Internrevisorerna
The Institute of Internal Auditors

GRC – står C för Compliance eller Control?

Förslag

Förslaget är att vi låter förkortningen GRC ligga kvar som den gör i visionen, och att den i marknadsföringen kompletteras med en beskrivande text med svar på frågorna:

1. Vad är GRC?
2. Vad innebär det att vara den ledande auktoriteten inom GRC?

Den beskrivande texten ska innehålla definitionen Governance Risk & Compliance men fokus ska ligga på att på ett visionärt sätt beskriva vad värdet med välfungerande GRC är.

Bakgrund

Som en del av föreningens strategi antog årsstämman följande vision:

IIA Sweden är den ledande auktoriteten inom GRC

Vid årsstämman lyftes frågan: Vad står GRC för i visionen, är det Compliance eller Control? Det konstaterades att detta behöver definieras men visionen godtogs ändå med den förkortningen som står.

En fråga med många svar

Som en del i bakgrundsarbetet har jag hört mig för med ett antal medlemmar och styrelseledamöter, läst rapporter och bloggar och frågat Richard Chambers, President och CEO för IIA Global, om råd. Sammanfattningsvis kan konstateras att det inte finns ett klart svar på frågan.

Internrevisorerna
Strandvägen 7A
114 56 Stockholm
www.theiia.se

Den mest vedertagna definitionen, både i Sverige och internationellt, är att GRC står för Governance, Risk och Compliance. Det är vad de allra flesta associerar begreppet till och det är den definition som oftast används. En tongivande person i området, Norman Marks, konstaterade redan i en blogg-post 2013:

” While many of us think it *should* stand for control, it doesn’t. That debate ended a long time ago. It stands for compliance and, given the roots of the term, that is appropriate.”[1]

Andra användningsområden inom Sverige

GRC-konferensen

I konferensen har vi valt att använda Governance Risk and Compliance. Bakgrunden är att det inte ger ett mervärde att IIA har en egen definition av begreppet. Syftet med konferensen är att föra samman GRC-funktionerna för att motverka silo-arbete och för att erbjuda en plattform där professionerna kan mötas och lära om och av varandra.

Konsultbyråerna

Konsultbyråerna använder Compliance, exempelvis PwC[2], KPMG[3], EY[4], Deloitte[5], Transcendent Group[6].

Vad säger IIA Global?

---

[1] https://normanmarks.wordpress.com/2013/07/31/iia-research-foundation-report-only-adds-to-confusion-about-grc/

[2] https://www.pwc.com/jp/en/assurance/services-governance-risk-management-compliance.html

[3] https://home.kpmg.com/bq/en/home/services/advisory/governance-risk-and-compliance.html

[4] http://www.ey.com/us/en/services/advisory/governance-risk-and-compliance

[5] https://www2.deloitte.com/us/en/pages/governance-risk-and-compliance/solutions/governance-risk-compliance-services.html

[6] http://www.transcendentgroup.com/sv/

IIA Global är relativt ensamma om att kalla det för *governance, risk management and control* (så som i den globala visionen). Samtidigt finns inte förkortningen GRC i IIA:s dokument, där används endast orden governance risk management and control utskrivna.

IIA:s vision:

”Internal audit professionals are universally recognized as indipensable to effective governance, risk management and control.

Definition of internal audit:

“Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.”

Value proposal: assurance

I IIA:s Internal Audit Value Proposition[7] används orden Governance risk & control för att beskriva assurance:

” **ASSURANCE = Governance, Risk & Control**
Internal auditing provides assurance on the organization’s governance, risk management, and control processes to help the organization achieve its strategic, operational, financial and compliance objectives.”

[7] http://www.theiia.org/theiia/about-the-profession/value-proposition/?sf1473960=1

IIA Research Foundation

I ett försök att reda ut begreppsförvirringen kring GRC och ERM tog IIA Research Foundation fram en omfattande rapport[8] baserad på en internationell studie. Studien utgår ifrån att orden GRC ska stå för Governance, Risk and Control. Slutsatsen är att det råder begreppsförvirring och i bloggosfären verkar konsensus vara att rapporten snarare bidrog till begreppsförvirringen än att reda ut den.

Richard Chambers

När jag bad IIA:s President och CEO, Richard Chambers, om hjälp för att hitta bra argument, fick jag tillbaka presentationer som han använt sig av när han pratat om ämnet. En av ppt-bilderna hade följande text:

What is GRC?

- A mindset / culture first
- A way to holistically look across risk and control functions
    - Enhance efficiency
        - Identifying and integrating common processes
    - Enhance effectiveness
        - Information and knowledge sharing
    - Common acknowledgement and focus on core strategic goals and value protection and preservation

Hur gör andra IIA-institut?

I våra systerinstitut världen över är det inte ovanligt att andra GRC-funktioner har en aktiv del i IIA-institutet. Två exempel är Ifaci (IIA France) som består till stor del av compliance officers och som även har compliance officers i styrelsen, samt IIA Norway som har risk managers som en egen medlemskategori inom IIA-institutet. De har inte fått några problem eller diskussioner med IIA Global med anledning av detta, även om Richard Chambers personligen är tveksam till om IIA globalt bör bli en organisation för fler professioner än internrevision.

[8] https://www.iia.nl/SiteFiles/IIA_leden/Contrasting%20GRC%20adn%20ERM_2013.pdf

Hur bör vi definiera GRC i visionen?

Mitt förslag är att vi fortsätter att använda den vedertagna definitionen Governance Risk and Compliance, men att vi inte skriver ut förkortningen i visionen. GRC är ett tillräckligt starkt begrepp för att det inte behöver skrivas ut, men det är viktigt att det finns ett svar om vad förkortningen står för när vi får frågan.

Däremot bör vi arbeta med att definiera GRC på ett sätt som är användbart, bortom vad orden står för. Förslaget är därför att när vi marknadsför visionen, exempelvis på hemsidan, skriver vi visionen med GRC och sedan två rubriker under:

1. Vad är GRC?
2. Vad innebär det att vara den ledande auktoriteten?

Vad är GRC?

Svaret på frågan bör gå bortom orden Governance Risk och Compliance, och bortom en organisationskarta. Fokus bör ligga på essensen av vad välfungerande GRC kan bidra med. Några definitioner att arbeta vidare utifrån är exempelvis:

"GRC is the integrated collection of capabilities that enable an organization to reliably achieve objectives while addressing uncertainty and acting with integrity. It encompasses the governance, assurance and management of performance, risk, and compliance."

Definitionen finns tillsammans med en längre beskrivning om vad GRC är och inte är, och vad det kan vara. Jag tror att vi bör ha en liknande visionär beskrivning på vår hemsida, där emfas ligger på värdet med GRC och inte på orden.

Exempel här: http://www.oceg.org/about/what-is-grc/

Vad innebär det att vara ledande auktoriteten inom GRC?

Norman Marks använde en metafor med en orkester[9] som fick illustrera vad GRC är och bör vara. Individuella instrument utan samordning kan vara bra var och en men låta förfärligt tillsammans. Att vara den ledande auktoriteten innebär att ta taktpinnen och leda orkestern framåt till en värdeskapande helhet.

Beroende på hur vi väljer att beskriva GRC på hemsidan, kan vi formulera en motsvarande beskrivning av vad "ledande auktoriteten" betyder.

---

[9] https://normanmarks.wordpress.com/2011/06/16/grc-metaphor/