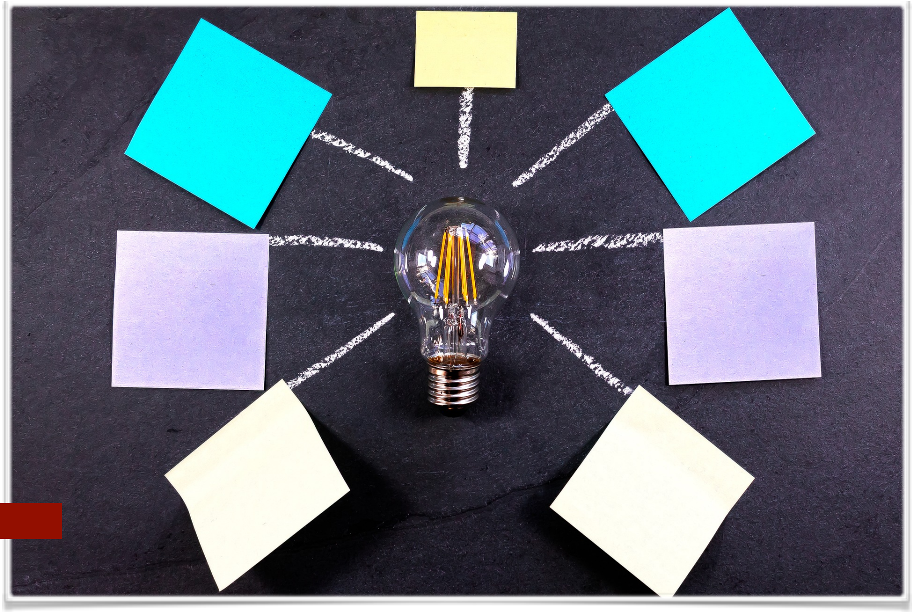

The Term We Use For “It”

We specialize in Governance, Risk Management, and Compliance, but we don’t do “GRC”.

By Evelin Biro

We specialize in governance structures, risk management practices, and compliance programs, but we do not do GRC. Because GRC became commoditized to the point of vanity, we have to find a different name for “it”.

We develop governance structures, risk management practices, and compliance programs, known as GRC in information technology and security. As the term “GRC” is often used for technology offerings or for siloed processes delegated to lower organizational levels, we can’t claim it as something we do. Instead, we must find a better term for “it”.

There is an enterprise-level “it” and a technical “it”. The enterprise-level “it” is not really an “it”, but rather is comprised of three different things: Organizational Governance, Enterprise Risk Management, and Compliance. The technical “it” is GRC.

The term GRC (Governance, Risk, and Compliance) has become so commoditized that many terms are now used to describe it: Compliance, Assurance, Audit, Governance, Security, CISO, SOC, Access Management, Sox, Policy Team, Controls Group, PMO, or “Milton, with the red stapler over there, can help you with that”. The most common alternative terms to GRC are “IRM” and “risk management”.

The term “IRM” (Integrated Risk Management) is Gartner’s attempt to rebrand GRC. The concept advocates integration of operational risk management, business continuity planning, IT risk management, legal, corporate compliance, vendor management, and audit (+/- digital & strategic risk) functions. Governance and compliance disciplines are not explicitly included.

"Risk management" has a dual meaning. It refers to the risk management discipline, and it is used as an umbrella term for functions/disciplines that are broadly related to the management of risks, issues, and overall vulnerabilities from strategic to tactical. This term includes governing processes, all risk management disciplines, and compliance efforts.

Unfortunately, none of these terms are perfect. GRC was the closest but became commoditized to the point of vanity. IRM is incomplete and excludes governance and compliance. Risk management is confusing because it reflects both the discipline and an overall concept.

Our website uses the terms "risk management", "risk operating model", and "GRMC". The terms are not fully interchangeable, but they are aligned with our approach.

Governance, Risk Management, and Compliance (GRMC)

The term "GRMC" recognizes **three disciplines as standalone entities** with their own processes, practices, goals, and objectives. The term reflects recognition that **effectiveness of these disciplines comes from their synergy** as they support, inform, and balance each other. Lastly, the term also recognizes our belief in the value and resilience that a **formal system of leadership, control, and enablement** (governance), **informed risk-taking** (risk management) & **cultural integrity** (compliance) bring to an organization.

To continue the conversation about governance, risk management, and compliance, contact:

Evelin Biro
Risk Management Enthusiast and Founder
evelin@biroconsulting.com

Visit us at www.biroconsulting.com