A Grand Unified Theory for Risk

Dr David Hillson
The Risk Doctor Partnership

Albert Einstein tried for decades to develop a single "Theory Of Everything", but he failed. Since then physicists have looked for a Grand Unified Theory to unify the various fundamental forces (weak, strong, electromagnetic and gravitational) and offer a more elegant understanding of the organisation of the universe and the nature of matter, energy, space and time. The drive towards a Grand Unified Theory is rooted in the conviction that everything in the universe is interconnected and interdependent, and that it must therefore be possible to describe this mathematically.

Is it possible to develop a "Risk Grand Unified Theory"? Is there a single underlying "Theory Of Everything" for risk? Perhaps enterprise risk management (ERM) is the answer.

There are many types of risk management, each with its own language, processes, tools and techniques, and each supported by specialists and experts. These include business continuity, corporate governance, health & safety, project and programme risk, operational risk, reputation risk, cyber risk, information security, and many more. ERM aims to integrate these various elements of risk management into a cohesive whole. It provides a single unifying framework within which each risk discipline can operate, allowing each specialism to focus on its own approach, but ensuring that they communicate with each other and support each other. ERM recognises that each risk discipline is distinct, but they are all interconnected and interdependent.

One key foundation for ERM is the existence of a "hierarchy of objectives" within the organisation. The overall objectives of the business are defined in the vision or mission statement. These are then implemented through departments and functions, each with their own set of objectives, where the sum of the lower-level objectives fully describes the top set. Further decomposition is possible, for example implementing operational objectives via a hierarchy of portfolios, programmes, projects and tasks, each with objectives at an increasing level of detail.

Risk is defined as uncertainty which can affect achievement of objectives, so ERM provides a hierarchical risk management framework that matches the organisational hierarchy of objectives. Risk management can then be applied in a cohesive and integrated manner from top to bottom across the hierarchy. This approach offers a Risk Grand Unifying Theory across the organisation, drawing together all the various applications of risk management into a single framework, and ensuring that risk is managed effectively at all levels.

Unfortunately, while ERM might work well within a single organisation, there is still no genuine Risk Grand Unified Theory that can be applied to any business, regardless of its size, industry sector or business model. Although there is some consensus and convergence over what ERM should look like, there is currently no

single ERM approach which works across all dimensions of the risk management universe. The international risk standard ISO31000 lays an important foundation of risk principles and guidance, but it is not yet clear whether this will ultimately lead to one best way of managing risk in all circumstances.

If Albert Einstein found it hard to define a Grand Unified Theory for the universe, perhaps we should not be surprised if it takes some time for us to sort out a unified approach for ERM to manage risk across the enterprise. But if Einstein thought it was worth trying, so should we.

To provide feedback on this Briefing Note, or for more details on how to develop effective risk management, contact the Risk Doctor (info@risk-doctor.com), or visit the Risk Doctor website (www.risk-doctor.com).

About the Author

Dr. David Hillson

The Risk Doctor

Dr David Hillson CMgr FRSA FIRM FCMI HonFAPM PMI-Fellow is The Risk Doctor (www.risk-doctor.com). As an international risk consultant, David is recognised as a leading thinker and expert practitioner in risk management. He consults, writes and speaks widely on the topic and he has made several innovative contributions to the field. David's motto is "Understand profoundly so you can explain simply", ensuring that his work represents both sound thinking and practical application.

David Hillson has over 25 years' experience in risk consulting and he has worked in more than 40 countries, providing support to clients in every major industry sector, including construction, mining, telecommunications, pharmaceutical, financial services, transport, fast-moving consumer goods, energy, IT, defence and government. David's input includes strategic direction to organisations facing major risk challenges, as well as tactical advice on achieving value and competitive advantage from effectively managing risk.

David's contributions to the risk discipline over many years have been recognised by a range of awards, including "Risk Personality of the Year" in 2010-11. He received both the PMI Fellow award and the PMI Distinguished Contribution Award from the Project Management Institute (PMI®) for his work in developing risk management. He is also an Honorary Fellow of the UK Association for Project Management (APM), where he has actively led risk developments for nearly 20 years. David Hillson is an active Fellow of the Institute of Risk Management (IRM), and he was elected a Fellow of the Royal Society of Arts (RSA) to contribute to its Risk Commission. He is also a Chartered Fellow of the Chartered Management Institute (CMI) and a Member of the Institute of Directors (IOD).

Dr Hillson can be contacted at *david@risk-doctor.com*.