The Controls That Cannot Fail

An organization can have thousands of completed inspections, strong injury-frequency numbers, and an impressive training record, yet still be one failed barrier away from a fatality, major fire, explosion, equipment loss, or long business interruption. High-severity risk demands a different question: which controls must work every time?

> A 97% inspection score is not reassuring if the failed 3% contains the control standing between normal work and catastrophic loss.

Not every control deserves equal weight

Traditional safety programs generate enormous amounts of activity. Inspections are completed. Procedures are reviewed. Courses are assigned. Audits produce action lists. Leading indicators count observations, meetings, corrective actions, and training hours.

Most of that activity can be useful. The problem is that a management system can accidentally treat controls as though they are equally important.

They are not.

A faded floor marking and a failed emergency shutdown device may both appear as inspection deficiencies. One deserves correction. The other may require an immediate decision about whether the process can continue at all.

This is the logic behind critical control management. Instead of starting with the entire universe of rules and controls, the organization starts with its most serious credible loss scenarios and asks which few controls are essential to preventing the event or limiting its consequences.

Critical control management is moving into the mainstream

The concept has deep roots in mining and process safety, but it is increasingly relevant to any organization managing high-consequence exposures.

In 2026, the International Council on Mining and Metals released an updated Critical Control Management Good Practice Guide. The guidance focuses on identifying the most serious health and safety hazards, selecting the controls that are truly critical, defining how those controls must perform, assigning ownership, and verifying that the controls are effective in practice.

The updated guidance also introduces readiness checks and a maturity model and makes the important point that the methodology can be adapted beyond health and safety to other operational risks.

That matters to insurers and general safety managers because the same discipline applies to fatal injury hazards, property loss, equipment breakdown, fleet catastrophe, fire protection, environmental loss, and business interruption.

Primary reference: ICMM Critical Control Management Good Practice Guide 2026

Start with the event you cannot afford

Safety programs often start by listing hazards. Critical-control thinking starts by defining the event.

What are the serious scenarios that could kill someone, cause permanent disability, destroy critical equipment, start a major fire, release hazardous material, disable a key site, or stop the business for weeks?

The wording matters. “Forklifts” is a hazard category. “Pedestrian struck by reversing forklift in a mixed-traffic loading zone” is a scenario. The second version is specific enough to identify which controls actually matter.

The same is true for property and operational risks. “Electrical” is broad. “Transformer failure causing fire and loss of the only incoming feed to the plant” is a high-consequence scenario that can be analysed.

Broad topic	High-consequence scenario	Possible critical controls
Mobile equipment	Pedestrian struck by moving equipment in a shared work area.	Physical separation, effective traffic design, functioning detection or warning systems, controlled reversing, competent operators.
Hazardous energy	Worker exposed to unexpected energization during maintenance.	Verified isolation, effective lockout, isolation-point integrity, test for zero energy, control of stored energy.
Work at height	Worker falls from an elevated work location.	Engineered prevention, compliant access, correctly selected and functioning fall protection, verified anchor or restraint system.
Fire	Ignition grows into a major property and business-interruption loss.	Ignition control, automatic protection, water supply, separation, tested fire-protection systems, impairment management.
Confined space	Worker enters an oxygen-deficient or toxic atmosphere.	Isolation, atmospheric testing, ventilation where required, entry control, rescue capability matched to the hazard.

Broad topic	High-consequence scenario	Possible critical controls
Critical equipment	Single-point equipment failure stops a major process.	Asset integrity, functioning safety devices, condition monitoring, tested contingency plan, critical spares.

These examples are illustrative. The organization must identify its own scenarios and controls through competent risk assessment. The point is not to copy a universal list. It is to distinguish the controls whose failure fundamentally changes the risk.

Use PROVE to manage high-severity controls

P: Pinpoint the high-consequence event

Describe the event clearly enough that people understand what must be prevented. Include the people, equipment, energy, location, and consequence. Avoid vague labels that hide the actual pathway to loss.

R: Reduce the list to truly critical controls

A critical control is not simply a useful precaution. It is a control whose absence or failure would materially increase the likelihood or consequence of the event. If every control is called critical, the organization loses the ability to focus.

O: Own the control

Name the person or role accountable for the health of the control. Ownership means more than completing a checklist. The owner must understand the performance standard, know when the control is degraded, and have authority to escalate.

V: Verify performance

Define what evidence demonstrates that the control is present, functioning, understood, and used under actual operating conditions. Verification should be proportionate to consequence and independent enough to detect normalization.

E: Escalate degradation

Decide in advance what happens when verification fails. Some degraded controls permit temporary compensating measures. Others should trigger immediate stop-work, shutdown, or removal from service. The decision should not be invented after the failure is discovered.

Performance standards make critical controls measurable

Saying that a control “exists” is not enough. A critical control needs a performance standard.

For a barrier, the standard may define location, load rating, dimensions, inspection frequency, and acceptable condition. For atmospheric testing, it may define instrument type, calibration, test locations, acceptable limits, frequency, and action thresholds. For a fire pump, it may define availability, testing, water

supply, alarm function, impairment response, and restoration requirements.

Performance standards turn verification from opinion into evidence.

They also improve training. Workers no longer learn only that a control is required. They learn what healthy performance looks like, how degradation appears, and what to do when the control cannot meet its standard.

Control state	Meaning	Typical response
Green	Control meets the defined performance standard.	Work continues with normal monitoring and scheduled verification.
Amber	Control is degraded but a competent assessment confirms temporary compensating measures can maintain acceptable risk.	Escalate, document compensating measures, shorten review interval, set expiry, and prioritize restoration.
Red	Control is absent, failed, or cannot meet the minimum performance requirement and compensating measures are not adequate.	Stop or restrict the activity until the control is restored or the risk is otherwise reduced to an acceptable level.

Verification is different from inspection volume

Organizations can drown in inspection data and still know surprisingly little about their highest-severity controls.

A monthly inspection may confirm that a control was present on the day of inspection. Critical-control verification asks whether the control remains healthy under the conditions that matter and whether the people relying on it would recognize degradation.

The ICMM model is useful because it expects verification at multiple levels. Frontline workers confirm controls before and during work. Supervisors verify implementation. Operational leaders look for systemic weakness. Specialists provide technical assurance. Senior leaders confirm that the organization is managing its fatal-risk controls effectively.

The goal is not to create five redundant checklists. It is to make sure a catastrophic control does not depend on one person, one inspection, or one optimistic assumption.

A strong safety metric can still hide catastrophic exposure

Low injury frequency is good news, but it is not proof that high-severity risk is controlled.

Many catastrophic events are low-frequency by nature. A plant can operate for years without a serious electrical incident while protective equipment quietly degrades. A fleet can log millions of miles without a fatal collision while an unsafe routing or fatigue pattern remains. A facility can have excellent housekeeping scores while a critical fire-protection impairment persists.

That is why insurers care about severity as well as frequency. The losses that threaten capacity, reputation, and continuity often come from a small number of scenarios with very large consequences.

Critical-control management gives safety managers and insurers a shared language for those exposures.

> The absence of a catastrophic loss is not evidence that the critical controls are healthy. It may simply mean they have not been challenged yet.

Training becomes sharper when workers know what cannot fail

Traditional training often gives every rule similar emphasis. Workers leave with a long list of requirements but little sense of which controls deserve absolute attention.

Critical-control training changes that. The worker still learns the broader procedure, but the trainer makes the high-consequence controls unmistakable.

For a lockout task, the message is not merely “complete the procedure.” It is “verified energy isolation is the barrier standing between this task and unexpected energization. If zero energy cannot be confirmed, work does not begin.”

For mobile equipment, the worker learns not only the traffic rules but which separation controls must be present before mixed pedestrian and vehicle activity can proceed.

This does not simplify the hazard. It improves prioritization. Workers should understand the purpose of the critical control, how to recognize its failure, what compensating measures are allowed, and when they have authority or obligation to stop.

- Why the control matters and which high-consequence event it prevents.
- What normal or healthy performance looks like.
- What degradation or failure looks like.
- Who owns the control and who can authorize temporary changes.
- What workers must do when the control is not available.
- Which conditions require stop-work rather than another corrective-action ticket.

Contractors need the same critical-control picture

Contractors often arrive with their own procedures, training, and terminology. That can create a dangerous mismatch when the host organization has specific critical controls for high-consequence work.

A competent electrician may still need to understand the host’s isolation standard. A crane contractor may understand lifting but still need the site’s exclusion-zone rules and communication protocol. A maintenance contractor may know confined-space entry but not the plant’s process-isolation boundaries.

Contractor orientation should therefore identify the controls that cannot fail, not bury them inside a 60-page site rulebook.

Critical controls connect safety, maintenance, and capital decisions

One of the most valuable features of the method is that it exposes when a “safety problem” is really an engineering or asset-management problem.

If a critical fire-protection system repeatedly fails verification, more training is not the primary solution. If pedestrian separation is impossible because the warehouse layout forces people through vehicle lanes, reminders to “stay alert” are weak controls. If a safety device has reached the end of reliable life, the capital plan may be the real risk-control plan.

This is important for insurers because verification findings create better risk conversations. The loss-control professional can see not only whether a policy exists, but whether the controls protecting the largest exposures are healthy and whether management responds appropriately when they are not.

The insurance conversation gets better when it focuses on control health

Insurance loss-control surveys often produce large numbers of observations. Critical-control thinking can make those observations more useful by connecting them to credible loss scenarios.

Instead of asking only whether the policyholder has a safety program, the insurer can ask whether the organization can identify its major loss scenarios, name the controls that protect them, show the performance standards, and demonstrate recent verification results.

That information can support underwriting, risk engineering, policyholder coaching, targeted training, and follow-up. It also helps separate organizations that produce safety activity from organizations that understand their exposure.

For policyholders, the same discipline helps prioritize limited resources. Capital, inspection, maintenance, training, and leadership attention can be directed toward the controls that influence potential severity most.

Monetize severity, not just frequency

Minor incidents occur often enough that their cost is visible. Catastrophic events are harder to price because they are infrequent. That can create a dangerous bias toward spending resources on the problems that happen most often rather than the events that could threaten the enterprise.

A practical business case does not require pretending the probability of a catastrophic event is known precisely. It asks what the credible consequence is, how much the critical control costs to maintain, and whether the organization is comfortable carrying the residual risk if the control is degraded.

OSHA’s business-case resources reinforce the broader economic point. Workplace injuries produce both direct costs and indirect losses such as investigation, replacement training, productivity loss, and property damage. A high-consequence event can add extended shutdown, legal exposure, emergency contracting, lost customers, and major capital replacement.

The comparison is rarely “spend money on safety or save money.” It is “spend

deliberately on the controls that prevent the largest credible losses or accept the financial exposure created when they fail.”

Financial reference: OSHA Business Case for Safety and Health

A critical-control dashboard should be small

The dashboard should not become another 100-metric scorecard. If leadership cannot see the health of the most important controls quickly, the system is too complicated.

Measure	Question it answers
Critical controls identified	Do we know which barriers matter most for each high-consequence scenario?
Performance standards defined	Do we know what healthy operation actually means?
Verification current	Have the controls been checked at the required frequency and level?
Controls degraded	How many are amber or red today?
Repeat degradation	Which controls repeatedly fail or require temporary compensation?
Time to restore	How long do degraded critical controls remain unresolved?
Stop-work decisions	Does the organization actually stop or restrict work when critical controls fail?
Learning closed	Are recurring failures driving engineering, maintenance, training, or management changes?

Where SafetyNow can support the system

Critical-control management is not a training program. It is an operational risk-management method. SafetyNow’s role sits in the human-performance layer.

Insurance partners and employers can use role-specific eLearning, mobile refreshers, supervisor tools, contractor modules, scenario exercises, and centralized learning records to make critical-control expectations consistent across locations and workforces.

The strongest use case is not “assign another course.” It is to connect training to the controls that matter most. Workers learn why the control matters, how to recognize degradation, and what to do when the barrier is not available. Supervisors receive a repeatable way to reinforce and verify those expectations.

Explore: SafetyNow Online Training | SafetyNow Insurance solutions

A 90-day critical-control pilot

Period	Action	Result
Days 1-30	Choose one high-consequence scenario. Define the event, map existing controls, and identify which are truly critical.	A focused control set rather than a broad hazard checklist.

Period	Action	Result
Days 31-60	Define performance standards, owners, verification methods, escalation rules, and worker training requirements.	Clear evidence of what healthy control performance looks like.
Days 61-90	Run frontline and leadership verification, test the escalation response, correct weak controls, and review findings with operations and risk leaders.	Evidence that the method works before scaling to other scenarios.

The next generation of loss prevention will ask for proof

Safety systems will always need procedures, training, inspections, and audits. The opportunity is to become more discriminating about what deserves the greatest attention.

For high-severity risk, counting activity is not enough. Leaders need evidence that the barriers protecting people, property, and continuity are healthy today.

That changes the management question from “Did we complete the inspection?” to “Can we prove the critical control works?”

For safety managers, that is a more operational conversation. For insurers, it is a better view of risk quality. For workers, it makes the line between normal work and unacceptable exposure much clearer.

The organizations that manage catastrophic risk well will not necessarily be the ones with the longest checklists. They will be the ones that know which controls cannot fail and act immediately when those controls begin to weaken.