



Inovo Global Safety

Training & Advisory Services



Official Partners: OSH Tree Training & Consultancy Qatar

CSP EXAMINATION PREPARATION

DOMAIN 2

Management Systems

Supplementary Learning Notes

Exam Weight: 25% of Total Score

Covering 14 Core Knowledge Areas

Contents

1.	Compare Performance Against Established Benchmarks.....	5
1.1	The Three-Level Standards Hierarchy	5
1.2	External Pressures Driving Benchmark Adoption	7
1.3	Gap Analysis — Seven-Step Process	7
1.4	Gap Analysis	8
2	Analyze Performance Standards to Determine Plan of Action.....	9
2.1	Performance Standards & Metrics	9
2.2	Five-Step Process.....	10
3	Determine How to Measure, Analyze, and Improve EHS Culture.....	12
3.1	Six Pillars of Safety Culture	12
3.2	Measurement Methods	12
3.3	Analysis Techniques	13
3.4	Culture Improvement Strategies	13
4	Determine Appropriate Incident Investigation Techniques (Root Causes) and Apply Corrective Actions.....	15
4.1	When and What to Investigate	15
4.2	Investigation Techniques Overview.....	15
4.3	Five-Component Approach — Investigation Questions	16
4.4	Investigation Techniques	17
4.5	Investigation Committee Composition	20
4.6	Ten Accident Investigation Mistakes to AVOID.....	20
4.7	Corrective Actions — CAPA and Hierarchy of Controls.....	21
5	Describe the Management of Change Process (Prior, During, and After).....	22
5.1	Core Purpose of MOC.....	22
5.2	Regulatory Basis — 29 CFR 1910.119(l)	22
5.3	Replacement in Kind (RIK) — The Critical Exam Distinction	22
5.4	Motivation for MOC.....	23
5.5	Required Considerations PRIOR to Any Change — 1910.119(l)	23
5.6	Personnel Training and Communication	24
5.7	PSI Update Requirement.....	24
5.8	MOC Linkages with Other PSM Elements	24

5.9	MOC Trigger Categories	25
5.10	Common OSHA-Identified MOC Problems	25
5.11	Three-Phase MOC Framework: Prior, During, After	25
6	Describe System Safety Analysis Techniques.....	30
6.1	Fault Tree Analysis (FTA).....	30
6.2	Failure Mode and Effects Analysis (FMEA) — Slides 64–66.....	34
6.3	Safety Case Approach.....	37
6.4	Risk Summation.....	39
6.5	Comparison Summary	40
7	Evaluate Leading and Lagging Indicators	41
7.1	Leading Indicators by Category	41
7.2	Lagging Indicators by Category	42
7.3	Key Safety Rate Formulas.....	43
7.4	Incident Costs – Compiled Explanation	44
8	Recognize Safety, Health, and Environmental Management and Audit Systems	46
8.1	ISO Standards — Key Distinctions.....	46
8.2	ANSI/ASSP Z10 — US National Standard	47
8.3	Standards Comparison Table.....	48
8.4	The PDCA Cycle — Foundation of All ISO Standards (Slides 14, 104).....	48
9	Applicable Requirements for Plans, Systems, and Policies	50
9.1	Safety & Health Programs	50
9.2	Emergency Action Plan (EAP) 29 CFR 1910.38.....	50
9.3	Fire Prevention Plan — 29 CFR 1910.39	51
9.4	Environmental Plans	51
9.5	OSHA HAZWOPER — 29 CFR 1910.120	51
9.6	ISO 9001, 14001, and 45001 System Requirements.....	51
9.7	Examples and Scenarios.....	52
10	Utilize Document Retention or Management Principles	54
10.1	Core Document Retention Principles	54
10.2	Categories of Records Requiring Retention.....	54
10.3	OSHA Records Retention Schedule	55
10.4	OSHA Forms Distinction	56

10.5	OSHA 3110 — Access to Medical and Exposure Records (29 CFR 1910.1020)	56
10.6	Mandatory Reporting Thresholds	57
10.7	Examples and Scenarios	57
11	Budgeting, Finance, and Economic Analysis Techniques and Principles	59
11.1	Key Financial Concepts	59
11.2	Accident Cost Framework — Heinrich's Iceberg	59
11.3	Return on Investment (ROI)	60
11.4	Budget Development Process	60
11.5	Timeline and Milestone Planning	61
11.6	Cost/Benefit Analysis (CBA)	61
11.7	Role in Procurement Process	61
11.8	Financing Risk Management Options	61
12	Differentiate Management Leadership Techniques	62
12.1	Management & Leadership Styles	62
12.2	Management and Motivation Theories	64
12.3	Management Styles	68
12.4	Workplace Discipline —	69
12.5	Workplace Communication Styles	71
13	Apply Project Management Principles and Techniques	75
13.1	PMBOK Knowledge Areas	75
13.2	Five Project Lifecycle Stages	75
13.3	RACI Chart — Responsibility Assignment Matrix	76
13.4	Project Scheduling Tools	77
13.5	Stakeholder Management – Power/Interest Matrix	79
14	Analyze and/or Interpret Data — Statistics, Exposure, Concentrations, Sampling	80
14.1	Sampling Data	80
14.2	Measures of Central Tendency	81
14.3	Degree of Variation	81
14.4	Normal Probability Distribution	82
14.5	Confidence Intervals	83
14.6	Scientific Calculator — Exam Information	88

DOMAIN 2 — PROGRAM MANAGEMENT

CSP V11.0 Examination Preparation • Exam Weight: 25% • All 14 Blueprint Objectives

1. Compare Performance Against Established Benchmarks

Benchmarking is the continuous, systematic process of comparing an organization's safety, health, and environmental (SHE) performance against reference points that represent excellence, compliance minimum, or industry norms. For the CSP candidate, benchmarking serves four strategic purposes: enabling meaningful comparisons with industry peers and leaders; identifying specific areas for improvement; providing a realistic basis for goal-setting; and supplying objective evidence of progress over time.

1.1 The Three-Level Standards Hierarchy

Level	Examples	Key Characteristic
Level 1 – Regulatory	OSHA (29 CFR), OSHAD (UAE), Health & Safety at Work Act (UK), State/Federal Acts	Legally enforceable. Non-compliance = citations, fines, or criminal liability. These are the MINIMUM requirements.
Level 2 – Consensus	ISO 45001, ISO 14001, ISO 9001, ANSI Standards, BSI Standards	Voluntary but widely adopted. Developed collaboratively through expert consensus. Provide common frameworks internationally.
Level 3 – Implementation	NFPA 70 (NEC), NFPA 101, IEEE Standards, ANSI specific codes	Detailed technical specifications for practical application. Organizations adopt to comply with Level 1 requirements.

Level-1 Regulatory Standards: OSHA, OSHAD, State or Federal Acts of Any Country

Regulatory standards are legally enforceable rules set by governmental bodies to ensure workplace safety and health. Examples include the Occupational Safety and Health Administration (OSHA) in the United States, which sets and enforces safety regulations, and the Occupational Safety and Health Administration of Abu Dhabi (OSHAD) in the UAE, which provides a framework for occupational health

and safety management. State or federal acts across various countries, such as the UK's Health and Safety at Work Act, mandate compliance with safety regulations to protect workers and reduce workplace hazards, ensuring legal accountability for organizations.

Federal regulations under 29 CFR (OSHA) and 40 CFR (EPA) constitute non-negotiable legal obligations. Non-compliance triggers enforcement, citations, and penalties.

- 29 CFR Part 1904 — Recordkeeping and Reporting of Occupational Injuries and Illnesses
- 29 CFR Part 1910 — General Industry Safety and Health Standards
- 29 CFR Parts 1915, 1917, 1918 — Maritime: Shipyards, Marine Terminals, Longshoring
- 29 CFR Part 1926 — Construction Safety and Health Standards
- 29 CFR Part 1928 — Agriculture Standards
- 29 CFR Part 1952 — State Plans (OSHA-approved state-level programmes)

Level 2 — Voluntary Consensus Standards

Consensus standards are developed through a collaborative process involving experts, stakeholders, and organizations to ensure best practices and consistency in various fields. ISO (International Organization for Standardization) provides globally recognized standards, such as ISO 45001 for occupational health and safety management systems. The American National Standards Institute (ANSI) develops standards for various industries in the U.S., while the British Standards Institution (BSI) provides standards for the UK. These standards are voluntary but widely adopted to improve safety, quality, and efficiency, offering a common framework that can be used internationally.

Developed through transparent, consensus-based processes. Frequently adopted by reference into OSHA regulations and treated by courts as evidence of the standard of care. Examples are:

- ISO — Founded 1947 (Geneva). TC 176 was formed in 1979; the ISO 9000 series was first published in 1987, revised in 1994, 2000, 2008, and 2015.
- NFPA — Founded in 1896. 300+ codes/standards. Key: NFPA 01 (Fire Code), NFPA 10 (Portable Extinguishers), NFPA 13 (Sprinkler Systems), NFPA 14 (Standpipe/Hydrant)
- ANSI, ASTM, ASSP — Major US consensus bodies for workplace safety standards

Level 3 — Industry / Company Internal or Implementation Standards

Implementation standards provide detailed guidelines and specifications for the practical application of technologies and practices to ensure safety, reliability, and efficiency. The Institute of Electrical and Electronics Engineers (IEEE) develops standards for electrical and electronic engineering practices. The

National Fire Protection Association (NFPA) sets standards for fire prevention and safety. ISO and ANSI also provide implementation standards across various sectors. These standards ensure consistent application of best practices, enhancing safety and operational efficiency, and are often adopted by organizations to comply with regulatory requirements and industry best practices.

Organization-specific performance targets, SOPs, and trade-association guidelines that set aspirational levels above the regulatory floor and reflect commitment to continuous improvement.

1.2 External Pressures Driving Benchmark Adoption

- Local Community — reputational expectations and social license to operate
- Insurance Companies — premium reductions linked to certified management systems
- Customers/Consumers — supply chain safety requirements (ISO 45001 certification)
- Legal-Regulators — enforcement, litigation, and liability exposure
- Parent Organizations — corporate governance and group-level EHS KPIs
- Employees — right to a safe workplace; union agreements and collective bargaining
- Media — public scrutiny following high-profile incidents

1.3 Gap Analysis — Seven-Step Process

A gap analysis is a structured comparison of current performance against a chosen benchmark, quantifying the delta that drives action planning.

- Step 1: Define the Benchmark — regulatory, consensus, or internal standard
- Step 2: Collect Current Data — incident rates, audit scores, compliance records, observation results
- Step 3: Compare — map actual performance against each benchmark criterion
- Step 4: Identify and Quantify Gaps — calculate the delta in measurable units (TRIR, % compliance)
- Step 5: Priorities by Risk — Severity × Probability × Exposure; highest-risk gaps first
- Step 6: Develop Action Plans — assign owners, timelines, resources, and success metrics
- Step 7: Track and Verify Closure — follow-up audits to confirm gap closure

Scenario — CSP Exam Scenario — Gap Analysis: A petrochemical facility, TRIR = 3.8 vs. industry benchmark = 1.9. Gap = 1.9 per 200,000 hrs. Pareto analysis reveals 80% of incidents in 3 of 12 departments. Priority: targeted BBS observations in the top 3 departments, supervisory leadership training, and a near-miss culture initiative. 6-month milestones with measurable KPIs assigned to department heads (Accountable); CSP as programme owner (Responsible).

1.4 Gap Analysis

A systematic comparison of actual performance against established benchmarks (regulatory, consensus, or implementation standards) to identify deficiencies and prioritize corrective actions.

Gap Analysis Process

1. **Define the benchmark or standard to compare against**
2. Collect current performance data (incident rates, audit scores, compliance records)
3. Compare actual performance to the benchmark
4. Identify and quantify the gaps (shortfalls)
5. Prioritize gaps by risk level (Severity × Probability × Exposure)
6. Develop action plans with owners, timelines, and resources
7. Track progress and verify closure of gaps

Industry Examples

Industry	Benchmark Example	Performance Metric
Manufacturing	Industry TRIR benchmark	Number of lost-time injuries per 100,000 hours worked
Construction	Fall prevention best practices	Frequency of fall-related incidents and injuries
Healthcare	Needlestick rates in top hospitals	Number of needlestick injuries reported per year
Oil & Gas	Hazmat handling practices	Number of spills or releases of hazardous materials

EXAM TIP

Exam questions often test whether you know the **DIFFERENCE** between regulatory (legally enforceable), consensus (voluntary/collaborative), and implementation (technical specifications) standards. Also know key abbreviations: ISO, ANSI, BSI, NFPA, IEEE.

2 Analyze Performance Standards to Determine Plan of Action

Translating performance data into actionable safety plans requires moving systematically from measurement through comparison, gap identification, risk-based prioritization, and corrective action development. The five-step workshop pathway maps directly to the PDCA cycle.

2.1 Performance Standards & Metrics

Performance Metric (Definition)

A specific, quantifiable measure used to evaluate the effectiveness of an organization's safety programs and practices. Metrics ensure that safety goals are being tracked and met.

Types of Performance Metrics

Metric Type	Definition & Examples
Key Performance Indicators (KPIs)	Specific measurable values showing effectiveness of safety objectives – e.g., TRIR, near-miss rates, training completion
Quality Metrics	Measure quality of safety programs – e.g., effectiveness of training, thoroughness of inspections
Efficiency Metrics	Assess resource utilization – e.g., cost per safety initiative, time to resolve safety issues
Effectiveness Metrics	Evaluate outcomes of programs – e.g., reduction in injuries, improvements in safety culture scores

2.2 Five-Step Process

Step 1 — Define Performance Standards

Establish measurable criteria using lagging indicators (TRIR, DART, severity rate); leading indicators (training completion rate, near-miss reporting rate, % planned inspections done); and compliance requirements (citations, audit findings, permit conditions, management system certification targets).

Step 2 — Collect and Compare Data

Review incident rates vs. BLS benchmarks; audit results vs. ISO 45001/ANSI Z10 criteria; inspection findings vs. regulatory checklists; safety observations vs. behavioral targets; trend data over rolling 12–36 month periods. Comparison at the enterprise, facility, department, and task level isolates where performance is deteriorating.

Step 3 — Identify Gaps and Root Causes

Determine where performance falls short and analyze underlying causes using root cause analysis tools: 5 Whys, fishbone diagrams, or change analysis. Categories as: system failures (inadequate procedure), process failures (inadequate control), behavioral failures (non-compliance), or resource failures (inadequate staffing/budget/equipment).

Step 4 — Prioritize Actions Based on Risk

Rank issues using: Severity × Probability × Exposure. Apply Pareto analysis (80/20 rule). Apply Hierarchy of Controls to assess feasibility: Elimination → Substitution → Engineering Controls → Administrative Controls → PPE. Highest-risk, highest-feasibility controls receive first priority.

Step 5 — Develop, Implement, and Track Action Plans

For each prioritized gap: specific control measure (WHAT); responsible owner with authority (WHO); implementation deadline with milestones (WHEN); resources — budget, personnel, equipment (WITH WHAT); success metric for verification (HOW MEASURED). Track through a CAPA system with regular management review.

Key Rate Formulas — Memorize for the Exam

TRIR: $(\text{Total Recordable Incidents} \times 200,000) \div \text{Hours Worked}$

200,000 = 100 workers $\times$ 2,000 hrs/yr — the base for ALL rate calculations in Domain 2.

DART Rate: $(\text{DART Cases} \times 200,000) \div \text{Hours Worked}$

DART = Days Away + Restricted + Transferred cases.

Severity Rate: $(\text{Lost Workdays} \times 200,000) \div \text{Hours Worked}$

Complements TRIR by measuring average severity, not just frequency.

Scenario — Worked Calculation: Company: 320 employees | 640,000 hours | 8 recordable incidents | 2 DART | 45 lost workdays. $\text{TRIR} = (8 \times 200,000) \div 640,000 = 2.5$. $\text{DART} = (2 \times 200,000) \div 640,000 = 0.625$. $\text{Severity Rate} = (45 \times 200,000) \div 640,000 = 14.1$. Action: compare TRIR of 2.5 against BLS benchmark; initiate gap analysis; investigate leading indicators for early warning.

EXAM TIP: 200,000-hour base is the most tested constant. TRIR, DART, and Severity Rate all use the same formula structure — only the numerator changes. Near-miss rate drop = leading indicator warning even when TRIR looks stable.

Reference: Brauer, R.L. (2016). *Safety and Health for Engineers, 3rd Ed., Ch. 36 — Performance Measurement.*

3 Determine How to Measure, Analyze, and Improve EHS Culture

Safety culture is the product of individual and group values, attitudes, competencies, and behavioral patterns that determine the commitment to, and proficiency of, an organization's health and safety programmes. It is distinct from safety climate (current attitudes snapshot) and from the safety management system (structural framework). The CSP exam tests all three concepts.

3.1 Six Pillars of Safety Culture

1. Demonstrated Management Commitment to Safety — leaders visibly model safe behavior; allocate adequate resources; hold themselves to the same standards as workers. Commitment must be observable and consistent, not merely stated in policy.
2. Integrating Safety as an Organizational Value — safety embedded in business strategy, performance reviews, procurement, and project planning; not treated as a separate compliance function.
3. Assuring Accountability at All Levels — defined safety responsibilities cascading from Board to frontline; safety KPIs in performance reviews; fair and consistent consequences for non-compliance.
4. Improved Supervisory Leadership — first-line supervisors are the most critical culture influencers. Training on safety observation, coaching, and feedback is essential for translating management intent into daily worker experience.
5. Empowering and Involving Workers — participative safety management: workers conduct hazard ID, contribute to risk assessments, lead toolbox talks, sit on safety committees. Mandatory requirement under ISO 45001.
6. Clear and Consistent Communication — multi-channel, bidirectional; transparent sharing of safety metrics; near-miss learnings communicated widely; workers know their reports resulted in action.

3.2 Measurement Methods

Quantitative (Survey-Based)

Validated safety culture survey instruments (e.g., NOSACQ-50; Hearts & Minds tool) produce numerical scores across culture dimensions. Statistical analysis identifies patterns, compares departments, and tracks trends over time. Surveys should be anonymous and with guaranteed non-punitive use of results.

Qualitative

Structured interviews with workers and supervisors; focus groups; safety observation tours (management walk-arounds with structured checklists); near-miss reporting rate trend analysis — a declining reporting rate often signals a deteriorating culture even when lagging metrics look stable.

3.3 Analysis Techniques

- Statistical analysis of survey data — identify patterns, strengths, areas for improvement
- Qualitative thematic analysis of interview transcripts — identify recurring concerns
- Benchmarking against industry or national culture survey databases
- SWOT Analysis (Strengths, Weaknesses, Opportunities, Threats) focused on cultural elements
- Correlation analysis — relate culture scores to lagging indicator trends over time

3.4 Culture Improvement Strategies

- Behavior-Based Safety (BBS) programmes — observation, data, feedback, recognition cycles grounded in behavioral psychology (Skinner)
- Apply Deming PDCA to culture improvement: set targets (Plan) → train and intervene (Do) → re-survey and analyze (Check) → adjust strategy (Act)
- SWOT analysis of cultural elements to identify leverage points
- Management safety walk-arounds with structured dialogue — conversation, not inspection
- Recognition programmes for positive safety behaviors (Herzberg motivators)
- Continuously monitor cultural progress through surveys, feedback, and observations.

EXAM TIP: A scenario describing high TRIR + low near-miss reporting + blame culture signals cultural deficiency. Trace symptoms to the six pillars framework. The appropriate intervention is always at the root cultural deficiency, not a poster campaign.

Overview of Safety Management from Chapter 35 of "Safety and Health for Engineers" by Roger L. Brauer

Chapter 35 of "Safety and Health for Engineers" by Roger L. Brauer delves into the comprehensive framework required for effective safety management in engineering environments.

Key Components:

1. **Safety Management Systems (SMS):**
 - The chapter discusses the implementation of structured SMS, integrating processes and procedures to ensure safety compliance and continuous improvement.

2. Hazard Identification and Risk Assessment:

- Emphasizes systematic approaches to identifying potential hazards and assessing risks, utilizing tools like HAZOP (Hazard and Operability Study) and FMEA (Failure Modes and Effects Analysis).

3. Safety Programs and Policies:

- Development and enforcement of safety programs and policies tailored to organizational needs, ensuring alignment with regulatory requirements and best practices.

4. Leadership and Employee Involvement:

- Highlights the critical role of leadership in fostering a safety culture and the importance of engaging employees at all levels to participate in safety initiatives and feedback mechanisms.

5. Training and Competence:

- Importance of ongoing safety training and education to ensure that all employees are knowledgeable about safety procedures, emergency responses, and their roles in maintaining a safe work environment.

6. Incident Investigation and Reporting:

- Procedures for investigating safety incidents and near-misses to determine root causes and implement corrective actions to prevent recurrence.

7. Regulatory Compliance:

- Ensures adherence to local, national, and international safety regulations and standards, such as OSHA (Occupational Safety and Health Administration) requirements in the U.S.

8. Performance Measurement and Continuous Improvement:

- Use of safety performance indicators (KPIs) and regular audits to monitor the effectiveness of safety programs, with a focus on continuous improvement through feedback loops and corrective actions.

9. Integration with Other Management Systems:

- Discusses the integration of safety management with other organizational systems, such as quality and environmental management, to create a holistic approach to risk management.

10. Technology and Innovation:

- Explores the role of new technologies and innovations in enhancing safety measures, such as the use of automation, real-time monitoring systems, and advanced data analytics.

Reference: Brauer, R.L. (2016). *Safety and Health for Engineers, 3rd Ed., Ch. 35 — Safety Culture.*

4 Determine Appropriate Incident Investigation Techniques (Root Causes) and Apply Corrective Actions

Incident investigation is the structured process of determining what happened, why it happened, and what can be done to prevent recurrence. The CSP must distinguish immediate causes (unsafe conditions or acts), contributing factors, and root causes (systemic deficiencies). Investigations stopping at the immediate cause will not prevent recurrence.

4.1 When and What to Investigate

- ALL fatalities and serious injuries — mandatory under OSHA
- ALL recordable injuries and illnesses (29 CFR 1904)
- Near-misses with high potential severity — even with no injury
- Significant property damage, environmental releases, process upsets
- Any event deviating significantly from expected system performance

4.2 Investigation Techniques Overview

Technique	Description & Best Use
5 Whys	Ask 'Why?' 5 times. Simple, quick. Best for straightforward incidents. Finds the root cause by tracing backwards through the causal chain.
Fishbone / Ishikawa Diagram	Visual tool categorizing causes into: People, Process, Equipment, Materials, Environment, Management. Good for complex, multi-cause incidents.
Fault Tree Analysis (FTA)	Top-down, deductive. Starts with the undesired TOP event and works backward using AND/OR logic gates. Calculates probability of failure.
FMEA	Bottom-up, inductive. Identifies all potential failure modes and their effects. Uses $RPN = Severity \times Occurrence \times Detection$ to prioritize.
Event & Causal Factor Charting	Maps the timeline of events and conditions leading to the incident. Good for complex incidents involving multiple sequential factors.
Barrier Analysis	Focuses on physical and procedural barriers that failed to prevent the incident. Identifies WHY the barriers failed.

Technique	Description & Best Use
Change Analysis	Investigates changes in process, equipment, or environment that preceded the incident. Compares 'before change' to 'after change' conditions.
Bow-Tie Analysis	Combines FTA (causes) with event tree (consequences) to visualize risk pathways. Identifies gaps in both preventive and mitigative controls.
Human Factors (HFACS)	Evaluates human error contributions: cognitive, organizational, and environmental. Uses the Human Factors Analysis and Classification System.
Pareto Analysis	80/20 rule – identifies the 20% of causes responsible for 80% of incidents. Displayed as bar chart + cumulative % line.

4.3 Five-Component Approach — Investigation Questions

When structuring investigation questions, use these five component categories:

5 Components – Investigation Question Categories

- Task-Related Questions: What task was being performed? Was the procedure followed? Was the task clearly defined?
- Material-Related Questions: Was the equipment/material defective? Was it the correct material for the job?
- Environment-Related Questions: What were the lighting, noise, and housekeeping conditions? Weather factors?
- Personnel-Related Questions: Was the employee trained? Were they fatigued? Did they have the right PPE?
- Management-Related Questions: Were adequate resources provided? Was supervision adequate? Were procedures enforced?

Task-Related: What task was being performed? Was there a written procedure? Was it followed? Was the task within the worker's authorization?

Material-Related: What materials, chemicals, or equipment were involved? Were they fit for purpose? Were SDS available and accessible?

Environment-Related: What were the physical, chemical, and organizational conditions? Was lighting adequate? Were there time pressures or distractions?

Personnel-Related: What was the worker's training level, experience, and physical state? Was fatigue a factor?

Management-Related: Was supervision adequate? Were procedures current and accessible? Was MOC followed for any recent changes?

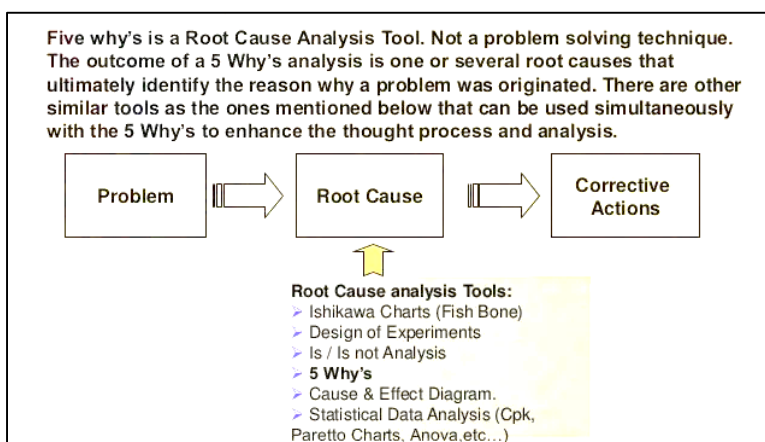
4.4 Investigation Techniques

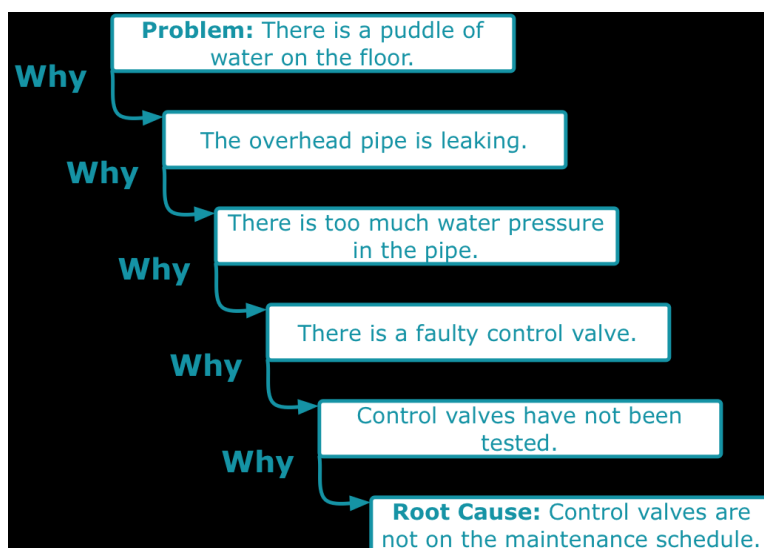
5 Whys — Sequential Root Cause Method

Begin with the immediate cause and ask "Why?" sequentially — typically 5 times — until a systemic root cause is revealed. Best for simple, single-pathway failure chains.

Classic Example: Machine Stoppage

Step	Answer	Level
Problem	Machine stopped working	
Why 1	The motor stopped running	Symptom
Why 2	The motor overheated	Symptom
Why 3	The cooling fan failed	Immediate cause
Why 4	The fan was not maintained properly	Contributing cause
Why 5 (Root)	There is no scheduled maintenance plan	ROOT CAUSE → Fix this!





Scenario — Classic 5 Whys Example — Laceration Incident:

Why did the laceration occur? → Guard was missing.

Why was it missing? → Removed for cleaning.

Why was there no LOTO procedure? → Task was not covered by the LOTO programme.

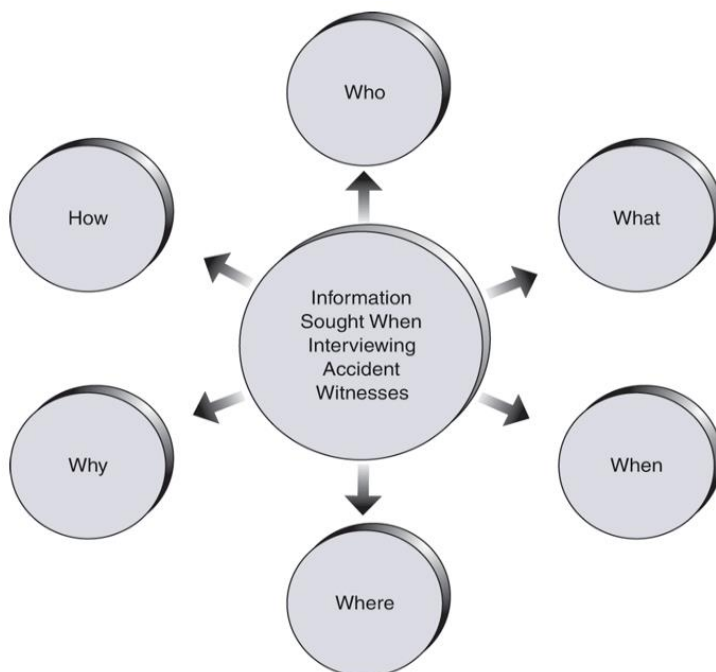
Why was it excluded? → MOC was not followed when the task was modified.

Why was MOC not followed? → No MOC awareness training for maintenance staff.

ROOT CAUSE: Systemic failure in change management and training programme.

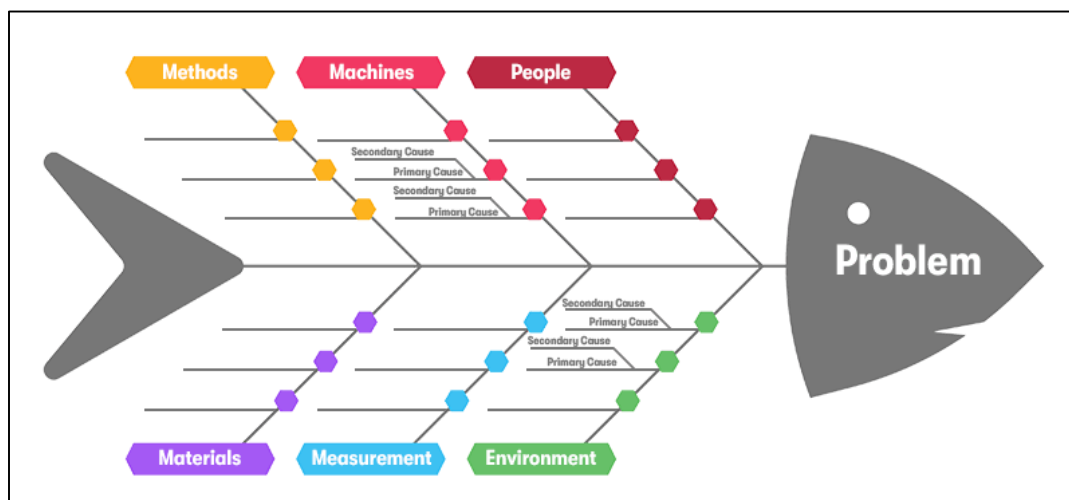
Witness Interview Framework (5W + 1H)

Question	What to Investigate
WHO	All individuals involved in or witness to the incident
WHAT	The events, actions, and conditions at the time of the incident
WHEN	Exact timing of the incident and related preceding events
WHERE	The precise location and environmental conditions
WHY	The reasons behind the decisions and actions taken
HOW	The manner in which the incident unfolded step-by-step



Fishbone / Ishikawa Diagram

Maps contributing factors across six categories (6Ms): Man, Machine, Method, Material, Measurement, Mother Nature (Environment). The incident is the "head"; categories are "bones"; specific causes are "sub-bones". Ideal for complex, multi-causal incidents.



Fault Tree Analysis — for Investigation

Top-down, deductive: start with the incident (top event) and work backward through logic gates to identify minimal combinations of failures (minimal cut sets) that caused it. Quantitative extension calculates the probability of recurrence.

Change Analysis

Compares pre-incident conditions vs. post-incident conditions to isolate changes that contributed to the incident. Particularly powerful when MOC failure is suspected.

4.5 Investigation Committee Composition

- Workers with direct knowledge of the task and work area
- Safety committee representatives from the safety oversight group
- Union representative (where applicable)
- Experienced accident investigators with relevant technical expertise
- Outside specialists and expert consultants as required
- Local government or regulatory representative as required by regulation or severity

EXAM TIP

The CSP exam may present an incident scenario and ask which investigation technique is MOST appropriate, or which step should come FIRST. Remember: Secure the scene and preserve evidence BEFORE interviewing witnesses.

Why Incidents Are NOT Reported

- Red tape — complex, time-consuming reporting processes discourage reporting
- Ignorance — lack of knowledge about what must be reported
- Embarrassment — fear of personal shame or peer judgement
- Record-spoiling — desire to protect the organization's or team's safety metrics
- Fear of repercussions — anxiety about being blamed or disciplined
- No feedback — perception that reporting generates no meaningful action

4.6 Ten Accident Investigation Mistakes to AVOID

1. Failing to investigate near-misses — lost prevention opportunities
2. Ineffective action — not identifying and fixing the root cause
3. Allowing personal biases to influence findings
4. Failing to investigate promptly — evidence degrades quickly
5. Failing to account for human nature during witness interviews

6. Failing to learn proper investigation techniques before investigating
7. Allowing organizational politics to compromise objectivity
8. Failing to conduct an in-depth investigation — stopping at the surface causes
9. Allowing conflicting goals (production vs. safety) to compromise thoroughness
10. Failing to account for the effects of uncooperative witnesses or management

4.7 Corrective Actions — CAPA and Hierarchy of Controls

Each identified root cause requires a corrective action that eliminates or controls the root cause, not just the symptom. Apply the Hierarchy of Controls: Elimination → Substitution → Engineering Controls → Administrative Controls → PPE. Assign owner, deadline, verification method, and effectiveness criteria. Follow up to confirm implementation and validate effectiveness.

Reference: Brauer, R.L. (2016). *Safety and Health for Engineers, 3rd Ed., Ch. 13 — Accident Investigation.*

5 Describe the Management of Change Process (Prior, During, and After)

Management of Change (MOC)

A formal, systematic process to evaluate and manage safety, environmental, and operational risks associated with any modifications to processes, equipment, technology, procedures, personnel, or facilities — ensuring no unintended hazards are introduced.

Management of Change (MOC) is a systematic process to evaluate and properly manage any modification to the design, control, or operations — including staffing — of a covered process before the change is implemented. The OSHA PSM standard preamble states this is "one of the most important and necessary aspects" of a PSM programme. MOC is among the most heavily tested PSM elements on the CSP exam.

5.1 Core Purpose of MOC

- Assure no unintended hazards are introduced into the process
- Assure risks are properly evaluated and minimized before implementation
- Keep current: process safety information (PSI), hazard analyses, operating procedures, training, mechanical integrity, pre-startup safety review
- Be completed BEFORE any change is implemented — OSHA requirement, not optional

5.2 Regulatory Basis — 29 CFR 1910.119(l)

The PSM standard requires: "The employer shall establish and implement written procedures to manage changes (except replacement in kind) to process chemicals, technology, equipment, and procedures and changes to facilities that affect a covered process."

5.3 Replacement in Kind (RIK) — The Critical Exam Distinction

OSHA 1910.119(b) defines RIK as "a replacement which satisfies the design specification." CCPS defines RIK as "an identical replacement or any other alternative specifically provided for in the design specification, as long as the alternative does not in any way adversely affect the function or safety of the item or associated items." Any deviation from design specification — material, capacity, operating conditions, or function — requires full MOC.

Scenario	Description	Action Required
Example RIK	Replacing a failed pump with an IDENTICAL model (same specs, materials, performance)	MOC NOT required — but document it
Example Change (NOT RIK)	Replacing a failed pump with a higher-capacity model or different material	FULL MOC REQUIRED
CCPS Guidance	Even RIK replacements require verification and documentation to maintain process safety integrity	Review process still needed

📌 EXAM TIP

Remember: MOC must be completed BEFORE changes are implemented. RIK does not trigger MOC but MUST be documented. The PSM standard (1910.119) applies to highly hazardous chemicals.

EXAM TIP: RIK vs. MOC is a classic CSP exam trap. Same model pump = RIK. Different capacity, material, or pressure rating = MOC. Your MOC programme should document specific RIK examples to prevent field confusion.

5.4 Motivation for MOC

- No plant or system is ever static — systems change continuously throughout their lifecycle
- A malfunctioning MOC programme directly and measurably increases process risk
- MOC is easily short-changed in the normal operational rush — a documented root cause of major incidents
- Regulatory requirement under OSHA 1910.119(l) — non-compliance is a PSM citation

5.5 Required Considerations PRIOR to Any Change — 1910.119(l)

- Technical basis for the proposed change: motivation/need, required work scope, design details, engineering calculations
- Impact on safety and health: how will the change affect personnel safety? Does it trigger a requirement for a new or updated PHA?
- Modifications to operating procedures: Do SOPs, MI inspection intervals, or PSSR checklists need updating? Updates must be completed before the restart.

- Necessary time period: distinguish temporary (fixed time limit + management system to prevent overrun), permanent (implementation timeline), and emergency changes (streamlined approval + full documentation post-emergency)
- Authorization: appropriate safety, engineering, and management personnel must review and formally sign off before implementation

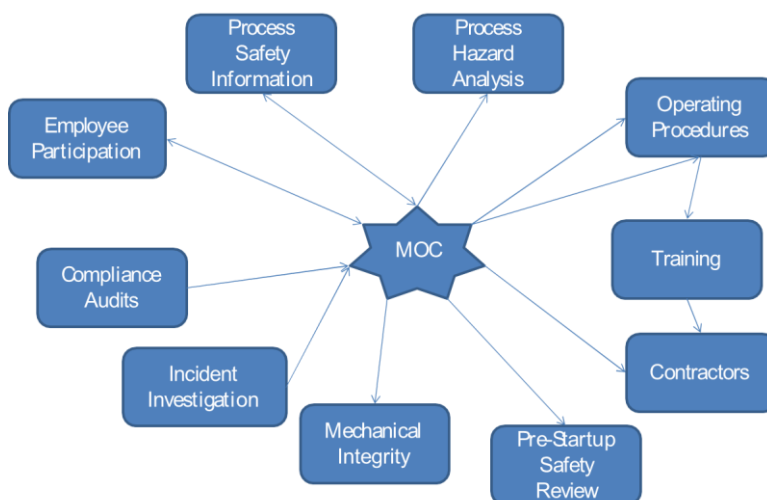
5.6 Personnel Training and Communication

Under 1910.119(l)(3): employees involved in operating a process and maintenance/contract employees whose tasks will be affected by a change must be informed of and trained in the change before startup of the changed process.

5.7 PSI Update Requirement

Under 1910.119(l)(4): if a change results in a change to process safety information (P&IDs, process flow diagrams, equipment specs, operating limits), such information must be updated accordingly.

5.8 MOC Linkages with Other PSM Elements



- Process Safety Information — must be updated when changed
- Process Hazard Analysis — triggered when change introduces new hazards
- Operating Procedures — must be revised before training and startup
- Training — must be completed before the changed process restarts
- Mechanical Integrity — inspection/test procedures may need updating
- Employee Participation — workers must be consulted on changes affecting their tasks
- Contractors — contract workers affected by changes must be informed and trained
- Pre-Startup Safety Review (PSSR) — required before starting any changed process

- Incident Investigation — MOC failures are frequently identified as root causes
- Compliance Audits — verify the MOC programme is being effectively implemented

5.9 MOC Trigger Categories

- PHA recommendations, incident investigation findings, compliance audit findings
- Addition of new process lines or production capacity
- Revisions to staffing levels or organizational structure (budget cuts, mergers, acquisitions, reorganizations)
- Changes to facility layout or infrastructure
- Programming changes to control systems (DCS, PLC, SIS)
- New contractor service agreements affecting covered processes
- Operational upsets (process operating outside normal parameters)

Scenario — Staffing MOC Example (Slide 36): Plant XYZ reduces refrigeration operators due to budget cuts. A full MOC is required to evaluate: whether SOPs require modification; whether the staffing reduction affects safe operation or emergency response capability; and what additional engineering controls may be needed to compensate for the loss of human oversight.

Scenario — Budget Cut MOC Example (Slide 37): Plant ABC reduces maintenance budget by 25%. MOC required to evaluate the impact on PM frequencies, mechanical integrity inspection/test schedules, and whether deferring PMs creates unacceptable risk. Engineering justification for reductions must be documented.

5.10 Common OSHA-Identified MOC Problems

- Written MOC programme not developed
- MOC process not used in practice to manage actual changes
- Authorization signatures missing — approvals not documented
- Overuse of "emergency" MOC designation to bypass full review
- No follow-through — P&IDs, procedures, and training records not updated after the change

5.11 Three-Phase MOC Framework: Prior, During, After

Phase 1 — PRIOR to Change

- Conduct risk assessment: HAZOP, What-If Analysis, or Checklist-based PHA
- Develop change management plan: scope, objectives, responsibilities, schedule
- Document technical basis: engineering rationale and calculations
- Evaluate impact on safety, health, and environmental compliance
- Update PSI before proceeding; obtain formal authorization
- Identify and schedule training for all affected personnel

Phase 2 — DURING Change

- Apply protective controls throughout implementation
- Monitor continuously for unexpected hazards or deviations from the approved plan
- Train affected employees on new procedures, equipment, or roles
- Document any deviations from the approved plan for review and analysis

Phase 3 — AFTER Change

- Pre-Startup Safety Review (PSSR): verify all safety measures in place before restart
- Verify all training is completed and documented before process startup
- Update all procedures, P&IDs, and PSM documents to reflect the change as implemented
- Close all punch-list items; monitor post-implementation KPIs
- Document lessons learned: what worked, what to improve in the MOC process

Summary OSHA 1910.119(I) – Management of Change (MOC)

OSHA 1910.119(I) refers to the **Management of Change (MOC)** requirements within the OSHA Process Safety Management (PSM) standard, specifically addressing the need for procedures to manage changes to processes, chemicals, technology, equipment, facilities, and procedures that could affect safety.

Key Components of OSHA 1910.119(I):

1. Written Procedures:

- Employers must develop and implement written procedures for managing changes to ensure safety is maintained.

2. Technical Basis for Change:

- The technical reasons for changes must be documented, providing a clear justification for the alteration.

3. Impact Assessment:

- The impact of the proposed change on health and safety must be assessed, considering potential hazards introduced by the change.

4. Modifications to Operating Procedures:

- Any changes to operating procedures must be updated and communicated to employees.

5. Authorization of Change:

- The change must be reviewed and authorized by appropriate personnel before implementation.

6. Informing and Training Employees:

- Employees affected by the change must be informed and trained on the new procedures or equipment.

7. Updating Process Safety Information (PSI):

- Process Safety Information must be updated to reflect any changes in chemicals, technology, or equipment.

8. Pre-Startup Safety Review (PSSR):

- If a change is significant, a PSSR must be conducted to ensure that all safety measures are in place before the process starts or resumes operation.

Importance:

OSHA 1910.119(l) is critical for preventing incidents caused by poorly managed changes. It ensures that changes in process conditions or equipment do not introduce new hazards or increase existing risks, thereby protecting workers and maintaining process integrity.

Application:

This standard is applicable to industries handling highly hazardous chemicals, including chemical manufacturing, petrochemicals, pharmaceuticals, and any other sectors that require stringent control over process changes to ensure safety.

By adhering to OSHA 1910.119(l), companies can maintain compliance, enhance safety, and prevent accidents related to changes in process conditions or equipment.

Summary OSHA 1910.119(b) – Process Safety Information (PSI)

Overview: OSHA 1910.119(b) is a crucial element of the Process Safety Management (PSM) standard, requiring employers to compile and maintain detailed process safety information (PSI) before conducting process hazard analyses (PHAs). This information provides the foundation for identifying and understanding the hazards associated with the processes involving highly hazardous chemicals.

Key Components:

1. Hazardous Chemicals Information:

- Employers must document information on the hazardous chemicals used, including:
 - Toxicity
 - Permissible exposure limits (PELs)
 - Physical and chemical characteristics
 - Reactivity data
 - Corrosivity data
 - Thermal and chemical stability
 - Hazardous effects of inadvertent mixing of different materials.

2. Technology Information:

- The PSI must include technology-related data, such as:
 - Block flow diagrams or simplified process flow diagrams.
 - Process chemistry and its effects on safety.
 - Maximum intended inventory of chemicals.
 - Safe upper and lower limits for such variables as temperatures, pressures, flows, or compositions.
 - An evaluation of the consequences of deviations, including those affecting safety and health.

3. Equipment Information:

- Information on the equipment used in the process, including:
 - Materials of construction.
 - Piping and instrumentation diagrams (P&IDs).
 - Electrical classification.
 - Relief system design and design basis.
 - Ventilation system design.

- Design codes and standards employed.
- Material and energy balances for the process.
- Safety systems (e.g., interlocks, detection, and suppression systems).

Importance:

This section ensures that employers have a comprehensive understanding of the chemicals, technology, and equipment involved in their processes. It serves as a critical foundation for conducting effective process hazard analyses, implementing safety measures, and ensuring regulatory compliance.

Application:

OSHA 1910.119(b) applies to industries handling highly hazardous chemicals, ensuring that detailed and accurate process safety information is readily available to guide safety management efforts and reduce the risk of catastrophic incidents. This information must be kept up-to-date and accessible to employees and others involved in maintaining process safety.

6 Describe System Safety Analysis Techniques

System safety analysis applies engineering and analytical methods to identify, evaluate, and control hazards throughout a system's lifecycle. The CSP must know key techniques, their distinguishing characteristics, and appropriate application contexts.

6.1 Fault Tree Analysis (FTA)

FTA

A top-down, deductive analytical method used to identify all possible causes of an undesired event (top event) by mapping logical relationships between events using Boolean logic gates (AND/OR).

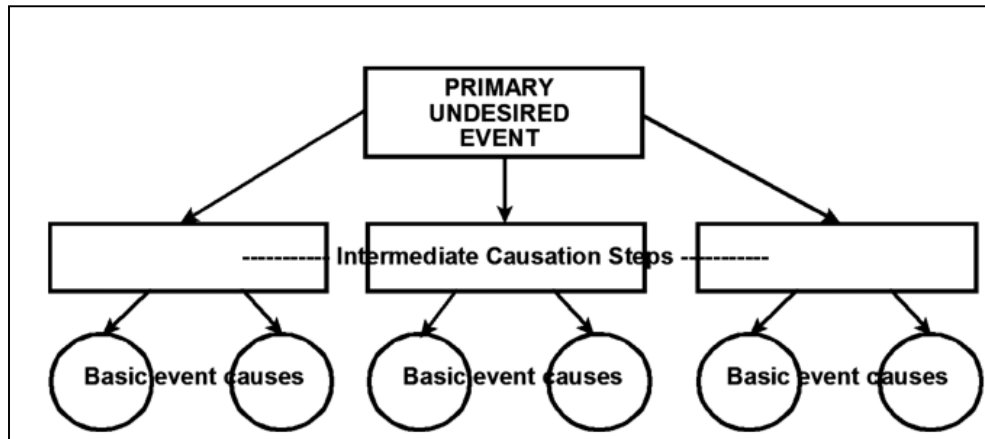
FTA is a top-down (deductive) analytical technique. Beginning with an undesired top event, the analyst works downward through a logic structure to identify the combinations of failures that can produce that event. Core question: "What caused this?"

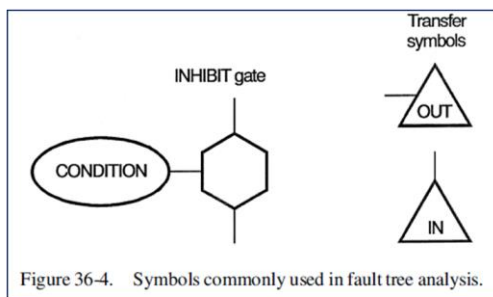
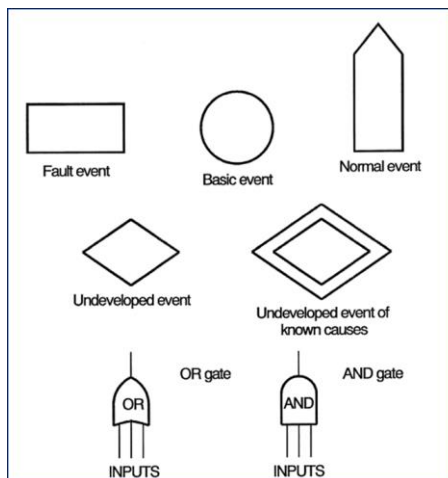
Key Characteristics

- Approach: Top-Down (deductive) — starts with failure, works backward to causes
- Uses logic gates: AND gate (all inputs must occur), OR gate (any one input sufficient)
- Quantitative: Can calculate probability of the top event occurring
- Output: Visual fault tree diagram with cut sets identifying critical failure combinations

Applications

- Aerospace, nuclear power, chemical processing, oil & gas facilities
- Investigating the causes of a specific accident or unwanted event
- Calculating probability of system failure for risk quantification





FTA Structure and Rules

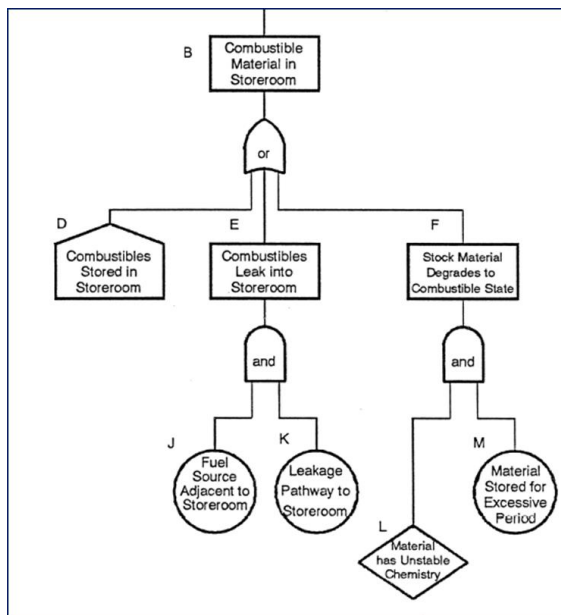
- Top Event: the undesired event being analyzed
- Intermediate Events: system failures contributing to the top event
- Basic Events (Root Causes): lowest-level events with available failure rate data
- AND Gate: ALL inputs must occur simultaneously → Probability = $P_1 \times P_2$ (multiply)
- OR Gate: ANY single input is sufficient → Probability $\approx P_1 + P_2$ (add)
- FTA Rules: No gate-to-gate connections; work level by level downward

FTA — OR Gate Probability: $P(A \text{ OR } B) \approx P(A) + P(B)$

Valid for small probabilities (rare events). More precisely: $P(A \cup B) = P(A) + P(B) - P(A \cap B)$.

FTA — AND Gate Probability: $P(A \text{ AND } B) = P(A) \times P(B)$

Assumes statistical independence of basic events.



Example 36-1 For the fault tree in Figure 36-5, the probabilities for some of the events are as follows:

Event	Probability for Events (frequency in days)
D	3.45×10^{-7}
J	6.89×10^{-4}
K	7.33×10^{-3}
L	6.05×10^{-3}
M	1.88×10^{-4}

What is the most likely cause for event B?

The probability for event D is given. The probability for event E is

$$P(J) \times P(K) = (6.89 \times 10^{-4}) (7.33 \times 10^{-3}) \\ = 5.05 \times 10^{-6}$$

The probability for event F is

$$P(L) \times P(M) = (6.05 \times 10^{-3}) (1.88 \times 10^{-4}) \\ = 1.137 \times 10^{-6}$$

Inovo Global Training & Advisory Services

Analogy with Reliability

• Series Reliability (OR)

▫ Add Failure Probability

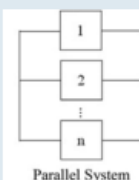
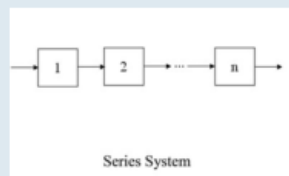
$$R_{\text{system}} = R_1 \times R_2 \times \dots \times R_n$$

• Parallel Reliability (AND)

• Multiply Failure Probability

$$R_{\text{system}} = 1 - (1 - R_1)(1 - R_2) \dots (1 - R_n)$$

Probability of Failure $P_i = (1 - P_s)$



Reliability Analogy

- Series system (OR gate logic): failure of ANY component causes system failure → Add probabilities
- Parallel system (AND gate logic): ALL components must fail for system failure → Multiply probabilities

Cut Sets and Minimal Cut Sets

A cut set is a set of basic events that, if they all occur, cause the top event. A minimal cut set (MCS) is the smallest combination sufficient to cause system failure — no event can be removed without losing that ability. MCSs identify the weakest points (SPFs) in a system and guide control priorities.

FTA Limitations

- Completeness depends entirely on analyst knowledge — missed events create blind spots
- Difficult to apply early in design when failure modes are not yet understood
- Assigning valid failure probabilities requires high-quality failure rate data — often unavailable
- Complex systems produce extremely large fault trees, difficult to analyze manually

6.2 Failure Mode and Effects Analysis (FMEA) — Slides 64–66

FMEA

A systematic, bottom-up inductive approach that identifies all potential failure modes of system components, analyzes their effects on system performance, and prioritizes risks for mitigation.

FMEA is a bottom-up (inductive) technique. Beginning with individual component failure modes, the analyst traces effects upward through the system. Core questions: "What can fail?" and "How can it fail?"

FMEA is primarily proactive — used during design review to prevent failures.

- Approach: inductive (component → system) — opposite direction to FTA
- Presented in spreadsheet format: one row per failure mode; scope must be defined clearly
- Risk Priority Number (RPN) = Severity × Occurrence × Detection
- FMECA extends FMEA with criticality ranking for higher-priority failure modes

Key Characteristics

- Approach: Bottom-Up (inductive) — starts with component failures, assesses system effects
- Risk Priority Number (RPN) = Severity × Occurrence × Detection
- Higher RPN = higher priority for corrective action
- Used proactively during design review to prevent failures

FMEA Factor	Definition
Severity (S)	How serious is the effect? (1-10 scale, 10 = catastrophic)
Occurrence (O)	How likely is the failure mode to occur? (1-10 scale, 10 = almost certain)
Detection (D)	How likely is the failure to be detected before causing harm? (1-10, 10 = cannot detect)
RPN	Severity × Occurrence × Detection — prioritizes which failure modes to address first

FAILURE MODE AND EFFECTS ANALYSIS								
System		Subsystem		Date	Analyst		Page	
Component or Part Name & Description	Failure Mode	Cause of Failure	Effect on...			Risk or Hazard Category	Probability of Effect	Comments
			Other Components	System	Personnel			

Process Step	Potential Failure Mode	Potential Failure Effect	SEV ¹	Potential Causes	OCC ²	Current Process Controls	DET ³	RPN ⁴	Action Recommended
What is the step?	In what ways can the step go wrong?	What is the impact on the customer if the failure mode is not prevented or corrected?	How severe is the effect on the customer?	What causes the step to go wrong (i.e., how could the failure mode occur)?	How frequently is the cause likely to occur?	What are the existing controls that either prevent the failure mode from occurring or detect it should it occur?	How probable is detection of the failure mode or its cause?	Risk priority number calculated as SEV x OCC x DET	What are the actions for reducing the occurrence of the cause or for improving its detection? Provide actions on all high RPNs and on severity ratings of 9 or 10.
ATM Pin Authentication	Unauthorized access	• Unauthorized cash withdrawal • Very dissatisfied customer	8	Lost or stolen ATM card	3	Block ATM card after three failed authentication attempts	3	72	
	Authentication failure	Annoyed customer	3	Network failure	5	Install load balancer to distribute work-load across network links	5	75	
Dispense Cash	Cash not disbursed	Dissatisfied customer	7	ATM out of cash	7	Internal alert of low cash in ATM	4	196	Increase minimum cash threshold limit of heavily used ATMs to prevent out-of-cash instances
	Account debited but no cash disbursed	Very dissatisfied customer	8	• Transaction failure • Network issue	3	Install load balancer to distribute work-load across network links	4	96	
	Extra cash dispensed	Bank loses money	8	• Bills stuck to each other • Bills stacked incorrectly	2	Verification while loading cash in ATM	3	48	

1. **Severity:** Severity of impact of failure event. It is scored on a scale of 1 to 10. A high score is assigned to high-impact events while a low score is assigned to low-impact events.
 2. **Occurrence:** Frequency of occurrence of failure event. It is scored on a scale of 1 to 10. A high score is assigned to frequently occurring events while events with low occurrence are assigned a low score.
 3. **Detection:** Ability of process control to detect the occurrence of failure events. It is scored on a scale of 1 to 10. A failure event that can be easily detected by the process control is assigned a low score while a high score is assigned to an inconspicuous event.
 4. **Risk priority number:** The overall risk score of an event. It is calculated by multiplying the scores for severity, occurrence and detection. An event with a high RPN demands immediate attention while events with lower RPNs are less risky.

Example:

RPN: Severity (1–10) × Occurrence (1–10) × Detection (1–10)

Maximum RPN = 1,000. Highest RPN values receive first corrective action priority.

EXAM TIP: FTA = Top-Down (Deductive). FMEA = Bottom-Up (Inductive). This distinction is tested repeatedly. FTA: "What caused this top event?" FMEA: "If this component fails, what happens to the system?"

6.3 Safety Case Approach

Safety Case

A structured argument, supported by evidence, that a system is acceptably safe for a given application in a specific environment. Produces a comprehensive, auditable safety assurance document.

A Safety Case is a structured argument, supported by documented evidence, that a system is acceptably safe for a given application in a given environment. It is goal-based — not checklist-based. Required by regulatory bodies in high-consequence industries.

- Used where regulatory bodies require a formal demonstration of safety (railways, defense, nuclear)
- Documents safety analysis, design decisions, operational procedures, and assurance activities
- Provides an auditable trail of how safety has been systematically achieved

Key Elements

- Claim: the safety property being asserted (e.g., "The warning light operates safely")
- Argument: the logical reasoning explaining WHY the claim holds
- Evidence: documented proof — FTA results, test data, failure rate calculations, inspection records
- Context and Assumptions: the boundaries within which the claim is valid

Safety Case vs. Compliance

Compliance approach: "We followed the rules." Safety Case approach: "We proved it is safe." The Safety Case is structured, explicit, auditable, and goal-oriented — it demonstrates safety rather than assuming it from regulatory adherence.

Industries Requiring Safety Cases

- Aviation — regulatory certification of new aircraft types and modifications
- Railways — infrastructure change approval and periodic safety reviews
- Nuclear — new plant licensing and periodic safety reports
- Automotive — ISO 26262: functional safety of road vehicles
- Medical devices — FDA and CE marking for high-risk devices

Goal Structuring Notation (GSN)

GSN is a visual language for representing safety cases.

Goal (G) = a safety claim; Strategy (S) = how the claim is argued;

Evidence (E) = proof (FTA, test reports, calculations);

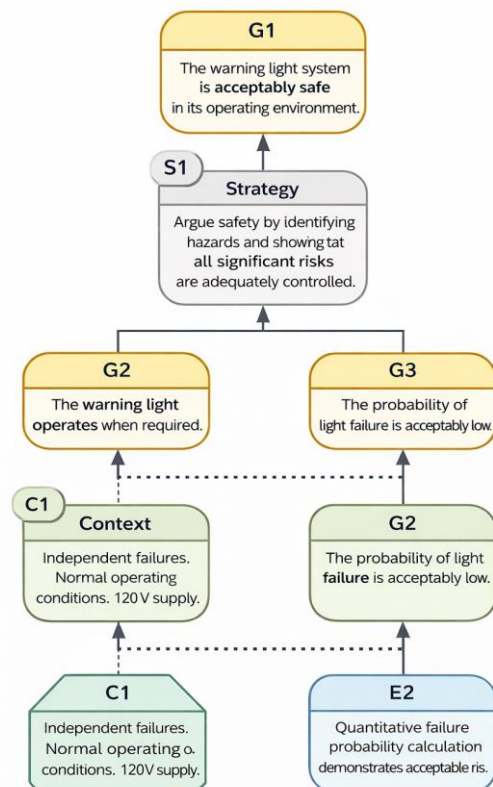
Context (C) = assumptions and environmental boundaries.

GSN allows every safety claim to be traced to its supporting evidence transparently.

Example: Warning Light System

- Claim: The warning light operates safely
- Hazard: Light fails to warn operator
- Risk: Operator unaware of fault
- Mitigation: Redundant switches, reliable power
- Evidence: Fault Tree Analysis, test results

GSN Example: Warning Light Safety Case



6.4 Risk Summation

Risk Summation

Aggregation of individual risks to understand the total (cumulative) risk posed by a complex system. Considers probability, severity, and exposure across multiple interacting risk factors.

Risk summation aggregates individual risk estimates across all hazard sources within a facility. By summing individual risk contributions, decision-makers can assess the cumulative risk profile, compare it against tolerability criteria (ALARP — As Low As Reasonably Practicable), and prioritize safety investment at the portfolio level. Used in process industries, oil and gas, and large-scale infrastructure.

- Used in process industries, oil & gas, and large-scale infrastructure with many interacting risks
- Enables decision-makers to assess cumulative risk and prioritize safety investments
- Supports enterprise-level risk management and portfolio-level decision making

Logical Process Risk Analysis

Frank and Morgan¹⁹ proposed a systematic method for helping managers allocate funds to achieve the greatest risk reduction across several departments within a plant. The method is also useful to compare several plants and allocate funds to each. The procedure applies risk concepts. The authors developed the method for chemical processing plants. The method involves six steps:

1. Compute a risk index for each department.
2. Determine relative risk for each department.
3. Compute the percentage risk index for each department.
4. Determine composite exposure dollars for each department.
5. Compute a composite risk for each department.
6. Rank all departments relative to each other based on composite scores.

Example 34-3 Six departments in a plant seek money to improve process safety. The company elects to use logical process risk analysis as a guide for allocating funds. The goal is to reduce potential losses. The company completes analysis for each department to determine hazard scores, control scores and exposure dollars. Table 34-10 presents the data. The company ranks departments based on the data. Table 34-11 presents the results.

TABLE 34-10 Data for Example 34-3

Exposure Dept	Hazard Score	Control Score	Property Value (\$ × 1000)	Business Interruption Cost (\$ × 1000)	Personnel Value (\$ × 1000)	Composite Exposure Dollars
A	257	304	2900	1400	900	5200
B	71	239	890	1200	653	2743
C	181	180	1700	720	1610	4030
D	152	156	290	418	642	1350
E	156	142	520	890	460	1870
F	113	336	2910	3100	1860	7870

Our Solution (Excel-based):

Departments	Hazard Score (HS)	Control Score (CS)	Dollar Exposure	Risk Index	Relative Risk	%Risk Index	Composite Exposure	Rank
A	257	304	5200	47	-176	19.32	1004.61	1
B	71	239	2743	168	-55	6.04	165.60	5
C	181	180	4030	-1	-224	24.59	990.91	2
D	152	156	1350	4	-219	24.04	324.53	4
F	156	142	1870	-14	-237	26.02	486.49	3
E	113	336	7870	223	0	0.00	0.00	6
					-911	100		
					Total			

Formula:

Risk Index= CS-HS

Relative Risk= Relative Index (RI) – RI_{max}

%Risk Index (RI)= (RI/RI_{Total})×100 %

Composite Exposure= Dollar Exposure×%RI

Reference: Brauer, R.L. (2016). *Safety and Health for Engineers, 3rd Ed., Ch. 10 — System Safety Analysis.*

6.5 Comparison Summary

Technique	Key Features	Primary Application
FTA	Top-down deductive; probability calculation; logic gates; specific failure	Aerospace, nuclear, chemical
FMEA	Bottom-up inductive; RPN = S×O×D; design review; component-level	Manufacturing, automotive, medical
Safety Case	Structured safety argument with evidence; regulatory compliance document	Railways, defense, nuclear
Risk Summation	Cumulative/portfolio risk; aggregates multiple risk factors	Process industries, infrastructure

EXAM TIP

KNOW: FTA is top-down and deductive. FMEA is bottom-up and inductive. RPN formula = Severity × Occurrence × Detection. Safety Case is used when regulators require a formal safety argument.

7 Evaluate Leading and Lagging Indicators

Leading Indicators

Proactive, preventive measures that predict and help reduce the likelihood of future incidents. They measure inputs and activities — things you DO to prevent incidents.

Lagging Indicators

Reactive, outcome-based measures that reflect past performance. They measure incidents or issues that have already occurred — the results of the system's outputs.

Performance measurement using both leading and lagging indicators is the CSP's primary mechanism for evaluating programme effectiveness, communicating safety status to leadership, and detecting deteriorating trends before they result in injuries. Rate calculation is consistently one of the highest-frequency quantitative skill areas on the CSP exam.

7.1 Leading Indicators by Category

Category	Examples	Character
Safety	Training completion rates; inspection frequency; near-miss reports submitted; JSA completion; stop-work authority use	Proactive – predict performance
Health	Employee participation in wellness programs; ergonomic improvement implementations; health screening frequency	Preventive – reduce illness
Environmental	Waste recycling/reduction %; energy consumption monitoring; proactive compliance audits conducted	Proactive – prevent violations
Security	Security drill frequency; breaches prevented; access control implementation; security training completion	Proactive – reduce incidents

- Near-miss and hazard reporting rate — most valuable predictive leading indicator
- Percentage of planned safety observations completed by supervisors
- Safety training completion rate (% of required training current)
- Percentage of corrective actions closed within the target date
- Management safety walk-around frequency and quality score
- Percentage of scheduled inspections/audits completed on time
- JSA/Risk Assessment completion rate for new or modified tasks

7.2 Lagging Indicators by Category

Category	Examples	Character
Safety	TRIR (Total Recordable Incident Rate); LTIFR (Lost Time Injury Frequency Rate); DART rate; fatal incidents	Reactive – measures past outcomes
Health	Occupational illnesses reported; absenteeism rates due to health issues; health compensation claims	Reactive – reflects past illness
Environmental	Environmental violations and fines; waste volume generated; spills and leaks; remediation costs	Reactive – past non-compliance
Security	Security incidents/breaches; losses from theft; time to respond to security incidents	Reactive – past failures

- TRIR — frequency of all recordable incidents; widely used for benchmarking
- DART Rate — Days Away, Restricted, or Transferred; severity-weighted subset of TRIR
- Lost Workday Case Rate — cases resulting in days away from work only
- Severity Rate — total lost workdays; measures average severity per incident
- Fatality Rate — per 100 million hours; used for national/industry-level reporting
- Workers' Compensation costs — financial impact of incidents
- OSHA citations — reflect compliance performance historically

7.3 Key Safety Rate Formulas

Rate/Metric	Formula
TRIR (Total Recordable Incident Rate)	$\text{TRIR} = (\text{Number of recordable incidents} \times 200,000) / \text{Total hours worked}$
DART Rate	$\text{DART} = (\text{Days Away} + \text{Restricted} + \text{Transfer cases} \times 200,000) / \text{Total hours worked}$
LTIFR (Lost Time Injury Frequency Rate)	$\text{LTIFR} = (\text{Lost time injuries} \times 1,000,000) / \text{Total hours worked}$
Severity Rate	$\text{Severity Rate} = (\text{Days lost} \times 200,000) / \text{Total hours worked}$

TRIR: $(\text{Total Recordable Incidents} \times 200,000) \div \text{Hours Worked}$

All subsequent formulas use an identical structure — only the numerator changes.

DART Rate: $(\text{DART Cases} \times 200,000) \div \text{Hours Worked}$

DART = Days Away + Restricted + Transferred.

Severity Rate: $(\text{Lost Workdays} \times 200,000) \div \text{Hours Worked}$

Complements TRIR: high severity rate with low TRIR signals few but severe incidents.

Fatality Rate: $(\text{Fatalities} \times 100,000,000) \div \text{Hours Worked}$

100M hour base used for national/industry fatality statistics.

Scenario — Full Worked Example — Practice: Construction firm: 800 workers | 1,600,000 hours | 16 recordable incidents | 5 DART cases | 120 lost workdays. $\text{TRIR} = (16 \times 200,000) \div 1,600,000 = 2.0$. $\text{DART} = (5 \times 200,000) \div 1,600,000 = 0.625$. $\text{Severity} = (120 \times 200,000) \div 1,600,000 = 15.0$. Alert: near-miss reporting dropped 60% YoY. Response: Investigate reporting culture barriers before TRIR increases.

 EXAM TIP

Leading indicators are PROACTIVE and PREDICTIVE. Lagging indicators are REACTIVE and HISTORICAL. The CSP exam will ask you to classify indicators — focus on whether they predict future performance (leading) or measure past results (lagging). A combination of both is always recommended.

EXAM TIP: Near-miss reporting rate is the MOST VALUABLE leading indicator. A declining near-miss rate is a warning sign even when TRIR looks stable. On the exam, always recommend addressing leading indicators BEFORE a lagging indicator deteriorates.

Reference: Brauer, R.L. (2016). *Safety and Health for Engineers, 3rd Ed., Ch. 36 — Performance Indicators.*

7.4 Incident Costs – Compiled Explanation

The term **incident** includes first-aid cases, recordable cases, restricted workday cases, lost-workday cases, permanent disability cases, near misses, and property damage cases.

Incident costs are broadly classified into two main categories:

Direct Incident Costs

Direct incident costs are the **actual cash expenses** directly attributable to the incident. These are expenditures that would not have occurred if the incident had not taken place.

Examples of Direct Costs

- Workers' compensation
- Medical-related treatment
- Medical treatment supplies
- Ambulance services
- Drug testing
- Job accommodations
- Purchase of new equipment

Indirect Incident Costs

Indirect incident costs refer to the **time, effort, and resource-related losses** resulting from the incident, excluding direct cash payments.

Examples of Indirect Costs

- Time spent by healthcare professionals
- Time lost by the injured worker
- Supervisor involvement
- Return-to-work management
- Incident investigation and review
- Loss of production/productivity
- Human resource activities
- Hiring and replacement costs
- Management time
- Process delays and interruptions
- Security-related activities
- Training costs
- Legal expenses

EXAM TIP: Multiple Scenarios can be given where you are required to distinguish between Direct & Indirect costs. In scenario-based questions, carefully identify whether the cost is an immediate financial expense or a secondary operational loss.

- **Direct Costs** involve actual cash outflows such as medical expenses or compensation.
- **Indirect Costs** involve time, productivity, supervision, delays, and other hidden organizational losses resulting from the incident.

8 Recognize Safety, Health, and Environmental Management and Audit Systems

EHS management systems provide the structural framework for systematic hazard identification, risk control, legal compliance, and continual improvement. The Annex SL High-Level Structure makes ISO 9001, 14001, and 45001 structurally identical, enabling integrated management systems. The exam tests recognition of each standard, its unique requirements, and historical context.

8.1 ISO Standards — Key Distinctions

History of ISO

- 1906 — International Electro-technical Commission established
- 1926 — International Federation of National Standardizing Associations (ISA) founded
- 1946 — London: delegates from 25 countries agreed to create a new international standards organization
- 1947 — ISO formally established, Geneva, Switzerland
- 1951 — First ISO standard published
- 1979 — ISO Technical Committee TC 176 formed for quality management
- 1987 — ISO 9000 series first published; revised 1994, 2000, 2008, 2015

Benefits of ISO 9001

- Customer satisfaction and better market value
- Continuous improvement culture and less operational errors
- Effectiveness, efficiency, consistency in services
- Increased profitability through reduced waste and rework

ISO 9001 — Quality Management Systems

Foundational quality standard and structural template for all subsequent ISO management standards. Key requirements: customer focus, leadership accountability, risk-based thinking, process approach, performance evaluation, and continual improvement through the PDCA cycle.

ISO 14001 — Environmental Management Systems

Framework for managing environmental responsibilities systematically. Scope: environmental policy; planning (legal requirements, significant aspects, objectives); implementing controls; checking (monitoring, audit, nonconformity); management review. Focus: minimize environmental impacts, ensure legal compliance, prevent pollution, and achieve continual improvement.

ISO 45001:2018 — Occupational Health and Safety Management Systems

International standard for OH&S management, published March 2018. Replaced OHSAS 18001 (transition period: 3 years). Two critical additions vs. OHSAS 18001: mandatory worker participation and consultation (non-negotiable); and explicit integration with organizational context and strategy.

- Requires: hazard identification, risk assessment, legal compliance evaluation, mandatory worker participation
- Annex SL structure enables full integration with ISO 9001 and ISO 14001
- Worker consultation and participation is a CORE REQUIREMENT — not optional

ISO 19011:2018 — Guidelines for Auditing Management Systems

Guidance on audit principles, managing audit programmes, and conducting management system audits. Applicable to ALL types of management system audits — quality, environmental, OH&S, and integrated. Key audit principles: integrity, fair presentation, due professional care, confidentiality, independence, evidence-based approach, risk-based thinking.

8.2 ANSI/ASSP Z10 — US National Standard

Complement OSHA regulatory requirements. Provides a structured management system approach for continuous improvement beyond regulatory compliance. Scope: planning, implementation, evaluation, and improvement. Emphasizes worker participation and voluntary adoption of best practices.

EXAM TIP: ISO 45001 replaced OHSAS 18001 in 2018. Worker consultation and participation is MANDATORY — this is consistently tested. ISO 19011 applies to ALL management system audits, not just OH&S.

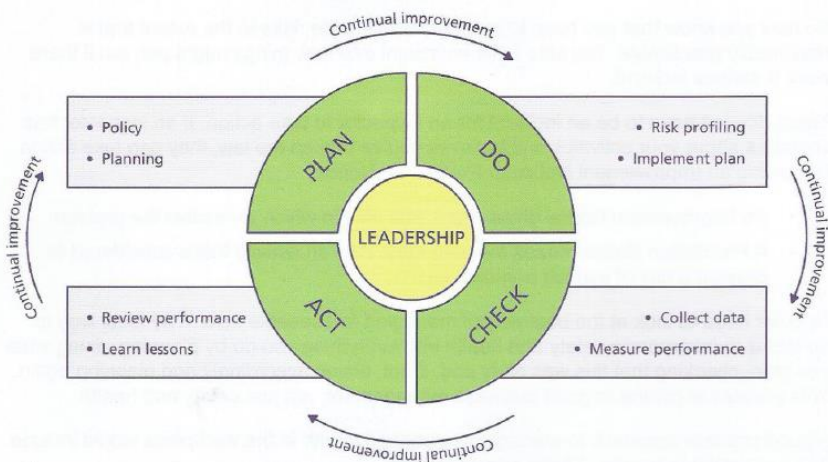
8.3 Standards Comparison Table

Standard	Scope	Primary Focus
ISO 9001	Quality Management	Customer satisfaction, process consistency, continual quality improvement
ISO 14001	Environmental Mgmt	Environmental performance, legal compliance, pollution prevention
ISO 45001	OH&S Management	Worker safety, hazard control, regulatory compliance, worker participation
ISO 19011	Audit Guidelines	Auditing management systems (internal and external); auditor competence
ANSI Z10	OH&S Mgmt (USA)	Risk reduction, safety culture, regulatory complement, continual improvement

8.4 The PDCA Cycle — Foundation of All ISO Standards (Slides 14, 104)

PDCA: Plan → Do → Check → Act (Deming / Shewhart Cycle)

Underpins ISO 9001, 14001, 45001, and ANSI Z10. The Check phase includes monitoring AND internal audit.



- **PLAN:** identify hazards, assess risks, establish objectives, determine legal requirements, allocate resources
- **DO:** implement controls, train personnel, execute operational procedures, communicate safety information
- **CHECK:** monitor and measure against objectives; conduct internal audits; investigate incidents; evaluate compliance

- ACT: management review; corrective action on nonconformities; update management system; close the improvement loop

EXAM TIP

ISO 45001 REPLACED OHSAS 18001. All ISO management standards share the PDCA cycle. ISO 19011 is for AUDITING (any management system). ANSI Z10 is the US-specific OH&S management standard. Questions may ask which standard to use for a given audit or management scenario.

Reference: Brauer, R.L. (2016). *Safety and Health for Engineers, 3rd Ed., Chs. 4, 37 — Management Systems and Auditing.*

9 Applicable Requirements for Plans, Systems, and Policies

The CSP must know the mandatory components of key regulatory and voluntary safety plans. Exam scenarios present incomplete plans and ask candidates to identify missing required elements. Roger Brauer Chapter 38 is the primary study reference for this objective.

9.1 Safety & Health Programs

Program	Required Elements
Hazard Communication (HazCom)	Written HazCom program, SDS for all chemicals, employee training, container labeling (29 CFR 1910.1200)
Lockout/Tagout (LOTO)	Energy control procedures, authorized/affected employee training, periodic inspections (1910.147)
Respiratory Protection	Written program, medical evaluation, fit testing, training, equipment maintenance (1910.134)
Personal Protective Equipment	Hazard assessment, written program, training on use/care, selection based on hazard level (1910.132)
Hearing Conservation	Noise monitoring, audiometric testing, hearing protectors, training (1910.95)
Bloodborne Pathogens	Exposure control plan, hepatitis B vaccination, post-exposure follow-up (1910.1030)

9.2 Emergency Action Plan (EAP) 29 CFR 1910.38

Written EAP is required when 11 or more employees. Elements that **MUST** be included (memorize as a complete list):

- Emergency escape procedures and emergency escape route assignments (posted floor plans required)
- Procedures for employees who remain to operate critical systems before evacuating
- Procedures to account for ALL employees after evacuation is complete (headcount/accountability)
- Rescue and medical duties for designated employees
- Means for reporting fires and other emergencies to external emergency services
- Names or job titles of persons to contact for further information about the plan

9.3 Fire Prevention Plan — 29 CFR 1910.39

- List of all major fire hazards and proper handling/storage procedures for hazardous materials
- All potential ignition sources associated with each major hazard and control procedures
- Type of fire protection equipment or systems required to control each hazard
- Housekeeping practices to control the accumulation of flammable and combustible materials
- Procedures to maintain and safeguard all heat-producing equipment from ignition sources

9.4 Environmental Plans

- SPCC Plan (40 CFR 112): required for facilities storing >1,320 gallons of oil aboveground or >42,000 gallons underground
- SWPPP: required under Clean Water Act NPDES permit for industrial stormwater discharges
- Hazardous Waste Management Plan: RCRA requirements for generation, storage, transport, and disposal
- Air Emissions Management: Clean Air Act compliance, permit conditions, monitoring programmes

9.5 OSHA HAZWOPER — 29 CFR 1910.120

Applies to hazardous waste clean-up operations and emergency response. Requires site safety plans and specific training levels: First Responder Awareness, Operations, Technician, Specialist, Incident Commander. Annual refresher training required for all levels.

9.6 ISO 9001, 14001, and 45001 System Requirements

Understanding the required components of management system plans per ISO standards is part of this objective. Each standard requires: scope definition, documented policies, documented objectives with plans to achieve them, documented procedures for key processes, records of performance results, and documented management review outputs.

Reference: Brauer, R.L. (2016). *Safety and Health for Engineers, 3rd Ed., Ch. 38 — Safety Programme Plans and Policies.*

9.7 Examples and Scenarios

1. Safety Requirements:

- **Overview:** Safety plans and systems are designed to prevent accidents and injuries in the workplace. They include hazard identification, risk assessment, safety training, and the implementation of control measures.
- **Example:** In a manufacturing plant, a safety plan may include regular inspections, the use of personal protective equipment (PPE), and safety drills to prevent machinery-related injuries.

Scenario: A worker in a factory regularly handles hazardous chemicals. The safety plan requires the use of gloves, goggles, and regular safety training sessions to minimize the risk of exposure.

2. Health Requirements:

- **Overview:** Health management systems focus on protecting employee well-being by preventing occupational illnesses and promoting health initiatives. This includes ergonomic assessments, health screenings, and wellness programs.
- **Example:** An office may implement an ergonomic program to prevent repetitive strain injuries by providing adjustable workstations and regular breaks.

Scenario: Employees in an office setting report frequent back pain. The health policy includes conducting ergonomic assessments and providing adjustable chairs and desks to alleviate the issue.

3. Environmental Requirements:

- **Overview:** Environmental management systems (e.g., ISO 14001) ensure that organizations minimize their environmental impact through waste reduction, pollution prevention, and resource conservation.
- **Example:** A company might implement a recycling program and monitor emissions to reduce its environmental footprint.

Scenario: A manufacturing plant needs to comply with environmental regulations regarding emissions. The environmental policy includes monitoring air quality and reducing pollutants through upgraded filtration systems.

4. Fire Safety Requirements:

- **Overview:** Fire safety systems and policies are designed to prevent, detect, and respond to fire emergencies. This includes fire detection systems, fire drills, and evacuation plans.
- **Example:** A commercial building might have fire extinguishers, smoke alarms, and regular fire drills to ensure preparedness.

Scenario: In a high-rise office building, the fire safety plan includes installing smoke detectors, conducting monthly fire drills, and training employees on using fire extinguishers.

5. Emergency Action Plans:

- **Overview:** Emergency action plans (EAP) provide procedures for responding to various emergencies, such as natural disasters, active shooter situations, or medical emergencies. These

plans include evacuation routes, communication protocols, and roles and responsibilities.

- **Example:** A school might have an emergency action plan that outlines steps for evacuating during a fire and lockdown procedures during a security threat.

Scenario: A hospital prepares for potential natural disasters by having an emergency action plan that includes relocating patients, ensuring backup power, and establishing communication lines with local authorities.

Review of Chapter 38: Safety Plan and Programs from "Safety and Health for Engineers" by Roger L. Brauer

Chapter 38 of Roger L. Brauer's "Safety and Health for Engineers" delves into the development and implementation of safety plans and programs, focusing on creating structured approaches to manage workplace safety and health risks.

Key Areas Covered:

1. Components of Safety Plans:

- The chapter outlines essential elements of safety plans, including policy statements, objectives, procedures, and accountability structures. It emphasizes the importance of aligning safety plans with organizational goals and legal requirements.

2. Development Process:

- The book provides a step-by-step guide for developing safety programs, from risk assessment to the establishment of safety committees. It discusses how to involve all levels of the organization in the planning process.

3. Implementation and Management:

- Brauer discusses strategies for effectively implementing safety programs, ensuring that they are integrated into daily operations. He emphasizes the need for leadership commitment, employee involvement, and regular training.

4. Evaluation and Continuous Improvement:

- The chapter stresses the importance of ongoing evaluation through audits, inspections, and incident investigations. It highlights methods for measuring the effectiveness of safety programs and making necessary adjustments to improve outcomes.

5. Specialized Programs:

- There is also discussion on specialized safety programs, such as those for hazardous materials, confined spaces, and machine guarding. Each program is tailored to address specific risks and regulatory requirements.

Examples and Scenarios: The chapter includes real-world examples and scenarios that demonstrate how to apply the principles discussed. For instance, Brauer might describe a scenario where a manufacturing plant implements a safety program to reduce machine-related injuries, detailing the steps taken from hazard identification to program evaluation.

10 Utilize Document Retention or Management Principles

Document retention is a legal and operational obligation. Failure to maintain required records exposes organizations to OSHA citations, EPA enforcement, and litigation liability. The CSP must know specific retention periods, employee access rights, and mandatory reporting thresholds — all directly tested.

10.1 Core Document Retention Principles

Principle	Description
Legal Compliance	Documents must be retained per legal and regulatory requirements. OSHA mandates specific retention periods for each record type.
Confidentiality & Security	Sensitive information (medical records, exposure data) must be protected from unauthorized access.
Accessibility	Records must be readily accessible to authorized personnel during audits, legal proceedings, or employee requests.
Integrity & Accuracy	Records must be maintained in a manner that preserves their accuracy and completeness over time.
Retention Schedules	Establish specific retention periods based on legal requirements and organizational needs.
Secure Disposal/Archiving	Follow proper procedures for secure disposal or archiving when retention periods expire.

10.2 Categories of Records Requiring Retention

- Incident investigation records — OSHA 300, 300A, 301 forms
- Training records — employee safety training completions per programme
- Exposure records — air monitoring, biological monitoring, SDS, noise dosimetry
- Maintenance records — equipment inspection and PM records
- Environmental management system records — audits, monitoring results, manifests
- Audit results — internal and external management system audit reports

10.3 OSHA Records Retention Schedule

Document Type	Retention Period	Notes
OSHA Form 300 (Injury Log)	5 years	Log of Work-Related Injuries and Illnesses
OSHA Form 301 (Incident Report)	5 years	Detailed individual injury/illness incident report
OSHA Form 300A (Summary)	5 years + post annually	Annual summary — must be posted Feb 1 – Apr 30
Medical Records (29 CFR 1910.1020)	Employment + 30 years	❗ CRITICAL: Retained for duration of employment PLUS 30 years
Exposure Records (29 CFR 1910.1020)	30 years	Air monitoring, biological monitoring, MSDS/SDS records
Training Records (general)	Duration of employment + 5 years (varies)	Evidence of completion of required safety training
Incident Investigation Reports	5 years minimum	Root cause analysis, corrective actions documentation
Environmental Monitoring Data	30+ years (per regulation)	Varies by pollutant and regulatory program
Audit Results	3–7 years	Internal and external audit findings and corrective actions
PSM Records (1910.119)	Life of process + 6 years	Process safety information, PHAs, MOC records

EXAM TIP: Medical records: Employment + 30 years. Exposure records: 30 years flat. OSHA 300 logs: 5 years. These three retention periods are the highest-frequency exam answers in this section.

10.4 OSHA Forms Distinction

Form	Purpose	Requirements
Form 300	Log of Work-Related Injuries and Illnesses	5 years – NOT automatically reported to OSHA
Form 301	Injury and Illness Incident Report	5 years – Detailed individual incident report
Form 300A	Annual Summary of Injuries and Illnesses	Must be posted Feb 1 – Apr 30 each year; submitted electronically to OSHA if required

EXAM TIP

The #1 exam memory point: Medical records = Duration of employment PLUS 30 years. Exposure records = 30 years. The new OSHA reporting rule (post-2015) requires reporting ONE hospitalization (not 3+), plus amputations and loss of eye.

10.5 OSHA 3110 — Access to Medical and Exposure Records (29 CFR 1910.1020)

Types of Exposures Covered

- Toxic chemicals — airborne contaminants and skin absorption hazards
- Biological agents — bloodborne pathogens, infectious materials
- Physical agents — noise, vibration, ionizing and non-ionizing radiation
- Radiation — ionizing radiation doses and accumulated exposures

Employee Rights

- Employees have a legal RIGHT to access their own medical and exposure records
- Employer must provide access within 15 working days of a written request
- OSHA can access all records upon request (no warrant required for 1910.1020 records)
- Designated representatives (union, personal physician) may access records with employee authorization

10.6 Mandatory Reporting Thresholds

- ALL work-related FATALITIES — report to OSHA within 8 hours
- ANY work-related IN-PATIENT HOSPITALISATION (even ONE worker) — report within 24 hours
- ANY work-related AMPUTATION — report within 24 hours
- ANY work-related LOSS OF AN EYE — report within 24 hours

Pre-2015 rule: reporting required only when MORE THAN 3 workers were hospitalized. The 2015 update dramatically increased reporting obligations. This change is a consistent exam question.

10.7 Examples and Scenarios

1. Incident Investigation:

- **Principle:** Legal Compliance & Accessibility
- **Explanation:** Incident investigation reports must be retained for a specific period to comply with legal requirements and to be available for future reference.
- **Example:** A factory keeps investigation reports for five years as required by OSHA, ensuring they are accessible if similar incidents occur or during audits.

2. Training Records:

- **Principle:** Integrity & Retention Schedules
- **Explanation:** Training records must be kept to demonstrate compliance with safety regulations and ensure employees have completed required training.
- **Example:** A construction company retains records of employee safety training for the duration of their employment plus five years, ensuring these records can be reviewed during safety audits.

3. Exposure Records:

- **Principle:** Legal Compliance & Confidentiality
- **Explanation:** Records of employee exposure to hazardous substances must be retained for long periods, often decades, to comply with regulations and to protect worker health.
- **Example:** A chemical plant retains records of employee exposure to asbestos for at least 30 years, as required by OSHA, ensuring these records are kept confidential and secure.

4. Maintenance Records:

- **Principle:** Accuracy & Retention Schedules
- **Explanation:** Maintenance records ensure equipment is serviced regularly and safely, and they must be retained for the life of the equipment plus additional time as required by regulations.
- **Example:** An airline retains aircraft maintenance records for the life of the aircraft plus seven years, providing a complete history for safety inspections and audits.

5. Environmental Management System (EMS):

- **Principle:** Compliance & Documentation Integrity
- **Explanation:** EMS documentation, including permits and monitoring reports, must be maintained to demonstrate compliance with environmental regulations.
- **Example:** A manufacturing company maintains its EMS records for ten years, including waste management logs and emissions data, ensuring they are accurate and available for regulatory inspections.

6. Audit Results:

- **Principle:** Retention & Integrity
- **Explanation:** Audit reports must be retained to demonstrate compliance and support continuous improvement initiatives within the organization.
- **Example:** A financial institution retains internal audit reports for seven years, ensuring they are securely stored and can be referenced during external audits or regulatory reviews.

11 Budgeting, Finance, and Economic Analysis Techniques and Principles

The CSP must make a compelling economic case for safety investments. This requires quantifying accident costs, calculating ROI, applying cost/benefit analysis, and understanding the role of safety in the procurement process. Financial literacy is increasingly expected of senior safety professionals.

11.1 Key Financial Concepts

Concept	Definition & Application
Budget Development	Forecast revenues and expenses; set financial targets; allocate resources to EHS programs. Separate capital vs. operating expenditures.
Timelines & Milestones	Establish schedules for financial projects. Milestones are key checkpoints indicating progress toward objectives (e.g., complete hazard survey by Q2).
Resourcing	Allocate human, financial, and material resources to achieve safety program objectives.
Return on Investment (ROI)	$ROI = (\text{Net Benefit} / \text{Cost of Investment}) \times 100\%$. Used to demonstrate the financial return of safety programs.
Cost-Benefit Analysis	Compare the costs of controls/programs against the cost of incidents. Account for direct AND indirect costs of accidents.
Financing Risk Management	Evaluate options: insurance, self-insurance, captives, surety bonds, letters of credit. Part of the total risk management strategy.
Role in Procurement	Use cost-benefit analysis to select suppliers and equipment. Life-cycle cost analysis balances purchase price with total ownership cost.

11.2 Accident Cost Framework — Heinrich's Iceberg

Heinrich's Iceberg Principle

For every \$1 in direct (insured) costs, there are \$4–\$10 in indirect (uninsured) costs. The 'true' cost of accidents is far greater than what appears above the surface.

Cost Category	Examples	Proportion
Direct / Insured Costs	Medical expenses, workers' compensation, rehabilitation costs	Visible – typically \$1 unit
Indirect / Uninsured Costs	Lost productivity, investigation time, training replacement workers, equipment repair, regulatory penalties, litigation, damaged morale	Hidden – typically \$4–\$10 per \$1 direct
Total Cost of Risk (TCOR)	Direct + Indirect + Administrative + Risk Control costs	Full economic picture

Direct costs (visible above the waterline): medical treatment, hospitalization, workers' compensation payments, OSHA fines, property damage. Indirect costs (hidden below the waterline, 4x–53x larger than direct): lost productivity, training replacement workers, supervisory investigation time, morale impact, administrative processing, reputational damage, and increased insurance premiums. Total incident cost = Direct + Indirect.

11.3 Return on Investment (ROI)

ROI (%): $[(\text{Net Benefit} \div \text{Programme Cost}) \times 100]$

Net Benefit = Total Savings (incident cost avoidance) – Programme Cost.

Scenario — ROI Calculation: Company invests \$50,000 in slip/trip/fall prevention. Year 1: \$200,000 in incident cost reduction. Net Benefit = \$150,000. $\text{ROI} = (\$150,000 \div \$50,000) \times 100 = 300\%$. Industry data: every \$1 invested in safety returns \$3–\$6 through reduced WC costs, productivity gains, lower insurance premiums, and reduced turnover.

11.4 Budget Development Process

- Identify all programme elements requiring funding: training, PPE, inspections, audits, monitoring equipment, and engineering controls
- Quantify costs using historical data, vendor quotes, and industry benchmarks
- prioritize expenditure by risk: highest-risk gaps receive first budget allocation
- Develop a multi-year budget with milestones — safety cannot be funded episodically
- Align budget submission with organizational budget cycle — early engagement with finance is critical

11.5 Timeline and Milestone Planning

- Develop a Gantt chart mapping safety programme activities to the fiscal year calendar
- Identify dependencies: training must precede procedure implementation; PPE must be procured before engineering controls are removed
- Set measurable milestones with go/no-go criteria at each stage

11.6 Cost/Benefit Analysis (CBA)

CBA compares the total anticipated benefits of a safety intervention against total costs over a defined period. NPV (Net Present Value) accounts for the time value of money. Payback period = time until accumulated benefits equal the initial investment.

11.7 Role in Procurement Process

CSP evaluates safety implications of procurement: inherent safety of purchased materials (substitution opportunity); SDS adequacy; vendor safety qualification; safety performance requirements in contracts; life-cycle cost analysis, including maintenance, training, and disposal costs; compliance with applicable safety standards as procurement specifications.

11.8 Financing Risk Management Options

- Workers' Compensation Insurance — state-mandated; premiums driven by EMR (Experience Modification Rate)

EMR: $\text{Actual WC Losses} \div \text{Expected Losses for Industry}$

EMR < 1.0 = better than average → premium reduction. EMR > 1.0 = worse than average → premium surcharge.

- Self-Insurance — large organizations retain risk; requires strong internal safety programme
- Captive Insurance — industry group owns the insurer; aligns incentives directly
- Risk Transfer through Contract — indemnification clauses; requires contractor safety prequalification

Reference: Brauer, R.L. (2016). *Safety and Health for Engineers, 3rd Ed., Ch. 5 — Economic Analysis of Safety.*

12 Differentiate Management Leadership Techniques

Management consists of planning, organizing, staffing, leading or directing, and controlling an organization (a group of one or more people or entities) or effort for the purpose of accomplishing a goal.

Safety professionals, at all levels, should have a thorough understanding of management principles, theories, and styles, as they will undoubtedly either become managers or become managed.

Safety professionals must understand management and leadership theories as diagnostic and prescriptive tools. The exam tests the ability to identify theories from descriptions, apply them to safety scenarios, and select appropriate leadership approaches for given organizational contexts.

12.1 Management & Leadership Styles

1. **Transformational Leadership:**
 - Focuses on inspiring and motivating employees to achieve their full potential and embrace change. Leaders create a vision and encourage employees to work towards shared goals.
2. **Transactional Leadership:**
 - Based on a system of rewards and penalties, this technique focuses on performance and results. Leaders provide clear instructions and expect compliance.
3. **Situational Leadership:**
 - Adapts leadership style based on the maturity and competence of the team. Leaders may shift between directive, supportive, and delegative approaches as needed.
4. **Servant Leadership:**
 - Prioritizes the needs of employees and helps them grow personally and professionally. Leaders lead by example and focus on serving their team.
5. **Participative Leadership:**
 - Involves team members in decision-making processes. Leaders encourage input and collaboration, fostering a sense of ownership and commitment among employees.
6. **Autocratic Leadership:**
 - Centralizes decision-making authority with the leader. This technique is effective in situations where quick decisions are needed, though it may limit employee creativity.
7. **Coaching Leadership:**
 - Focuses on developing employees' skills and talents through guidance, feedback, and mentorship. Leaders help individuals reach their personal and professional goals.
8. **Laissez-Faire Leadership:**
 - Provides employees with autonomy to make decisions and manage their work. Leaders offer support when needed but allow team members to take the lead in their tasks.

Examples and Application Scenarios

1. **Transformational Leadership:**
 - A leader in a tech startup motivates the team to innovate and adapt to new market trends, leading to the successful launch of a new product.
2. **Transactional Leadership:**
 - A sales manager sets clear targets and offers bonuses for meeting sales quotas, ensuring the team stays focused on results.
3. **Situational Leadership:**
 - A project manager adjusts their leadership style when managing a team of experienced engineers versus a group of interns, providing more guidance to the latter.
4. **Servant Leadership:**
 - A leader in a nonprofit organization focuses on meeting the needs of their volunteers, ensuring they feel valued and supported in their roles.
5. **Participative Leadership:**
 - In a marketing agency, the leader involves the team in brainstorming sessions, leading to more creative and diverse campaign ideas.

6. Autocratic Leadership:

- During a crisis, a factory manager makes quick decisions to halt production and ensure worker safety, minimizing potential harm.

7. Coaching Leadership:

- A leader in a retail company mentors a promising employee, helping them develop the skills needed for a future management role.

8. Laissez-Faire Leadership:

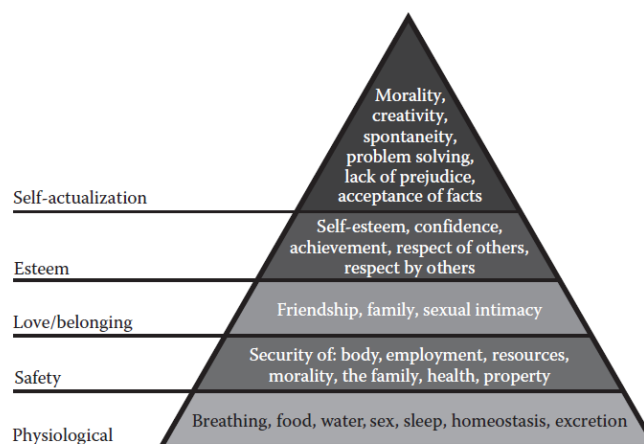
- In a research and development department, the leader allows scientists to pursue their projects independently, fostering innovation.

Functions of Management

- Planning: set safety objectives; identify hazards; determine strategies and tactics
- Organizing: structure safety resources, committees, and responsibilities
- Staffing: recruit, select, develop, and retain competent safety personnel
- Leading/Directing: motivate workers and supervisors to maintain safe behavior
- Controlling: monitor safety performance; compare against objectives; take corrective action

12.2 Management and Motivation Theories

Maslow's Hierarchy of Needs



Five levels: 1-Physiological → 2-Safety/Security → 3-Social/Belonging → 4-Esteem/Recognition → 5-Self-Actualisation. People are motivated by their LOWEST unmet need. Safety Application: workers cannot pursue safety excellence (Level 4/5) if fundamental safety needs (Level 2) remain unmet. Leaders must ensure basic physical and psychological safety before pursuing cultural engagement initiatives.

Maslow's theory posits that human needs are arranged in a hierarchy, starting from basic physiological needs to safety, love/belonging, esteem, and self-actualization. For example, a company ensures that employees' basic needs (e.g., fair wages) are met before focusing on higher-level needs like recognition and career development.

Scenario: A tech firm first offers competitive salaries and health benefits (physiological and safety needs) and then introduces recognition programs and career growth opportunities (esteem and self-actualization).

McGregor's Theory X and Theory Y

Theory X: Workers dislike work; avoid responsibility; require tight control and threat of punishment. It assumes employees are inherently lazy and require strict supervision

Theory Y: workers are self-motivated; seek responsibility; enjoy work under the right conditions. It views employees as motivated and capable of self-direction.

For instance, a factory manager using Theory X might enforce strict rules, while a Theory Y leader in a creative agency encourages autonomy.

Application: Theory Y assumptions underpin participative safety management and BBS programmes. Theory X drives top-down, command-and-control cultures — less effective for culture improvement and engagement.

Scenario: A creative agency manager empowers designers to manage their own projects (Theory Y), fostering innovation and job satisfaction.

Herzberg's Two-Factor Theory

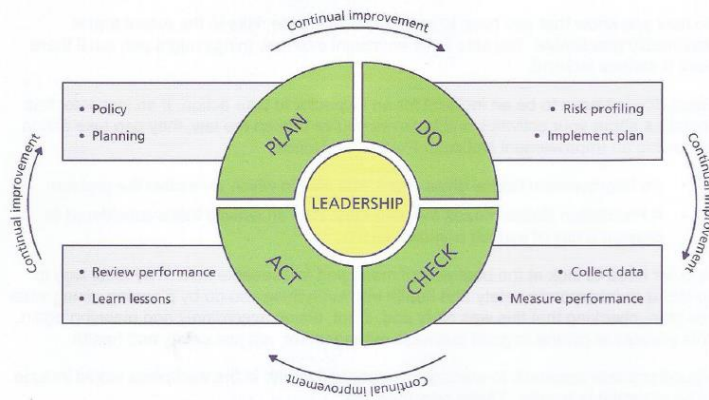
Hygiene Factors (prevent dissatisfaction): supervision quality, interpersonal relationships, physical working conditions, and salary. Motivating Factors (drive engagement): achievement, advancement, recognition, responsibility. Safety Application: safe physical conditions (hygiene) prevent dissatisfaction; recognizing safe behavior and giving workers safety responsibility (motivators) drives genuine engagement.

Herzberg's Two-Factor Theory identifies **hygiene factors** (e.g., salary) that prevent dissatisfaction and **motivators** (e.g., recognition) that promote satisfaction. For example, providing a well-paid job with opportunities for advancement can lead to higher employee engagement.

Scenario: A hospital introduces a recognition program for nurses who exceed patient care standards (motivator), while also ensuring competitive salaries and safe working conditions (hygiene factors).

- Hygiene Factors
 - Supervision
 - Interpersonal relationships
 - Physical working conditions
 - Salary
- Motivation Factors
 - Achievement
 - Advancement
 - Recognition
 - Responsibility.

Deming's PDCA Cycle



The PDCA cycle (Shewhart) is an operational expression — and the backbone of ISO 9001, 14001, 45001, and ANSI Z10. Key point: Deming placed primary responsibility for quality (and safety) with management, not workers.

1. Plan:

- Policy and Planning: Set objectives and identify risks.
- Example: A manufacturing company plans to reduce defects by setting new quality standards.

2. Do:

- Risk Profiling and Implement Plan: Execute the plan with leadership driving the process.
- Example: Implement the new quality standards on the production line.

3. Check:

- Collect Data and Measure Performance: Monitor results and evaluate success.

- Example: Inspect products for defects and compare them against the new standards.

4. Act:

- Review Performance and Learn Lessons: Analyze outcomes and make necessary adjustments.
- Example: Identify issues in the implementation and refine the process to further reduce defects.

Leadership:

- Central Role: Ensures alignment of actions with strategic goals and drives continuous improvement across all stages.
- Example: A leader communicates the importance of quality improvement, supports the team, and ensures the process is followed effectively.

Scenario: An automotive plant identifies a flaw in the assembly line, implements a new procedure, monitors defect rates, and adjusts the process based on data to ensure consistent quality.

Management by Objectives — MBO

Peter Drucker: set specific, measurable, agreed-upon objectives collaboratively between managers and employees. Regular progress reviews. Adjust strategies based on performance data. Safety Application: safety objectives (TRIR targets, audit completion rates, training rates) become part of every manager's and supervisor's formal performance review.

Scenario: A retail chain manager works with store employees to set sales targets, tracks progress weekly, and adjusts strategies to meet the objectives by the end of the quarter.

Other Theories

Contingency Theory:

- Contingency Theory suggests that the best management style depends on the specific circumstances. For example, a crisis may require an autocratic style, while a stable environment may benefit from a participative approach.
- **Scenario:** A project manager in a construction firm adopts a directive style when a project is behind schedule but shifts to a participative style during the planning phase of a new project.

Systems Theory:

- Systems Theory views an organization as an interconnected system where changes in one part affect the whole. For instance, implementing new technology in supply chain management may require adjustments in procurement, production, and customer service.
- **Scenario:** A logistics company upgrades its tracking system, which improves delivery accuracy but also requires adjustments in inventory management and customer communication processes.

Chaos Theory:

- Chaos Theory acknowledges that organizations operate in complex, unpredictable environments. Leaders must be flexible, embracing uncertainty and using it as a catalyst for innovation. For example, a startup may pivot its business model in response to unexpected market changes.
- **Scenario:** A tech startup faces sudden market shifts and uses the opportunity to innovate by launching a new product line that meets emerging customer demands.

Summary:

- Contingency Theory: no single best management approach; optimal style depends on task complexity, team experience, and urgency
- Systems Theory: organizations are complex interacting systems; safety incidents arise from system interactions, not just individual failures
- Chaos Theory: small initial conditions can produce large non-linear outcomes (butterfly effect); in safety, small procedural deviations can cascade to major incidents

12.3 Management Styles

- Autocratic (Authoritarian): leader makes decisions unilaterally; appropriate for emergency response and imminent danger situations
- Permissive (Laissez-Faire): workers self-manage with minimal direction; high risk in safety-critical environments
- Directive Democrat: tells people WHAT to do but invites input on HOW — hybrid approach
- Directive Autocrat: tells people what to do AND how — command and control
- Permissive Democrat: worker has broad autonomy on what and how — appropriate for professional safety staff
- Transformational Leadership: inspires workers beyond compliance toward a shared vision — most effective for sustained culture improvement

Broad Styles**1. Directive Democrat:**

- **Description:** The leader seeks input from the team but retains final decision-making authority. This style combines employee involvement with clear guidance.
- **Example:** A project manager consults with the team on a project timeline but ultimately sets the final deadlines.

2. Directive Autocrat:

- **Description:** The leader makes decisions independently and expects strict compliance, providing clear directions with little to no input from employees.

- **Example:** A factory supervisor dictates safety procedures and expects workers to follow them without question.
- 3. **Permissive Democrat:**
 - **Description:** The leader encourages team input and often follows the consensus, giving employees significant control over their work while maintaining a collaborative atmosphere.
 - **Example:** A department head holds regular team meetings to gather ideas and allows the team to choose the best approach to a project.
- 4. **Permissive Autocrat:**
 - **Description:** The leader makes decisions independently but allows employees the freedom to decide how to implement those decisions.
 - **Example:** A CEO decides on the company's strategic direction but gives department heads autonomy in executing the plan as they see fit.

12.4 Workplace Discipline —

Workplace discipline theories provide frameworks for managing employee behavior, ensuring adherence to organizational rules and standards. Here are some key theories:

1. Hot Stove Rule (Douglas McGregor):

- **Theory:** Discipline should be immediate, consistent, impersonal, and include a warning.
- **Example:** An employee is immediately reprimanded after violating safety rules, and the same consequence is applied to everyone who breaks the rule.

2. Progressive Discipline:

- **Theory:** Disciplinary actions should escalate with repeated offenses.
- **Example:** A tardy employee receives a verbal warning first, then a written warning, and finally suspension if behavior doesn't improve.

3. Positive Discipline:

- **Theory:** Focuses on counseling and problem-solving rather than punishment.
- **Example:** A manager meets with an underperforming employee to identify the root cause of issues and develop a plan for improvement.

4. Employment-at-Will Doctrine:

- **Theory:** Employers can terminate employment for any reason, except illegal ones, without warning.
- **Example:** An employee may be dismissed immediately for misconduct without prior warnings, as long as the dismissal is legal.

5. Just Cause Doctrine:

- **Theory:** Requires fair and valid reasons for disciplining or terminating an employee.

Example: An employer conducts a thorough investigation and provides clear evidence before disciplining an employee for policy violations.

Fayol's 14 Principles of Management

1. Division of Work: Specialization increases productivity by allowing workers to focus on specific tasks.
2. Authority: Managers must have the authority to give orders and the responsibility to ensure they are followed.
3. Discipline: Employees must respect rules and agreements to maintain organizational order.
4. Unity of Command: Each employee should receive orders from only one superior.
5. Unity of Direction: Teams with the same objective should work under one plan.
6. Subordination of Individual Interests: Organizational interests take precedence over individual interests.
7. Remuneration: Fair compensation motivates employees.
8. Centralization: The extent to which decision-making is centralized or decentralized.
9. Scalar Chain: A clear line of authority from top to bottom.
10. Order: Resources and people should be in the right place at the right time.
11. Equity: Fairness and kindness should be applied to all employees.
12. Stability of Tenure of Personnel: Long-term employment is crucial for developing skills and loyalty.
13. Initiative: Employees should be encouraged to show initiative.
14. Esprit de Corps: Promoting team spirit builds harmony and unity.

Relationship to Workplace Discipline:

Fayol's principles directly relate to workplace discipline through principles such as Authority, Discipline, Unity of Command, and Equity. These principles emphasize the importance of clear rules, fair treatment, and proper authority, all of which are foundational to maintaining discipline in the workplace. For example, the principle of Discipline specifically underscores the need for employees to follow rules and respect authority, which is essential for an orderly and productive work environment.

Important Summary:

- Unity of Command: each employee reports to only ONE supervisor — critical for clear safety accountability
- Unity of Direction: one safety plan aligned to shared objectives across the organization
- Scalar Chain: clear authority hierarchy from CEO to frontline worker
- Discipline: clear expectations, consequences, and consistent enforcement across all levels
- Equity: fair and consistent treatment — essential for a just safety culture
- Esprit de Corps: team cohesion and morale support a collaborative safety culture
- Subordination of Individual Interest: organizational safety goals take precedence over individual convenience

Henri Fayol's 14 Principles of Management

- 1 • Division of Work
- 2 • Authority and Responsibility
- 3 • Discipline
- 4 • Unity of Command
- 5 • Unity of Direction
- 6 • Subordination of Individual Interest
- 7 • Remuneration
- 8 • The Degree of Centralization
- 9 • Line of Authority/Scalar Chain
- 10 • Order
- 11 • Equity
- 12 • Stability of Tenure of Personnel
- 13 • Initiative
- 14 • Esprit de Corps/Team Spirit

12.5 Workplace Communication Styles

Workplace communication styles refer to the ways in which people express themselves, share information, and interact with others in a professional setting. These styles can greatly influence team dynamics, collaboration, and overall productivity.

Passive	Passive Aggressive	Aggressive	Assertive
Emotionally dishonest, indirect, inhibited, self-denying, blaming, apologetic.	Emotionally dishonest, indirect. Self-denying at first. Self-enhancing at expense of others later.	Inappropriately honest, direct, expressive, attacking, blaming, controlling, self-enhancing at expense of others.	Appropriately honest, direct, self-enhancing, expressive, self-confident, empathic to emotions of all involved.
"Others' rights and needs take precedence over mine"	"I subtly make clear that my rights and needs prevail"	"I boldly insist that my rights and needs prevail"	"I clearly express that we both have rights and needs"

1. Assertive Communication:

- **Description:** Clear, direct, and respectful communication that expresses needs and opinions confidently without infringing on others.
- **Example:** An employee who is assertive might say, "I believe we should prioritize the marketing campaign first because it aligns with our strategic goals."

- **Scenario:** During a team meeting, an assertive manager provides clear feedback on a project, listens to others' opinions, and ensures that everyone has a chance to contribute.

2. Aggressive Communication:

- **Description:** Forceful, often disrespectful communication that seeks to dominate or control the conversation.
- **Example:** "This is how we're doing it, and that's final!" is an aggressive way of shutting down discussion.
- **Scenario:** A manager criticizes an employee harshly in front of others, leading to a tense and uncomfortable work environment.

3. Passive Communication:

- **Description:** Indirect and often self-denying communication where the speaker avoids expressing their own opinions or needs.
- **Example:** "I'm okay with whatever the group decides," even if they disagree with the decision.
- **Scenario:** An employee who disagrees with a project plan does not speak up during the meeting, leading to unresolved issues later.

4. Passive-Aggressive Communication:

- **Description:** Indirect communication where someone expresses negative feelings subtly rather than openly.
- **Example:** A coworker agrees to a task but later complains about it behind the person's back.
- **Scenario:** An employee agrees to take on extra work but then intentionally delays completing it as a form of silent protest.

5. Collaborative Communication:

- **Description:** Open, inclusive communication that encourages input from all team members to reach a consensus.
- **Example:** "Let's discuss all possible solutions and decide on the best course of action together."
- **Scenario:** A project leader facilitates a brainstorming session where everyone's ideas are valued, and a decision is made collectively.

6. Directive Communication:

- **Description:** Clear, concise communication where the speaker gives specific instructions or directions.
- **Example:** "Please complete the report by Friday and send it to the entire team."
- **Scenario:** A manager gives clear tasks and deadlines to the team during a project briefing to ensure clarity and focus.

Scenarios in the Workplace:

- **Team Collaboration:** In a collaborative communication environment, team members feel empowered to share ideas, leading to innovative solutions and a cohesive work atmosphere.
- **Conflict Resolution:** Assertive communication is key in resolving conflicts, as it allows both parties to express their views openly and work towards a mutually agreeable solution.
- **Project Management:** Directive communication is often used by project managers to ensure that everyone understands their roles, responsibilities, and deadlines, which helps keep projects on track.
- **Performance Feedback:** Effective feedback often requires a blend of assertive and collaborative communication, ensuring that feedback is clear, constructive, and encourages employee development.

Understanding and applying the appropriate communication style in different workplace scenarios is crucial for fostering a productive and positive work environment.

The 4 Communication Styles



1. The Relator (Indirect, Slow-paced, Open Relationships):

- **Characteristics:** Warm, friendly, and a good listener. Prioritizes building relationships and prefers big ideas and conceptualization.
- **Example:** A team member who focuses on creating a positive team environment before diving into tasks.

2. The Socializer (Direct, Fast-paced, Open Relationships):

- **Characteristics:** Enthusiastic, persuasive, motivated by praise, and thrives in lively environments. Enjoys trying new things.
- **Example:** A marketer who excels in brainstorming sessions and is driven by positive feedback.

3. The Thinker (Indirect, Slow-paced, Reserved Relationships):

- **Characteristics:** Efficient, perfectionist, works well alone, prefers written communication, and values facts and logic.
- **Example:** An analyst who prefers to work independently and presents detailed reports based on thorough research.

4. The Director (Direct, Fast-paced, Reserved Relationships):

- **Characteristics:** Focuses on results and solutions, prefers clear and concise communication, likes to take control, and avoids small talk.
- **Example:** A project manager who gives direct instructions and is keen on meeting deadlines efficiently.

Summary:

- Assertive: clear, direct, respectful — gold standard for safety communication
- Passive: avoids conflict; withholds critical safety information — dangerous in high-hazard settings
- Aggressive: confrontational; may generate fear-based compliance but damages reporting culture
- Passive-Aggressive: indirect resistance; erodes safety culture from within over time.

EXAM TIP

Maslow, McGregor (Theory X/Y), Herzberg (Hygiene vs. Motivators), PDCA (Deming), Fayol's 14 Principles — all are exam favorites. Know the difference between hygiene factors (prevent dissatisfaction) and motivators (create satisfaction). Remember: assertive communication is the most effective workplace style.

Reference: Brauer, R.L. (2016). *Safety and Health for Engineers, 3rd Ed., Ch. 35 — Management and Leadership.*

13 Apply Project Management Principles and Techniques

The planning, executing, and overseeing of a project to achieve specific goals within defined constraints of time, budget, and resources is Project Management.

Safety professionals design, manage, and close complex projects — EHS programme launches, facility modifications, audit remediation, and technology implementations. The CSP must apply project management frameworks, RACI charts, scheduling tools, and budget management to safety-specific projects.

13.1 PMBOK Knowledge Areas

1. Project Integration Management — coordinating all aspects of the project
2. Project Scope Management — defining what is and is not included
3. Project Schedule Management — defining, sequencing, and controlling timelines
4. Project Cost Management — budgeting, estimating, and controlling costs
5. Project Quality Management — ensuring deliverables meet defined requirements
6. Project Resource Management — planning and managing human and physical resources
7. Project Communications Management — effective information exchange among stakeholders
8. Project Risk Management — identifying, analyzing, and responding to project risks
9. Project Procurement Management — acquiring goods and services from external vendors
10. Project Stakeholder Management — identifying and managing stakeholder engagement

13.2 Five Project Lifecycle Stages



- Initiating: define project at high level; identify stakeholders; obtain formal authorization
- Planning: develop detailed scope, WBS, schedule, resource plan, budget, risk register
- Executing: coordinate resources; implement planned activities; manage team performance
- Monitoring & Controlling: track against baselines; manage changes; report status to stakeholders
- Closing: finalize deliverables; obtain acceptance; document lessons learned; archive records

13.3 RACI Chart — Responsibility Assignment Matrix

RACI eliminates ambiguity about who does what and prevents both gaps and overlaps in accountability.

- Responsible (R): performs the work. Multiple Rs may share work on one task.
- Accountable (A): final decision authority. Only ONE person can be Accountable per task — most critical RACI rule.
- Consulted (C): subject matter experts whose input is sought before task completion
- Informed (I): stakeholders kept updated on progress and outcomes

Scenario — RACI Safety Example: Confined space programme rollout across 5 sites in 60 days. R: Site safety coordinators execute assessments. A: Corporate CSP — single accountability for quality and deadline. C: Industrial hygienist for exposure methodology; engineering for space classification. I: HR (training schedule); operations managers (access coordination).

KEY RULE

There can only be ONE Accountable person per task. Multiple Responsible persons are acceptable. Consulted is two-way communication; Informed is one-way.

13.4 Project Scheduling Tools

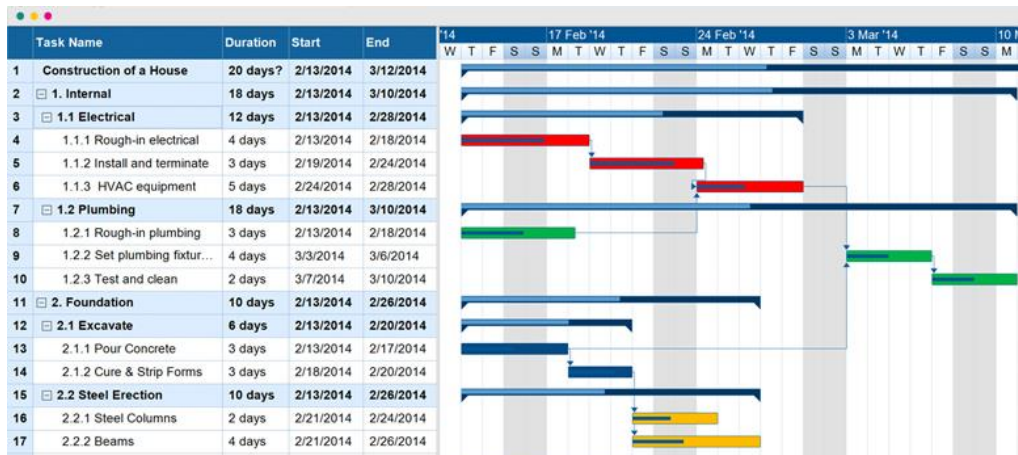
Tool	Description & Key Formula
Gantt Chart	Visual bar chart showing tasks against a timeline. Displays start/end dates, duration, dependencies, and progress. Most commonly used project scheduling tool.
Critical Path Method (CPM)	Identifies the LONGEST sequence of dependent tasks (critical path). Determines minimum project duration. Tasks on the critical path cannot be delayed without delaying the project.
PERT Chart	Program Evaluation Review Technique. Uses three time estimates per task: Optimistic (O), Most Likely (M), Pessimistic (P). PERT estimate = $(O + 4M + P) / 6$.
Earned Value Management (EVM)	Measures project performance by comparing planned work (PV) with actual completed work (EV) and actual cost (AC). Calculates CPI and SPI.
Kanban Board	Visual card-based system for managing workflow in real-time. Shows task status (To Do → In Progress → Done).
Lean PM	Maximizes value by eliminating waste (non-value-adding activities) and improving process efficiency.

Gantt Chart

Horizontal bar chart displaying project tasks on the vertical axis against a time calendar on the horizontal axis. Best for communicating schedule status to non-technical stakeholders. Limitation: does not explicitly show the critical path.

Critical Path Method (CPM)

Network-based scheduling techniques identifying the longest sequential chain of dependent tasks (the critical path) which determines the minimum project duration. Tasks NOT on the critical path have "float" or "slack" schedule flexibility that can be exploited to reallocate resources. Any delay to a critical path task delays the entire project.



Time Scheduling:

- **Definition:** The process of organizing tasks and activities within a project to ensure timely completion.
- **Example:** A construction project where tasks like foundation laying, plumbing, and electrical work are scheduled to occur sequentially or concurrently to meet the project's deadline.

Gantt Chart:

- **Definition:** A visual project management tool that displays tasks on a timeline, showing their start and end dates, duration, and dependencies.
- **Example:** In the provided Gantt chart, the construction of a house is broken down into tasks like "Electrical" and "Plumbing," with each task's timeline, dependencies, and progress displayed.

Key Features:

1. **Tasks and Subtasks:** The chart lists tasks and subtasks (e.g., "Rough-in electrical") with their durations.
2. **Timeline:** Horizontal bars represent the duration of each task over a calendar period.
3. **Dependencies:** Arrows indicate dependencies between tasks, showing the sequence in which tasks should be completed.
4. **Progress:** Colored bars may represent the completion status of each task.

Example Scenario:

Construction Project: The Gantt chart for a house construction project helps the project manager see that "Electrical" work starts on 2/13/2014 and ends on 2/28/2014. It shows how tasks like "Install and terminate" depend on "Rough-in electrical," and their progress is tracked visually, helping ensure the project stays on schedule.

PERT — Program Evaluation and Review Technique

PERT Expected Time: $tE = (O + 4M + P) \div 6$

O = Optimistic | M = Most Likely | P = Pessimistic. Used when task durations involve uncertainty.

PERT accounts for duration uncertainty using three estimates. Widely used for safety programme planning where durations depend on regulatory timelines, resource availability, and contractor scheduling.

13.5 Stakeholder Management – Power/Interest Matrix

Stakeholder Category	Strategy
High Power + High Interest	MANAGE CLOSELY: Regular meetings, detailed updates, involve in key decisions (e.g., Project Sponsor)
High Power + Low Interest	KEEP SATISFIED: Periodic updates to maintain support (e.g., Senior Executive not directly involved)
Low Power + High Interest	KEEP INFORMED: Regular communication, gather feedback (e.g., End users of a new system)
Low Power + Low Interest	MONITOR (Minimum Effort): Occasional updates only (e.g., Distant department minimally impacted)

EXAM TIP

Know the RACI roles precisely — especially that only ONE person is Accountable. For scheduling, know the difference between Gantt (bar chart/timeline), CPM (critical path, cannot delay), and PERT (probabilistic time estimates). The 10 PMBOK knowledge areas are commonly tested.

14 Analyze and/or Interpret Data — Statistics, Exposure, Concentrations, Sampling

Statistical literacy is one of the most important and frequently underprepared competency areas for CSP candidates. Objective 14 requires calculation, interpretation, and application of descriptive statistics, probability, confidence intervals, Pareto analysis, and exposure data interpretation. This section follows the workshop slides directly and references David Yates (The Practice of Statistics) as the primary statistical study reference as per lecture.

14.1 Sampling Data

Sampling is the process of selecting a representative subset (sample) from a larger group (population) to draw conclusions without measuring every individual. Fundamental to industrial hygiene exposure assessment, environmental monitoring, and safety inspection programmes.

- Random Sampling: each population member has an equal probability of selection, which is essential for unbiased results and legally defensible exposure assessments
- Stratified Sampling: population divided into subgroups (strata); samples drawn proportionally — ideal when departments or jobs have very different exposure levels
- Systematic Sampling: every nth member selected from a ranked list — practical and defensible

Scenario — Sampling Example: Factory: 10,000 bolts/day. Inspecting all is impractical; inspect 100 randomly. 3 defective → estimated defect rate = 3%. Safety parallel: rather than monitoring all 50 workers in a department for noise, monitor 10 from each similar exposure group (SEG) and extrapolate to the group. This is the basis for the industrial hygiene exposure assessment strategy.

Reference: Yates, D.S., Moore, D.S., & Starnes, D.S. (2012). *The Practice of Statistics, 4th Ed., Ch. 4 — Designing Studies.*

14.2 Measures of Central Tendency

Mean (Arithmetic Average)

Mean: $\bar{x} = \Sigma x \div n$

Sum of all values divided by number of observations. SENSITIVE to extreme values (outliers).

The mean is appropriate for symmetrically distributed data without extreme outliers. In safety: mean TRIR across multiple years reveals trend direction; mean noise exposure across a workday provides the basis for TWA calculations.

Median

The middle value in a dataset is ranked in ascending or descending order. If n is even, the median = average of the two middle values. The median is NOT affected by outliers — making it the preferred central tendency measure for skewed distributions: workers' compensation claim values (a few catastrophic claims distort the mean), accident severity data, or any dataset with extreme outliers.

Mode

The most frequently occurring value. A dataset can be unimodal, bimodal, or multimodal. Most useful for categorical data (most common injury type, most common body part injured, most common root cause) and for identifying clusters in grouped exposure data. The ONLY central tendency measure is appropriate for nominal/categorical data.

EXAM TIP: Mean is affected by extreme values (outliers). Median is NOT. For skewed distributions (injury severity, WC claim costs), the median is more representative. Mode is used for categorical data. These distinctions are high-frequency exam questions.

Reference: Yates et al. (2012). *The Practice of Statistics, 4th Ed., Ch. 1 — Exploring Data.*

14.3 Degree of Variation

Central tendency alone is insufficient — spread (variability) around the mean is equally important for safety data interpretation.

Population Variance: $\sigma^2 = \Sigma (x - \mu)^2 \div N$

μ = population mean; N = total population size. Use when you have data for ALL individuals.

Sample Variance: $s^2 = \Sigma (x - \bar{x})^2 \div (n-1)$

Use $(n-1)$ — Bessel's correction — for sample variance to correct for bias from using sample mean.

Standard Deviation: σ (population) = $\sqrt{\sigma^2}$ or s (sample) = $\sqrt{s^2}$

Standard deviation is in the same units as original data — more interpretable than variance.

Small SD: data points clustered near the mean (consistent performance). Large SD: high variability (inconsistent performance across departments or time periods). High variability in exposure measurements signals need additional monitoring or controls.

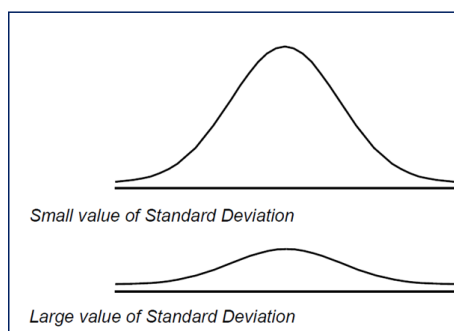
EXAM TIP: Refer the Practice using Scientific calculator as guided in lectures, to understand how to input and get output of statistical data using physical/on-screen calculator.

14.4 Normal Probability Distribution

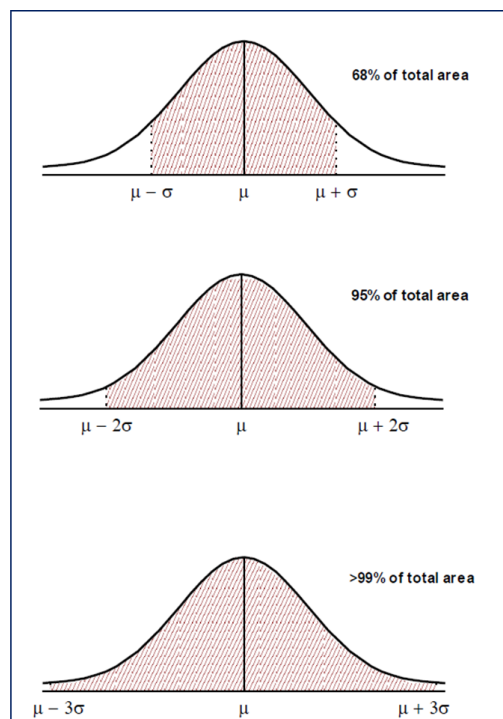
The normal distribution, also known as the Gaussian distribution, is a continuous probability distribution characterized by a symmetric, bell-shaped curve. It is defined by its mean (μ) and standard deviation (σ). Many statistical tests assume normality because of its useful properties in inferential statistics. The normal distribution (bell curve) is symmetric, with mean = median = mode. Empirical Rule (68-95-99.7 Rule):

- 68% of data falls within ± 1 standard deviation of the mean
- 95% of data falls within ± 2 standard deviations of the mean
- 99.7% of data falls within ± 3 standard deviations of the mean

Chemical concentration data often follows a log-normal distribution — the logarithms of measurements are normally distributed. For log-normal exposure data, geometric means is the appropriate measure of central tendency.



1 std dev = 68% of the data set
 2 std dev = 95.45% of the data set
 3 std dev = 99.73% of the data set



Reference: Yates et al. (2012). *The Practice of Statistics, 4th Ed., Ch. 2 — Modelling Distributions of Data.*

14.5 Confidence Intervals

A confidence interval (CI) provides a range of plausible values for an unknown population parameter based on sample data. It quantifies the uncertainty inherent in estimation from a sample.

Confidence Interval: $CI = \bar{x} \pm (z^* \times SE)$

$\bar{x}$ = sample mean | z^* = critical value (1.645 for 90%, 1.96 for 95%, 2.576 for 99%) | $SE = s/\sqrt{n}$

Correct Interpretation

A 95% CI means: if the sampling procedure were repeated many times, 95% of the calculated intervals would contain the true population mean. It does NOT mean there is a 95% probability that the true value is in this specific interval.

Factors Affecting CI Width

- Larger sample size (n) → narrower CI → more precise estimate
- Lower confidence level (e.g., 90% instead of 95%) → narrower CI → less certainty
- Smaller population standard deviation → narrower CI

Safety Applications

- Industrial hygiene: 95% CI around TWA estimate — if upper bound < PEL/TLV, exposure is controlled at required confidence level
- Risk assessment: wide CI around injury rate estimate signals need for more data collection
- Epidemiology: CI around relative risk estimates determines statistical significance

Scenario — CI Calculation Example: 25 noise measurements in packaging department. $\bar{x} = 85$ dB, $s = 4$ dB. 95% CI = $85 \pm (1.96 \times 4/\sqrt{25}) = 85 \pm 1.57$. CI: [83.43 dB, 86.57 dB]. Upper bound 86.57 dB < OSHA PEL 90 dB — exposure appears controlled at 95% confidence. However, proximity to 85 dB action level warrants engineering review.

Reference: Yates et al. (2012). *The Practice of Statistics, 4th Ed., Ch. 8 — Estimating with Confidence.*

Probabilities

Probability: $P(\text{Event}) = \text{Favorable Outcomes} \div \text{Total Possible Outcomes}$

Range: $0 \leq P \leq 1$. Total probability of all outcomes = 1 (100%).

Key probability rules (CSP exam favourites):

- $0 \leq P \leq 1$ for any event. $P = 0$ means impossible; $P = 1$ means certain.
- Sum of all mutually exclusive outcome probabilities = 1 (100%)
- Multiplication Rule (Independent Events): $P(A \text{ and } B) = P(A) \times P(B)$
- Addition Rule (Mutually Exclusive Events): $P(A \text{ or } B) = P(A) + P(B)$

Scenario — Probability Examples: 4 out of 20 workers had minor injuries: $P(\text{injury}) = 4/20 = 0.20$. $P(\text{wears PPE}) = 0.9$. $P(\text{no injury} \mid \text{PPE}) = 0.95$. $P(\text{wears PPE AND no injury}) = 0.9 \times 0.95 = 0.855$ (85.5%). FTA application: OR gate $P(A \text{ or } B) \approx P(A) + P(B)$ for rare events. AND gate $P(A \text{ and } B) = P(A) \times P(B)$ assuming independence.

Inovo Global Training & Advisory Services

Probabilities

- **Formula**

$$\text{Probability} = \frac{\text{Number of favorable outcomes}}{\text{Total possible outcomes}}$$
- **Example**
 Out of 20 workers, 4 had minor injuries. $P(\text{Injury}) = \frac{4}{20} = 0.20 = 20\%$
- **Key Rules (CSP Favorite)**
 - $0 \leq \text{Probability} \leq 1$
 - Total probability = 1 (100%)
 - If events are independent: $P(A \text{ and } B) = P(A) \times P(B)$
- **Example**
 - $P(\text{worker wears PPE}) = 0.9$
 - $P(\text{no injury} | \text{PPE}) = 0.95$
 - $P(\text{PPE AND no injury}) = 0.9 \times 0.95 = 0.855$

85.5% chance




Reference: Yates et al. (2012). *The Practice of Statistics, 4th Ed, Ch. 5 — Probability: What Are the Chances?*

Pareto Analysis — 80/20 Rule

Pareto analysis identifies the small number of causes responsible for the majority of problems or costs. Applies the Pareto Principle: ~80% of outcomes are produced by 20% of causes. Shown on the exam as a bar chart with a cumulative percentage line.

- Purpose: focus corrective action on the 20% of causes producing 80% of incidents/costs
- Method: collect data on causes, rank highest to lowest by frequency or cost, plot as Pareto chart with cumulative % line
- Decision rule: address causes up to the 80% cumulative line first
- CSP Applications: rank injury types by frequency; rank departments by TRIR; rank hazard types by severity; allocate programme budget to the top 20% of causes

Scenario — Pareto Safety Example: 12 months incident data: slips/trips 42, struck-by 18, overexertion 14, caught-in 9, chemical 7, other 10 = 100 total. Pareto ranking: slips/trips 42% → struck-by 60% cumulative → overexertion 74% → caught-in 83%. Action: focus 80% of corrective investment on slips/trips, struck-by, and overexertion — these three account for 74% of all incidents.

EXAM TIP: Pareto charts are frequently displayed with bar chart + cumulative line. The 80% cumulative line identifies the "critical few" causes. Always state the 80/20 rule and name which causes fall within the critical 80% in your answer.

Example

Causes of workplace accidents:

Cause	Number of Accidents
Slips	40
Falls	25
Cuts	20
Burns	10
Others	5

 Slips + Falls = 65% of accidents

Exposure and Release Concentrations

Release Concentration

The amount of a hazardous substance released at the source or point of discharge (leak, vent, stack, spill). Expressed as ppm, mg/m³, or kg/hour. Used for worst-case and credible release scenario assessment; process safety analysis; emergency planning (EPCRA); and environmental permit compliance.

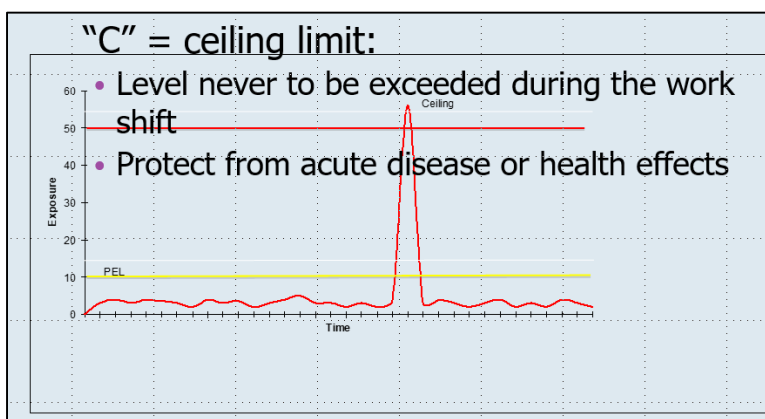
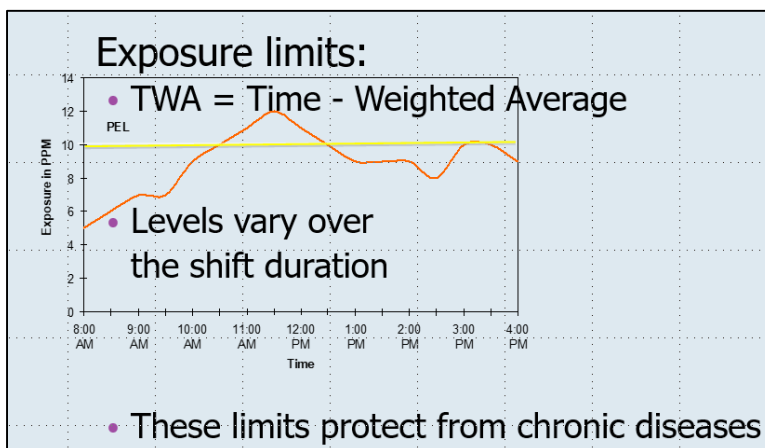
Exposure Concentration

Exposure refers to the amount of a hazardous substance to which workers or the public are actually subjected. It is typically measured at the breathing zone or receptor location and compared against established health-based exposure limits such as OELs, TLVs, PELs, and IDLH values. Exposure assessment is used to evaluate potential health risks and to determine the need for appropriate control measures, including engineering controls, personal protective equipment (PPE), and administrative controls.

Key Exposure Limits — Terminology

- PEL (Permissible Exposure Limit): OSHA's legal standard; maximum allowable airborne concentration; based on 8-hour TWA. Enforceable. Many PELs are outdated (largely unchanged since 1971).
- TLV (Threshold Limit Value): ACGIH guideline; more health-protective and regularly updated; not legally enforceable but treated as standard of care in litigation.
- STEL (Short-Term Exposure Limit): maximum 15-minute exposure; complement to 8-hour TWA; protects against acute effects of brief high-concentration exposure.
- Ceiling (C): concentration that must NEVER be exceeded at any time during the work shift; protects against acute, immediate health effects; no time averaging permitted.

- IDLH (Immediately Dangerous to Life or Health): concentration posing immediate risk to life; requires SCBA for entry; NIOSH-defined.



Time-Weighted Average (TWA)

$$\text{TWA} = \frac{\sum (C_i \times T_i)}{8}$$

C_i = concentration during period i / T_i = duration in hours / Denominator = 8 hours (full shift).

$$\text{TWA} = \frac{(C_1 T_1) + (C_2 T_2) + \dots + (C_n T_n)}{\text{total hours worked}}$$

TWA represents average exposure weighted by duration across an 8-hour workday. Both OSHA PEL and ACGIH TLV are expressed as 8-hour TWAs. Protects against chronic, long-term health effects.

Scenario — TWA Calculation: Benzene exposure: 2 ppm for 3 hours, 0.5 ppm for 4 hours, 0 ppm for 1 hour. $TWA = [(2 \times 3) + (0.5 \times 4) + (0 \times 1)] \div 8 = [6 + 2 + 0] \div 8 = 1.0$ ppm. OSHA PEL for benzene = 1.0 ppm. Exposure equals the PEL — engineering controls or substitution should be evaluated immediately.

Extended Shift PEL/TLV Adjustment

When workers operate 10- or 12-hour shifts, standard PELs must be adjusted downward to account for extended exposure and reduced recovery time. The Brief & Scala model is the most commonly applied adjustment approach.

$$PEL_{n \text{ hours}} = \frac{PEL(\text{or TLV}) \times 8 \text{ h}}{(\text{actual shift worked in hours})}$$

Brief & Scala Adjustment: $RF = (8/h) \times [(24-h)/16] \rightarrow \text{Adjusted PEL} = PEL \times RF$

h = hours worked per shift. RF = Reduction Factor.

Scenario — Extended Shift Example: 10-hour shift. $RF = (8/10) \times [(24-10)/16] = 0.8 \times 0.875 = 0.70$. A substance with PEL = 100 ppm (8-hr) becomes 70 ppm on a 10-hour shift. Any exposure above 70 ppm on a 10-hour schedule exceeds the adjusted limit.

Reference: Yates et al. (2012). *The Practice of Statistics, 4th Ed., Chs. 1–2, 4–6, 8 — Core Statistical Methods.*

Reference: Brauer, R.L. (2016). *Safety and Health for Engineers, 3rd Ed., Ch. 26 — Exposure Assessment and Air Monitoring.*

14.6 Scientific Calculator — Exam Information

- Casio: FX-115, FX-250, FX-260, FX-300 series
- Hewlett-Packard: HP 9, HP10, HP12, HP30 series
- Texas Instruments: TI-30, TI-34, TI-35, TI-36 series

On Screen calculator is also available in Exam equivalent to TI-30 model.

Practice all rate calculations (TRIR, DART, ROI, PERT), statistical calculations (mean, standard deviation, CI), and probability calculations using your approved model before exam day.

Key References

Brauer, R.L. (2016). Safety and Health for Engineers, 3rd Edition. John Wiley & Sons. [Chs. 3, 4, 5, 10, 13, 26, 35, 36, 37, 38 — Referenced across Objectives 1–13]

Yates, D.S., Moore, D.S., & Starnes, D.S. (2012). The Practice of Statistics, 4th Edition. W.H. Freeman. [Chs. 1–2, 4–6, 8 — Referenced in Objective 14: sampling, mean/median/mode, standard deviation, normal distribution, confidence intervals, probability]

BCSP (2024). CSP V11.0 Examination Blueprint. Board of Certified Safety Professionals. www.bccsp.org

ISO 45001:2018. Occupational Health and Safety Management Systems — Requirements with Guidance for Use.

ISO 19011:2018. Guidelines for Auditing Management Systems.

ISO 14001:2015. Environmental Management Systems — Requirements with Guidance for Use.

ANSI/ASSP Z10.0-2019. Occupational Health and Safety Management Systems.

OSHA 29 CFR 1910.119. Process Safety Management of Highly Hazardous Chemicals. [MOC — Objective 5]

OSHA 29 CFR 1910.1020. Access to Employee Exposure and Medical Records. [Objective 10]

OSHA 29 CFR 1910.38 / 1910.39. Emergency Action Plans / Fire Prevention Plans. [Objective 9]

Project Management Institute (2021). PMBOK Guide, 7th Edition. [Objective 13]

ACGIH (2024). Threshold Limit Values for Chemical Substances and Physical Agents. [Objective 14]

Inovo Global Training & Advisory Services. CSP V11.0 Workshop Slides — Domain 2 (143 Slides). [Primary structural reference for this expanded lecture notes edition]

INOVO GLOBAL Training & Advisory Services | www.inovoglobals.com | info@inovoglobals.com

Confidential — For Registered Candidates Only. Do not copy or disclose without prior consent.