strategy, operations, culture, and everyday processes.
4. ISO 31000 emphasises a structured and comprehensive method to ensure consistency, transparency, and repeatability.
5. The framework highlights the importance of leadership commitment, clear roles, and continual improvement.

ISO 31000 – Principles & Framework: Key Takeaways

6. The risk management process includes:
   - **Communication & Consultation**
   - **Setting Scope, Context, Criteria**
   - **Risk Assessment** (identify → analyse → evaluate)
   - **Risk Treatment**
   - **Monitoring, Review, Recording & Reporting**
   - Applying ISO 31000 supports safer operations, improved performance, and reduced operational disruptions.

ISO 45001 – OHS Management System

PDCA Cycle (Plan–Do–Check–Act)

Plan

- Identify hazards, assess risks and opportunities.
- Establish OHS objectives and processes aligned with organisational goals.
- Define resources, responsibilities, and documentation requirements.

Do

- Implement the processes and controls defined in the planning stage.
- Provide training, communication, and operational controls.
- Manage contractors, emergency preparedness, change management and competence.

ISO 45001 – OHS Management System

PDCA Cycle (Plan–Do–Check–Act)

Check

- Monitor performance: inspections, audits, incident reports, KPIs.
- Evaluate compliance and effectiveness of controls.
- Involve workers in verifying what is actually happening on the ground.

Act

- Take corrective actions based on monitoring results.
- Address nonconformities and root causes.
- Update systems, improve controls, and strengthen organisational learning.

Emphasize that PDCA never stops — it drives ongoing improvement of the OHS management system.

ISO 45001 – OHS Management System

Leadership Commitment

ISO 45001 places strong emphasis on leadership engagement. Leaders must:

- Demonstrate visible commitment to safety.
- Provide resources and remove obstacles.
- Establish roles and accountability.
- Promote a culture of consultation and participation.
- Leadership isn’t just about signing policies; it’s about active involvement and presence

ISO 45001 – OHS Management System

Worker Participation

Workers must be engaged at all stages, including:

1. Hazard identification and risk assessments.
2. Incident investigations and corrective actions.
3. Development and review of procedures.
4. Safety committees and toolbox talks.
5. ISO 45001 elevates workers from participants to partners in safety.

Integration with Business Processes

An effective OHS management system must be integrated into:

- Strategic planning (risk-based decision-making, budgeting).
- Operational processes (maintenance, procurement, change management).
- Human resources (competence, training, onboarding).
- Performance management (KPIs, audits, review cycles).

ISO 45001 is not a standalone safety program — it is part of the organization's DNA.

What challenges do you foresee in implementing ISO 45001?

1. **Leadership Commitment Gaps**

- Some leaders may see ISO 45001 as “extra work” rather than a strategic advantage.
- Competing business priorities (production, deadlines, cost pressures) may dilute attention on safety.
- Without genuine commitment, workers quickly perceive the system as a “tick-box exercise.”

What challenges do you foresee in implementing ISO 45001?

2. Resistance to Change

- Workers and supervisors accustomed to old habits may resist new procedures.
- “We’ve always done it this way” culture can make implementation slow or superficial.
- Introducing new controls often creates temporary discomfort or adjustment periods.

What challenges do you foresee in implementing ISO 45001?

3. Integration into Business Processes

- Embedding OHS into procurement, HR, maintenance, and project planning can be difficult.
- Some departments may still treat safety as the responsibility of the "H&S team" rather than a shared function.
- Existing systems and documentation may not align with ISO 45001 requirements.

What challenges do you foresee in implementing ISO 45001?

4. Worker Participation Challenges

- Employees may hesitate to speak up due to fear of blame or lack of trust.
- Contractors, temporary staff, and multilingual workforces can complicate communication.
- Engaging night shifts and remote workers is often overlooked.

What challenges do you foresee in implementing ISO 45001?

5. Resource Limitations

- Smaller organisations may lack budget, competent personnel, or time for full implementation.
- High-risk industries often require investment in engineering controls (ventilation, guarding, PPE), which may be costly.
- Training, internal audits, and documentation demand ongoing resources.

What challenges do you foresee in implementing ISO 45001?

6. Documentation and Bureaucracy Perception

- Some employees may view ISO 45001 as paperwork-heavy.
- Excessive documentation can undermine engagement and slow operational processes.
- The challenge is to keep documentation useful and streamlined.

What challenges do you foresee in implementing ISO 45001?

7. Contractor and Supply Chain Compliance

- Many industries rely heavily on contractors whose safety culture varies.
- Ensuring they align with OHS requirements (competency, permits, risk assessments) is a major challenge.
- Supply chains in construction, manufacturing, and logistics can be complex.

What challenges do you foresee in implementing ISO 45001?

8. Maintaining Momentum After Initial Implementation

- Organisations often focus heavily during certification or initial rollout, then lose steam.
- Without continual improvement, audits become crises instead of routine checks.
- Sustaining worker involvement and leadership engagement over time is difficult.

What challenges do you foresee in implementing ISO 45001?

9. Aligning with Production Pressures

- In fast-paced industries, safety may be compromised in favour of output.
- Competing priorities (e.g., tight delivery schedules) may create real-world conflicts.
- ISO 45001 requires balancing safety with business goals — not always easy.

What challenges do you foresee in implementing ISO 45001?

10. Cultural & Communication Barriers

- Multilingual or multicultural workplaces may struggle with consistent understanding of safety expectations.
- Workers may be reluctant to question authority or report unsafe conditions.
- Psychological safety is often overlooked, yet essential.

ISO 45001 – Key Takeaways

1. ISO 45001 provides a structured OHS management system built around the PDCA (Plan–Do–Check–Act) model for continual improvement.
2. Leadership and worker participation are central: safety improves when leaders drive the culture and workers actively contribute.
3. The standard requires integration of OHS into business processes, not treating it as a standalone function.
4. Focuses on risk-based thinking, identifying hazards, assessing risks, and implementing effective operational controls.
5. Promotes a proactive approach to preventing incidents, not just reacting to them.
6. Strengthens organisational resilience by aligning safety with performance, productivity, and strategic objectives.
7. Encourages ongoing monitoring, audits, and corrective actions to refine and improve the system over time.

ILO-OSH 2001 (Occupational Safety and Health Management System)

Key Points

1. International Labour Organization (ILO) framework for safety & health management.
2. Promotes continuous improvement, employer responsibility, and worker participation.
3. Focus on policy → organizing → planning → implementation → evaluation → improvement.
4. Serves as a foundational model for modern OHS management systems.

How It Adds Value

1. Strong emphasis on tripartite participation (employers, workers, government).
2. Provides global baseline principles that align closely with ISO 45001.

ISO 45003 (Psychosocial Risks & Wellbeing)

Key Points

1. First global standard focused on psychosocial risk management.
2. Addresses stress, workload, bullying, harassment, fatigue, remote work risks.
3. Provides guidance for creating a psychologically safe workplace.

How It Adds Value

1. Enhances ISO 45001 by covering non-physical hazards.
2. Encourages organisations to address mental health as part of OHS.
3. Helps integrate wellbeing into organisational culture.

How These Frameworks Complement ISO Standards

Key Integrations

1. **ILO-OSH 2001**

Reinforces worker participation & foundational OHS principles → complements ISO 45001 structure.

2. **ISO 45003**

Expands ISO 45001 by addressing psychosocial hazards and wellbeing → supports comprehensive hazard coverage.

Key Takeaway

Together, these guidelines provide a holistic, complementary ecosystem for managing safety, health, and enterprise risk at all levels

Why These Matter to High-Risk Industries

- Provide a multi-layered approach: physical safety, mental health, and enterprise-level risk.
- Help organisations meet legal, social, and governance expectations.
- Strengthen resilience by integrating OHS into strategy, culture, and operations.
- Create a consistent language across departments (HR, Finance, Operations, Safety).

Which of these guidelines do you think your organisation uses — and where are the gaps?”

- Psychosocial risks?
- Worker participation?
- Risk governance?
- Integration challenges?
- Alignment with existing ISO systems

Application & Integration

How to Combine ISO 31000 and ISO 45001 & Develop Systematic Risk Management Processes

Why Integration Matters

Key Teaching Points

1. ISO 31000 and ISO 45001 share a common risk-based foundation.
2. ISO 31000 provides the enterprise-level risk framework, while ISO 45001 applies it specifically to occupational health and safety risks.
3. Integrating both creates a single, consistent risk approach across the organisation.
4. Helps avoid duplicated processes, mismatched risk criteria, and siloed systems.

ISO 31000 vs ISO 45001

ISO 31000

1. High-level risk management principles & framework
2. Applies to all types of organisational risk
3. Defines risk identification, analysis, evaluation & treatment
4. Focus on strategic and enterprise-wide integration

ISO 45001

1. Management system for occupational health & safety
2. Applies risk management specifically to workplace hazards
3. Includes legal compliance, worker participation, PDCA cycle
4. Integrates OHS into operations & culture

How to Combine ISO 31000 & ISO 45001

Key Integration Points

1. Use ISO 31000 to set organisation-wide risk criteria, applied uniformly across safety, environment, quality, operations, finance.
2. Apply ISO 45001's OHS-specific process within this broader framework.
3. Align hazard identification with ISO 31000's risk identification stage.
4. Ensure risk treatment follows both ISO 31000's options & ISO 45001's hierarchy of controls.
5. Use PDCA from ISO 45001 to drive continual improvement of the integrated system.

Integrated Risk Workflow (Example)

Step-by-step Flow

1. **Define Context (ISO 31000)**
- Organisational objectives, legal requirements, stakeholder needs.
2. **Identify OHS Hazards (ISO 45001)**
- Physical, chemical, psychosocial, ergonomic, biological.
3. **Assess Risks (ISO 31000 + ISO 45001)**
- Likelihood × severity, using shared risk matrices.
4. **Select Treatments (Both Standards)**
- ISO 31000: avoid, reduce, transfer, accept.
- ISO 45001: hierarchy of controls (eliminate → engineering → admin → PPE).
5. **Implement Controls (ISO 45001)**
- Procedures, training, engineering solutions, procurement integration.
6. **Monitor & Review (Both Standards)**
- Incident reporting, audits, KPIs.
6. **Improve (PDCA)**
- Corrective actions → updated risk registers → lessons learned

Creating a Systematic Risk Management Process

1. **Unified risk criteria**– Shared definitions of likelihood, severity, risk appetite.
2. **Standardised risk assessment tools**– Templates, matrices, checklists.
3. **Clear governance structure**– Roles & responsibilities across levels.
4. **Integrated risk registers**– Enterprise + OHS risks in the same system.
5. **Continuous improvement**– Built-in mechanisms for learning, adapting, correcting.

Key Takeaways (Summary)

1. ISO 31000 = enterprise risk framework
2. ISO 45001 = OHS management system
3. Together they create a comprehensive, aligned approach to risk management.
4. Integration reduces duplication and strengthens strategic & operational outcomes.
5. Systematic processes ensure consistency, clarity, and continual improvement.

1. What is the main purpose of ISO 31000?
2. Is ISO 31000 a certification standard?
3. Which ISO standard focuses specifically on occupational health & safety?
4. What is the core continuous improvement cycle behind ISO 45001?

5. In ISO 31000, what are the three key ideas behind effective risk management?
6. What is the first step in the ISO 31000 risk management process?
7. Which standard focuses on psychosocial risks like stress or bullying?
8. What is a key cultural factor that influences risk reporting?

9. What is ISO 45001's view on worker participation?

10. Name one legal expectation common across most OHS regulations.

11. What is the relationship between ISO 31000 and ISO 45001?

12. What is the main advantage of integrating multiple risk standards into one system?

13. What is a common challenge when implementing ISO 45001?

14. Why is documentation required in risk management?

15. Which stage of PDCA involves audits and performance monitoring?

16. What does “context of the organization” refer to in ISO standards?

17. How does culture affect risk management?

18. What is the purpose of a risk register in risk management?

19. In ISO 45001, what is meant by “hierarchy of controls”?

20. What is a common mistake organizations make when assessing risks?

Next: Lecture 14: Risk Management for Emerging Workplace Hazards

Learning Objectives

- Identify emerging workplace hazards (automation, robotics, nanomaterials, remote work ergonomics).
- Understand the risk implications of technological and organizational changes.
- Apply risk assessment methodologies to new and uncertain hazards.
- Develop proactive strategies for integrating emerging risks into existing risk management systems.
- Explore regulatory trends and standards addressing new workplace hazards.