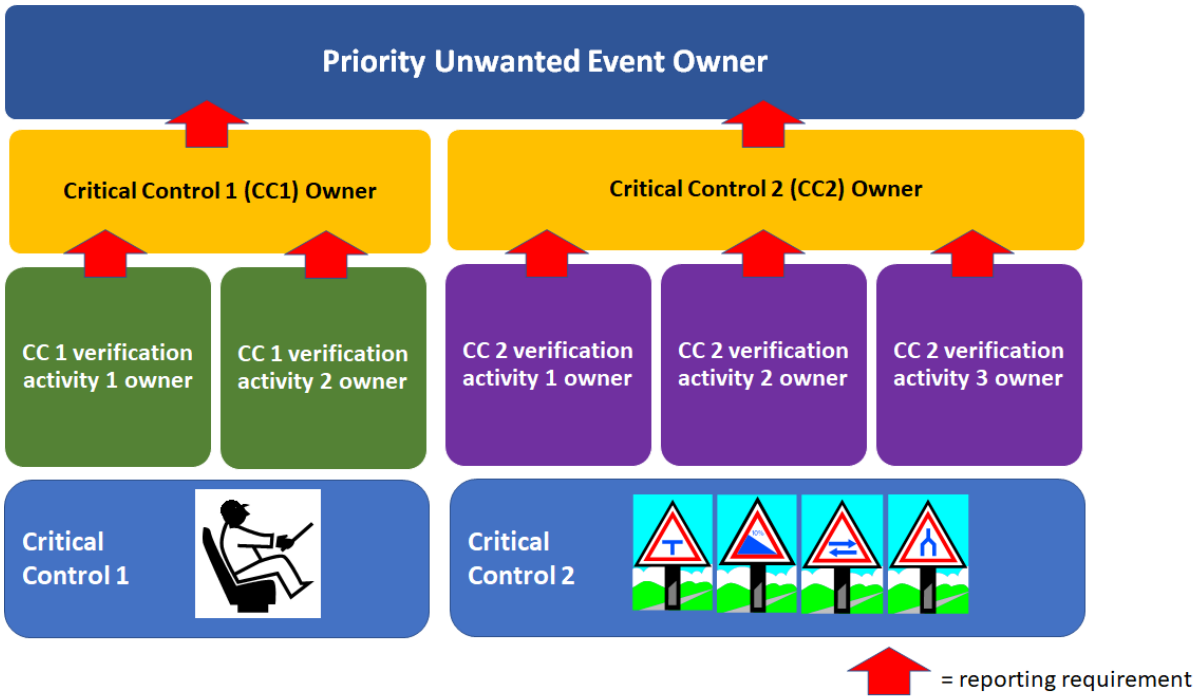
Article 13 – Defining accountabilities and the reporting process

Welcome to the 13th article in a series. This article will discuss establishing accountabilities and a reporting system so that the critical controls are effectively managed. As mentioned in previous articles, the Critical Control Management (CCM) process includes good practice risk assessment and analysis methods, plus an important greatly improved ingredient; more systematic management.

The last article addressed the careful definition of the verification mechanisms that gather data in a timely and effective manner. This is the 'check' in the Plan-Do-Check-Act model of management. Now we need effective reporting to connect the 'check' (verification) with the 'act' or action to improve by setting the accountabilities and defining the verification data-related information that should be reported to the accountable individuals.

The illustration below suggests an ownership model to set accountabilities for critical control verification and reporting. A site or company identifies several priority unwanted events (PUEs) that are included in their CCM initiative. Each of the PUEs is assigned to an owner. The owner is usually a line manager with responsibilities that include the activities where the PUE could occur. For example, at a site level the production manager could be the owner of a PUE related to vehicle collisions. If the CCM initiative is managed at the corporate level the vehicle collision PUE might be owned by a production executive.



The above illustration suggests three levels of ownership. The example PUE is related to vehicle collisions. Two example critical controls involving specific driving acts and road signage are provided.

In the example, two verification activities have been identified for critical control 1 (CC1) and three for critical control 2 (CC2). An owner is assigned for each of the verification activities. They are accountable for gathering the verification data with the defined frequency and forwarding that data to the critical control owner. Note that some assembly or interpretation of the data may be required before it is forwarded to the control owner. Acceptable levels of critical control effectiveness should have been defined as part of the performance requirements (see article 10). Formats such as stoplight reports, considering defined performance levels, might be helpful to concisely communicate verification data.

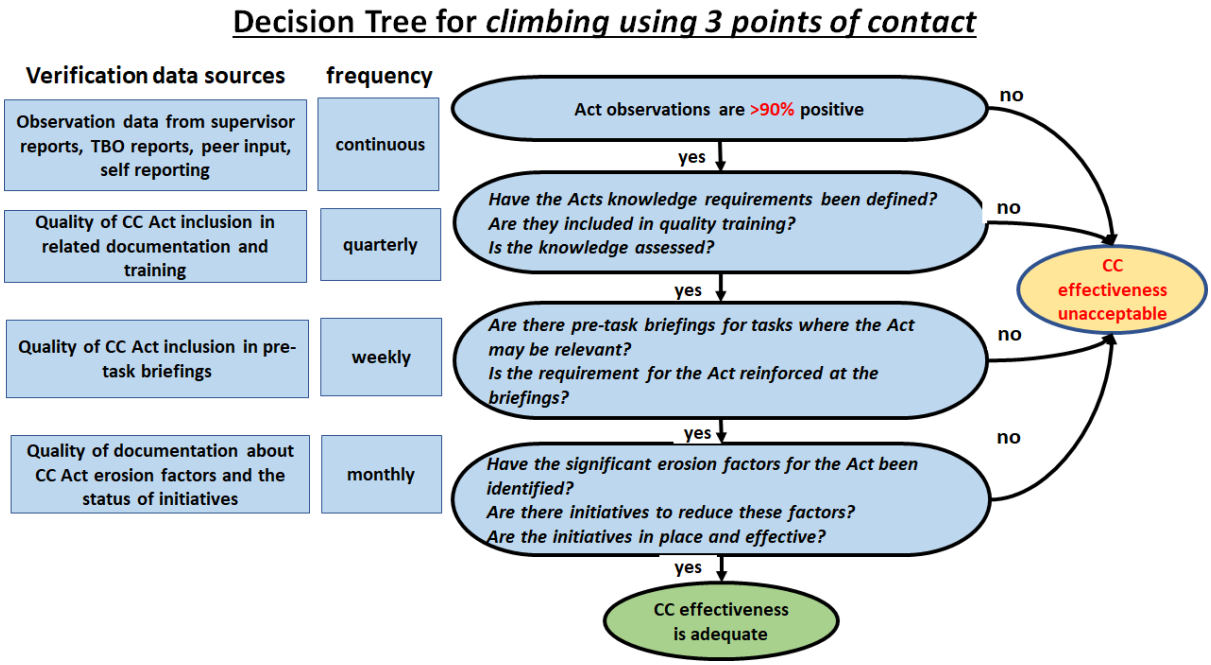
The illustration shows two critical control owners. Note that there may be more critical controls for a single PUE. The critical control owners assemble the data information from the verification activity owners to provide a single indicator of control effectiveness to the PUE owner.

As a result of this process, the PUE owner should get regular reports on the effectiveness of all critical controls related to his/her PUE with low and unacceptable effectiveness results

highlighted. Action should be taken to address unacceptable effectiveness as soon as possible, including the decision to stop the activities where the risk exists.

Managing the data and generating concise reporting can be a big challenge in this step of CCM. The above illustration shows only a small example segment of the process. If a site has 10 PUEs with 6 critical controls for each, there may be 5 verification activities for each control. That results in 300 sources of data and a team of 370 owners at various levels. Clearly a 'hard copy' paper-based approach to this size will be very punishing for a site or organisation. Data management technology should be considered.

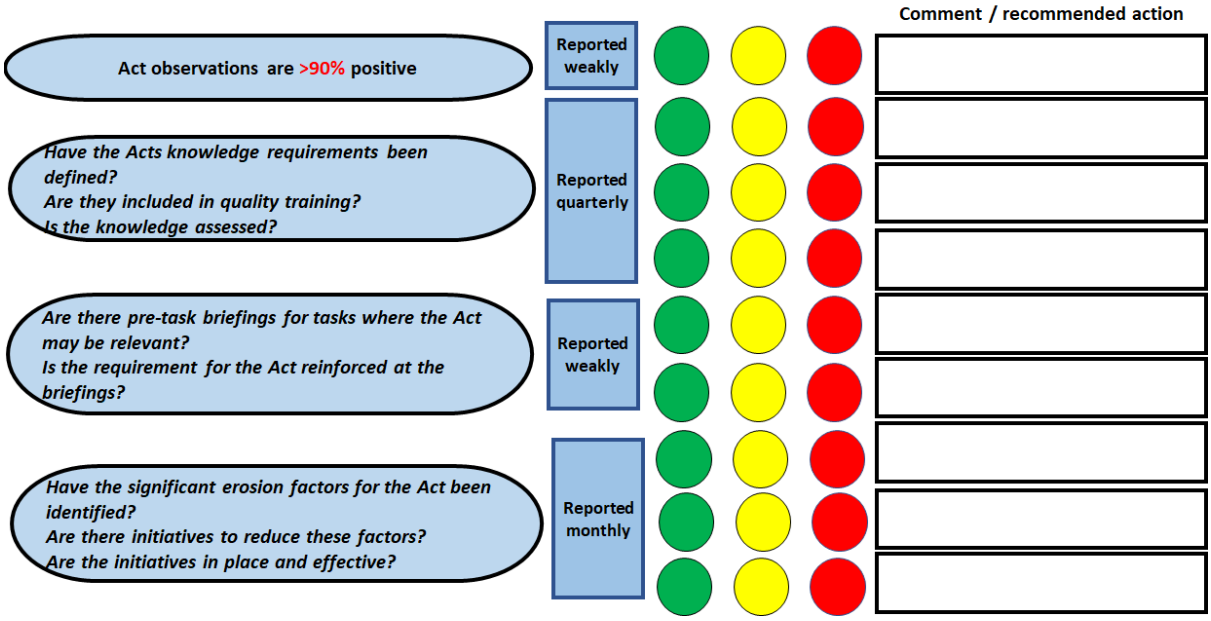
The example verification process outline from article 12 can be used to discuss electronic gathering of data and computer-assisted assembly and analysis.



In the above example there are four verification data sources (left boxes) that need to be gathered, assembled and reported to the appropriate owners. Each of the four sources has a different defined frequency for data gathering ranging from continuous to quarterly. Part of reporting system design should include the required reporting frequency. The site or company will decide on whether each of the four data sources is reported to the relevant owner separately or as one report. The latter is recommended.

If one report format is used for communicating verification information from several sources, such as the four areas illustrated above, then the report should be sent to the PUE owner at least weekly with information on the continuous and weekly verification activities. The monthly and quarterly verification data would be updated on the report when data was available. A rough illustration is provided below as an example.

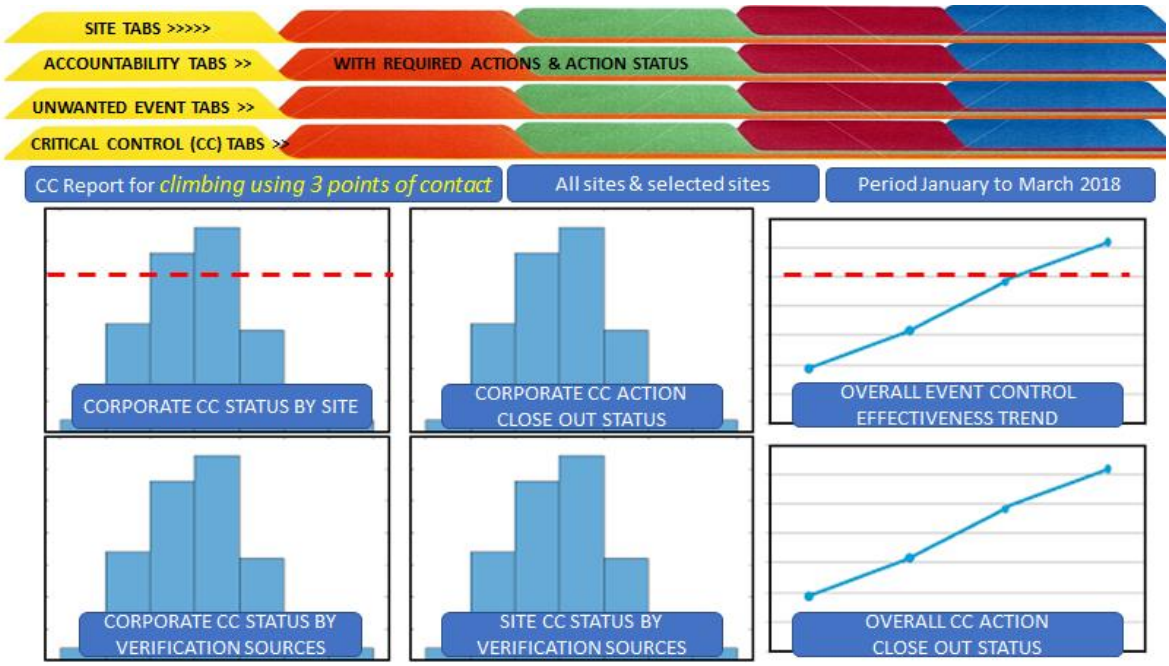
PUE Owner Weekly Critical Control Verification Report
For *climbing using 3 points of contact*



The previously established verification areas and frequencies have been included in a basic stoplight report that critical control owners would create, including their comments on any results including potential recommendations for addressing a yellow or red light. Trigger levels for verification data should be defined to establish green, yellow or red reports. For example, for "Act observations are 90% positive, at 90% or greater the result would be green. Red would be observation results below a figure usually identified in the verification design, for example 75%. Yellow would be an observation data levels between the 75 and 90% level. Other verification questions may require a more subjective guideline.

Computer systems offer an opportunity for streamlining input to this and other reports by gathering and aggregating data electronically, rather than using paper-based reports. As mentioned earlier, the data gathering magnitude for a site may be quite large, so it is recommended that electronic data input and analysis be part of the design of the verification and reporting system from initial setup.

Executive committees or company boards may also require summary reports that include critical control status for all priority unwanted events at relevant sites. Of course, a good data management approach should facilitate the provision of effective 'dashboards' for the organisation. A basic example is provided below.



The above example suggests that a dashboard that includes all data about priority unwanted events, critical controls, verification activities, ownership and required actions for all sites or locations where the events may occur. Reports generated from this dashboard should be designed by engaging the recipients for input. Executive committees and boards will want CCM summary reports that answer the questions that are important to the organisation. If the data is well managed and analysable as the above example suggests, this dashboard can be used to provide a report or answer any questions from the executive committee or board.

Clearly verification and reporting are major components of an effective CCM initiative. The time and establishment costs should be considered in the design of the CCM initiative.

The next article will address the learning opportunities from CCM that can not only improve the process but also optimise critical controls. Huge opportunities exist in sharing critical control learnings between sites and companies that offer more rapid and more effective improvements for major mining risks.