UNIVERSITY OF BIRMINGHAM

# Systematic Elaboration of Compliance Requirements

## Using Compliance Debt and Portfolio Theory

**Bendra Ojameruaye**, **Rami Bahsoon**

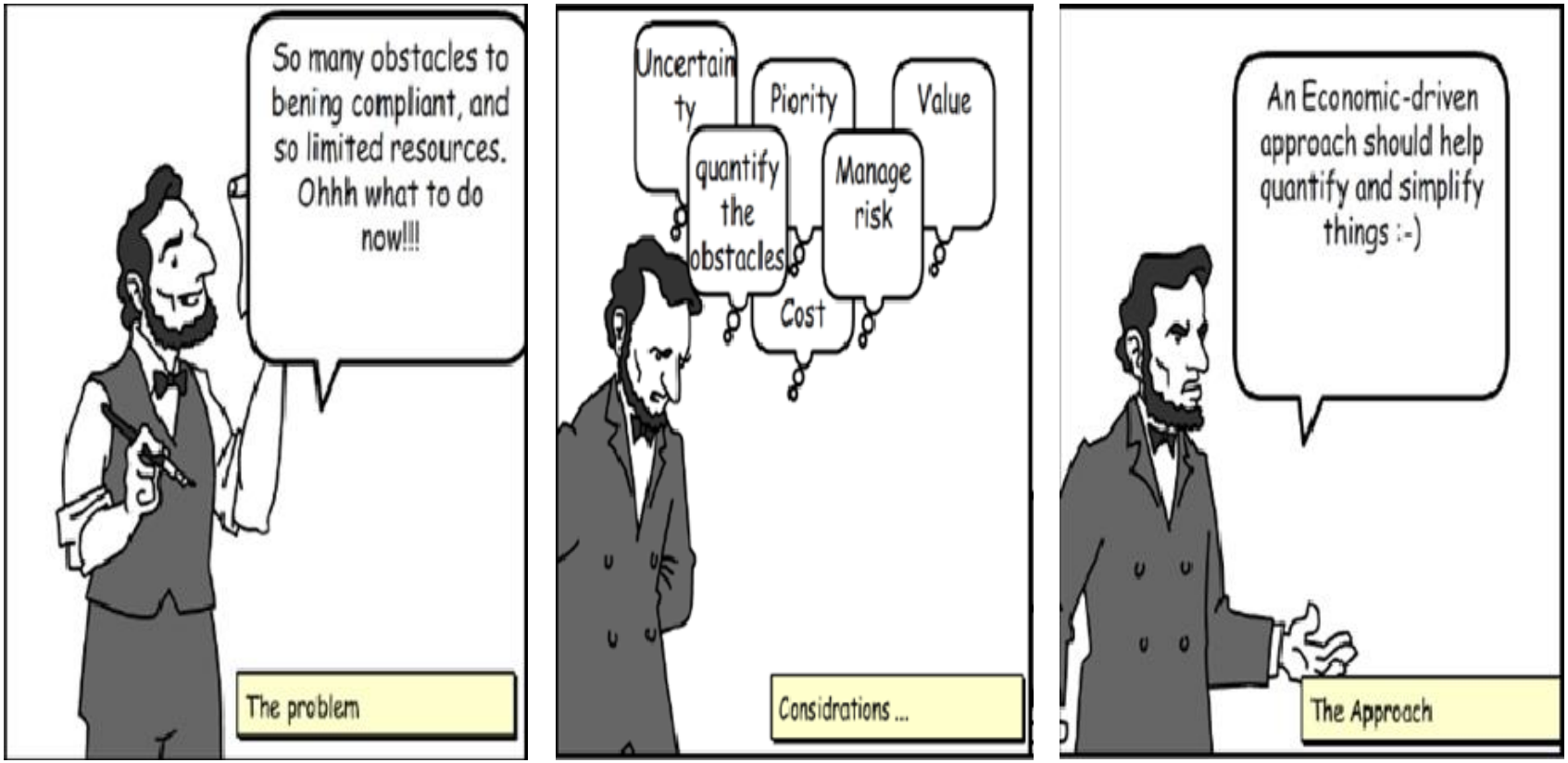
University of Birmingham, UK

# Outline

- Introduction - Simple Scenario
- The  Problem
- Why is this important
- The Approach
- Evaluation
- Future Work
- Conclusion

UNIVERSITY OF BIRMINGHAM

# Motivating Example




UNIVERSITY OF BIRMINGHAM

# The problem to be solved

We want to be compliant at the best cost.

We need to account for uncertainty and manage resources.

Prioritise obstacles to manage cost, create value, sustain the solution and reduce risk.

UNIVERSITY OF BIRMINGHAM

# Why it is Important

Minimizing risks and the associated trade-offs.

Selecting the right compliance goals under uncertainty

Minimising cost and risk generally have a higher impact on creating value

UNIVERSITY OF BIRMINGHAM

# Concepts

| Concepts | Definition |
| --- | --- |
| Compliance | Compliance is the responsibility to operate in agreement with established laws, regulations, standards, and specifications |
| Goal | A goal is an objective or a “statement of intent that a system should satisfy” |
| Obstacle | obstacles capture undesired properties that may prevent the goal from being satisfied |

# Concepts

| Concepts | Definition |
| --- | --- |
| Portfolio | A collection of weighed compositions of assets |
| Portfolio Theory | The goal is to select the optimal combination of assets using a formal mathematical procedure that can minimise risk while accounting for uncertainty of the real world |

# Proposed Solution

A value-driven and risk-aware solution

Obstacles handling,

Portfolio-based thinking

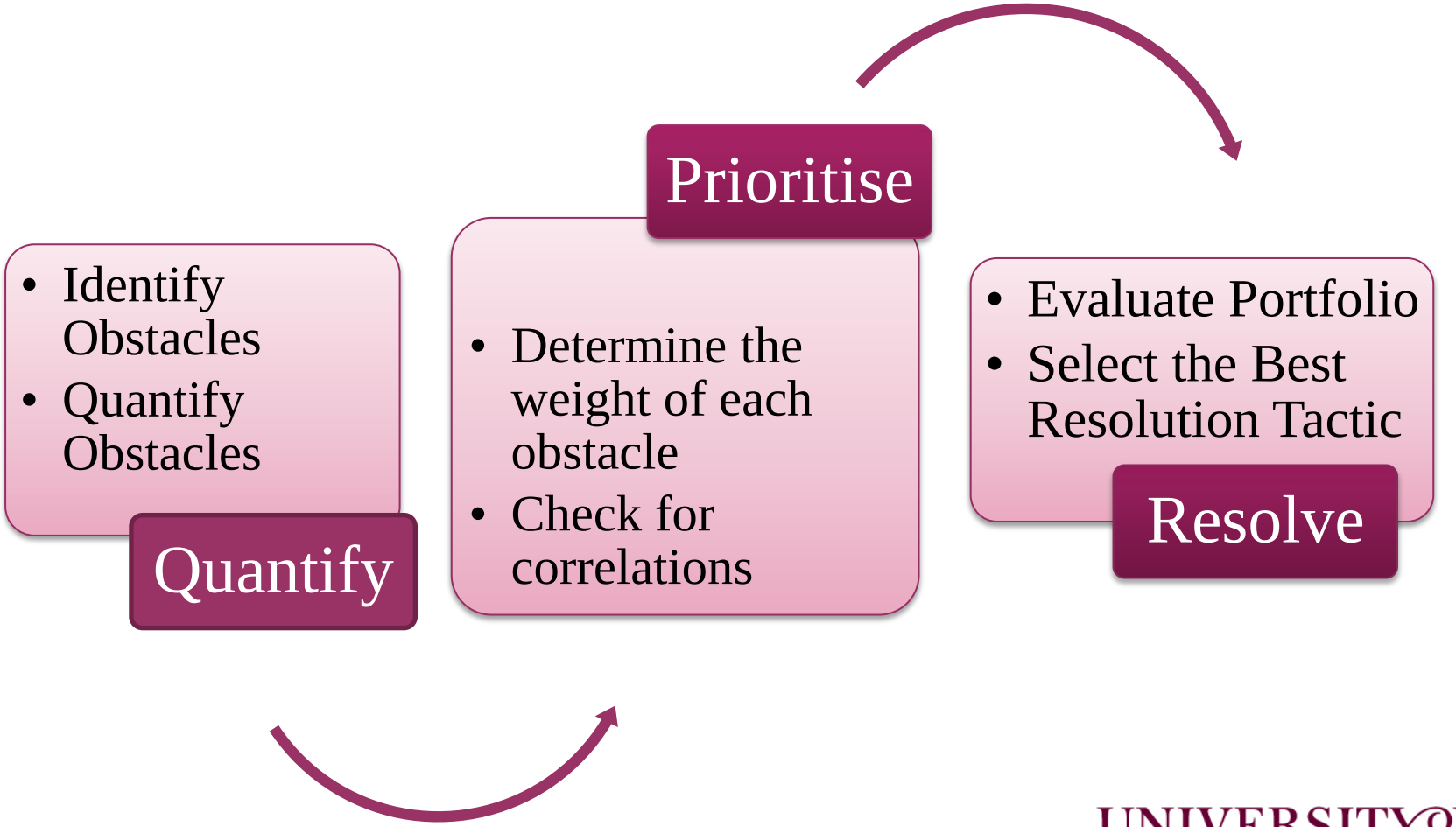
Goal and elaboration levels.

Optimal portfolio of obstacles to be resolved.

Compliance Debt as a form of a technical debt

UNIVERSITY OF BIRMINGHAM

# Proposed Solution - Approach




UNIVERSITY OF BIRMINGHAM

# Proposed Solution - Approach

- Quantify Obstacles that Needs to be Resolved
  - $R_O = I_P * I_A$
  - $V_O = P * I_P * I_A$
- Determine the Weight of Each Asset in the Portfolio
  - Optimisation techniques

# Proposed Solution - Approach

- Determine the Correlation Coefficient
- Evaluate the Portfolio of Obstacles to be Resolved

$$\sum_{i=1} \mathrm{Ep} = 1$$

$$Rp = \sqrt{\sum_{i=1} w1^2 R1^2 + \sum_{i=1}^{m} \sum_{j=2}^{m} WiWjRiRjPij}$$

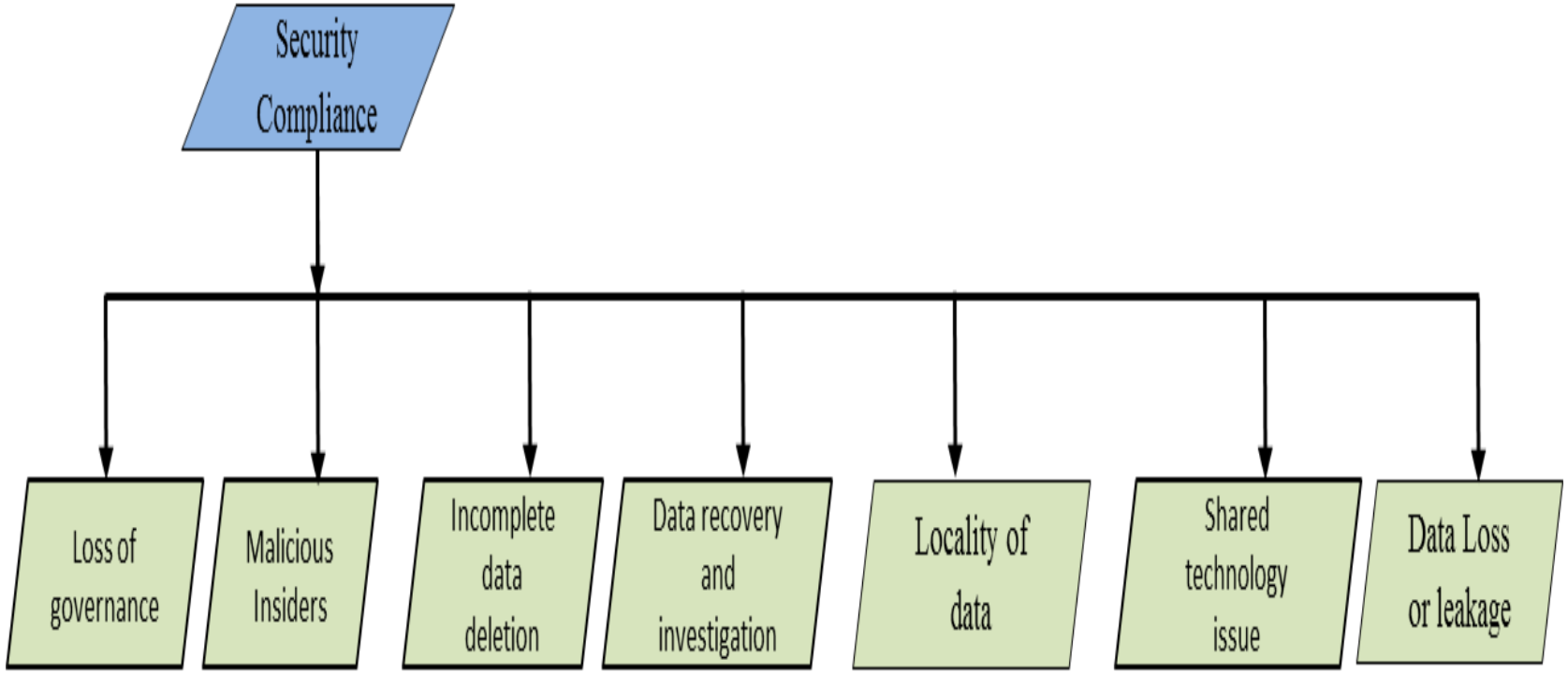
UNIVERSITY OF BIRMINGHAM

# Proposed Solution - Approach

- **Evaluate and Select the Best Resolution Tactic**
  - value of the resolution tactic
    - » $R_T = P * I_P * I_A$
  - the compliance debt
    - » $T_D = IR_T - R_T$

UNIVERSITY OF BIRMINGHAM

# Evaluation


Security Compliance
Loss of governance
Malicious Insiders
Incomplete data deletion
Data recovery and investigation
Locality of data
Shared technology issue
Data Loss or leakage

# Evaluation

| Goal | Obstacle | Agent |
|---|---|---|
| Achieve [Store Personal Data in United Kingdom] | •Data centre not located in the United Kingdom<br>•Subcontracting to another cloud provider as a backup plan | Cloud Provider |

# Evaluation

| Obstacle | Likelihood | Criticality | Risk Value | R1 (%) | Cost / Principal | Optimum Weights % (W1) (AHP) | Amount to be invested |
|---|---|---|---|---|---|---|---|
| Loss of governance | 1 | 3 | 3 | 9.09 | 1 | 0.06 | 0.54 |
| Malicious Insiders | 1 | 3 | 3 | 9.09 | 2 | 0.06 | 0.54 |
| Incomplete data deletion | 3 | 2 | 6 | 18.18 | 1 | 0.16 | 1.45 |
| Locality of data | 3 | 3 | 9 | 27.27 | 2 | 0.40 | 3.59 |
| Shared technology issue | 3 | 2 | 6 | 18.18 | 3 | 0.16 | 1.45 |
| Data Loss or leakage | 2 | 3 | 6 | 18.18 | 3 | 0.16 | 1.45 |
| **Portfolio Risk Value** | **12.01%** | | | | | | |

UNIVERSITY OF BIRMINGHAM

# Evaluation

| Resolution Tactic | P | $I_P$ | $I_A$ | Value | Risk Value | Risk % | TD% |
|---|---|---|---|---|---|---|---|
| Store and process personal data in-house | 2 | 1 | 2 | 4 | 2 | 7% | 4% |
| Assign the responsibility of obstructed goal to trusted cloud platform | 3 | 1 | 1 | 3 | 1 | 3% | 0% |
| Avoid the obstacle by negotiating terms and conditions with cloud provider | 2 | 1 | 3 | 6 | 3 | 10% | 13% |
| Reduce the obstacle by getting a US-EU safe harbour certification that will allow data to be stored in a wider area | 2 | 2 | 2 | 8 | 4 | 14% | 22% |
| Relaxing the requirements to include storing of data in the EU as this is covered by the Data Protection Act. | 2 | 2 | 2 | 8 | 4 | 14% | 22% |
| The requirement to alert the organisation when that won't be able to store the data in the United Kingdom. | 1 | 3 | 2 | 6 | 6 | 21% | 13% |
| Do nothing | 1 | 3 | 3 | 9 | 9 | 31% | 26% |

UNIVERSITY OF BIRMINGHAM

# Future Work

## Challenges

- Measurements and quantification
- Not enough historical data
- Requires expert knowledge

## Future Work

- Further empirical investigation is required
- Better measurement metrics
- How resolving an obstacle will affect the resolution of other obstacles.
- Correlations between goals and obstacles

UNIVERSITY OF BIRMINGHAM

# Summary

- We have explored the link between obstacles and compliance debt.
- We have proposed a portfolio-based approach for managing obstacles.
- Our technique is integrated into existing methods for handling obstacles with the aim of managing trade-offs and deriving more value-driven requirements based on their economics and risks

# Conclusion

- The main objective of the approach is to improve compliance by reducing the risks and costs associated with goals obstruction through a diversified portfolio.
- The Compliance debt metric aims to provides better insights on the significance of a tactic in mitigating risks given the resources in hand.