

Integrated Risk Management (IRM)

Integrated Risk Management - a better way to manage risks and cyber security in the digital era

By adopting IRM, organizations can deliver efficient and actionable risk mitigation strategies that align with business objectives.



Key benefits of an IRM approach to cyber security

Better visibility of risks

Given that all of the data is stored in one place, IRM offers better accuracy and greater visibility of risk and compliance status. This means that risks can be easily identified, addressed, tracked and reviewed – reducing the likelihood of adverse outcomes and improving decision making.

Enhanced accuracy

Again, due to the centralization, IRM tools can offer a higher degree of automation. When configured appropriately, it recognises the complex relationships between the data sets (for example: risks and controls, or vulnerabilities and incidents) – not only does this save a substantial amount of time (where there's a skills shortage) but it also reduces the likelihood of human-error.

Effective reporting

IRM solutions provide actionable risk-based insights and streamline the reporting process. It takes minutes to pull meaningful reports – unlike traditional GRCs which can take days.

Please feel free to contact the Acuity team, if you would like to know more about these points or discuss your own specific requirements.

Improved efficiency & cost savings

Traditional GRCs tend to be quite modular and therefore require individual customization. This makes it difficult to make sense of the information as it is often spread across different platforms in different forms. It is therefore difficult to update and maintain. IRM platforms on the other hand, fully integrate the different data sets needed to truly understand risk – with access permissions restricting the activity to designated individuals only. In addition, they are designed to scale.

Contact us

EMAIL | info@acuityrm.com
WEBSITE | acuityrm.com

 @AcuityRM

 Acuity Risk Management