THE ART & SCIENCE OF ENTERPRISE RISK MANAGEMENT

JEFFREY DRIVER, ESQ.

ALASKA REGIONAL HEALTHCARE COMPLIANCE CONFERENCE

FEBRUARY 21, 2019

OBJECTIVES

- Appreciate the history of managing corporate risk and compare TRM with ERM
- Explore the disciplines of risk management, compliance, and governance in relation to mega trends
- Understand 'effectiveness' in each discipline in theory and practice
- Explore emerging trends and experiments (hard & soft tactics) in corporate risk models and explore why they may, or may not improve effectiveness
- Preview a frame for thinking as you/we move forward with next generation ERM potential

THE HISTORY OF ENTERPRISE RISK MANAGEMENT

A (PARTIAL) TIME LINE IN RISK MANAGEMENT

- 1945- Origin of modern risk management post WWII, but no studies or University courses on risk management until 1963 (Mehr and Hedges) and 1964 (Williams and Hemes)
- 1977 – Foreign Corrupt Practices Act (in response to 400 U.S. companies admitting to paying bribes or other illegal or questionable payments to foreign governments)
- 1985 – "($37B Spare Parts Scandal" – Defense industry and Pentagon; $7K+ coffee maker, $435 hammer, $600 toilet seat (no crime, but certainly ethics was implicated)… Jack Walsh and 17 other CEO's of defesnce industry formed the Defense Industry Initiative on Business Ethics and Conduct (DII) which formed the earliest Compliance Programs with 6 principals (promulgation and adherence to a code of conduct, EE training, EE accountability, procedures for voluntary disclosure to government)
- Late 1980's continued with the Saving & Loans banking crisis due to reckless loans (750 S&L's collapsed; over half had failed)
- 1991- Federal Sentencing Guidelines for Organizations; incentives to prevent, detect and self report illegal and unethical conduct; 7 elements, up to 90% reduction in penaltirs)

A (PARTIAL) TIME LINE IN RISK MANAGEMENT

- 2000-2002 Enron, Worldcom, Adelphia, HealthSouth, Global Crossing, TYCO multi-billion frauds and private looting of public corporations
- 2002 – Sarbanes Oxley Act passed imposing very strict internal controls on corporations.
- 2004 – FSG updated to require compliance programs to create "ethical cultures" to qualify as effective. COSO ERM Guidelines issued.
- 2007-2008 – Investment banks and brokerage scandals (Lehman Brothers, Bear Stearns, Merrill Lynch), America's largest Insurance Company AIG failed, and so did Freddie Mac and Fannie Mae; now known as the great recession, Americans lostt more than a quarter of their net worth.
- The beat goes on…

THE FUTURE OF THE US TO 2025

- Citizens of tomorrow and the rise of the Millennials to 43.8% of the workforce; late job starts, increasing demands to support an elderly population, job automation
- Communities of tomorrow and connectivity; geographically dispersed families, communities as families
- Cities of tomorrow will shift to mid-tier cities and smart cities
- Business in 2025 will reflect changing skills, culture, and operations

* Frost & Sullivan's research service on The Future of the United States offers a comprehensive analysis of the Mega Trends that will impact American citizens and businesses through 2025. Based on Macro to micro methodology the study also offers strategic recommendations and predictions backed by relevant facts and statistics.

TWO LEADING MODELS FOR ERM: COSO

COSO: CONTEXT

Establishing Context: This includes an understanding of the current conditions in which the organization operates on an internal, external and risk management context.

COSO: RISK IDENTIFICATION

Identifying Risks: This includes the documentation of the material threats to the organization's achievement of its objectives and the representation of areas that the organization may exploit for competitive advantage.

COSO: ANALYZING & QUANTIFYING RISKS

Analyzing/Quantifying Risks: This includes the calibration and, if possible, creation of probability distributions of outcomes for each material risk.

COSO: INTEGRATING RISKS

Integrating Risks: This includes the aggregation of all risk distributions, reflecting correlations and portfolio effects, and the formulation of the results in terms of impact on the organization's key performance metrics.

COSO: PRIORITIZING RISKS

Assessing/Prioritizing Risks: This includes the determination of the contribution of each risk to the aggregate risk profile, and appropriate prioritization.

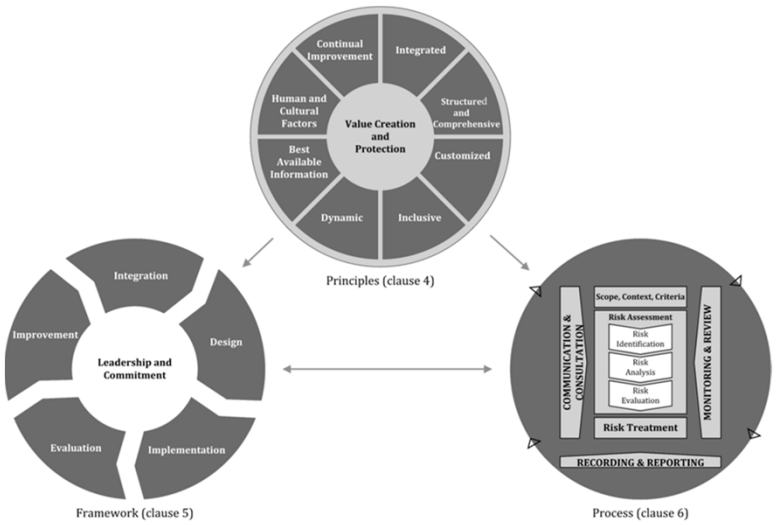
COSO: TREATING & EXPLOTING RISKS

Treating/Exploiting Risks: This includes the development of strategies for controlling and exploiting the various risks.

COSO: MONITORING & REVIEWING

Monitoring and Reviewing: This includes the continual measurement and monitoring of the risk environment and the performance of the risk management strategies.

TWO LEADING MODELS FOR ERM: ISO 31000



TRADITIONAL COMPARED TO ENTERPRISE RM

Traditional Risk Management	Enterprise Risk Management
Insurable	Not necessarily covered by insurance
One-dimensional assessment (potential impact)	Multi-dimensional assessment
Manages risks one-by-one	Analyzes material risks and how they relate
Occurs within one business unit ("siloed")	Spans the entire organization ("holistic")
Reactive & sporadic	Proactive & continuous
Considers only downside (loss)	Considers both upside and downside
Focuses solely on loss prevention	Focuses on business goals, adding value and more
Disjointed activities	Embedded in culture and mindset

https://www.erminsightsbycarol.com/traditional-risk-management-erm-differences

HOW DO YOU DEFINE COMPLIANCE EFFECTIVENESS?

HOW DO YOU DEFINE RISK MANAGEMENT EFFECTIVENESS?

HOW DO YOU DEFINE GOVERNANCE EFFECTIVENESS?

ASSESSING EFFECTIVENESS

The degree to which objectives are achieved and the extent to which targeted problems are solved. In contrast to efficiency, effectiveness is determined without reference to costs and, whereas efficiency means "doing the thing right," effectiveness means "doing the right thing."

Read more: http://www.businessdictionary.com/definition/effectiveness.html

REVIEW OF ERM LITERATURE

Findings (92 retrieved articles): ERM literature tends to focus on the TECHNICAL aspects of ERM, namely:

- Characteristics of ERM adopters
- Determinants of ERM adoption
- Impact of ERM adoption to firm value and performance
- The roles of various functions, (CRO, CFO, IA, BOD)

Togok SH, Ruhna, C, Zainuddin S. Institutional Conference on Technology and Business Management; March 24-26

REVIEW OF ERM LITERATURE

- Conclusion: There tends to be a general consensus on the technical aspects of ERM such as the drivers and characteristics for ERM adoption, conflicts exist in the impact of ERM on firm values.
- Conclusion: The main gap in ERM research is believed to be in the wider social, institutional, and organizational context in which it operates (i.e. ERM effectiveness).
- Conclusion: "There is a lack of research done in the aspects of ERM effectiveness."
- Conclusion: Much of the reported literature is done empirically, reflecting a dire need for an in-depth understanding on the topic.

Togok SH, Ruhna, C, Zainuddin S. Institutional Conference on Technology and Business Management; March 24-26

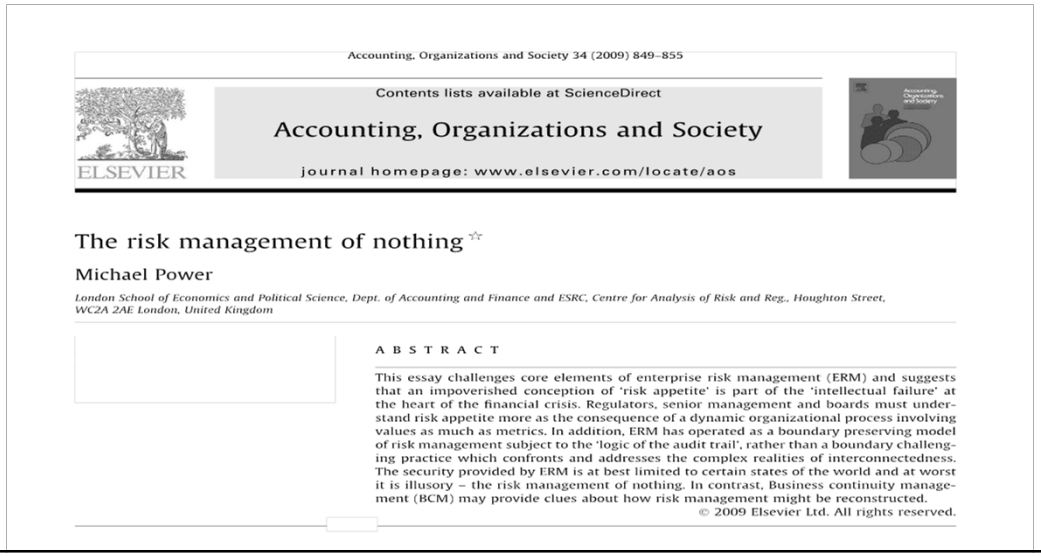
HOW DO YOU DEFINE GRC EFFECTIVENESS?

CRAFTED: The essence of good corporate governance is ensuring trustworthy relations between the corporation and its stakeholders. Therefore, good governance involves a lot more than compliance. Good corporate governance is a culture and a climate of:

- **C**onsistency
- **R**esponsibility
- **A**ccountability
- Fairness
- **T**ransparency, and
- **E**ffectiveness that is **D**eployed throughout the organization

Read more at https://knowledge.insead.edu/leadership-organisations/measuring-the-effectiveness-of-corporate-governance

ENTERPRISE RISK MANAGEMENT EFFECTIVENESS . . .



Accounting, Organizations and Society 34 (2009) 849–855

Contents lists available at ScienceDirect

Accounting, Organizations and Society

journal homepage: www.elsevier.com/locate/aos

The risk management of nothing ☆

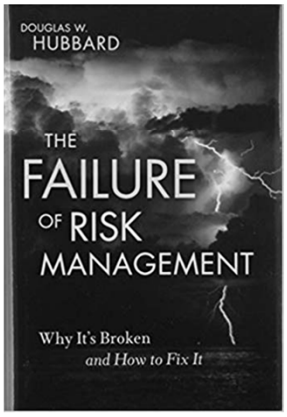
Michael Power

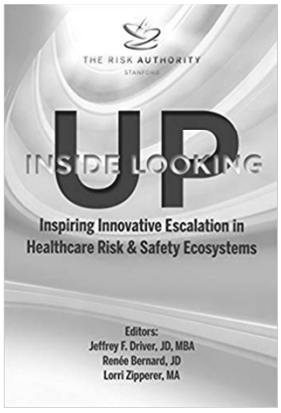
London School of Economics and Political Science, Dept. of Accounting and Finance and ESRC, Centre for Analysis of Risk and Reg., Houghton Street, WC2A 2AE London, United Kingdom

ABSTRACT

This essay challenges core elements of enterprise risk management (ERM) and suggests that an impoverished conception of 'risk appetite' is part of the 'intellectual failure' at the heart of the financial crisis. Regulators, senior management and boards must understand risk appetite more as the consequence of a dynamic organizational process involving values as much as metrics. In addition, ERM has operated as a boundary preserving model of risk management subject to the 'logic of the audit trail', rather than a boundary challenging practice which confronts and addresses the complex realities of interconnectedness. The security provided by ERM is at best limited to certain states of the world and at worst it is illusory – the risk management of nothing. In contrast, Business continuity management (BCM) may provide clues about how risk management might be reconstructed.

HOW DO YOU DEFINE GRC EFFECTIVENESS? AND OPPOSING VIEWS . . .



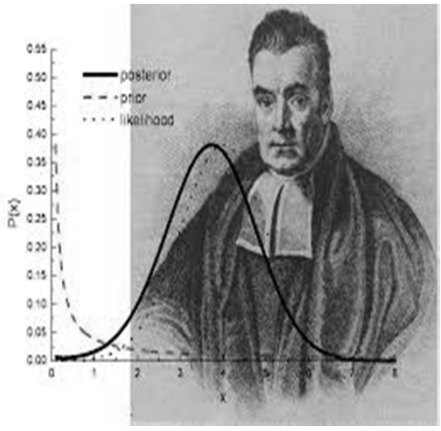


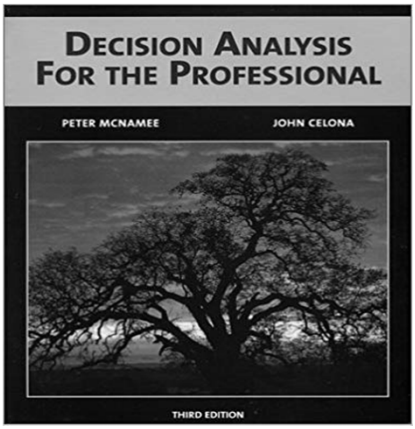
EXPERIMENTS IN NEXT GENERATION ERM: TACTICS TO LIFT EFFECTIVENESS

ERM Trends & Stanford Risk Experiments

- Rebalancing risk focus adding in the upside of risk through Value Driven (Quantifiable) Enterprise Risk Management (VDERM)
- Fundamental cultural shifts in risk operations and PEARL as the central vision
- Using NLP and artificial intelligence(AI) to identify risk (Innovence Pulse)
- Using a design thinking approach to solving problems (the formation of Innovence Lab)
- Experimenting outside of the Stanford campus; the US-UK Partnership for Patient Protection (P4P2)

INFUSING DECISION SCIENCE INTO ENTERPRISE RISK MANAGEMENT



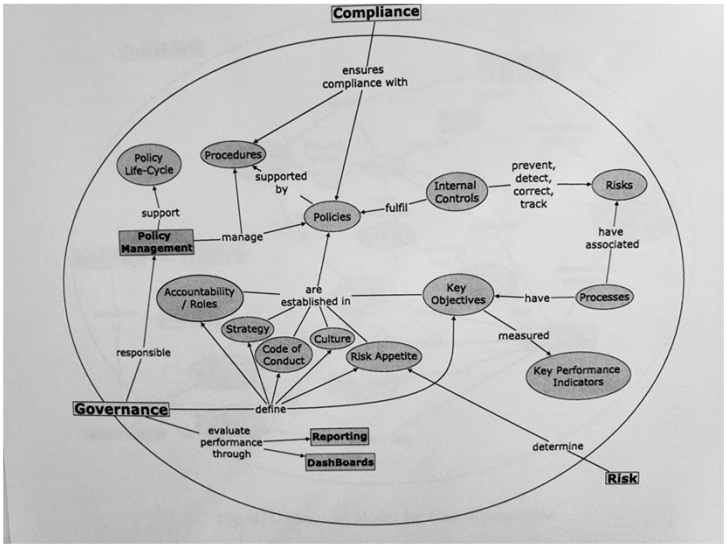


A CONCEPTUAL MODEL FOR NEXT GENERATION INTEGRATED GOVERNANCE, RISK AND COMPLIANCE: (MAXIMIZING EFFECTIVENESS?)

Pedro Vicente and Miguel Mira da Silva
Instituto Superior TÅLecnico, Universidade TÅLecnica de Lisboa,Avenida Rovisco Pais, 1, 1049-001 Lisboa, Portugal {pedro.vicente,mms}@ist.utl.pt

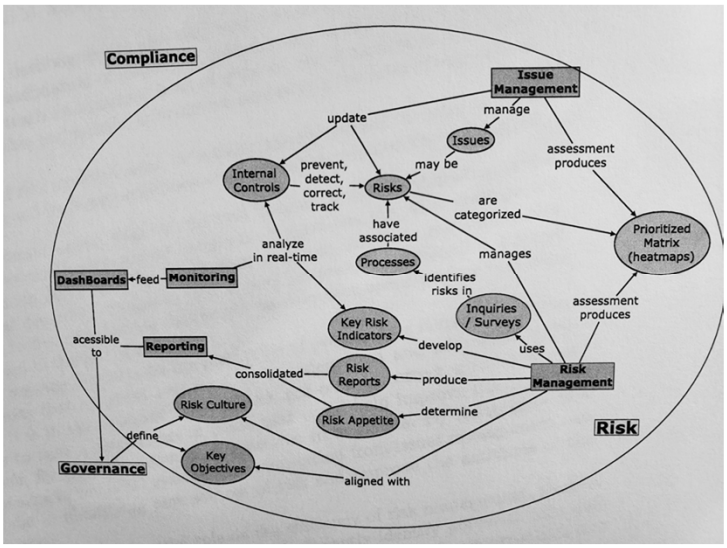
H. Mouratidis and C. Rolland (Eds.): CAiSE 2011, LNCS 6741, pp. 199–213, 2011. Springer-Verlag Berlin Heidelberg 2011

Conceptual Model for Governance



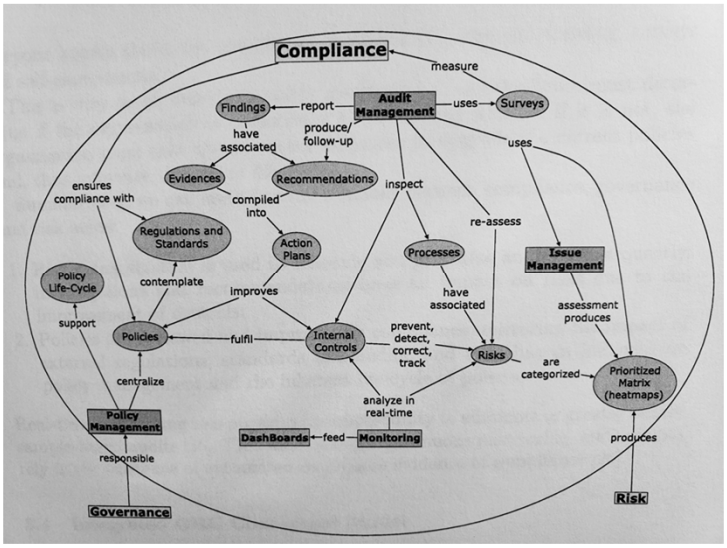
Pedro Vicente and Miguel Mira da Silva
Instituto Superior TÃLecnico, Universidade TÃLecnica de Lisboa,Avenida Rovisco Pais, 1, 1049-001 Lisboa, Portugal
{pedro.vicente,mms}@ist.utl.pt

Conceptual Model for Risk Management



Pedro Vicente and Miguel Mira da Silva
Instituto Superior TÃLecnico, Universidade TÃLecnica de Lisboa,Avenida Rovisco Pais, 1, 1049-001 Lisboa, Portugal
{pedro.vicente,mms}@ist.utl.pt

Conceptual Model for Compliance



Pedro Vicente and Miguel Mira da Silva
Instituto Superior TÂLecnico, Universidade TÂLecnica de Lisboa,Avenida Rovisco Pais, 1, 1049-001 Lisboa, Portugal
{pedro.vicente,mms}@ist.utl.pt

Conceptual Model for Integrated GRC

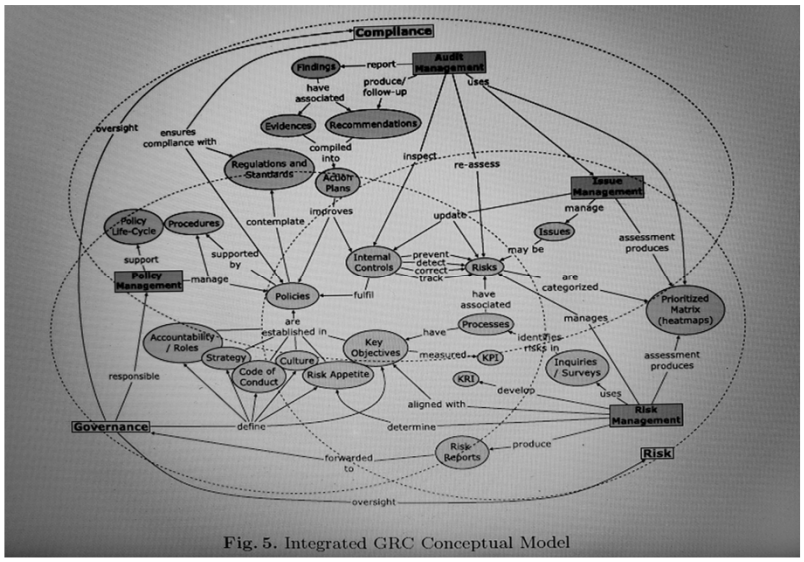


Fig. 5. Integrated GRC Conceptual Model

Pedro Vicente and Miguel Mira da Silva
Instituto Superior TÂLecnico, Universidade TÂLecnica de Lisboa,Avenida Rovisco Pais, 1, 1049-001 Lisboa, Portugal
{pedro.vicente,mms}@ist.utl.pt

Pedro Vicente and Miguel Mira da Silva
Instituto Superior TÃ©cnico, Universidade TÃ©cnica de Lisboa,Avenida Rovisco Pais, 1, 1049-001 Lisboa, Portugal {pedro.vicente,mmsj@ist.utl.pt

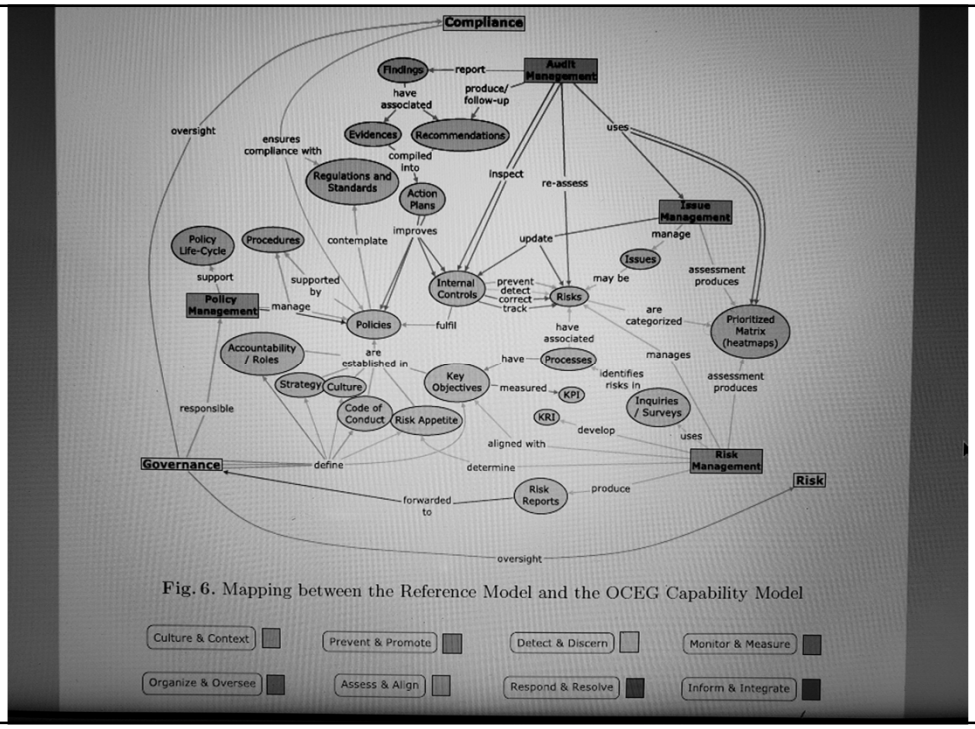


Fig. 6. Mapping between the Reference Model and the OCEG Capability Model

USING DESIGN THINKING TO REIMAGINE & PROTOTYPE NEXT GENERATION ERM MODELS AND MORE!

- Phase 1: Scope
- Phase 2: Prepare
- Phase 3: Discover
- Phase 4: Synthesize
- Phase 5: Generate
- Phase 6: Prototype
- Phase 7: Pilot
- Phase 8: Spread

USING DESIGN THINKING TO REIMAGINE & PROTOTYPE NEXT GENERATION ERM MODELS AND MORE!

- Phase 1: Scope - Explore data and organization. Determine what to work on (HMW)
- Phase 2: Prepare – Gather your team and plan the project
- Phase 3: Discover – Conduct research to understand the problem space
- Phase 4: Synthesize – Interpret learning and define opportunities
- Phase 5: Generate – Brainstorm and conceive new ideas
- Phase 6: Prototype – Select promising ideas to develop and test (Use DA here)
- Phase 7: Pilot – Pilot idea in successive steps. Prove value by measuring impact
- Phase 8: Spread – Make the business case, secure support, and launch into the world

OUR JOURNEY GOING FORWARD . . .

- "We can't solve problems by using the same kind of thinking we used when we created them." – Albert Einstein
- "The designer has a dream that goes beyond what exists, rather than just trying to fix what exists. The designer wants a solution that fits in a deeper or social sense." – David Kelly