panaseer

Continuous Controls Monitoring for Risk and Compliance

It's a struggle for today's risk, compliance and audit professionals to provide quantitative evidence of internal security policy and regulatory compliance.

Security, risk, audit and compliance teams are left overwhelmed by a constantly increasing set of privacy and data protection regulations, security technologies and company policies. Legacy GRC and IRM tools are effective in documenting the policies but don't measure if, or how well, the controls are working. As regulatory demands continue to increase, changes to existing policies need to be implemented across all business processes, units and operations. At the same time, organisations must align their own policies to maintain internal thresholds for risk and comply with those regulations.

The answer is not to equip more auditors with clipboards and longer checklists, but rather use technology to automate the process of checking your organisation's cyber posture to see if it's compliant with existing and newly implemented policies. This provides risk and compliance teams with immediate, on-demand access to quantitative evidence of where and when you're compliant, and where and when there are gaps.

The need to automate internal security policy and regulatory compliance measurement

Currently, to assess cybersecurity compliance with industry regulations or established internal policies, organisations rely on external audits or a laborious internal process of manual data processing and self-attestations.

These approaches come with their own share of challenges. Issues are compounded if there is a need to implement changes to the policies or change the scope of the policies:

External audits are expensive and conducted infrequently.

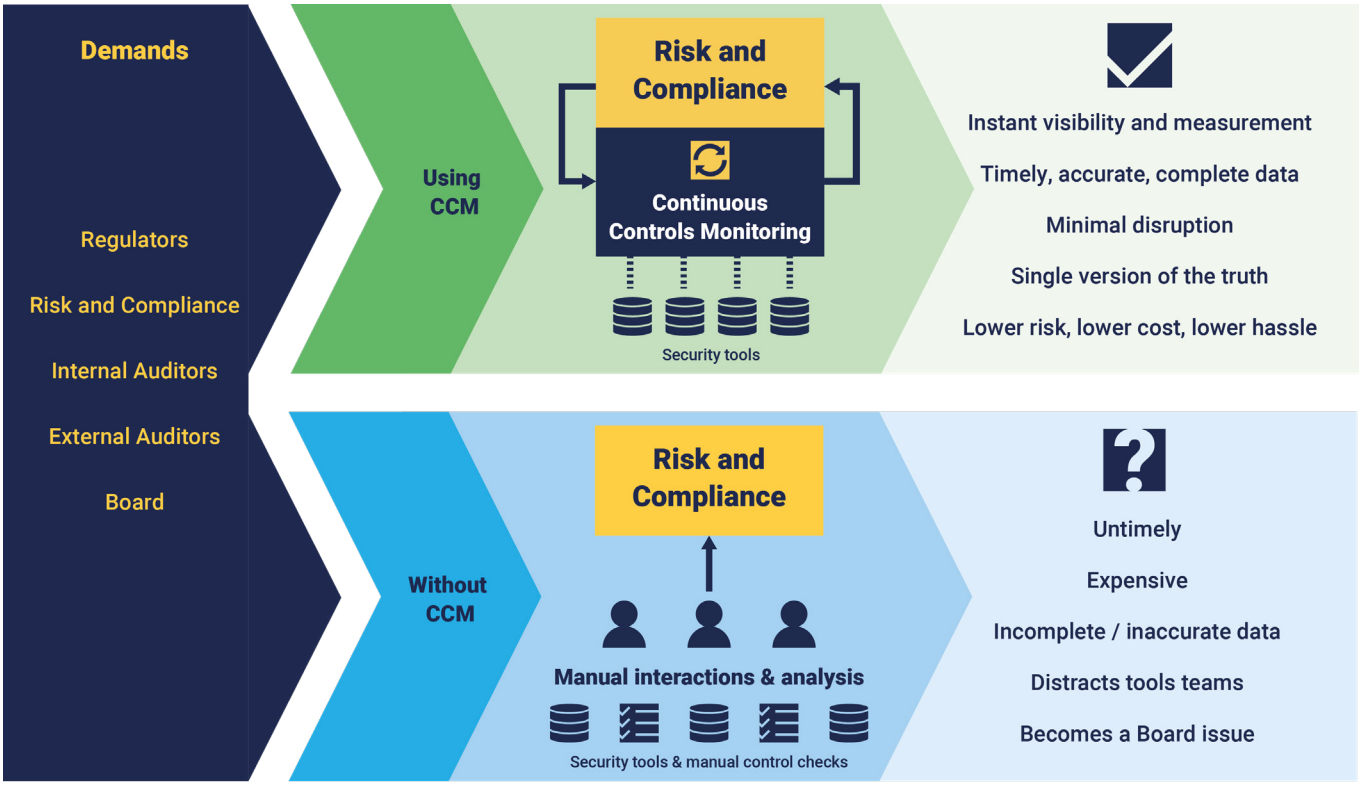
Manual data processing can be extremely time consuming and error prone leading to unreliable results because of the human-in-the-loop nature of DIY internal reviews.

There is the additional issue of assessing internal policy compliance status through qualitative checklists. This makes it even more difficult to use qualitative information to substantiate regulatory compliance.

Elevate compliance monitoring with a data-based approach

Panaseer's Continuous Controls Monitoring (CCM) for Risk and Compliance capability provides automated evidence of compliance with policies that increases confidence in risk posture. For example, Singapore's Notice 655 'Requirements for Cyber Hygiene for Banks' requires banks to ensure that a malware protection solution is installed and functioning on every device all the time. Demonstrating this compliance manually will be an arduous, time-consuming challenge, not to mention the evergreen question of data quality and integrity in a manual approach. In order to substantiate compliance to that level, automation is essential.

The CCM for Risk and Compliance capability supports security, risk, audit and compliance teams in several ways. Users can rely on automated, data-backed, quantitative assessment versus subjective opinions to conduct audits, assess internal policy compliance, and substantiate regulatory compliance. Historical time-stamped data that is held in perpetuity allows them to do so for any given time-frame on any given device. The capability also allows users to configure the measurement criteria to reflect their internal policies and standards, tailoring measurements to individual organisations.



If you are interested in finding out more about CCM for Risk and Compliance, get in touch at **success@panaseer.com**, or request a demo at **panaseer.com**