**The Governance, Risk & Assurance Trilogy – The ‘Other Iron Triangle’**

Author: Roy Millard

**A bridge over a body of water with a city in the background

Description automatically generated**

We all know about project governance, risk management and assurance, don’t we? But have you thought much about how they interact with each other?

They are often thought of existing in a hierarchical way (e.g. assurance as a part of governance), or as quite separate from each other. But both of these are wrong.

In fact, all three are equally important but are mutually dependent on each other. So much so that I refer to them existing in a tripartite relationship, a sort of **‘other iron triangle’**.

OK, it’s not really the same thing as the famous time/cost/quality Iron Triangle in project management, but it does reflect a similar interplay, and encourages more holistic thinking and planning.

Let me explain.

**An idiot’s guide to governance, risk management and assurance**

Firstly, let’s be clear about what we mean by the three terms. (Forgive the APM-speak, but using some definitions can be useful.)

**Governance** is the framework of authority and accountability that defines and controls the outputs, outcomes and benefits from projects, programmes and portfolios. The mechanism whereby the investing organisation exerts financial and technical control over the deployment of the work and the realisation of value.

**Risk** is the potential of a situation or event to impact on the achievement of specific objectives, and **Risk Management** is the set of processes established to manage those risks.

**Assurance** is the process of providing confidence to stakeholders that projects, programmes and portfolios will achieve their objectives for beneficial change.

Good **governance** ensures that sound decisions are made at the right time about the right things, based upon a good understanding of the exposure to **risks**, and **assurance** that the information upon which the decisions are being made is reliable.

So, it’s clear that governance relies on risk management and assurance. But there are risks that governance arrangements may not work properly. And we also need assurance that risk management is good enough. So, we immediately start to see mutual dependence, with effectiveness of one being reliant on the other two.

*Governance, risk management and assurance must all be strong. A weakness in one weakens the effectiveness of the other two.*

Risk management is simply another element of project management. Therefore, just like any other process and control it needs to be assured in project reviews and audits. However, there is never much point in spending much time and effort in assuring things that are low risk. One of the principles of good assurance is that it is risk-based.

*Assurance must focus on areas of greatest risk.*

From where does assurance get information about where the highest risks are? From risk management, of course. Therefore, not only do we need assurance that risk management is working well for the benefit of the project, we need it so assurance can rely on it to know where to focus.

Valuable assurance needs to inform decision-making at the right time with the right information. It therefore needs to be risk-based and organised around decision points. What is assured and when depends as much on governance arrangements as risks.

*Assurance needs to be hard-wired into governance structures.*

**Governance, risk & assurance – the GRA Trilogy**

By thinking of all three when setting up and managing projects, we can ensure effective interaction. The concept of an ‘iron triangle’ reinforces the equal importance of each and their mutual dependence.

Diagram

Description automatically generated

It can be very useful to illustrate this interplay as an overlay to a project lifecycle.



The best way to capture how these relationships and interactions will work in an organisation is to document them within a ‘**GRA Framework’**.

*Relationships and dependencies between governance, risk and assurance must be clearly defined and understood.*

**Getting it right**

Implementing this GRA approach is not easy. It takes senior-level sponsorship and a willingness of the people involved in the three components to work together collaboratively.

Often, the most problematic component will be assurance, partly because of the ‘independence’ mindset of assurance functions, and partly because assurance in organisations is typically fragmented.

*Governance, risk management and assurance will work most effectively in organisations that have implemented ‘Integrated Assurance’.*

Organisations are not static. All sorts of factors, such as stakeholder requirements, reporting lines, risk appetites, business priorities, change all the time. These will impact on how governance, risk management and assurance work. An organisation’s GRA framework should therefore be a dynamic one; one that is reviewed at intervals that reflect the rate at which these factors change.

**Project GRA vs Organisational GRA**

This article focusses on governance, risk management and assurance from a project perspective.

That does not mean that they are only project management matters, or that we only look at them from a project management perspective.

Projects are merely one part of what an organisation is doing. They are usually key to delivering a part of the organisation’s strategy and day-to-day business. Therefore, a project’s governance, risk management and assurance arrangements operate within the arrangements for the overall organisation.

*Project GRA needs to interface seamlessly with organisational GRA.*