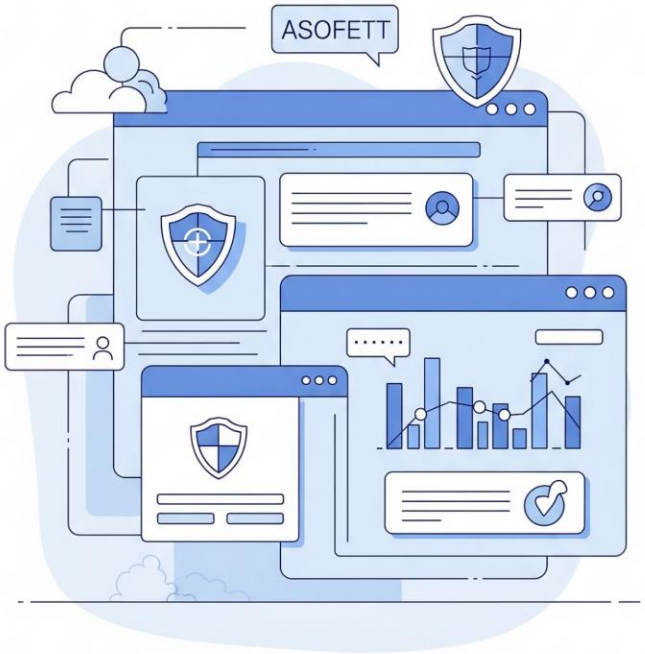
Why AI Is Replacing Manual Critical Control Management

Where are you watching from?

What's your one question?



CHRISTIAN YOUNG / IMPRESS SOLUTIONS / CRITICAL RISK AI

35–45 MINUTES + Q&A

MINE GUARD AI

Why AI Is Replacing Manual Critical Control Management

Practical tactics first. Risks and guardrails. Then a better way.

EKIN ERAYDIN | MINEGUARD AI / CRITICAL RISK AI

35–45 MINUTES + Q&A

MINE GUARD AI

How do you currently use AI in Critical Control Management?

Where are we spending our time?

The big time sink isn't CCM thinking — it's the rework: drafting, formatting, quality assurance, version drift, and constant rewrites that consume your team's capacity. Most risk professionals spend more time reformatting documents than actually managing risk.

AI Reduces Effort By:

Drafting

Structured first-passes for bowties, standards, and verifications

Standardising

Language and quality consistency across documents

Checking

Logic, duplication, and missing pieces automatically

Generating

Fit-for-purpose verification packs ready to deploy

Question

Where do you lose the most time today?

- Drafting bowties
- Discussing and aligning on a bowtie
- Defining Controls and Critical Controls
- Drafting Performance standards
- Verification design and update
- Assurance/QA
- Keeping things current
- Other?

Who We Are

Industry leaders in safety with proven results in the mining sector

Ekin Eraydin

Director, Mine Guard AI

15 Years Mine Site Operations

Site Senior Executive (Statutory role)

UQ MBA, M.Sc.

Cem Caglar

Technical Director, Mine Guard AI

20 years of enterprise software development

Expert in software architecture and design

Principal AI Engineer

Christian Young

CEO, Impress Solutions

25 years of experience across sites

Internationally recognised HSE executive

Change management and strategic HSE Advisor

*Piloting partners

Mine Guard AI has been selected as one of the CORE Innovations Hot 30 in the Australian Resources Sector – one of only two companies from Queensland recognized this year.

MINE GUARD AI

The "Right Way" to Think About Generic AI in CCM

Generic AI Is Best Used As:

Draft Engine

Creates structure and wording quickly, giving you a solid starting point rather than a blank page

Quality Checker

Ensures consistency and completeness across documents, catching gaps before they become problems

Translation Layer

Turns your standards into usable, verifiable steps that field teams can actually implement

Not Ideal As:

- The final authority on critical controls
- The single source of truth without human oversight
- A replacement for SME review and approval processes

Chat Question: Which best describes your current use of AI for CCM?

1) Not using it
2) Ad hoc drafting
3) Some standards/templates
4) Formal workflow
5) Fully governed

AI can draft a Bowtie Fast (Without Losing Quality)

The key to effective bowtie development with generic AI is providing the right context and structure from the start. This transforms a potentially chaotic process into a repeatable, quality-driven workflow.

01

Provide Context

Define the Material Unwanted Event (MUE), operational boundaries, and key assumptions

02

Request Structure

Ask for threats → preventive controls → degradation factors → recovery controls → consequences

03

Force Format

Demand structured output: tables with clear control wording, not narrative text

04

Quality Check

Request identification of what's missing and what's duplicated

> **Mini Prompt Pattern:** "Draft a bowtie for [MUE] in [context]. Output a table. Label assumptions. Separate controls vs verifications. Include degradation factors."

Chat Question: What MUE would you pick for a 30-minute pilot? Drop one in chat.

AI can turn create Performance Critical for each Critical Control (Fast)

Vague controls are the enemy of effective verification. Generic AI excels at converting high-level control statements into testable, measurable requirements that your teams can actually verify in the field.

Purpose & Scope

What the control achieves and where it applies

Measurable Criteria

Clear pass/fail conditions that remove ambiguity

Tolerances & Thresholds

Specific limits where relevant to the control

Evidence Required

What proves the control is working as intended

Degradation Factors

How the control fails and what to watch for

Escalation Triggers

What to do when the control fails

Training

What specific training is required

Chat Question: What's your most "hard to write" performance standard? (e.g., fatigue, berms, exclusion zones, speed management, gas monitoring, isolation...)

Design Verification That Isn't Tick-and-Flick

Effective verification requires more than a checkbox. Generic AI can produce consistent, comprehensive verification plans that actually test whether controls are working — not just whether paperwork exists.

1. **What to Verify**
   Design, condition, usage, competency, monitoring
2. **How to Verify**
   Observe, test, review, or interview
3. **Who Verifies**
   Line versus independent verification
4. **Frequency**
   Risk-based scheduling aligned to exposure
5. **Acceptance Criteria**
   Clear pass/fail definitions
6. **Escalation Pathway**
   What happens when verification fails
7. **Evidence**
   What evidence is required to demonstrate control rating

Chat Question

Which problem do you see most in verification?

- Wrong thing verified
- No pass/fail criteria
- Poor evidence collection
- Wrong frequency
- No action after failure

QA & Standardisation (The "Hidden 90%" Win)

The real power of AI isn't just creating content — it's maintaining quality at scale. Automated quality assurance catches issues that would otherwise require hours of manual review, and it does so consistently across your entire control framework.

Use Generic AI to Automatically:

Detect Duplicates

Identifies near-duplicates across bowties that create confusion and maintenance burden

Apply's Quality Principles

Controls Vs Support Activities Vs Monitoring Activities; Bowtie MUE must be a loss of control event

Flag Weak Language

Catches vague controls like "ensure...", "as required...", or training-only controls that don't prevent events

Identify Missing Degradation

Highlights controls without degradation factors — a critical gap in most CCM frameworks

Check Alignment

Verifies that threats, controls, standards, and verifications all connect logically

Produce Action Lists

Generates prioritised "fix these 10 items first" reports that focus improvement efforts

Risks of Generic AI (The 5 Ways It Bites)

Generic AI delivers speed, but it introduces operational risks that can undermine your CCM framework if not managed properly. Understanding these risks is the first step to implementing practical guardrails.

Hallucinations

Confident but completely wrong outputs that look professional

Prompt Roulette

Different outputs per user, destroying consistency

No Traceability

Why is this control here? Who approved it? Unknown.

Data Governance

Where did the input go? Who can see it? Unclear.

Change Drift

Standards and verifications silently go stale over time

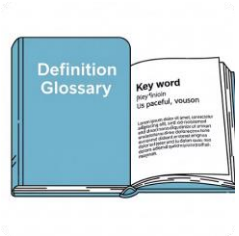
Chat Question: Which risk worries you most? 1–5

Minimum Guardrails (Safe, Practical, "Start Tomorrow")

You don't need a 50-page policy to start using AI safely. A lightweight governance model addresses the major risks whilst maintaining the speed benefits that make AI worthwhile.

Draft-Only Rule

AI creates drafts; humans always approve final content



Approved Definitions

Clear distinctions: control vs verification, critical vs non-critical

De-Identify Sensitive Details

Remove site-specific or confidential information from prompts

Audit Trail

Track input → output → reviewer → final version

The Real Friction: Scaling Generic AI Beyond One Champion

What Typically Happens:

- One person gets great results
- Others try, outputs vary
- Confidence drops
- Documents don't match
- No version control
- QA becomes manual again
- People revert to old ways

> **Key Message:** Generic AI works... until you need **consistency, traceability, and governance**.

The challenge isn't getting AI to work for one expert user. The challenge is getting it to work reliably for 50 supervisors, maintain quality across 200 controls, and still meet audit requirements six months later.

What a "Better Way" Looks Like

To make AI truly sustainable for CCM, you need more than clever prompts. You need a system designed specifically for critical control management — one that builds in the governance, structure, and quality controls that generic AI lacks.

Structured Data Model

Bowties and controls in a proper data structure, not free-text chaos

Standardised Templates

Performance standards that follow consistent formats automatically

Built-In QA Rules

Quality checks that aren't optional or easily skipped

Versioning & Audit Trail

Complete history of who changed what and when

Controlled Libraries

Approved controls, degradation factors, and verification types

Clean Exports

Outputs that export directly into governance packs without reformatting

Critical Risk AI: Solves the Generic AI Problems (And Keeps the Speed)

Critical Risk AI is purpose-built for CCM work. It delivers the speed benefits of AI whilst addressing the governance, quality, and consistency challenges that make generic AI difficult to scale across an organisation.

1

Structured Bowtie Model

Bowties generated and edited inside a proper data model, not documents

2

Consistent Templates

Performance standards drafted using standardised, approved templates

3

Built Verification

Verification steps created with pass/fail criteria and evidence expectations

4

Automated QA

Finds duplicates, weak controls, missing degradation factors, and misalignment automatically

5

Human-in-the-Loop

Approvals and audit trail show who approved what and when

MineGuard AI Enterprise EHS Platform

An integrated ecosystem designed to transform safety evidence into defensible action across your entire operation.

Incident AI

Live now – Investigation Workbench

Coming: Event Reporting and Notification

Risk AI

Operational risk management and mitigation

DEPLOY: Critical Risk AI

Identify, analyse, and manage critical risks and critical controls proactively

PILOT: Safety Management AI (SHMS)

Write, review and manage controlled documents

Assurance AI

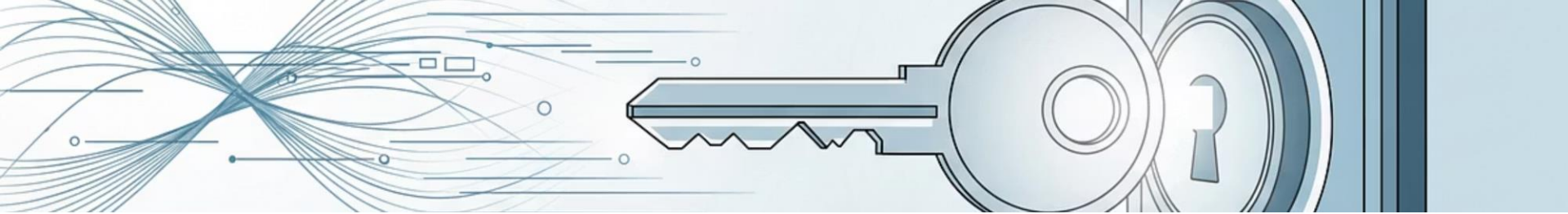
Real-time compliance monitoring and verification

Field Leadership AI

Enter, report, assess quality of your leadership

MINE GUARD AI

What's your one key learning / takeaway?



Your Free Trial Awaits: Critical Risk AI

As an exclusive offer for webinar attendees, claim your free trial license for Critical Risk AI. Experience the speed, consistency, and governance that will transform your Critical Control Management.

Request Free Trial License - Critical Risk AI – Fill in form

Next Bowtie Analysis Masterclass

Help is here – If you want the knowledge, tools and template to implement the CRM framework

IMPRESS SOLUTIONS
saving lives at work™

2-day Critical Risk Management Masterclass Brisbane 9th / 10th June

The Future of CRM	Industry trends and future developments
Elements of a CRM	Key components of a successful CRM program
Identification of Critical Risks	Developing and delivering a leading Baseline Risk Assessment
Analysis of Material Critical Risks	Bowtie Analysis, Layers of Protection Analysis, Identification of Controls and Critical Controls
Critical Control Performance Standards	Developing statistically significant verification processes
Site Implementation	Ensuring successful and sustainable CRM implementation
Verification, Reporting, and Response	Effective CRM reporting and response strategies