

https://dspace.org/

An analytical model for dynamic data contextualisation to inform resilience in the South African financial services industry

Herron, Caroline

2022
https://hdl.handle.net/10539/34141

Downloaded from a DSpace repository. https://dspace.org/



University of the Witwatersrand, Johannesburg
School of Electrical and Information Engineering

Dissertation

An analytical model for dynamic data contextualisation to inform resilience in the South African financial services industry

Author
Caroline Herron

Supervisors
Prof. Ken Nixon

A dissertation submitted to the Faculty of Engineering and the Built Environment, University of the Witwatersrand, in fulfilment of the requirements for the degree of Master of Science in Engineering by advanced research.

Johannesburg, 2022

Declaration

I declare that this research proposal is my own unaided work. It is being submitted to the degree of Master of Science in Engineering by advanced research to the University of the Witwatersrand, Johannesburg. It has not been submitted before for any degree or examination to any other university.



Caroline Jean Herron

14th day of February year 2022

Abstract

The work presented extends and contributes to research in business continuity management systems and focuses on a data driven approach to organisational context as defined by Clause 4 of the ISO22301 Standard. Although previous work in this area has produced resilience and business continuity Frameworks, practical systems design principles and measurement, there has been limited investigation into the commonly encountered scenario of effectively managing data to inform the Business Continuity Strategy (Clause 8). In the report presented, a systems thinking approach has been applied to extend the Business Continuity Management Frameworks practically integrating a system of insight into environmental scanning and information seeking components of the system. Environmental scanning simulation and taxonomy classification mapping results were obtained through ethnographic standardisation and subsequent data modelling of a system of insight. This represents a unique and valuable contribution to practitioners and systems engineers working in the field of Business Continuity Management and Business Resilience.

Dedication

I dedicate this work to my family who have always believed in me through many years of study.

To my parents who have been my greatest support and have provided me with guidance and wisdom.

I dedicate the outcomes of this work to my father you has been my mentor and colleague and who has given me more knowledge that I could ever have wished for. This is the greatest gift that a father could ever bestow upon a daughter.

To my husband and son who through thick and thin have provided me with the unconditional love and the space and time to work. You are two of the "greatest among men" (Mathew 23:11).

Acknowledgements

I would like to extend special thanks to Prof Ken Nixon and Nic Cloete-Hopkins for their guidance and support in producing this report.

I would like to express my special thanks to my industry reviewers Dr David Funchall (Nottingham Trent University, School of Science and Technology) and Dr Clifford Ferguson (Strategy, Policy and BCM, Government Pensions Administration Agency (GPAA), for providing me with industry standard assurance in terms of the direction being undertaken in this report.

I acknowledge and thank Amit Vallabh (Client Technical Architect) and Mukta Singh (Product Management Executive, Customer Experience and Development leader) from IBM for their ongoing professional support in data best practice.

I thank all my colleagues and mentors at Caridon, Standard Bank, Nedbank and Capitec Bank for wisdom in application and the experience that has been afforded to me in applying the knowledge and skills gained in my tenure in these organisations.

Contents

1 Introduction **1**

2 Financial Services Background **6**

3 Problem Statement **10**

3.1 Introduction 10

3.2 Data Contextualisation Methods 14

3.3 Conclusion 15

4 Standards **16**

4.1 Prudential Standards 16

4.2 Business Continuity Management: BCBS189 18

4.3 ISO22301:2012 Societal Security - Business Continuity Management Systems 18

4.4 Data Management: BCBS239 19

4.5 Business Continuity Institute Good Practice Guideline 19

4.6 ISO22313 Societal Security - Business Continuity Management Systems - Guidance 2012 19

4.7 DAMA DMBoK 2018 20

4.8 Guiding Principles according to DAMA 20

4.9 Standards Adoption and Application 21

5 Resilience Research **22**

5.1 Introduction 22
5.2 Definitions of Resilience 25
5.3 Global Risk Perspectives - Business Continuity Institute Horizon Report 26
5.4 South African Risk Perspectives - Institute of Risk Management South Africa 27
5.5 Resilience and Business Continuity Management Frameworks 29
5.6 Quantitative and Mathematical Models and applied Qualitative Approaches used to Measure Resilience 33
5.6.1 Systems Engineering Approach 33
5.6.2 Expert-based Indirect Approach 35
5.6.3 Performance-based Direct Approach 37
5.6.4 Anti-fragility Adaptive Systems 37
5.7 Organisational Resilience 40
5.8 Resilience Research Conclusion 44

6 Resilience System **45**

6.1 Soft Systems Methodology 45
6.2 Checkland Stage 1: Situational Problem for Consideration 46
6.3 Checkland Stage 2: Situational Analysis 47
6.4 Checkland Stage 3: Root Definitions of Purposeful Activity Systems . 49
6.5 Checkland Stage 4: Conceptual Systems Model 51
6.6 Checkland Stage 5: Comparison of Models 55
6.7 Checkland Stage 6: Feasibility 56
6.8 Checkland Stage 7: Systems Engineering Master Plan 58

7 Risk and Banking System Data **59**

7.1 Risk Data 59
7.2 Risk Data Measurement 61
7.3 Summary of Data Analysed and Captured 62

7.4 Banking Data 63
7.5 Other supporting Data Sets 64
7.6 Data Management 65

8 Data Contextualisation - an Analytical Model 67

8.1 System and Conceptual Data Model Mapping 67
8.2 Logical Data Model 75
8.2.1 Organisational Context L0 and L1 75
8.2.2 Party/Arrangement (Use Case) L0 and L1 76
8.2.3 Business Resources L0 and L1 76
8.2.4 Business Continuity L0 and L1 77
8.2.5 Strategy L0 and L1 79
8.3 Physical Data Model 81
8.4 Data Contextualisation Analytical Model 81
8.4.1 The Concept of Dynamic Contextualisation 81
8.4.2 Organisational Context: Contextualisation Variable V1(1-n) . 81
8.4.3 Environmental Risk Assessment: Contextualisation Variable V2(1-n) 82
8.4.4 Data Contextualisation Variable Result Stated 83
8.4.5 Integrated Context with the Business Continuity Management System 83
8.4.6 System of Insight 83
8.5 Illustrative Data Results 85
8.5.1 Derivation of V1.1 and V1.2 85
8.5.2 Taxonomy Reference Data Definitions 90
8.5.3 Derivation of V2.1 and V2.2 92
8.5.4 Validation 93
8.5.5 Integrated BCMS Systems Result 95

8.5.6 Business Continuity Strategy 99
8.5.7 Results Conclusion 99
8.5.8 Other Considerations 100

9 Conclusion **101**

9.1 Summary 101
9.2 Conclusion 104
9.3 Future Work 104

10 Appendix **106**

10.1 Systems Engineering Management Plan 107
10.2 Physical Data Model Standards 117
10.3 Physical Data Model 119
10.4 Data Profile and Database Scripting 138

List of Figures

2.1 Emerging Threats [11] 8

3.1 Data contextualisation approach with reference to the ISO22301 [3, 18] 12

4.1 BASEL Standards and Principles. Adapted from Helmich et el 2014 [23]. 17

5.1 Resilience Framework [31] 31

5.2 Direct expert-based approach schematic (adapted from Cere et al. “Critical review of existing built environment resilience frameworks" directions for future research [34]”) 36

5.3 Adapted from “Two dimensional determinant for organisational resilience: a conceptual model”. The addition of a data dimension (three dimensional conceptual model) [42, 32, 43] 42

6.1 Situation Consideration - Rich Picture 48

6.2 Root Definition - CATWOE adapted from “Generic and quantitative approaches for system resilience as a function of time” (Henry Jose Emmanuel and Ramirez Marquez, 2011) [18, 9, 46] 50

6.3 System Conceptual Model, [3, 17, 18, 9] 54

6.4 Comparison of Models 56

6.5 How Now Brown Cow, adapted from YouTubeZA; “Mastering the Requirements Process - The Brown Cow Model”; Robertson S. and Robertson J 30 July 2015 57

6.6 V-Model 58

8.1 Step 2: System Requirement Mapping - in relation to the system problem statement [2, 3] 68

8.2 Step 3: System Conceptual Model in Context 69

8.3 Step 4: Conceptual Data Model - System Representation in Data Terms 70

8.4 BCBS239 Principles derived from the standard and based on currently published Deloitte methodologies [17, 67]. 74

8.5 L0 Organisational Context Logical Data Model [3, 18] 75

8.6 L0 Business Resources Logical Data Model [3, 18] 77

8.7 L0 Business Continuity Logical Data Model [3, 18] 79

8.8 L0 strategy Logical Data Model [3, 18] 80

8.9 Ethnographic Study by Risk Category 86

8.10 Aggregated Risk Scores by Standardised Risk Descriptions (V1.1) and Associated Key Risk Indicators 87

8.11 Taxonomy Mapping 89

8.12 Taxonomy Distinct Categories (applied) 89

8.13 Taxonomy Definitions 90

8.14 Taxonomy Definitions 91

8.15 Risk Assessment 92

8.16 Result Validations: Result 1: Financial System Weakness 93

8.17 Result Validations: Result 2: Regulatory Risk 94

8.18 Systems Integration Business Impact Analysis: Result 1: Financial System Weakness 96

8.19 Systems Integration Business Impact Analysis: Result 2: Regulatory Risk 97

8.20 Banking Systems Data - Risk Data Mart 98

List of Tables

2.1 Banking Innovations [11, 14] 9

5.1 Summary of literature review 24

5.2 "Analytical criteria of a system of systems [42]", adapted from Johnson and Gheorghe (2013) and Jackson and Ferris (2013) [41, 47] 39

7.1 Reporting Data Characteristics 63

8.1 Step 5: Conceptual Systems to Conceptual Data Model Mapping . . 71

10.1 Systems Engineering Management Plan (SEMP) aligned to clauses in the ISO/IEC/IEEE 247-1:2018 Standard. Details of Clauses have been included for completeness. 107

1

Introduction

"Since the 2019 Business Continuity Institute (BCI) Horizon Scan Report, we are starting to see a widening and more unpredictable risk landscape. With new threats emerging that business continuity professionals have previously seldom encountered, the importance of horizon scanning, monitoring incidents that have occurred in other organisations and updating plans accordingly is of the utmost importance [1]."

With new threats emerging that are forcing business to focus on and update their business continuity plans in mind, it should be noted that this report documents the development of an analytical model as it is applied to the components of the best practices required by an ISO22301 compliant Business Continuity Management System (BCMS).

Through the integration of a framework of standards, this report provides a definition, method and approach to the contextualization of risk data that influences the assessment of organisational risk, analysis of business impact and formulation of a business continuity strategy as integrated components of a holistic systems design in the scope of financial services.

A key contribution of this report is to bring together the often disparate disciplines of data and business continuity management to provide a practical and integrated approach to data driven design and implementation of business continuity management systems. Previous resilience research highlights the need to include data considerations in the design of these systems. The discussion is influenced by curation methods needed to support measurement and predictive analytics. The context of the data as an integrated system component is often neglected with the result that opportunities to use environmental data to increase organisational resilience through enhanced operating context insight requires additional effort to integrate once systems are in operation.

The approach taken in this report shows how the application of environmental context to data can be used to improve business resilience in the South African financial services industry use case and specifically focuses on operational risk which falls under the definition of Compliance and Operational Risk, set out by the South African Reserve Bank as follows:

"Operational risk is the risk of a possible financial loss or damage to the Bank's reputation arising from human errors, internal control failure, systems failure or external events that have an adverse impact to the Bank. The Bank has an incident reporting tool which enables the process of self-reporting for any operational risk related events. Action plans are drawn on reported incidents and follow-ups done with relevant business areas." It is therefore also important to note that data solutions need to be designed within the Business Continuity Management System of Interest [2].

Consideration has been given to the effectiveness of applying environmental context to the Risk Assessment and Business Impact Analysis components of a Business Continuity Management System and specifically addresses clause 4 and 8 of the International Standards Organisation ISO22301 Standard for Societal Security - Business Continuity Management Systems (2012) [3]. It is noted however, that systems must be considered holistically and as such related clauses in the standard are referenced where appropriate.

Through standardisation of methods and applying systems thinking as an approach, the outcomes of this report aim to show that the analytical model presented is also applicable to other industry scenarios in its adoption. It provides a foundation for future work in the areas of governance and compliance, data management and data science as well as organisational systems.

As a background to this work, the risk landscape is considered and covers a five year retrospective as published through industry survey both in South Africa and globally. Over the past 12 months health incidents outranked IT and telecoms outages as the greatest cause of organisational disruption with a risk index of 13.9 according to the 2020 BCI Horizon Scan Report [1]. In 2019, the risk index of health incidents was 12.88 second to IT and telecoms at 13.22 [4]. In 2019, the top three main concerns of business continuity professionals for 2020, according to the report were cited as cyber attack and data breach, IT and telecom outage, and adverse weather and natural disaster [4]. Health incidents did not register in the top 5 risk assessment for 2021 [1].

At the time of publishing the 2020 Horizon Scan report in March 2020, the World Health Organisation (WHO) declared a global pandemic of the COVID-19 virus as cases rose across the globe. The number of cases registered globally by the John Hopkins Corona virus Resource Centre was 156 400 with 5 833 deaths [5, 6]. Locally in South Africa, cases had reached 82 across three provinces and on the 15th March 2020, many countries declared hard lock downs limiting interpersonal contact to prevent further spread of the disease [7]. South Africa responded with stern cautionary measures. This triggered organisations to invoke emergency response plans.

At a macro-economic level, interest rate cuts to boost economies were implemented. This also provided a background to innovating new ways to assist borrowers to continue to honour their loan repayments. As businesses became less able to operate in this new context, many people lost their livelihoods and despite interest rate cuts, defaults became more probable, thereby increasing the risk of financial loss to banks.

Governments were also called upon to provide relief. The UK offered to pay the salaries of unemployed persons affected by the pandemic. This was an unprecedented response, the results and implications of which remains untested. The South African Department of Labour was similarly investigating special regulations offering Unemployment Insurance Fund relief to companies that find themselves in distress due to the COVID-19 outbreak.

Global socio-economic impact was felt as self isolation and quarantine measures were undertaken. Large gatherings were cancelled, entry to borders were restricted and misinformation lead to panic in many regions. Economic impacts included supply chain disruption, impact to the financial markets and loss of production. The systemic impact from a social and economic perspective is complex and interrelated.

In the financial services industry, the BASEL Committee met in February 2020 to review vulnerabilities and emerging risks impacting the banking system to further strengthen the implementation of BASEL III [8]. In a press release on the 27th February, the BASEL Committee provided the details of the discussion which included minimising the impacts of the COVID-19 virus, inter-bank rate reforms and climate related financial risk. According to the release, a special committee was established to stock take members current climate related risk initiatives [8].

Local impacts in South Africa have different levels of complexity as the country faces a pandemic, recession and critical infrastructure failure. Eskom continues to work on the maintenance of old power plants and load shedding reduced international investor confidence. Rating agencies reflected the same as South Africa suffered several ratings agency downgrades. Recovery from a pandemic over and above the existing risks and issues in the system will be challenging given limited reserves to allocate to this.

It is this type of emergence in the environmental context that needs to be considered more critically as opportunities arise to influence the improvement of resilience measurement and response formulation through the contextualisation of diverse data sets associated with emerging risk.

This report is structured as follows:

Section 2: Financial Services Background
In this section, the report begins by providing an operating context overview of the financial services system use case. This section includes an introduction of the history of banking and how emerging environmental factors have shaped the regulatory and innovation landscape. This section also outlines the critical industry responses that continue to influence and build resilience into the financial system.

Section 3: Problem Statement
This section introduces and defines data contextualisation and positions the integrated context component into the framework of standards as they apply to the BCMS. The discussion positions and highlights the need for data contextualisation as an integrated system component to provide operating context insight at the point of decision making during risk assessment and business impact analysis. The dis-

cussion in this section includes a focus on the methods that are currently adopted to analyse and store data to support systems of insight.

Section 4: Standards
This section sets out the framework of standards to be applied in the approach with their corresponding guidelines and principles. The scope of standards discussed in this section are business continuity and data management systems standards. More specific regulatory standards applicable to the scope of this report discussion have been included to align to the industry operating context (financial services). The corresponding guidelines of good practice are introduced as important to the method of development and operation of the resilience system in this report.

Section 5: Resilience Research
This section provides a review of the current global and South African risk perspectives as researched over the past 5 years from 2016 to 2020 to show the extent and span of risk types that have been discussed and researched. This section also provides an integrated definition of resilience and how this has evolved through research across multiple engineering and business management disciplines with the overall objective to introduce the adopted definition for the purposes of this report. Resilience frameworks and measurement methods research is also included in this section to show the relevance of holistic system design. The underlying importance of data system integration is highlighted as an evolving topic with new methods being investigated to more fully integrate data into organisational systems thereby improving organisational responses to their operating context(s).

Section 6: Resilience System
In this section the System of Interest that forms the basis of the analytical model is described using Checkland's soft systems methodology [9] and builds on the problem statement through situational analysis. The system definition is formalised using the root definitions of purposeful activity systems and includes the integration of the resilience system framework.

The Conceptual systems model is defined and validated by applying the comparison of models' technique. Through a process of discussion and collaboration with key stakeholders and interested parties, the current system situation is modelled. Outcomes of this process results in the development of a proposed future system model. The future system model is tested against desirable change criteria and feasibility. All models are developed conceptually. Once a feasible future systems model is achieved, a Systems Engineering Master Plan can be developed providing a detailed plan to implement the future system and to affect desirable change which can be observed and measured.

Section 7: Risk and Banking System Data
This section introduces the data sources adopted for system simulation by applying Data Governance (principle 1: BCBS339). All data sources applied are subjected to the test for authoritative principles with clearly defined data ownership and stewardship. Data sources include the dimensions of quantitative measurement, analysis and survey results as well as banking system data at a fundamental level of aggregation.

Section 8: Data Contextualisation - an Analytical Model
The development of the system of interest is described in this section. The system and data conceptual models integration is discussed and applied with the subsequent development of the logical and physical data models. In this section the adoption of industry reference data models are used to refine the system principles are they apply to financial services. The development of the contextualisation variables is described in this section within the boundaries of the system(s) of interest. The resulting system of insight is simulated with both system and validated results and includes resulting data visualisations to reflect the system outputs.

Section 9: Conclusion
The concluding chapter summarises the contextualisation model results and findings and provides a position on the extensibility of the resultant model as well as possibilities for future work.

Section 10: Appendix The appendix of this report includes the following:

1. **System Engineering Management Plan**: Detailed Systems Engineering Management Plan using the ISO/IEC/EEE 247-1:2018 Standard.
2. **Physical Data Model Standards**: Detailed table of defined physical data model naming and data type standards.
3. **Physical Data Model**: A detailed translation of the logical data model into physical data model structures which are mapped to the conceptual systems model in tabular form. Detailed attribute definitions are included in this table for reference (metadata best practice). The contextualisation variables are described in the physical data model to show the application of the derivations from a data systems perspective.
4. **Data Profile and Data Scripting**: Includes the data profiles for the data resident in the physical tables. This section also includes the scripting that is applied to the development of the database along with additional data model descriptions in annotation.

2

Financial Services Background

This report discusses business resilience in the financial services industry and it is important to position the operating context that has shaped the innovation and regulatory landscape over its long history. During its lifetime, the banking industry has adapted to the needs and requirements of its interested parties through the development of financial products and services. The resilience of the financial system has had significant impacts to the global economy. As events shape the world, the financial system has responded and adapted over time and has introduced a number of regulatory standards of operation to ensure its sustainability. The ability of the financial system to effectively recover following significant word events is consistently tested with responses spanning improved regulation to operational improvement and innovation. A short history of banking with a focus given to the major events that have shaped its past are discussed in this section to introduce the operating context in which financial institutions operate.

Banking has been a part of society since 1800 BC. The credit journey of financial services started with the earliest moneylenders. Early Roman banks introduced more formal mechanisms of banking, which allowed people to safeguard their money in the form of deposits and to obtain a line of credit in the form of loans [10, 11].

Modern banking started with the fractional reserve system in the 17^{th} and 18^{th} centuries, in which only a fraction of a banks' deposits were backed by actual cash. These deposits were then made available for withdrawal. The effect of this is that capital was freed up to be loaned to other interested parties. Economic enablement and expansion became possible and this system was the foundation on which banking systems operate today [10, 11].

Since this time, modern banking has experienced many waves of innovation from Industry 1 and now moving into the new wave of Industry 5. Modern banking ushered in technological change to make the lives of banking customers easier and more convenient through the implementation of ATM machines, online banking channels and then into digital hybrids in which multiple transactional channels were made available to customers in the last ten years. With the advent of the Fintech revolution, the banking industry has been challenged by digital business models and solutions and there have been a number of new players in the financial services

marketplace that operate exclusively on digital platforms [10, 12, 13].

Advances in technology have challenged the mental models of banks and have called for solution design to suit digital native customers. This generation of customers (the iGen/GenZ generation) and those into the future who have been brought up from an early age with technology have different expectations of banking systems. Their expectation, and their world view is that banking systems are online twenty four hours of the day with uninterrupted service [11, 14].

Banks have responded to the needs of these customers with system design that includes a highly personalised omni-channel experience. All of these systems require data to operate effectively and are underpinned with advanced analytics, machine learning models and artificial intelligence. Many more advances are being made and the rate of innovation is ever increasing in this regard. With this rapid innovation landscape, sensitivity to risks also increases with many new risks becoming important to manage to ensure business resilience and business continuity in the event of a disruption. Financial services organisations face the ever increasing challenge to continue to build resilient systems and sound business continuity strategies to respond to potential business disruption [11, 14].

Notable banking innovations have been summarised in Table 2.1.

Business resilience in the Financial Services industry is guided by the regulations and standards issued by the BASEL Committee. The primary objective of setting up the BASEL Committee in 1974 was to improve cooperation across the banking industry globally and to work towards ensuring that the system is appropriately regulated and protected from systemic shocks from emerging threats [15].

As modern banking systems evolved and changed with advances in thinking and technology, more risks need to be monitored. Banking risk management strategy is focused on both regulatory as well as other risk factors that may affect and impact business operations. Risks have always had a presence in banking systems and their impacts have been experienced in varying degrees of severity as disruptive events influenced and tested the resilience of banking systems [16].

Emerging threats have been contextualised in figure 2.1 [11] and continue to emerge as the operational environment in which banking systems operate shift and change. The potential ability to respond to a rapidly changing operating environment with clarity of purpose and intent is a critical consideration in increasing the resilience of banks and the financial system [11].

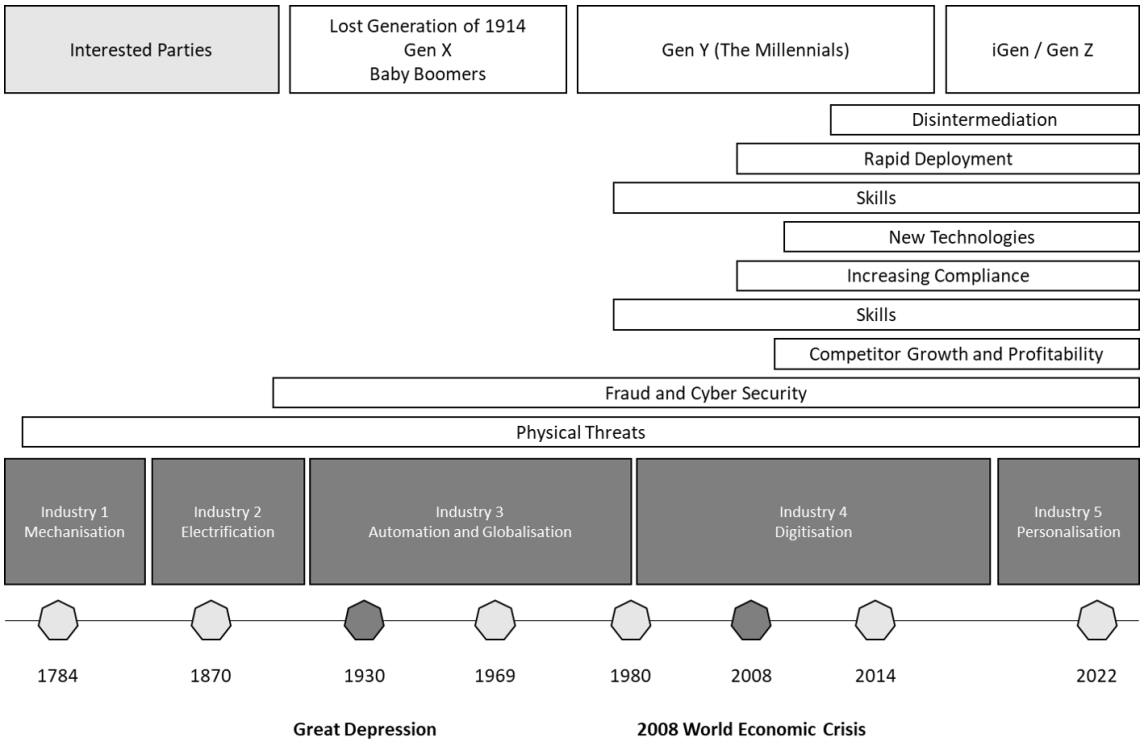


Figure 2.1: Emerging Threats [11]

Changes in legislation and the regulatory landscape is constant with regulators being focused on the sustainability of the banking system post several shocks that had global implications. Most notably these included the Great Depression of 1930 and the 2008 Global Financial Crisis. Having said that, the world faces numerous threats each year ranging from adverse weather conditions, cyber security and data breaches, to outbreak of diseases (such as SARS, MERS and now COVID-19) [1]. In the course of the data analysis of this report, 42 standardised risks have been analysed across two organisational data sets spanning 5 years [1].

What is evident from this analysis is that operational risk is extensive and difficult to manage in an integrated manner. Integration of risk landscape information into the Business Continuity Management Systems of banks may be helpful to maintain up to date Business Continuity Management Strategy with informed prioritised decision making [8, 13, 16].

Table 2.1: Banking Innovations [11, 14]

Innovation	**Description**
Deep Personalisation	Needs of the customer are primary.
Mobile	Available on all devices and wearables.
Robot advisors	Available to assist customers to make sound financial decisions.
Analytical	Machine learning and analytics will enable the bank to monitor and identify threats, both internally and externally.
Platform	Operations that run using robotics and algorithms.
Personal bank account	Bank accounts that allow the customer to shop for banking services from different financial providers.
Secure and distributed ledger	Secure identity sharing and transacting.
Social	Banking services available on social networks.
Dis-inter-mediated	"Online crowd-sourcing strategies that induce masses of people" to solve for their banking requirements will become a viable option for lending.
Decentralised	Decentralisation will take away the need for banks as intermediaries with point to point transactions being more mainstream.
Quantum	Quantum computing will become mainstream, helping financial services to support client management by making sense of client behaviours, predicting trading market behaviour with ever more accuracy, optimising risk management and understanding and streamlining complex operational processes. Quantum computing may also disrupt public key encryption and secure ledgers. This in turn may have a negative effect on the Fintech industry that are increasingly reliant on these technologies.
Crypto Currencies and Blockchain	Crypto currencies are increasingly becoming mainstream and a recognised form of legal tender. Combined with secure ledgers, the potential for high speed, secure transactions is a potential disruptor to traditional payment systems.

3

Problem Statement

The financial system continues to seek new and innovative ways to ensure control is maintained in the system. Monitoring of risk remains a priority and is subject to assessment and regulatory scrutiny. Key risk indicators and metrics form a foundational basis on which to ensure visibility of control over the position of financial institutions at a given time. This has become an integral part of the banks data and information systems. However the focus remains on the curation of data to produce accurate metrics through sound data management practice. Systems of insight that respond to the changing needs of customers and other interested parties share a common requirement for well managed data assets. This has led to the development of sophisticated and world class methods of risk management and customer engagement. The challenge is that well curated data that is structured to support regulatory compliance and insight requires a vital aspect of the changing operating context as an integrated system component. It is essential that data systems also provide for the capture of business narrative in their design.

3.1 Introduction

As an introduction to this problem, this section examines the implementation of business continuity management systems and the role that data context can potentially play in enhancing their operation.

Business Continuity Plans globally, according to the 2020 Horizon Scan Report, follow relatively standardised approaches based on the ISO22301 Standard with 71 percent of organisations certified or using it as a framework [1].

When implementing an ISO22301 compliant Business Continuity Management System, Clause 4 requires that the “organisation shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its Business Continuity Management System (BCMS) [3]."

The standard requires that "the organisation identifies and documents the following [3]:

1. the organisation's activities, functions, services, products, partnerships, supply chains, relationships with interested parties, and the potential impact of a disruptive event,
2. links between the business continuity policy and the organisation's objectives and other policies, including its overall risk management strategy; and
3. the organisation's risk appetite."

The Business Continuity Management System Operations, according to the ISO22301 Standard Clause 8 includes [3]:

1. The Business Impact Analyses (BIA) and Risk Assessment(s) (RA) - Clause 8.2.
2. Business Continuity Strategy, which includes the establishment of resources and requirements as well as protection and mitigation for risk treatment - Clause 8.3.
3. Business Continuity Management Procedures including an incident response structure, warning and communications, business continuity plans and recovery. - Clause 8.4.
4. Exercising and Testing - Clause 8.5.

Integrated data plays a significant role in the operations of the Business Continuity System and should be applied in the context of identified risks and impacts as best practice. This is currently a challenge in the design of these systems due to the variable nature of the risk landscape and ever increasing data sources.

Data provides a basis on which to establish quantifiable resilience indicators on which to measure organisational resilience over time. Business Continuity Management Systems that contain well contextualised data that integrates with the Business Impact Analyses, Risk Assessments and Business Continuity Strategy may positively affect a bank's ability to anticipate and respond to changing environmental factors when a change or disruption is detected in a defined resilience indicator [17].

The scope of this report is shown in 3.1 with Integrated Context being the component proposed to enhance future Business Continuity Management Systems.

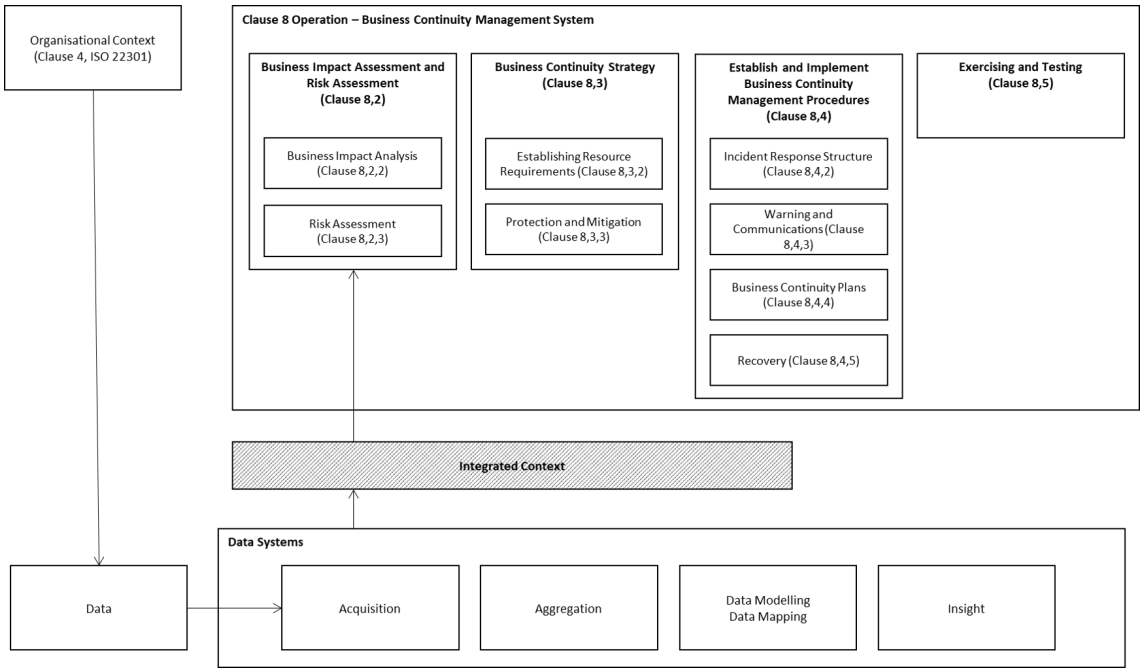


Figure 3.1: Data contextualisation approach with reference to the ISO22301 [3, 18]

When selecting a data set to support the risk assessment and business impact analysis, the context of the data set becomes an important consideration [19]. This selection may or may not be effective, or may become more effective over time. Integrated data sets that are linked to organisational context (ISO22301 Clause 4) within the Business Continuity System has merit and bearing on the resilience measurement of the organisation and its interrelated systems [3].

Business continuity management professionals in banking systems work collaboratively with data management professionals and engineers to derive the data insights that they require. Data curation methods can be lengthy and often require extensive engagement, data modelling and mapping. In the event of a disruption or crisis, obtaining data that is current and appropriately mapped is needed to inform the most appropriate response. Data curation processes become impediments when this arises, but these are necessary to improve the reliability of data [19]. Data analytics also requires reliable data on which to derive insights. The availability of business metadata provides an additional advantage to agility and response [17].

The common inhibitor to response formulation and planning is the collection of multi-faceted views of the data and reaching consensus of the data definition and the most appropriate and useful application of the data set to a defined business continuity management problem statement. This along with the skills required to deal with the data are challenges cited in the Business Continuity Profession [1].

Environmental data consists of both internal and external data sets. External data has varying degrees of big data characteristics including volume, variety, velocity and variability. Sourcing external data sets often removes system of record context.

Internal organisational data also forms part of such systems and is recorded within the context of operational systems. Both types of data are required to form a holistic record of organisational history.

Integrated context as shown in figure 3.1 has the following systemic considerations:

1. It is mapped to the context of the organisation (clause 4) as defined by the Business Continuity Management System [3],
2. It is scoped to the organisation's taxonomy [17],
3. It has an association to the Business Impact Analysis (clause 8.2.2 of the ISO22301 standard) and the Risk Assessment (clause 8.2.3 of the ISO22301 Standard) of the business continuity management system [3],
4. It informs the business continuity management strategy (clause 8.3) by providing a quantifiable basis on which to determine resilience indicators (enhanced though expert judgement) [3] and
5. Risk assessments can be associated with a risk taxonomy through the analysis of the business metadata of a selected data set.

Data that is contextualised and structured with business resilience indicators becomes useful in the design and implementation of Business Continuity Management Systems of the future.

Ongoing focus in the financial services industry globally is to increase the strength and resilience of the system. In the past 20 years, there have been a number of events that led to disruptive incidents. The most significant recent disruption being the 2008 global financial crisis. This crisis was caused by inadequate management of credit systems. Following this crisis there has been an increasing awareness of several risk factors that must be assessed and managed on an ongoing basis. History has shown that many environmental factors converge to disrupt business in a rapidly changing multi-faceted risk landscape. As a result the study of network risk analysis between 2017 and 2020 is an emerging research theme [20, 21, 22].

For data to become useful, it is associated with a business requirement and through the curation process is structured according to a set of technical and business rules. The BASEL Committee regulation specifies that risk data is subject to its 14 data management principles for risk data aggregation (BCBS239, 2013) , specifically in the use case where risk reporting is concerned. This standard is also good practice according to DAMA and can be extended to all data systems that affect any risk type [17, 19].

In the financial services industry, data and information is increasingly important for both the regulatory use cases as well as in the fulfilment of use cases that deal with competitiveness (i.e. commercialisation of data) and risk management [23]. It is also becoming increasingly important to Business Continuity Management Systems that deal with organisational resilience [1].

Organisational resilience requires an understanding of a banks' operating context and systems interactions and this is where data begins to play a central role. During a disruptive event, operating context changes. The business continuity system of the bank contains the strategy and plan to be followed when the event requires these to be invoked [24].

Effective resilience requires banks to respond to environmental disruption and change with clarity of intent and purpose and to invoke its strategies and plans in an informed manner. It also requires the bank to anticipate environmental changes and to continuously review the plans and strategies for appropriateness through ongoing assessment (ISO22301 Clause 9) [2, 3].

3.2 Data Contextualisation Methods

The definition of context according to the Oxford English Dictionary is "the interrelated conditions in which something exists or occurs [25]". This definition is adopted as the standard for this report.

In the industry, banks may contextualise data in three ways; mapping against an industry standard data model, semantic data modelling against a specific use case data model or through a data analytics process that looks for data correlations. All three methods are used to support specific requirements and the process is aligned to best practice guidelines according to DAMA [19].

Mapping against an industry model - This method supports industry standard reporting requirements through and Enterprise Data Model that is fit for purpose for the bank and its operations. The bank's data is scoped to a set of data concepts that describe the bank and its operations. In this method, data is curated into a whole system data design that is fully integrated. Data is expressed in the relationships between concepts and is never viewed in isolation. This is the longest and most complex form of data curation as enterprise agreement of the mapping of data must be reached before it can be integrated into the data model. Once mapped the data becomes useful within a defined banking data concept, for example customer, where all instances of customer data are conformed. In this method, data is physically moved from its originating source through a data load and transformation process to fully contain and store organisational history. Data modelling is required for credit risk data according to the BCBS239 Principles for Risk Data Aggregation and Reporting.

Semantic data modelling - This method supports a view of the data that can be changed in an agile manner to support a specific requirement without the physical movement of data. In this method, data is still mapped, however the data model can either inherit concepts from an underlying data model or could be defined specific to the use case to be solved. Data virtualisation techniques are used to make this data available.

Data Analytics - This method uses quantitative and qualitative methods to analyse data sources and to identify trends and correlations in data that are useful to enhance organisational insight. In this method, data is sourced, analysed and categorised into associations and specific outcomes within an acceptable margin of error. Data analytics supports business requirements that are predictive in nature or that are required by an "interested party" to inform an action [3].

Business continuity professionals in banks work with data management professionals and engineers to derive the data insights that they require. Data curation methods can be lengthy and often require extensive mapping and gathering of metadata. Risk taxonomies and data modelling taxonomies are loosely related, but are often not applied in an integrated manner.

3.3 Conclusion

In the event of a disruption or crisis, obtaining data that is current and contextualised is needed to inform the appropriate action to be taken. It is proposed that through the integration of risk taxonomies and data taxonomies, suitable connections of data into the Business Continuity Management System becomes a useful driver of organisational resilience through an integrated system of insight that is connected to the activities of risk assessment and business impact analysis.

4

Standards

This chapter presents the framework of applicable standards needed to complete the system engineering portion of this report. This section will discuss in detail the various prudential standards as well as the international standards and good practice guidelines that are adopted in the development of the resilience system and its associated system of insight.

4.1 Prudential Standards

The BASEL Committee mandate states: "The BCBS is the primary global standard setter for the prudential regulation of banks and provides a forum for cooperation on banking supervisory matters. Its mandate is to strengthen the regulation, supervision and practices of banks worldwide with the purpose of enhancing financial stability [26]".

According to the history published by the BASEL Committee, it was established in 1974 to "enhance financial stability by improving the quality of banking supervision worldwide, and to serve as a forum for regular cooperation between its member countries on banking supervisory matters [27]."

The committee issued its first accord in the 1980's which focused on capital adequacy. Since its inception, in the last 45 years, the BASEL Committee issued three new accords to deal with emerging risks in global banking [27].

The BASEL I Capital Accord issued in the early 1980's deals with capital adequacy and market risks.

The BASEL II New Capital Framework issued in June 1999 replaced the first accord and provided a "framework for capital adequacy that focuses on minimal capital requirements, supervisory review and effective disclosure [27]."

BASEL III was issued in 2009 in response to the 2008 global financial crisis and deals with the strengthening of the Capital Framework.

In 2010, the BASEL III International framework for liquidity risk measurement, standards and monitoring and the Basel III Global regulatory framework for more resilient banks and banking systems were issued to further supplement the third accord. An applicable summary of the prudential legislation is shown in figure 4.1 [15].

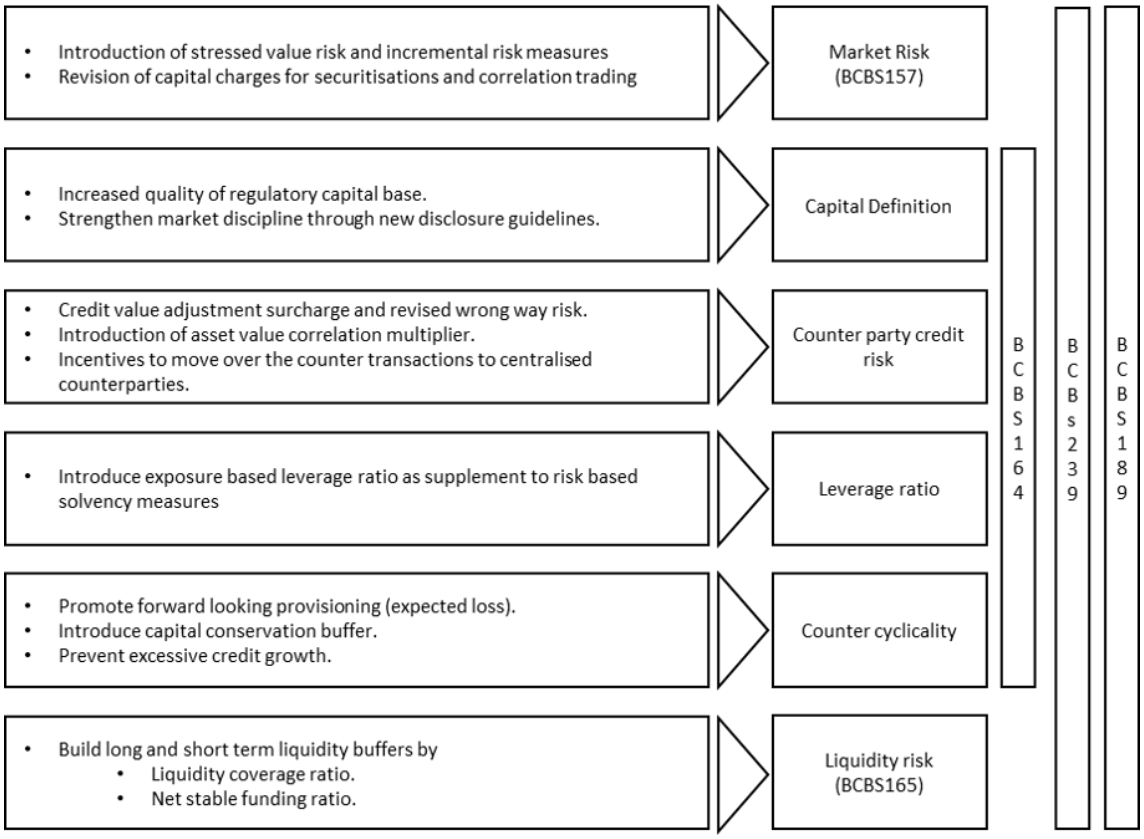


Figure 4.1: BASEL Standards and Principles. Adapted from Helmich et el 2014 [23].

The Basel Committee for Banking Supervision (BCBS) issued two legislative standards to which banks must comply, these are: The High Level Principles for Business Continuity Management (BCBS189, August 2006); and The Principles for Effective Risk Data Aggregation and Reporting (BCBS239, January 2013) [2, 17].

These two standards are used in this report along with the following:

1. ISO22301:2012 Standard for Societal Security - Business Continuity Management Systems [3],
2. ISO22313:2012 Guideline for Societal Security - Business Continuity Management Systems [18],
3. Business Continuity Management Good Practice Guide [24],

4. The Data Management Association Body of Knowledge [28],

5. The Data Management Association Dictionary [19].

4.2 Business Continuity Management: BCBS189

According to the BCBS189, "Financial authorities and financial industry participants have a shared interest in promoting the resilience of the financial system to major operational disruptions [2]."

The BCBS189 legislation was issued in 2006 in response to "Acts of terrorism in New York, London, Istanbul, Madrid and elsewhere, outbreaks of Severe Acute Respiratory Syndrome (SARS) and the Avian Flu, and various widespread natural disasters have served to heighten that priority by underlining the substantial risk of major operational disruptions to the financial system [2]."

Business Continuity Management is concerned with operational risk management and deals with emerging environmental risks and impacts through the establishment, planning, operation and maintenance of a Business Continuity Management System [24].

It is noted that some revisions to the BCBS189 standard were introduced in December 2017 in response to the global financial crisis. Additional provisions were made in these revisions to provide for the management of risk in economic systems. [15].

4.3 ISO22301:2012 Societal Security - Business Continuity Management Systems

ISO, the International Organisation for Standardisation is a worldwide federation of national standards bodies. ISO prepares standards through technical committees who adhere to and apply a set of directives for standards that provide rules for standards published [3].

The ISO22301 specifies the requirements for setting up and operating an effective Business Continuity Management System (BCMS). "This standard can be used to implement a compliant Business Continuity System that meets the needs of the organisation and its interested parties [3]."

ISO Standards apply Demming's Plan-Do-Check-Act cycle (PCDCA) to "plan, establish, implement, operate, monitor, review, maintain and continuously improve the effectiveness of the system to be implemented [3]".

Business Continuity Systems that are implemented according to this standard may be audited against the criteria set-out in its clauses. [18]

4.4 Data Management: BCBS239

According to the BCBS239 (2013), "Some banks were unable to manage their risks properly because of weak risk data aggregation capabilities and risk reporting practices. This had severe consequences to the banks themselves and to the stability of the financial system as a whole [17]."

The BCBS239 principles for risk data aggregation was issued in 2013 to strengthen the finance systems of the bank through compliant information technology platforms and trusted data aggregation and reporting [17].

According to the Data Management Association (DAMA), data management deals with the development and execution of "plans, policies, practices and projects that acquire, control, protect, deliver and enhance the value of data [17, 28]." BCBS239 principles align to this best practice.

4.5 Business Continuity Institute Good Practice Guideline

The Business Continuity Management Good Practice Guideline focuses on the establishment of an effective response structure [24]. According to the guide, "the response structure established command, control, and communication systems to help the organisation manage incidents and minimise the impact of disruption [24]".

In this report, response structures are important organisational considerations as the work aims to ensure that the response structure includes information that is well contextualised and available to help banks to manage an incident should it arise.

The Business Continuity Institute Good Practice Guide proposes that when establishing an effective response structure, consideration should be given to "the requirements of the business continuity policy" and that "it supports the agreed continuity solutions [24]."

4.6 ISO22313 Societal Security - Business Continuity Management Systems - Guidance 2012

The Guideline for the ISO22301 Standard which is documented into the ISO22313 provides the methods and techniques that should be considered during the implementation of a compliant Business Continuity Management System. This guideline is adopted in this report to ensure that the system meets industry standard criteria in its implementation approach [3, 18].

4.7 DAMA DMBoK 2018

"Data management is the science of actively managing data definitions, data quality, privacy, architecture and data life cycle along with the value and risk associated with data [29]."

A guideline for ensuring that projects that use data as a resource, is to set data management principles that are applicable to the activities and functions being performed through the data development life cycle.

The data life cycle (not the same as the data development life cycle) deals with sourcing of data, storage and curation of the data, data usage, archiving of data and the results of the curation and usage process and finally the purging of data. All these steps should be done responsibly and ethically. Transparency of data transformation through data solution development is included with verifyable results [19].

In this report the Systems Engineering Management Plan (SEMP) and V-Model in figure 6.6 reflect the DAMA Principles as they have been applied.

4.8 Guiding Principles according to DAMA

According to the DAMA Data Management Body of Knowledge (DMBoK) the following guiding principles apply [28]:

1. "Data and information are valuable enterprise assets.
2. Manage data and information carefully, like any other asset, by ensuring adequate quality, security, integrity, protection, availability, understanding and effective use.
3. Share responsibility for data management between business data stewards (trustees of data assets) and data management professionals (expert custodians of data business function and a set of related disciplines.
4. Data management is also an emerging and maturing profession within the Information Technology field."

Data management principles are applied in data functions and activities. These functions and activities include: data governance, data architecture management, data development, data operations management, data security management, reference and master data management, data warehousing and business intelligence, metadata management, and data quality management [19, 28].

Within each of these activities and functions, specific principles applicable to this report are defined and applied according to this guideline in subsequent sections.

4.9 Standards Adoption and Application

The positioning from the Basel Committee on Banking Supervision - BCBS239 and Business Continuity Management - BCBS189 form the basis of the systems context of this report which aims to improve information practices for operational risk specifically in the area of business continuity management. Particular focus is given to the application of data to inform business continuity management planning outcomes [2, 17].

Good practice guidelines have been used to ensure that methods and techniques applied in the design and prototype of the Resilience System are in line with both Business Continuity Management and Data Management Practice. The application of standards also provides an opportunity for future work through standardisation of method where appropriate.

5

Resilience Research

5.1 Introduction

Resilience research has been applied to many industries and applications some of which include; the built environment, organisations and ecological systems. There are many quantitative and qualitative measurements that have been proposed since C.S. Holling's research of adaptive environmental assessment and management for ecological systems in 1973 [30]. Since then resilience has been studied, researched and discussed over the past four decades. During this time, resilience research themes have included organisational resilience and resilience frameworks, quantitative methods of resilience measurement applied to the built environment, systems engineering and mathematical models for resilience.

Given the multiple domains in which resilience research has been conducted, this review considers the evolution of principle based resilience work to support the hypothesis that contextualising data is a new concept that may be useful in future work which can be applied to business continuity management systems design.

Applied principles form the basis of most resilience work and are foundational to resilient systems design. The basic principle of resilience in systems is the ability of the system to continue to function and perform under conditions that are expected and unexpected. Also that systems are able to recover to a state that is the same or better following a disruption. Holling describes the ability of ecological systems to stabilise and adapt to changing conditions. Holling's work focuses on the adaptive cycles of ecological systems and their ability to transform into either a new state or an improved state over time. He also notes that systemic shocks are not always deterministic and that systems may be subjected to numerous random events that affect and shape them.

Subsequent work by Burnard and Bhamra, Sutcliffe and Vogus builds on Holling's adaptive cycle principles [31, 32]. Principle based resilience work has lead to the development of risk taxonomies [33], standards and frameworks to deal with disruptive events in a more structured and quantifiable manner [33, 31].

A tabular summary of research considered is provided in table 5.1, which outlines the classification of systems (Checkland, 1999) reviewed along with five themes that are prevalent in the literature [9]. Despite growing business continuity management and resilience research especially following the 2008 Global Financial Crisis, there is limited research that specifically deals with risk trend analysis and the role that systems of insight can play in integrated business continuity management systems [1, 31].

This is problematic when designing business continuity management systems that can derive benefit from the increasing number of data sets that are becoming available to practitioners. In addition to this, researchers have indicated that the use and management of data in business resilience systems is a topic for future work [31, 34, 35].

The literature reviewed applies the following principles in its inclusion:

1. Global and South African risk perspectives which aim to identify the operating context of financial services organisations and the risks associated with these,
2. Resilience measurement frameworks and/or methods. Both quantitative and qualitative methods,
3. Applied systems thinking approach to organisational resilience which is foundational to understanding how systems thinking approaches are applied and
4. Disaster management case studies and emergency response plan references.

Literature resources consulted include: Google Scholar, the British Library Ethos, Web of Science, Research Gate, government and industry sources, legislation and University of the Witwatersrand Library Services.

Table 5.1: Summary of literature review

Classification	Reference	Year	1	2	3	4	5
Designed Abstract System	Cliff Ferguson	2017	X	X		X	
	Christos Ellinas, Neil Allan and Caroline Coombe	2018	X	X		X	X
	Tovio Niskanen	2018	X	X		X	X
Designed Physical System	Enrico Colera	2007		X	X		X
	Scott Jackson and Thimothy Ferris	2012	X	X			
	Henry, Emannuel and Marquez	2012		X		X	
	John Johnson and Adrian V. Georghe	2013			X	X	
	Ayhan Jaaron and Chris Backhouse	2014					X
	Guilia Cere, Yacine Rezgui and Wanhqing Zao	2017	X	X	X	X	X
Human Activity System	C.S. Holling	2001	X	X	X		X
	Edward H. Powley	2009	X				
	K J Burnard and R Bhamra	2011					
	Kathleen M. Sutcliffe and Timothy J. Vogus	2014					X
	Dnezil Kennon, Corne S.L. Schutte and Eric Lutters	2015		X	X	X	
	Ariella Helfgott	2017		X		X	X
Natural System	C.S. Holling	1975	X	X	X		X

The study of resilience spans a wide variety of applications and is multi-disciplinary. In order to understand the considerations in previous literature, the following themes have been investigated and are represented by the numerical values in the table.

1 = Principles, 2 = Frameworks, 3 = System Dynamics, 4 = Measurement Methods, 5 = Systems Thinking [9].

Peter Checkland (Checkland, 1999) divides systems into five classes: natural systems, designed physical systems, designed abstract systems, human activity systems and transcendental systems. These classifications have been used to group resilience systems research [9].

5.2 Definitions of Resilience

This section begins with the positioning of the definitions of resilience that have been formulated and adopted by resilience researchers in various engineering disciplines. With this as a foundation both global and local risk perspectives are provided as a basis on which the context of current organisations is set.

The current business resilience research covers a broad spectrum of risks as risk management is complex and includes many internal and external factors that influence a system's ability to recover after the impact of a disruption [22, 36]. Research sources provide insight into both the ability to prepare for and anticipate risks as well as to effectively recover from a disruption, which uses the generally held definitions and descriptions of resilience [31].

A.Helfgott, K. Burnard and R. Bhamra, Coiera et al, and Patriarca et al, provide definitions of resilience that have been widely referenced and used. Although there are several definitions that have emerged over a number of years, there is general agreement that a holistic systems approach is needed [37, 36]. Resilience according to A.Helgott refers to a systems ability to withstand disturbance and are able to recover to an acceptable state [35]. Burnard and Bhamra note in their definitions that it is not only systems recovery that is important in building resilience, but that consideration should be given to continuous improvement to ensure that systems remain viable in uncertainty and change [31]. The focus is on systems remaining competitive which is of particular importance in organisations [31]. Resilience research in the built environment (Cere et al, 2017), offers similar themes to describing resilience and its importance [31].

Guila Cer et al broadly categorise disruptions as "external or systemic according to their origin or relation to the system" in the built environment [34].They describe the need to design for anticipated disruption and to ensure that resilience indicators and respective tolerances are defined and quantified. Their research in a "Critical Review of Existing Built environment Resilience Frameworks: Directions for Future Research" (2017) provides a foundation for performance based resilience measurement. Their work identifies the need for more holistic and context specific data sets and structured resilience indicators [34].

The E-CSR currently describes resilience as follows: "Business resilience is a business-wide term that comprises crisis management and business continuity and that represents the ability of organisations to rapidly adapt and respond to all types of risks – such as natural disasters, cyber- attacks, supply chain disruptions, among others. Besides the ability to face the consequences of a major incident, business resilience also includes the capacity of an organisation to adapt and adjust to a new environment and new circumstances [38]."

5.3 Global Risk Perspectives - Business Continuity Institute Horizon Report

According to the Business Continuity Institute, "Horizon scanning is an activity used to monitor and identify potential threats to an organisation and considers longer term change and underlying trends. Information provided by the Horizon Scan is useful when undertaking a risk assessment as part of the business continuity program [24]."

The Business Continuity Institute Horizon Scan Reports, provide line of sight of "near and long term business threats [4]." It is notable that 70 percent of the respondents that contributed to the report in 2020 use the Horizon Scan as a risk and threat assessment tool [4]."

The BCI Horizon Scan Reports include a previous twelve month retrospective along with a future outlook for the next twelve months and global perspectives of the top ten disruptions reported in a previous year. In addition it provides surveyed measurement of the uptake of the ISO22301 Standard in formal business continuity management programs [1].

Between 2016 and 2019 ISO22301 uptake has increased from 51 percent in 2016 to 69 percent in 2019 [4, 39]. From the respondents in the 2019 report, 55 percent use the ISO22301 standard as a framework however, this fell to 50.5 percent in 2020 [1, 4]. The major reason for this was that there was no business requirement for certification within their organisations along with other factors such as lack of management commitment and budget. 18.3 percent of respondents in the 2020 report indicated that there was a perception that the standard did not add business value [1]. There is still a lot of work to be done in the standardisation of methods, taxonomy and the value proposition of implemented business continuity management systems with certification [4].

The 2020 Horizon Scan Report notes that compared to previous years, fewer organisations are conducting longer term risk trend analysis. This was reported, despite the fact that organisations are seeking and using multiple data and other resources to understand the threats facing their organisations. These resources were cited as both internal and external. From the respondents surveyed, the following inhibitors to doing trend analysis in their organisations were evidenced from the surveys conducted [1]:

1. Mostly trend analysis happened departmentally rather than centrally,
2. The tools, resources and skills required to do this type of analysis are not easily available within organisations,
3. Due to decentralisation of efforts, practitioners have had to implement frameworks to make sense of data that is available to them such as the BCI Horizon Scan, internal Country Risk Assessments that are published, information from suppliers, Social Media and other free resources,

4. The business case to gain access to more detailed data sources is difficult to justify without a business requirement.

The above-mentioned reasons, indicate that there is a need to organise resources and apply them appropriately to inform strategic responses to potential threat and disruption scenarios [20]. There is still a lot of work to be done to bring the awareness of a data driven approach to risk analysis and to provide practical approaches to the management of appropriate data sets that do not require extensive data curation and analytical modelling skills [33, 20]. Sources of literature continue to emphasise a pragmatic and systems based approach [32, 40, 41].

The methods professionals are following to conduct trend analysis include: internal risk and threat assessment, risk registers, external reports and industry insight, participation in industry events and conferences, social medial monitoring, automated systems for cyber security. A small percentage (4.6 percent), mentioned other mechanisms to conduct trend analysis [1].

Close to 90 percent of respondents indicated that internal risk and threat assessment is their preferred method of identifying trends, followed by 62.5 percent using risk registers and 58.2 percent using external reports and industry insight [1].

With slightly more than half the respondents now relying on external sources of data for trend analysis, the need and importance of managing this data centrally has increased [1]. Also, trend analysis data is not always integrated into to Business Continuity Management Systems, which may lead to missed or inconsistently interpreted insight in organisational silos potentially diminishing the value of these organisational assets [34].

Data Management Principles will not necessarily solve this systemic issue [19]. Further work is needed to manage the data in the context of the insight required. Derived insights from data systems integrated into business continuity management systems provides a possible foundational platform to improve an organisation's disruption response and to scale up as additional data sources become available [31, 34, 42, 43].

5.4 South African Risk Perspectives - Institute of Risk Management South Africa

The Institute of Risk Management South Africa (IRMSA) Risk Reports provide a source of horizon scanning in the South African context. According to the authors of the IRMSA Report, in 2019, it "creates awareness of the risks facing the achievement of the South African country and industry objectives [44]". It stimulates debate on how to best manage the risks highlighted in the report through communicating current challenges clearly to create effective risk treatment plans benefiting the country and all South Africans [44]." The IRMSA report is compiled through the gathering of opinions from subject matter experts and through industry survey. These are

summarised in the report, which includes both country and industry evaluations of the top risks affecting South Africa. The IRMSA 2019 report also states that it "recognises the South African Development Plan (2012) as the legitimate summation of the joint goals of the public and private sector [44]."

To establish the context and importance of the South African resilience perspective, Ferguson writes in the Journal of Business Continuity and Emergency Planning Volume 11 Number 3 (2017) that at the time of writing, 23 years had elapsed since the African National Congress "accepted the newly drafted constitution [45]". Ferguson discusses the importance of South Africa, as the 47th largest economy in the world that "must continue to maintain and protect its infrastructure, wealth of resources and essential services [45]." Ferguson references the The South African National Development Plan 2012 which, "describes resilience as a key foundation for the stability and sustainability of South Africa's people and its economy [45, 7]."

South African Legislation and operating context is unique in its tightly interrelated risk landscape and close interactions between the public and private sector. South Africa has a strong financial services industry that is well regulated in line with international standards [44].

The South African Development Plan (2012) is a nine point plan to achieve national resilience. These are listed as follows [7]:

1. "Resolving the energy challenge,
2. Revitalising agriculture and the agro-processing value chain,
3. Advancing beneficiation or adding value to mineral wealth,
4. More effective implementation of a higher impact Industrial Action Policy Action Plan (IPAP, 2020),
5. Encouraging private-sector investment,
6. Moderating workplace conflict,
7. Unlocking the potential of SMMEs, cooperatives, townships and rural enterprises,
8. Boosting the role of state-owned companies, information and communication technology infrastructure and broadband roll-out, water, sanitation, transport infrastructure as well as science, technology and innovation and
9. Operation Phakisa". (According to the South African Department of Forestry, Fisheries and the Environment, Operation Phakisa focuses on unlocking the economic potential of South Africa's oceans and aims to add R177 billion Rand to GDP by 2033).

Horizon scanning should be done taking into consideration the operating context of countries and organisations as standard practice [24]. The South African National Development Plan provides a foundation for country specific resilience focus [7].

South African Risk Perspectives reported annually by IRMSA provides a holistic understanding of the focus areas of the country and also how these risks are emerging as potential factors influencing the performance of the financial services industry. In 2020 approximately 25 percent of the respondents to the IRMSA Risk Report surveys and expert analysis were from the financial services industry. Indicating the ongoing commitment to risk assessment and management in this sector [44].

5.5 Resilience and Business Continuity Management Frameworks

Risk metrics are an integral part of risk systems which span global and local regions and are also applied to organisations.

Measurement of risk tolerance has been an important part of ensuring that there is continuous improvement in the resilience of financial systems globally and this equally applies in the local South African context [7]. Key Risk Indicators have been defined in financial services legislation and provide the basis of reporting to financial regulators [26]. Cumulatively, these metrics provide a valuable indication of the health of financial systems and the responses needed to ensure long term sustainability. This is in line with resilience research work and the need to define measurement which is used for assessment, monitoring and continuous improvement.

To provide a degree of certainty in measurement, good quality data that is well managed is required [19]. In the case of financial services, key risk metrics that are applicable to credit risk data are subject to the BCBS239 principles. The data used for reporting is generated by internal transaction and data warehousing systems and other external sources of data where appropriate and these system architectures are subject to regulatory scrutiny [17].

Banking systems in themselves generate data and this data is currently used to quantitatively determine key risk metrics for self assessment and regulatory reporting. To remain competitive in a rapidly changing business context, financial institutions have had to consider wider systemic data which influences transactions and interactions. External data sources are increasingly being used to get additional insight that can either increase competitiveness, improve operational efficiency or manage risk.

External data sources particularly those that increase a bank's ability to manage risk better than a competitor provides an opportunity to enhance an organisation's responses to changes in operating context. Integration of well managed data and information with business continuity systems and strategy formalises this process in a holistic system design [19, 9].

Increasing effective risk response through enhanced monitoring of changing operating context is the area of interest in this report [3].

Literature that deals with the identification and appropriate use of resilience indicators, metrics and the quantification of risk is also diverse in nature. There is however, consensus on the following:

1. Risks are complex and interrelated: They can be represented in a network which can be qualitatively and quantitatively assessed. These methods have been discussed by Jackson and Ferris (2012) and Henry, Emmanuel and Marquez (2012) and Ellinas, Allan and Coombe (2018) [20, 41, 46].

2. Burnard and Bhamra (2011) note that "resilience is a multidisciplinary and multifaceted concept" [31]. Their framework for resilient systems includes horizon scanning and information seeking as essential system framework components (figure 5.1) [31]. Holling also provides context to this level of complexity through the understanding of system adaptive cycles. Systems adapt and change according to changing conditions. This process considers multiple influencing factors that are interrelated to trigger change to an adjusted system state [30].

3. Qualitative and quantitative approaches can be used to evaluate and assess risks and threats. Research in the area of resilience measurement provides several different models and methods including: probabilistic anti-fragility models (Johnson and Ghorge, 2013 and Kennon, Shutte and Lutters, 2015), direct and indirect expert approaches (Henry, Emmanuel and Marquez, 2012 and Cere, Rezgui and Zhao, 2017) and mathematical models for operationalising resilience (Helfgott, 2017). Helfgott further acknowledges the "pluralism" that exists in the definition and understanding of resilience and that this leads to a variety of approaches which have validity and merit in application [34, 35, 42, 46, 47]. In all cases of the literature, standardisation remains a theme for future work.

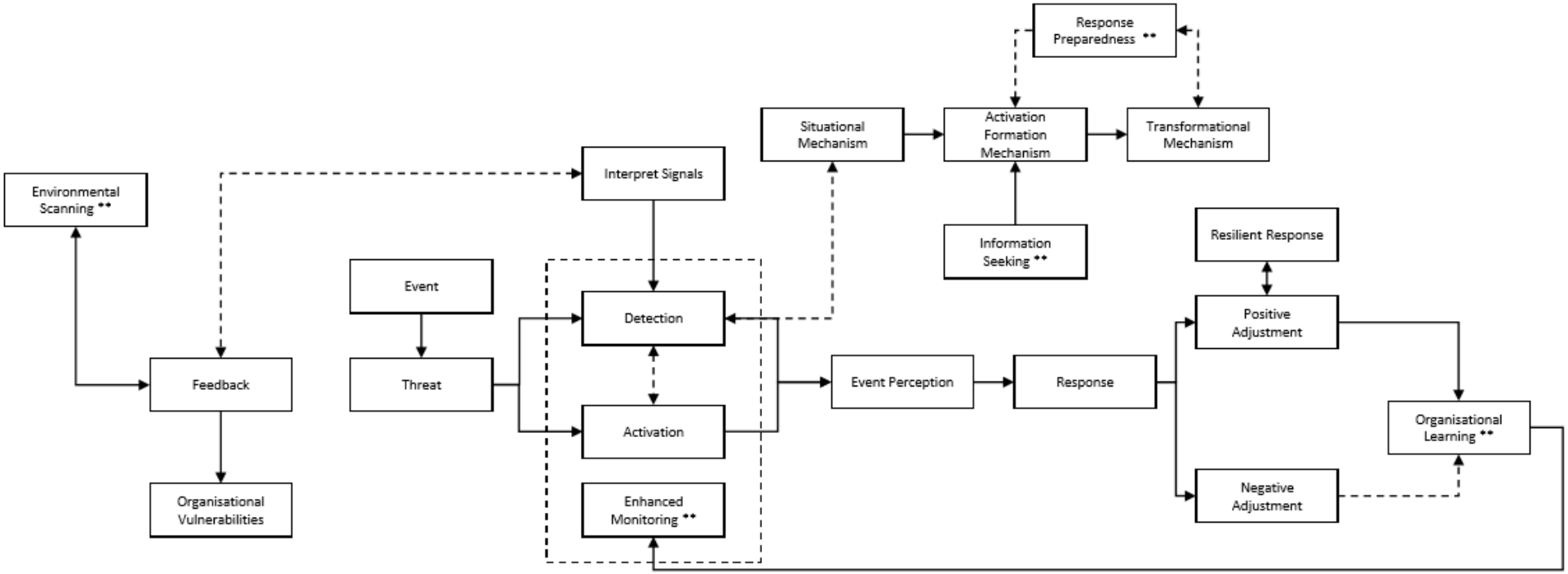


Figure 5.1: Resilience Framework [31]

Ellinas, Allan and Coombe (2017) address the complexity in the risk landscape and use an evaluation of horizon scanning capacity as a basis to "Identify, to analyse, to evaluate and treat" a particular risk [20]. This work sets the principle, that horizon scanning should be the first step in the process of understanding the different classes of risks across a risk network. Their work sets out the method to analyse and evaluate risk networks and to provide mechanisms to evaluate high focus risks. This is a basis on which to quantify and understand the cumulative effect of interrelated risks and gives insight into how risks should be evaluated in an "empirical based, quantitative risk network" rather than traditional risk assessments [20].

The work-ability of this model has been tested on financial data sets with successful outcomes in measuring the sensitivity of the system to changing risk factors with the conclusion that "distinct risks threatening the operation of individual systems can no longer be treated in isolation [20]".

This recent work along with the findings noted in the 2020 BCI Horizon Scan Report and other sources begin to highlight the requirement to assess the risk landscape and to enhance an organisations' ability to respond and adapt [1, 20, 40].

"Future research should focus on finding a pragmatic, real-time and concretely useful framing of resilience, able to encompass holistically a range of hazards relying on meaningful parameters that can be adjusted according to the addressed disruption [34]." A list of future work directions is specifically addressed by Cere et al. as follows, which provides a useful summary of the themes emerging in recent years [34]:

1. "Pragmatic/useful in practice,
2. Flexibile/adjustable according to the analysed disruptions,
3. Inclusive/holistic,
4. Embed pragmatic emergency planning strategies and
5. Context specific."

Although this work was more specifically applied in the built environment, the principles of risk management continue to remain consistent across industries and findings would still provide useful guidance to the financial services industry that has a similarly quantitative approach to risk management.

Burnard and Bhamra (2011) also identify future research opportunities which is to "focus on identifying enabling conditions for organisational resilience and developing an enhanced understanding of the dynamics of organisational responses to high impact events [31]." What is noted in their work is the need to "identify the organisational capabilities that influence an organisations resilience response [31]." Sutcliffe and Vogus "Organising for Resilience" (2014) provides a similar theme for future work which indicates the need to assess past and present conditions that "pose a threat" and to "determine the criteria for what would constitute positive adaptation" of organisational systems [32].

Most recent research into the taxonomy of risk (Tovio Niskanen, 2017), has built on the theme that taxonomies provide an opportunity to gain insight into qualities of resilience in the context of occupational health and safety to help to "develop proactive safety measures [22]". This work provides a method of survey using a taxonomy to derive better insight from respondents. Niskanen has given the field a pragmatic approach to the handling of multi-body system data by applying taxonomy data representation. He has demonstrated the work-ability of the use of taxonomies and standardisation in an applied occupational health and safety use case. Niskanen notes that resilience engineering systems surveys could be further advanced by incorporating built-in structured data. As risk assessment and trend analysis largely relies on survey data, this is an important consideration when handling data results in future business continuity management system design [22].

Taxonomy emergence is developing in the open source landscape with the growing need to standardise and to link data sets to themes for greater insight [22, 33]. The application of metadata and master and reference data management also supports this in best practice [19].

In summary, resilience frameworks and business continuity management systems research covers the structures of these systems, consideration that data and information is an important factor that contributes to successful strategy as well as the need for standardisation in classification of risk and associated data sets.

5.6 Quantitative and Mathematical Models and applied Qualitative Approaches used to Measure Resilience

Quantitative and qualitative resilience measurement models have developed through various disciplines and can be used when analysing data and developing quantitative analytical models. These are summarised in the below sections for completeness and to demonstrate that there needs to be an understanding of the different mathematical approaches in application.

5.6.1 Systems Engineering Approach

Henry et al. recommend that focus be given to a systems engineering approach to resilience [46].

In their work they use systems engineering to define the "system of interest " when approaching a resilience problem [9, 46]. It is recognised that resilience is time dependent. Using business continuity good practice definitions and standards, they express the resilience of a system as the ratio of recovery time to loss suffered by the system at some previous time. This ratio indicates the ability of a system to recover. If a system is "fully resilient", then "recovery is equal to loss [46]".

The model is described below [46]:

Resilience R as a function of time t can be expressed as a ratio of Recovery as a function of time t to the loss suffered by the system at a previous point in time d in equation 5.1.

$$R(t) = \frac{Recovery(t)}{Loss(d)} \tag{5.1}$$

Within the system of interest, it is noted that there may be several components which are related to each other and reference is made to a figure of merit to describe its delivery function. Figures of merit describe system interrelationships in a connected network [9]. Figures of merit are useful to describe flow or delay in system processes. A system of interest may contain several sub systems each with their own figures of merit [3, 46]. It is also important to note that figures of merit may be related to each other systemically [46].

The mathematical representation of the value of resilience corresponding to a specific figure of merit evaluated over time under a disruptive event as proposed by Henry el al is provided in equation 5.2.

$$R_F(t_r|e_j) = \frac{F(t_r|e_j) - F(t_d|e_j)}{F(t_0) - F(t_d|e_j)} \tag{5.2}$$

1. "$R_F(t_r|e_j)$, indicates the proportion of delivery function that has been recovered from its disrupted state.
2. The resilience metric $R_F(t_r|e_j)$ is quantifiable if and only if the figure of merit$F(t_r|e_j)$ is quantifiable.
3. The minimum value of $R_F(t_r|e_j)$ equals 0, obtained when $F(t_r|e_j) = F(t_d|e_j)$. In this situation, the system has not recovered from a disruptive state. In this instance one of two options is possible. Either no activation has occurred (Figure 5.1) or the resilience action taken has been totally ineffective.
4. Wherever $F(t_r|e_j) = F(t_0)$, the value of resilience $R_F(t_r|e_j) = 1$, the disrupted system recovers to its original stable state and its associated delivery function $F(t_0)$. It is also possible for the system to recover to a better state than its original state.[31], [46]. In this case, $F(t_r|e_j) > F(t_0)$".

Time and cost dimensions can be further added into the measurement method.

Time Dimension

$$T_R(e_j) = \sum_{s(i)}^{s(j)} t(i) \tag{5.3}$$

Where s is a component of a system S and t is the time taken to restore the system component.

Cost Dimension

$$C_R(e_j) = \sum_{s(i)}^{s(j)} c(i) \tag{5.4}$$

Where s is a component of a system S and c is the cost incurred to restore the system component. Additional losses also need to be factored into the statement of disruption of cost which would include: "losses incurred due to a system's inability to perform at the normal level. This loss could be a combination of time-dependent and time-independent factors" depending on the nature of the system. These would be added to the costs calculated in equation 5.4 [46].

This is useful when applied to the business impact analysis and business continuity strategy in aggregation across all time and cost variables.

5.6.2 Expert-based Indirect Approach

Cere, Rezgui and Zhao (2017), investigate approaches to the measurement of resilience in the built environment and other use cases in their work "Critical review of existing built environment resilience frameworks: Directions for future research". Both qualitative and quantitative approaches are presented work. They write that "several attempts have been made to quantify resilience over time and there has been a shift from qualitative frameworks to more numerical metrics [34]."

In the instance of quantitative methods, Cere et al, broadly categorise their methods into "multi-hazard/wide spectrum and single-hazard small scale approaches [34]". Further classification of small-scale approaches include "expert based indirect approaches and direct performance based approaches [34]."

In the application of each of these approaches to the built environment, the differences are noted as follows [34]:

1. "Expert based indirect approaches identify representative indicators and leads to resilience formulation based on the input of these,
2. Performance based direct approaches rely on fragility curves (expressing the probability of a system exceeding a certain damage threshold, referring to a specific parameter."

The methods of Cere, Rezgui and Zhao have been included in the scope of this report as an additional method of resilience measurement and validation. Small

scale approaches are more appropriate as these consider system components and their specific resilience factors and influences. In the example cited in their work, small scale approaches provide for "resilience of what" and "resilience to what" as the basis of their quantification of resilience [34].

The expert-based direct approach of resilience measurement is "obtained subjectively by assigning weighting parameters" to indicators of resilience in the system that is being measured. Indicators are also assigned a numerical factor based on its relevance towards overall system resilience. This method allows for the identification of contributing indicators of resilience and provides a quantitative method that evaluates these holistically. Through the combination of relevance and weighting of the indicators in summation, overall system resilience may be calculated as described in equation 5.5 and in figure 5.2 [34].

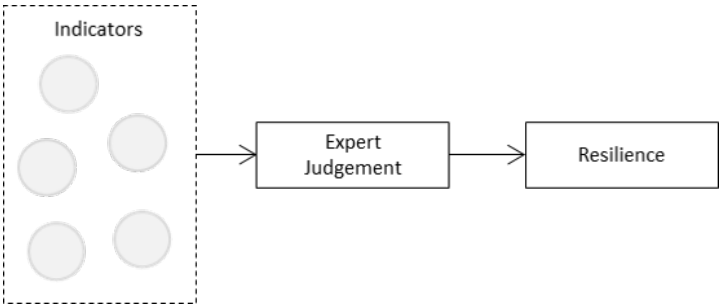


Figure 5.2: Direct expert-based approach schematic (adapted from Cere et al. "Critical review of existing built environment resilience frameworks" directions for future research [34]")

$$R = \sum_{(i=1)}^{n} (\delta(j).\frac{\varphi(j)}{\sum_{j=1}^{n} \varphi(j)}.I(j)) \tag{5.5}$$

1. R indicates total system resilience.
2. $\delta(i)$ "is a binary variable".
3. $I(i)$ represents the resilience indicator varying according to the system feature. "The expression between the described variables represents $\omega(j)$ which summarises the weights assigned to the specific (j)-th resilience indicator based on the relevance co-efficient $\varphi(j)$ which values are included between 0 and 1."

It is noted that using this method, a quick estimation of system resilience can be obtained. This is useful as a verification method for modelling resilience of systems. The resilience system design in this report adopts these principles.

5.6.3 Performance-based Direct Approach

The performance-based direct approach of resilience measurement are based on the probability of a system exceeding a specific damage threshold. This method has been successfully applied in built environment use cases as it offers a "continuous model" instead of a "discrete and fragmented analysis such as the one achieved through expert based indirect methodologies [34]."

Performance based approaches in the built environment rely on detailed analysis of structures and the application of a performance ratio to measure resilience. For example the proposed work of "Biodini and colleagues (2011 - 2020) which achieves earthquake-relevant and explicit formulation of system performance in equation 5.6. In this model, the performance measure of the structure is expressed as ratios of the outputs of structural analysis over time. A point in time measurement expressed as a ratio against an initial measurement for a given performance variable. These measurements vary from structure to structure [34]."

Biodini's work has been summarised by Cere et al in the following mathematical model [34]:

$$Q(t) = \frac{a(g)(t)}{a(g,0)} \tag{5.6}$$

1. $Q(t)$ represents the performance measure of a structure based on its structural analysis.
2. $a(g)(t)$ represents the acceleration-bearing activities of the structure considered at time (t).
3. $a(g,0)$ represents the initial value of acceleration-bearing activities of the structure.

Using performance-based approaches, threshold's may be defined and plotted into fragility curves to understand structural elasticity. This theory is based on tensile test methodology [34].

5.6.4 Anti-fragility Adaptive Systems

Kennon, Corne, Schutte and Lutters (2015) define anti-fragility as "positive sensitivity to volatility caused by external stressors that intervene with the intended functionality of these systems [42]". By assessing positive system sensitivity, consideration is given to both the emergence in the positive and negative response to risk. In so doing, systems design is not only focused on the reduction of risk, but also for systems to prosper as a result of risks arising in dynamic environments. This method, uses a combination of quantitative and qualitative methods in its approach [42].

Kennon et al state that "with fragility being a non-desired quality, it makes sense to define the opposite. Often this opposite is thought to be something that is resilient or robust. However, by logical deduction, the opposite of that which is negatively sensitive to volatility; anti-fragile systems thus thrive during or on volatility [42]."

The example cited is as follows: "Apple positioned itself to prosper from the upside of volatility through the launch of the iPhone software development kit in 2007. A free download was available to independent developers, which included documentation, bug testing software, graphical layout, design software and programming applications. Applications were designed and tested by the developers and submitted to the App Store for approval to sell. The income generated from the sale of the application is split between Apple and the developer, increasing both the turnover through the application sales and the value that Apple consumers get from their devices [42]."

Kennon et al provide a basis on which to apply anti-fragility methods using systems engineering as a basis. They also adapted the method undertaken from the work of Johnson and Gheorghe (2013) and Jackson and Ferris (2013). The method uses a stakeholder survey information gathering based on a set of derived anti-fragility criteria and the Delphi method in its final analysis [42, 47, 41].

The principles in the method are summarised as follows [42, 47, 41]:

1. An "evaluation system is built on the attributes that are of interest to the system stakeholders: strategies, policies, governance, structure, components, sub-systems and processes,
2. Questions are contextualised for a system in terms of how it would respond to the stressor based on a set of system criteria,
3. Johnson and Gheorghe propose that systems are then measured "according to the system criteria" through quantitative responses to their questions on an "interval scale" and
4. Using the Delphi method, stakeholder responses gathered according to the criteria set out are converged allowing for "order, distance and the application of statistics and applied inferences to be derived".

A summary of systems criteria adopted is included in table 5.2.

Table 5.2: "Analytical criteria of a system of systems [42]", adapted from Johnson and Gheorghe (2013) and Jackson and Ferris (2013) [41, 47]

Key	**Criteria**	**Definition**
F1	Emergence	Emergent outputs, there is little/no traceability between micro- and macro- level results of a system, has greater black swan event exposure compared to resultant due to an increase in the amount of unintended system states.
F2	Efficiency and risk	Efficiencies are often gained at the expense of increased potential for harm due to stress. Less redundant systems designs are more efficient, but more fragile.
F3	Requisite variety	Regulators in a system of systems attempt to control the outcome and behaviours in the system. Black swan events increase as a result of the number of regulators being insufficient relative to the number of agents (unpredictable behaviour).
F4	Stress starvation	Protecting a system from stress or attempting to reduce uncertainty can cause weakness, fragility and expose them to hazardous black swan events.
F5	Redundancy	Duplication of components to meet the same objective create excess capacity in a system and are effective tools for extreme stressor deficiencies. Redundancy tends to stabilise systems and improve robustness.
F6	Absorption	Absorption in systems can be used to improve robustness. Design margins that increase the magnitude and duration it can take during potential stresses to ensure it continues functioning as it should increases the absorption ability of the system.
AF1	Induces small stressors	Some systems are found to improve with greater exposure to stress. Controlled stress to a system can increase its robustness and potentially lead to anti-fragility where the system 'learns' from these controlled responses.
AF2	Non-monotonicity	Learning from negative consequences induced by stressors can lead to new information. New information can result in improved practices and approaches. Stresses, when learned from, can thus cause a system to improve.

Kennon et al note that the disadvantage of the Johnson and Georghe approach is that should the criteria change, the scale of measurement may not be valid and therefore propose that future research should focus on standardisation of measurement. They also note that the measurement "in itself" is not adaptive [42]."

There is currently limited research on the structure of an anti-fragility assessment and propose that focus be placed on a systems "ability to gather information on the consequence of a stressor, the processes in place to assess the information gathered, the processes in place to act and the process of action validation [42]."

Results of the anti-fragility method are averaged per criterion and a corresponding standard deviation is calculated statistically. "The average is not intended to determine the system response, but to assess whether the organisation's (anti) fragility improved in one of two ways" [42]:

1. "Did consensus improve on the impact of the criterion (indicated by a reduced standard deviation)?
2. Did changes in the average assessed criteria improve the organisation's (anti)fragility?"

Kennon et al. note in conclusion that this method provides an initial proposal for future research in which the method should be enhanced through an increased understanding of system criteria which "will allow for more accurate measurements/-comparisons as well as increased understanding of the stakeholders' in the system [42]."

5.7 Organisational Resilience

Organisations that have the ability to deal effectively with disruption and crisis have a few defining characteristics. This most important of which is a positive culture. Resilient organisations are those where the purpose of the business is known and understood and where employees are highly engaged and customer focused. The Vanguard Method developed by Vanguard Consulting in England (Sneddon 2003) is an approach that can be used to define these types of organisations and provides a basis on which resilient organisations can be organised. [9, 43].

The Vanguard method drives the customer requirement of organisations to be "highly responsive to customers" and focused on "minimising non-value adding activities". The method emphasises the role of self managing teams who fully own the service process, thereby ensuring that individuals and teams are fully committed to delivery. Using this theory "organisations become organically structured with employees having autonomy to "think, analyse, judge and make decisions". In this type of organisational structure, "flexibility and quick response" fulfils the need of the organisation to "absorb variation in environmental demand" [43].

The operationalisation of the Vanguard method "follows three main action steps of check-plan-do [43]". The method starts with the check stage "in order to show

business managers the failings of their current system and to provide them with solid evidence for the need to change the way they think and manage things [43]". The cycle of planning and doing is then implemented with the view to continuously improve the system. The Vanguard method supplements this thinking with a customer demand dimension through "the identification of new demands coming in to the service department" and "designing new processes" to deal with these [3, 43].

The outcomes of the Vanguard method are measured as a function of "the employee's emotional attachment to the organisation, the strength of identification with the goals of the organisation and strength of commitment to its success and continuous improvement, The employee remains a part of the organisation because s/he wants to do so [43]."

In this method, measurement of organisational resilience is based on the concept of "affected commitment" which can be measured qualitatively through an Organisational Commitment Questionnaire (OCQ) which is correlated to improved customer demand performance. The outcomes of the method tested by Jaaron and Backhouse in two organisational case studies indicated that customer demand performance indicators improved with a higher degree of "affected commitment" [43]. Powley (2009) also provides insight into the role that empathy has to play in high degrees of employee engagement [48]. However it also requires good leadership practice to achieve this according to Kennon et al (2015) and therefore resilience is built across all levels of engagement and commitment across an organisation. [42, 43, 48].

Jaaron and Backhouse propose that future work be done to "help organisations to apply the Vanguard method to build internal capabilities and processes to enhance the learning process of understanding the business environment to become better performers [43]."

It can also be proposed that in order for employees to effectively understand the business environment, data and information is required in a format that supports the employee in an enhanced understanding of their business environment and therefore become better performers [32, 42].

The Vanguard method provides a human factor dimension to analytical model outcomes within an organically structured organisation. It also becomes more important to ensure consistency of understanding in a highly adaptive organisation. Figure 5.3 includes the additional dimension of data as a proposed extension to the two dimensional determinant conceptual model into three dimensions in the context of this report [43].

Sutcliff and Vogus' work compliments the principles of the Vanguard Method by providing insight into "how organisations continually achieve desirable outcomes amid adversity, strain, and significant barriers to adaptation and development [32]." They note that "resilience emerges from relatively ordinary adaptive processes that promote competence, restore efficacy, and encourage growth, as well as the structures and practices that bring about these processes [32]."

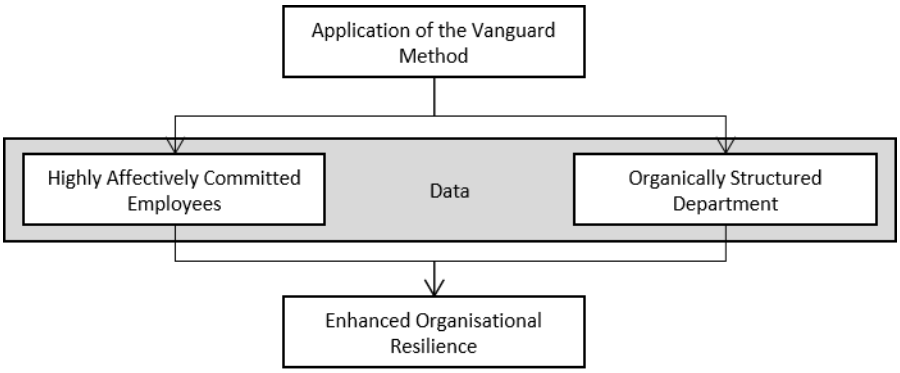


Figure 5.3: Adapted from "Two dimensional determinant for organisational resilience: a conceptual model". The addition of a data dimension (three dimensional conceptual model) [42, 32, 43]

"In organisational theory, resilience (sometimes resiliency) often has been used to refer to a characteristic or capacity of individuals or organisations, or more specifically the ability to absorb strain and preserve (or improve) functioning despite the presence of adversity (both internal adversity - such as rapid change, lousy leadership, performance and production pressures - and external adversity such as increasing competition and demands from stakeholders [32]."

Sutcliff and Vogus state that in the context of organisational learning that "overall there has been little systematic empirical work and it has received little independent attention [32]. They state that the domain of resilience is worthy of scholarly attention as it can provide insight into etiology and course of positive adjustment or adaptability under challenging conditions [32]. It is on this basis that their work on "organising for resilience" has been positioned in this report. Several other works including that of Peter Senge (2006) highlight the importance of the learning organisation for improved business resilience [49]. The adaptive cycles of ecological systems is a naturally occurring process and harnessing the power of adaptability in human activity systems provides a foundation for positive system adjustment in times of adversity. [30, 32, 42, 49].

The noteworthy theme is that organisational resilience work is based upon the resilience of individuals within organisations as well as providing individuals access to "human, social, and material capital [32]". When individuals have experiences that add to their growth, competence/expertise, and efficacy", in conjunction with having the appropriate resources, it is possible for individuals to exercise "judgement, discretion and imagination [32]" [43, 49].

In the rapidly changing environment, organisational resilience is essential and it is possible to augment the effectiveness of the individual by providing a strong basis on which people can make decisions and apply their expertise. Data systems provide an additional set of resources to support individuals in exercising judgement in disruptive situations. Therefore the human factor in data systems is an especially important consideration in its design [32, 42].

Edward Powley focuses on the resilience of organisations during crisis activation. Powley's work (2009) provides investigation into social systems in organisations and

the value of individuals sharing their experience and knowledge thereby ensuring that this is captured into organisational memory. Powley also places an emphasis on building the ability of organisations to pin point and effectively use areas of knowledge and experience. This work also positions the need for empathy as an important organisational value to drive "compassionate witnessing" and to learn from every crisis not only in the hard systems, but also in the human factor [48].

Most organisational resilience work proposes that organisations use crisis as a positive change agent to strengthen either the product or service offering or to strengthen the people and processes that underlie their delivery. Kennon, Schutte and Lutters also propose that to build resilient organisations, strong leadership is critical and state that "strategic leaders in an organisation have an important role preparing their organisations for risk [42]" . They cite the 2008 global financial crisis as a failure in the leadership structures of the institutions at the time. Along with the social and human factor, Kennon, Schutte and Lutters make the point that good governance structures are essential to building positive strength into systems [42]. Their work also asks the questions that define good data governance in times of crisis which includes [42]:

1. "What is the systems ability to gather information on a consequence of a stressor?
2. Are processes in place to assess the information gathered?
3. Are processes in place to act and are they validated?"

The consideration of organisational context not only looks to the environment in which it operates but also considers the organisation's interested parties both internally and externally, the processes that are in place and the knowledge and competence that exists in the organisational narrative. Good governance and leadership are also important to set and review strategy and to drive the culture and values of the organisation. This clarity, provides high levels of engagement and increases an organisation's response to ensuring that in time of activation, recovery is not only possible, but results in learning and positive outcomes.

5.8 Resilience Research Conclusion

There is a significant body of work that has been done in the areas of risk assessment, business continuity management and resilience. The field of study has many dimensions and spans multiple disciplines. To fully understand and design resilient systems, a holistic systems based approach is needed to any proposed solution of the future.

It is also consistently mentioned that the need for standardisation in measurement, taxonomy and resilience criteria would be useful areas for future work. In addition to this, those system components studied, cannot be considered in isolation. Systems thinking provides a meaningful foundation to consider all aspects of risk and data systems in the context of the organisation and its interested parties.

The theme of the need for good quality data that is useful within any systems design is also an ongoing conclusion in most work where either qualitative and/or quantitative methods of assessment or trend analysis is used.

The concept of the learning organisation also requires data to provide insight into areas for improvement and learning. Checkland's Soft Systems Methodology provides a good framework on which to develop aspects of resilience systems as well as to design and develop future Business Continuity Management Systems [9]. This has been applied very successfully in the Vanguard Method as well as in Systems Engineering approaches. Previous works have spanned Checkland's five system classes which provide useful reference points in this report [9, 43].

Data Systems have a role to play in all disciplines and aspects of resilience and business Continuity Management. The scope of the application of data to the system needs to be placed in the context of a system component and its corresponding metrics and this is where recent developments in taxonomies have useful results.

This report, proposes that by the addition of a single system component that provides an enabler for data context to be managed, this can provide a degree of standardisation so that data becomes useful to improving a systems ability to adapt to disruption and change.

6

Resilience System

The Resilience System of interest in this report is described holistically to support organisations and the organisational context in which they operate. This system is a soft system by nature and therefore, Checkland's Soft Systems Methodology has been adopted. Previous work reviewed also provides direction and insight of using a systems approach when considering resilience systems design [9].

6.1 Soft Systems Methodology

"Hard problems are problems characterised by the fact that they can be well defined. You assume that there is a definite solution and you can define a number of specific goals that must be accomplished. In essence, with a hard problem you can define what success will look like prior to embarking on implementing the solution. The "WHAT" and the "HOW" of a hard problem can be determined early on in the methodology" [50].

Soft problems, on the other hand, are difficult to define. They will have a large social and political component. When we think of soft problems, we don't think of problems but of problem situations. We know that things are not working the way we want them to and we want to find out why and see if there is anything we can do about it. It is the classic situation of it not being a "problem" but an "opportunity" [50].

Resilience systems have both hard and soft components and also rely on a human activity system (the organisation, its people and processes) where formulated responses to disruptions and crisis will be required for effective outcomes.

In the literature, there is a significant amount of resilience work that has been dedicated to Human Activity Systems as an essential part of all resilience problems and systems. Systems thinking approaches are adopted to describe the problem with the necessary proposed system designs, frameworks and potential outcomes.

In this report, the addition of data as a hard system component is shown to be a

necessary and important part of building effective resilience and provides a basis on which organisations can formulate an effective response to potential risk and to a disruption. This does not mean that the addition of data systems can replace the human activity system in the context of resilience, but is rather an additional component to support the human decision making process.

"Resilience develops as enabling conditions (i.e. Competence, Growth and Efficacy) increase the likelihood of positive adjustment". Effective data integrated into organisational systems is a resilience activator not only in time of disruption or crisis, but as part of the learning organisation through providing a means of assessment and enhanced monitoring [32].

6.2 Checkland Stage 1: Situational Problem for Consideration

The current situation suggests, that data in the context of resilience measurement relies on both qualitative and quantitative approaches through direct expert based consultation and surveys. There are three considerations that are taken into account in organisational systems as follows:

1. Scanning of environmental factors and applying these to the context of the organisation.
2. Information seeking where data can either be sourced internally or externally. This data is modelled through a process of structuring and curation which then allows for decision making in the risk and business impact assessment.
3. Decision making is influenced by the decision maker (human factor).

Pro-active approaches are difficult to manage in these instances and decisions are usually retrospective. Results are also dependent on a continuous refresh of direct expert consultation and ongoing industry survey.

The variables in the problem to be considered include resilience indicators, data and the maintenance of the association of data to resilience. The situational factors that form part of the problem statement are as follows:

1. Resilience indicators are dynamic and can be derived,
2. Resilience indicators are related,
3. Derived resilience indicators are a reasonable indication of environmental context within acceptable parameters,
4. Derived resilience indicators can be associated to banking data concepts in an accepted industry data model,

5. Derived resilience indicators can be associated to a reasonable risk taxonomy (defined or sourced) and

6. Based on mapping to data sources, data can be dynamically associated to risk indicators to enable predictive risk insight.

The above situational factors are the basis on which dynamic context is defined in this report.

6.3 Checkland Stage 2: Situational Analysis

A Situational Analysis, is represented in rich picture format in figure 6.1. The common experience of the data requestor is that the process of data curation does not necessarily answer the question of the data within the emerging risk landscape context. This means that further analysis work is required to place results of data curation into the context of the changing risk landscape. The Business Continuity Horizon Scan Report also noted in 2020 that Risk Trend Analysis is a current challenge to business continuity management and risk professionals who rely on both internal and external data sources on which to base their decisions. Leveraging off systems of insight is currently only used by a few organisations in an integrated manner with Business Continuity Management and Risk Systems [1].

Dynamic contextualisation based on the insights of the "context of the organisation" (ISO22301 Clause 4) is required to meet the needs of resilience and business continuity practitioners in a rapidly changing environment. Time to respond to emerging environmental context is becoming shorter. Rich insight into how to positively adjust in near real time is an important systems problem consideration in the future [3].

Degrees of separation in the data development life cycle between the data requestor and data engineering teams is a situational challenge. Development teams rely on the perspective and expertise of the data requestor that is usually gathered through interview and documentation processes. Gathering of multiple perspectives requires further analysis. The data requestor relies on the expertise of the data engineering team to curate data into the formats that are required and data engineering teams require expertise from the requestor to effectively present the data in context. Bridging the gaps between these two unique skill sets is needed in the design of the system and to improve efficiency through learning and continuous improvement.

Contextualisation of emerging risks requires inputs from all interested parties in the data development life cycle which is a human activity system. Semantic data discovery processes are able to match data to data models, however context discovery is a useful process which presents an opportunity for better efficiency in the system operation.

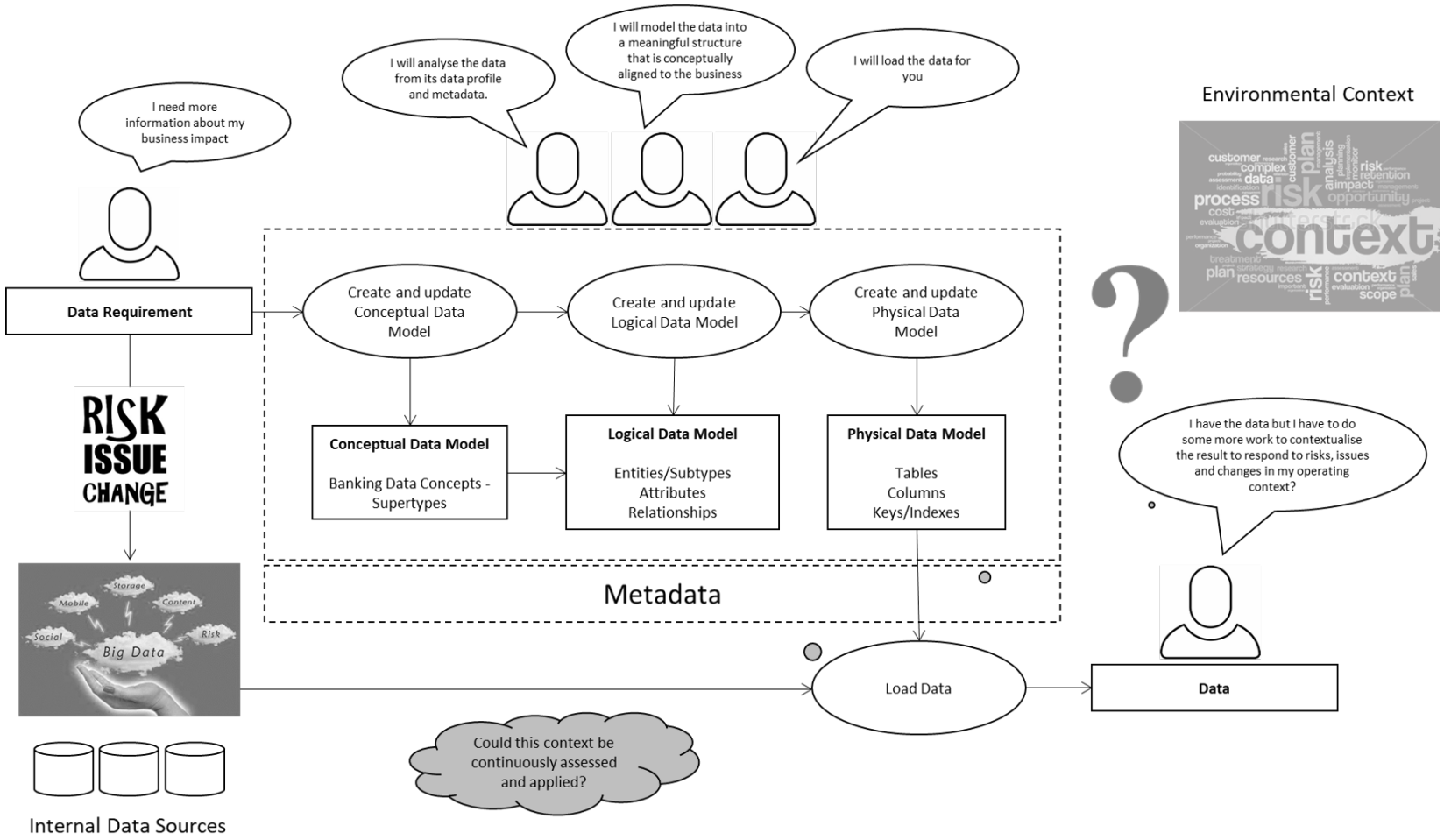


Figure 6.1: Situation Consideration - Rich Picture

6.4 Checkland Stage 3: Root Definitions of Purposeful Activity Systems

"The Root Definition is a statement of purpose that captures the essence of the particular situation of the relevant system [51]." The purpose of this section is to capture a clear definition of the system that has been tested in this report using a CATWOE analysis [9, 51].

The root definition includes the following perspectives which are applied here as follows [51]:

1. **Customer** - "The individual(s) who receive the output from the transformation (in recent times it has been recognised that the output of the transformation may be "negative" for some customers and "positive" for others,
2. **Actors** - Those individuals who would do the activities of the transformation if the system were made real.
3. **Transformation** - The purposeful activity expressed as a transformation of input to output.
4. **World View** - It is the belief that makes sense of the root definition.
5. **Owner** - The wider system decision maker who is concerned with the performance of the system,
6. **Environment** - The key constraints outside the system boundary that are significant to the system."

The proposed system in the scope of this report includes the purposeful activities in terms of its root definition shown in figure 6.2 as a determinant of success.

The root definition of the system of interest in this report is stated as: A system owned by the Head of Operational Risk who together with the Chief Information and Data Officer use teams' knowledge skills and expertise to contextualise data and information to continually improve business resilience using data as an asset (in the system of insight). This is done with the understanding that rapid change in the environment has the potential to have significant business impact.

In the ISO22301 standard, Customers, Actors and Owners are referred to as "interested parties [3]".

Root Definition	CATWOE
A system owned by the Head of Operational Risk who together with the Chief Information and Data Officer use teams' knowledge, skills and experience to contextualise data and information to continuously improve business resilience using data as an asset. This is done with the understanding that rapid change in the environment has the potential to have significant business impact.	**Customer** – Business Units, Risk Management Professionals, Regulators, Executive Committees
	Actors – Chief Information, and Data Officers, Heads of Risk, Technical and IT Enablement Teams, Risk Management Teams, Business Continuity and Resilience Teams, Crisis Management Teams, Regulators.
	Transformation – To use knowledge, skills and experience to contextualise data and information to continuously improve business resilience using data as an asset.
	World View – While the organisation seeks to be compliant in BCBS239 principles, organisations, there is a need to add context to its data and information to effectively manage emerging change in the environment.
	Owner – Head of Operational Risk
	Environment – Transformational, and rapidly changing, where emerging factors potentially have significant business impact.

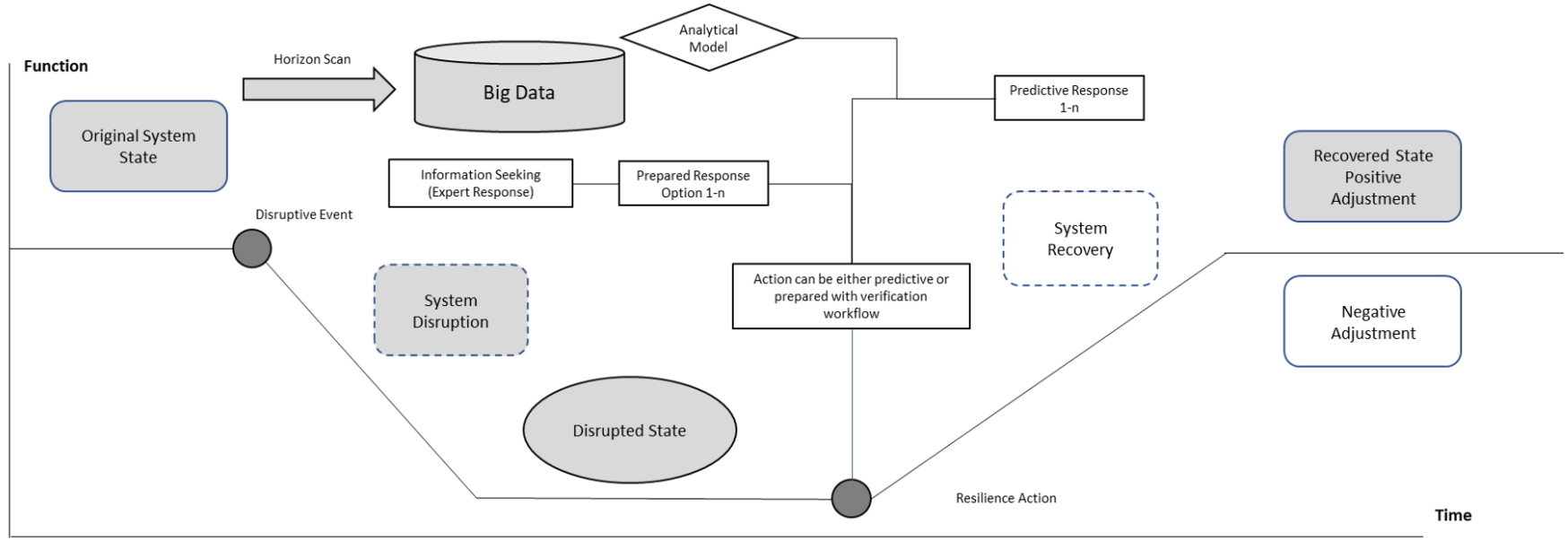


Figure 6.2: Root Definition - CATWOE adapted from "Generic and quantitative approaches for system resilience as a function of time" (Henry Jose Emmanuel and Ramirez Marquez, 2011) [18, 9, 46]

6.5 Checkland Stage 4: Conceptual Systems Model

Conceptual systems model consists of the following components which are defined as follows:

1. **Data Sources** - Sources of data that are both internal and external to the organisation. External data is a representation of the operating environment of the bank (for example risk horizon data). Internal data arises from the bank's interactions with its external operating environment (for example loan book data). Source data can be defined as the point at which data is created. "In computer programming, source data or data source is the primary location from where data comes. The data source can be a database, a data-set, a spreadsheet or even hard-coded data. When data is displayed in a web page or application, in a column-row format or other formats, the data is retrieved from its data source and presented in the format defined in the code. "Originating data is referred to as System of Record Data" [52].

2. **Big Data** - "Big data is high-volume, high-velocity and/or high-variety information assets that demand cost-effective, innovative forms of information processing to enable enhanced insight, decision making, and process automation [53]." This Data is external in this report and although not a large volume of data, it has variability and through taxonomy associations surfaces a number of other related data sources. This is exponentially variable and potentially large. It is also noted that the Data Sourced from industry survey used in this report was already aggregated in key results. A degree of curation and interpretation already applied.

3. **Contextual Data** - "Contextual data is information that provides context to a risk, event, person, or item. This data is important for providing a broader understanding of specific pieces of information and placing them in a larger picture. One major point of concern with big data is that many times, information without a context lacks real value. Adding layers of context helps unlock the insights data points offer, and can lead to more informed and accurate decisions on an organisational level [54]". Context is provided through the standardisation of definitions of risk data reported along with an associated relationship to taxonomy. This is the system component that forms part of the investigation of this report.

4. **Industry Data Model** - "An industry data model is a set of business and technical data models that are pre-designed to meet the needs of a particular industry. In this report, financial services has been selected as an illustrative use case. It acts as a blueprint that provides common elements derived from best practices, government regulations and the complex data and analytic needs of an industry-specific organisation [55]"

5. **Data Lake** - "Data lakes are next-generation hybrid data management solutions that can meet big data challenges and drive new levels of real-time analytics. Their highly scale-able environment can support extremely large

data volumes and accept data in its native format from a wide variety of data sources. Data lakes can help break down silos, enabling organisations to gain 360-degree views of information and conduct cross-department analytics. The data lake serves as a repository of internal and external data that has the ability to store data in multiple formats". In this report a data lake is simulated as a set of staged data tables used to ingest data sources [56].

6. **Dimensional Data Warehouse (Data Marts)** - Curated data in dimensional structures representative of the business solution. "Dimensional data modelling techniques" (Kimball, 2020) are used to design Dimensional Data Warehouses [57].

7. **Business Continuity Management System** - "A BCMS is a comprehensive approach to organisational resilience and helps organisations cope with incidents that affect their business-critical processes and activities [3, 58]." This report uses the ISO22301 Standard on which to base the system.

8. **Inferential Analytical Model** - "Inferential statistics is a statistical method that deduces from a small but representative sample the characteristics of a bigger population. In other words, it allows the researcher to make assumptions about a wider group, using a smaller portion of that group as a guideline [59]".

9. **Text Mining** - "Text mining is the process of analysing collections of textual materials in order to capture key concepts and themes and uncover hidden relationships and trends without requiring that you know the precise words or terms that authors have used to express those concepts. Although they are quite different, text mining is sometimes confused with information retrieval. While the accurate retrieval and storage of information is an enormous challenge, the extraction and management of quality content, terminology, and relationships contained within the information are crucial and critical processes [60]." Text mining is done manually in this report, using ethnographic analysis however the basis on which report text mining could be applied is contained in the method of standardisation of risk descriptions.

Processes that form part of the conceptual model are as follows:

1. **Source Metadata** - "Metadata sources have been mapped to the correct attributes and entities of the metadata repository [61]". Metadata sources are the structures and definitions of all the data sources (system of record).

2. **Data Mapping** - Mapping based on the structure of the source metadata has been done to associate source data structures to the industry data model.

3. **Ethnographic Study** - Ethnographic study of the categories of risk in the horizon. Standardisation indexes have been applied to the risk data to indicate the standardisation result.

4. **Source data load** - into appropriately structured repositories. This is defined as the System of Insight.

5. **Acceptable operating levels** - of a defined business continuity system have been defined in simulation.

6. **Analytical modelling simulation** - of resilience sensitivity against a single Key Risk Metric i.e. Expected Loss is included in the scope of the analysis based on the data contained in the loan book.

The conceptual model of the system is shown in figure 6.3

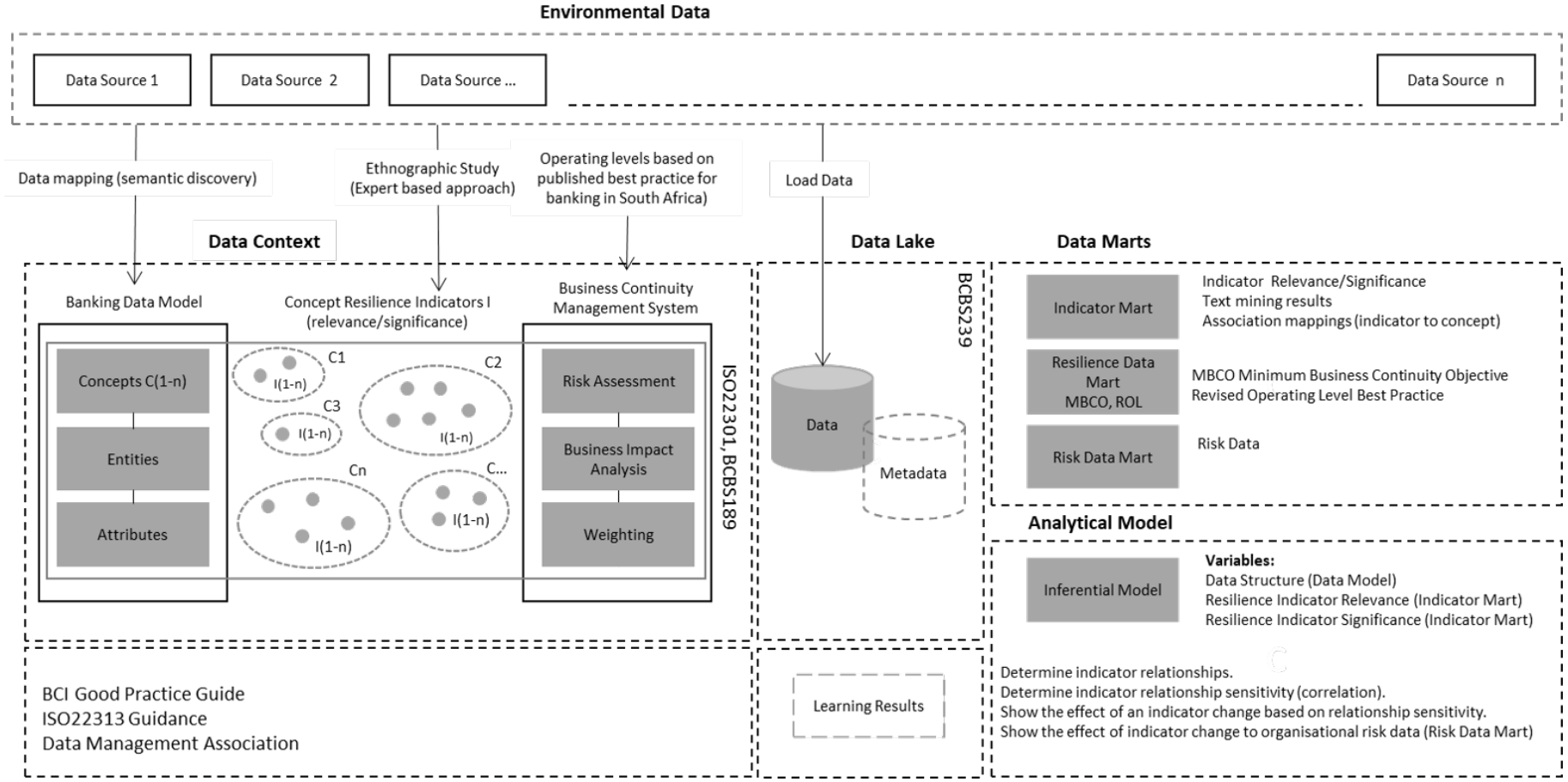


Figure 6.3: System Conceptual Model, [3, 17, 18, 9]

,

6.6 Checkland Stage 5: Comparison of Models

According to Burge, "the comparison of models involves testing of the model against the "real world" and comparing the reality we experience with that captured in the models. The purpose of the comparison is to initiate discussion from which changes to improve the situation can be identified. The approach uses the comparison to provide a means of perceiving a different view of reality by testing assumptions that may exist but are ill founded. It is the differences between what happened in reality and the logical model that raises the questions that will ultimately lead to change [51]."

Comparison of models is summarised in figure 6.4. The difference in existing and current mental models is the opportunity to integrate and automate analytical insight into Business Continuity Management Systems.

The validation of real world models against proposed changes is done according to the following:

1. Derivation of standardised risks based on assessment,
2. Simulation of the model against a South African financial services case study single risk metric with a narrative validation,
3. Comparison of real world case study actions against possible new actions based on the model and
4. Comparison with a second derived risk in the model.

Validation of the model is based on both quantitative and qualitative methods which will be noted through the process according to the standards set out for the applicable conceptual model components.

It is expected that text mining should reasonably compare to manual ethnographic processes. The two risk data sources are expected to closely correlate in themes and identified risk indicators based on the input of specific key words.

The control data source is expected to differ significantly in its results to the identified risk data sources.

It is expected that case study simulations will either yield new suggested actions with measured outcomes or no new suggested actions. In both instances, the final outcomes of the case study should provide insight into the work-ability of the model against the real world with additional insight.

Conceptual Model Activities	Real World	What we could do (proposal)
Identify resilience indicators (Horizon Scanning).	Resilience indicators in the real world are derived qualitatively through direct expert approaches.	1. Identify resilience indicators automatically through text mining of expert based documentation sources.
Identify data sources for resilience measurement (Information Seeking).	Resilience data sources are identified through industry knowledge and other unstructured and unstructured forms of data that may contain correlation.	1. Note: Identification of sources remains subjective. 2. Apply a system of semantic data discovery. 3. Stream data into Big Data Systems.
Map data sources into concepts for banking using data modelling techniques.	Once data sources are identified, these are structured and mapped to an industry data model for banking. This is done manually by data professionals.	1. Apply semantic data discovery to data mapping. 2. Use Artificial Intelligence and Machine Learning to automate suggested mapping. (not in the scope of this proposal)
Associate resilience indicators to data concepts.	This is not a usual step in data analysis where context is associated with a data concept. Associations are generally applied in the risk assessment and business impact assessment following information seeking processes.	1. Associate resilience indicators to data model concepts and entities. 2. Extend the data model through association of resilience indicators. 3. Monitor indicator changes against the data model. 4. Monitor data changes against indicator associations.
Identify insights based on changes in variables: Data Structure Change Resilience indicator significance change Resilience indicator relevance change	This is done through monitoring of operations and regular exercising. Data changes are not associated in context quantitatively and operational incidents and outages are a current indicator of data change impact.	1. Perform hypothesis testing and inferential modelling applied to derive resilience insights for decision making.
Apply insights to the Business Continuity Management System	This is applied through the continuous improvement process of the Business Continuity Management System	1. Interpretation of insights applied as learnings into the Business Continuity Management System. 2. Measure resilience outcomes.
Apply standards	Apply Good Practice BCM Standards Apply Basel Standards – Data Management and Business Continuity Management	1. Apply and automate data management standards. 2. Apply BCMS standards.

Figure 6.4: Comparison of Models

6.7 Checkland Stage 6: Feasibility

This report project adopts "lean start-up principles" to deliver a minimal viable product (MVP). The proposed system change is shown in the "How Now Brown Cow" model in figure 6.5 [62].

"A MVP enables us to use a minimum amount of effort to generate the maximum amount of learning when experimenting with customers [62]." In the context of this report, stakeholders (interested parties) are defined in the CATWOE (figure 6.2). "The goal of the MVP is to execute an experiment that tests the assumptions of our hypothesis as cheaply, quickly and effectively as possible, in order to learn if our solution addresses the customer (stakeholder) problem as we have identified [62]."

A MVP mindset and experimentation loop will form the basis of execution steps as follows [62]:

1. Identification of one metric to test the validity of the hypothesis (research questions). "when designing MVPs to experiment, it is important to identify one key metric that will tell us if the assumptions (statements) in our hypothesis are valid."

2. Verification of direct expert based approaches qualitatively (manual ethnographic, thematic analysis).

3. Create the experiment through system design and engineering, including testing.

4. Validate the outcomes qualitatively, through definition of testing scenarios.

5. Evaluate "outcomes to pivot, preserve or stop".

Following the MVP cycle, in this report uses direct expert based approaches based on survey and expert judgement assessed as follows:

1. Quantitative and qualitative assessment of the BCI Horizon Scan Report and the IRMA Report,
2. Input of quantitative results into MVP Business Continuity Management System (BCMS),
3. Quantitative assessment of direct expert based approaches through the standardisation of risk descriptions and logical groupings against the Open Risk Taxonomy (containing both financial services and other industry risk classifications and definitions) and
4. Evaluation of the MVP "outcomes to pivot, preserve or stop [62]." It is noted that several iterations of risk reporting analysis resulted in the final MVP table in the database.

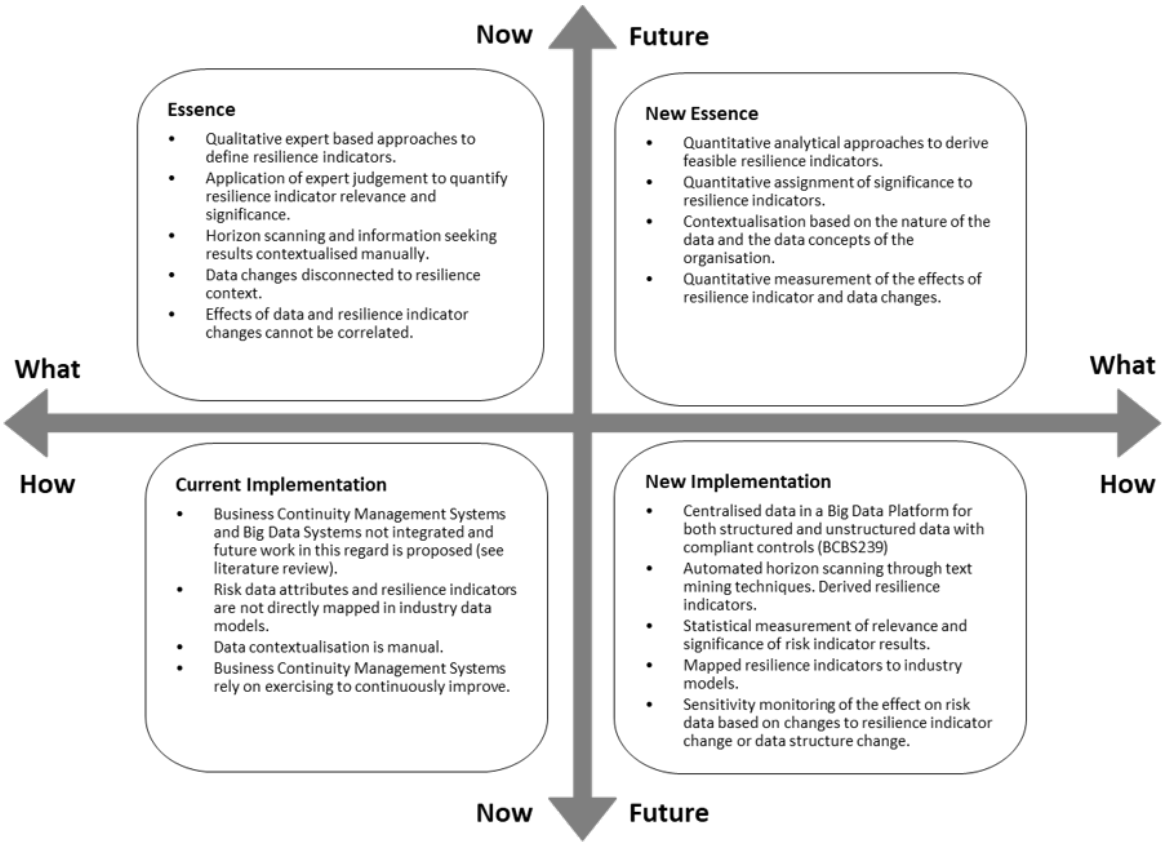


Figure 6.5: How Now Brown Cow, adapted from YouTubeZA; "Mastering the Requirements Process - The Brown Cow Model"; Robertson S. and Robertson J 30 July 2015

6.8 Checkland Stage 7: Systems Engineering Master Plan

The development of this section adopts the V-Model in figure 6.6 and a standardised approach based on the "ISO/IEC/IEEE 24748-1:2018 Systems and software engineering -Guidelines for life cycle management [63]". The stages and clauses have been included in table 10.1 in the Appendix Section 10.1 .

This research report applies the ISO/IEC/IEEE standard as a reference to best practice life cycle management and as such a checklist has been included in the proposed stages (table 10.1).

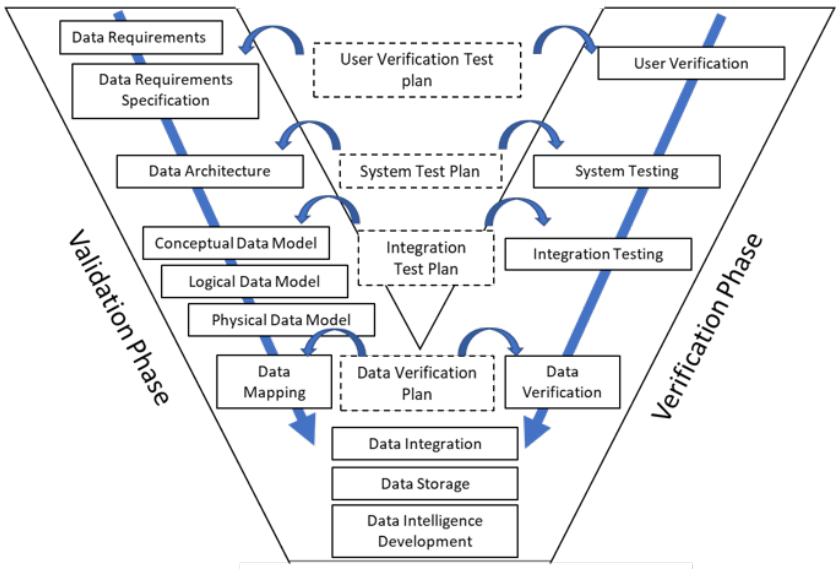


Figure 6.6: V-Model

7

Risk and Banking System Data

7.1 Risk Data

The approach taken to data collection was to identify and source data that sets the risk context that can be applied to the business continuity management system (BCMS). Risk assessment is an integral component of the BCMS. The sources of data chosen were identified to have at least five years of data to show a dynamically evolving risk environment and include both a local and global perspective. There are several sources of risk data available and for the purposes of this report, risk sources were chosen based on the following criteria:

1. Data is based on industry survey and assessment,
2. Has financial services industry representation,
3. Is subject to peer review and publishing,
4. Has consistent publishing periodicity,
5. Contains consistent in risk measurement i.e. not more than two risk measurement methods. Risk score and ranking as an advantage,
6. Have expert commentary where appropriate,
7. Risk descriptions are well described, thereby enabling standardisation and mapping to a risk taxonomy in metadata and
8. Sources are accessible in either the public domain or by affiliation and/or subscription to the publication.

The sources of risk data chosen for this report that fulfilled these criteria included the Business Continuity Institute (BCI) Horizon Scan Report Data and the Institute of Risk Management South Africa Annual Report. These sources of data include aggregated results of surveys and results of consultation with industry experts who

provided expert judgement analysis for the year. In both cases, the reports are released annually in March, based on a survey of the previous year. In addition to a retrospective view, these reports include a risk landscape outlook over a twelve month period and in some cases, an eighteen month and three year outlook. There has also been one instance of a ten year outlook provided in the 2016 IRMSA Report. The ten year outlook data has been included in this report's data set.

The BCI and IRMSA Annual Risk Reports are released to affiliated members and the public. Data set results and expert judgements contained within the reports are subjected to executive and peer review by members of these institutions and are widely referenced within the field of Business Resilience, Business Continuity Management and Risk Management.

The following reports were analysed in the following steps:

Step 1: Capture of aggregated risk context data quantitatively provided in the reports.

Step 2: Standardisation of capture into a single data source, appropriately structured into database table format to facilitate data analysis and integration into a Risk and Business Impact assessment data visualisation tool.

Step 3: Standardisation of arising risks through a grouping of common themes using qualitative ethnographic analysis and interpretation of risk description. This considered both the identification of common key words and interpretation of risk description and an understanding of the risk commentary provided in the report. Many were consistently reported, however there were some nuances in terms of ensuring that frequency of key word was not the only measure by which to group risks identified.

Once standardised, common risks are assigned a risk identifier, ensuring no alteration in the source data reported, in line with data warehousing principles where data should not be changed in data acquisition.

Step 4: Risks are grouped into categories based on the Open Risk Manual Risk Taxonomy.

The Principles of the Open Risk Taxonomy are as follows and must be noted [33]:

1. "It is based on voluntary contributions by individuals willing to spend their own time to provide a quality entry that will be of use to every risk manager, anywhere, anytime released under a Creative Commons license,
2. It requires approved Author registration before one can add-to or edit the Manual. This restriction serves multiple purposes, ranging from website security to enabling a more consistent outcome,
3. The objective and style of the manual is that of a technical manual, not an encyclopedia or a textbook,

4. Articles are structured for easy problem solving, not academic learning. The focus on tools, not theory and

5. There is no particular effort for bibliographic completeness."

What the Open Risk Manual has been able to accomplish through contribution and review is a hierarchical taxonomy of risk types that allows for specific risks to be grouped in a common vocabulary and definition that is openly accessible. In addition, there are specific sources of risk data associated in an emerging taxonomy that enrich its usefulness and application and allow for several risk data sources to be grouped into themes. The open risk taxonomy data model is developing and will in future allow for API access [33].

Associated Data Sets include [33]:

1. The Digital Data Breaches data set,

2. A structured description of regulatory agencies by national financial regulators,

3. Fintech events which is a "collection of risk events that are being migrated from the Manual to the Database as a demo of an Open Risk Data use case",

4. Fintech Risk Event Model and

5. Databreach Risk Event Model.

Global pandemic risk data is also included in the Manual for SARS and MERS and COVID-19 is an emerging data source [33].

7.2 Risk Data Measurement

The data analysed is text based and is largely unstructured qualitative data. The reports contain expert analysis as a narrative along with supporting quantitative survey results data.

There are several ways in which risk horizons have been represented in these data sources as follows:

1. **Method 1**: A concern rating in which respondents were asked "Based on your analysis, how concerned are you about the following threats to your organisation". A list of threats were provided. The concern ratings included. Threats are ranked on the basis of the responses in order. Level of concern provides an outlook on the threats that remain high on the agenda of business continuity and resilience professionals in the next reporting period [39, 64].

2. **Method 2**: In this method, level of concern remains the same. An additional metric added further dimension where respondents were asked to provide an indication of actual disruption experienced in the period. The survey question posed to respondents was as follows: "Have you experienced a business disruption due to the following threats in the last 12 months". This method more formally measured a previous period actual versus a next reporting period outlook [64, 65].

3. **Method 3**: Risk score method which calculates a score based on likelihood and impact. This method uses risk assessment as a basis for reporting. In the previous reporting period, likelihood is measured in terms of frequency and impact and for the outlook into the next 12 month reporting period, likelihood (probability) and impact are measured. Scales varied across the various reports.[4, 1, 44]

It is noted that all three methods have been captured in reporting data gathered from 2015 - 2020 in the 2016, 2017, 2018, 2019 and 2020 reports.

Comparative analysis requires a degree of standardisation and ranking to determine risk trends across the data sources over time.

7.3 Summary of Data Analysed and Captured

The summary of the data analysed and captured is shown in table 7.1. This table includes the data sources, report date and period of reporting along with details of analysis contained in the report and relative sizes of populations surveyed across the results in the reporting year.

Definitions of the table columns are as follows:

Risk Measurement Method

1: Concern Rating: 1 - 5 scale - 1=Extremely Concerned, 2=Concerned, 3=Somewhat Concerned, 4=Not Applicable

2: Concern Rating: 1 - 5 scale - 1=Extremely Concerned, 2=Concerned, 3=Somewhat Concerned, 4=Not Applicable Disruption count (Y/N)

3a: Risk Score: Likelihood (Frequency) 1-5 scale 1=Remote to 5=Imminent; Impact: 1-4 scale - 1=Minor to 4=Extreme

3b: Risk Score: Likelihood 1-5 scale 1=Rare, 2=Unlikely, 3=Moderate, 4=Likely, 5=Almost Certain; Impact 1=Insignificant, 2=Minor, 3=Moderate, 4=High, 5=Critical

Table 7.1: Reporting Data Characteristics

			Measurement				Analysis		Survey Details		
Report	**Year**	**Applicable Timeframe**	**1**	**2**	**3a**	**3b**	**1**	**2**	**Max Score**	**Range N**	**%**
BCI	2016	2015 - 2016	X				X	X		400-500	X
BCI	2017	2016 - 2017	X				X	X		600-700	X
BCI	2018	2017 - 2018		X		X	X	X	25	595	X
BCI	2019	2018 - 2019				X	X	X	25	335	X
BCI	2020	2019 - 2020				X	X	X	25	665	X
IRMSA	2016	2015 - 2026			X		X	X	20	1007	X
IRMSA	2017	2016 - 2017			X		X	X	20	1557	X
IRMSA	2018	2017 - 2020			X		X	X	20	Not stated	X
IRMSA	2019	2018 - 2019			X		X	X	20	Not stated	X
IRMSA	2020	2019 - 2020			X		X	X	20	585	X

7.4 Banking Data

To build the banking data system relative to the Business Continuity Management System, a need to establish a database in data warehouse format is required with a data set that reasonably represents a real banking scenario and also one that has common and generic characteristics to a best practice use case.

To support the development of the contextual model, a data set needed to be selected that would be representative of the system of interest in this report i.e. the banking system in conjunction with the business continuity management system. It also needed to contain data that is representative of the period in which the risk reporting data has been acquired from the various reporting sources i.e. the BCI and IRMSA.

Kaggle is a subsidiary of Google and is a community based data science and machine learning platform where data is shared for the purposes of model and solution development. Tools training and collaboration are the many benefits of operating in this open community. Data scientist and machine learning engineers are also able to compete with each other to solve specific data science challenges.

There are many instances of new models emerging from this platform that have use within various industries. Due to the open, transparent and licensed nature of the platform, data that is shared is controlled and governed. Data owners are assigned to manage the various data sets that are made available and these have traceability to their sources as well as an acknowledgement by the source data owner that the publishing of the data set has all the necessary controls in place.

For the purposes of this report, a data set containing loan book data is selected to represent a single banking system feature (credit), to which key risk metrics are assigned. Loan books are also generally sensitive to emerging operating environment risks.

The "Lending Club" data set has been selected for this purpose and has been used fairly widely in the Kaggle community both in training scenarios, for instance to simulate the calculation of expected loss (key risk metric) as well as the simulation and development of several other key risk metrics and analysis. The data set is also periodically updated and maintained with the data set on Version 2 released in April 2020.

Details of this data set are as follows:

Kaggle Data Science: "These files contain complete loan data for all loans issued through the 2007-2015, including the current loan status (Current, Late, Fully Paid, etc.) and latest payment information. The file containing loan data through the "present" contains complete loan data for all loans issued through the previous completed calendar quarter. Additional features include credit scores, number of finance inquiries, address including zip codes, and state, and collections among others. The file is a matrix of about 890 thousand observations and 75 variables. A data dictionary is provided in a separate file."

Data Owner: Wendy Kan, Position: Data Scientist at Kaggle. Location: San Francisco, California, United States. Last Data Set Update: 2020-04-26. Lending Club Data: https://www.kaggle.com/wendykan/lending-club-loan-data.

7.5 Other supporting Data Sets

For verification purposes and in order to support the development of the system, other data sources have also been included in this report as follows:

1. Business Continuity Institute Emergency Communications report 2019 and 2020,
2. Business Continuity Institute Disruptive Technologies report 2019,
3. Business Continuity Institute Organisational Resilience Perspectives from the Industry Report 2019.

In the instances of case studies of arising risk events, there are several descriptive case studies published in the Business Continuity Management Community and these have been used to provide a narrative to the systems of interest in this study.

7.6 Data Management

The following data management principles have been applied to the data sets used in this report [19]:

1. **Metadata**: The data set must be traceable and have business and technical metadata. In the usage of the data set, business definitions applied have been documented and provided in the Appendix. As the system has been developed using standard Microsoft SQL tool sets, operational metadata is inherent in the system tables of the database and in the data conversion scripting applied.

2. **Master and Reference Data**: The data sets that have been selected are authoritative and have been reviewed and published. Reference data has been standardised either using an authoritative taxonomy source or have been defined and consistently applied in a standardised manner.

3. **Data Security**: The data is secured on a local computer that is monitored with anti-virus software, has strong password protection and secure network access. There is only one user that has access to the computer operating system. Database connections are secured using an authenticated password.

4. **Database Operations Management**: The database selected is SQL Server Lite Version 15 and the standard tools and utilities adopted to manage the creation of database tables through SQL scripting as well as the loading, staging and warehousing of research data that is applicable to this report.

5. **Data development**: The database model has been designed using engineered and normalised methods and where applicable industry standard taxonomy has been loosely adopted from the IBM Banking Data Warehouse Model.

6. **Data Warehousing**: The data warehouse architecture for this solution, included a staging area where acquired data has been loaded directly from its source. Staging tables where appropriate data cleansing and standardisation needed to be done and the loading of the data into a Data Warehouse structure in the database. Data provisioning to the Business Continuity Management System and dashboard has been done in scripted views to consolidate and combine the data for ease of data visualisation.

7. **Document and Content Management**: Document and content management is also an important part of the formulation of this report. Documents have been managed both electronically with the reference database. Hard copies of reports have been maintained with suitable indexing for ease of analysis. It is noted that documentation will be destroyed after two years following the completion of the work.

8. **Data Quality Management**: Key data items used in calculations and data visualisations have been profiled to identify data quality anomalies and these have either been cleansed from the data set or have been reported as having an impact to the results. Data profiles have been included in the Appendix.

9. **Data Architecture Management**: The data architecture has been documented and included in the results section of this report.

10. **Data Governance**: The principles of the BCBS239 which are in line with the DAMA principles used in this list have been applied wherever possible to stay true to credit banking systems from a governance perspective.

11. **Business Intelligence and Advanced Analytics**: Visualisation of the results from the database have been rendered in Microsoft PowerBI as this is a generally used business tool that organisations are adopting for data self service. Business Intelligence and advanced analytics work in conjunction with each other to show and derive insights in the data results.

The data sets selected have been included to determine the possibility of increasing organisational resilience through the development of a contextual model that can be applied to a best practice Business Continuity Management System that is sensitive to behaviours in this data.

8

Data Contextualisation - an Analytical Model

To address the issues previously described, this chapter introduces the contextualisation model based on the meaning of environmental context and business continuity management. Then the contextualisation model is discussed in detail identifying the system components needed for its operation, thereby developing a more thorough and usable system of insight.

8.1 System and Conceptual Data Model Mapping

The financial services data model has been loosely based on industry standard concepts published in various open source and other industry models including IBM, Teradata, and Oracle. Most banking data models include the concepts of Party, Arrangement, Event, Resource Item, Location, Business Direction (Strategy and Activity), Product, Condition and Classification (reference data). The conceptual industry reference data model used in this report is the IBM Banking Data Model and represents the nine core data concepts as they apply to financial services [66].

It is noted, however that any industry can adopt this approach by substituting the industry specific data concepts. For example, in healthcare, the health care industry model concepts would be applied. This therefore shows that the model described in this chapter can be extended to alternative industries and their corresponding systems. Industry model references are indicated by an "*" in the conceptual data model mapping shown in table 8.1. To extend the data model to alternative industries these concepts would need to be reviewed accordingly.

The financial systems use case is built using the attributes that are of interest to system stakeholders (interested parties - ISO22301 clause 4.2) including governance and compliance structure (ISO22301 - Clause 5.3), components, sub-systems and processes (ISO22301 clauses 6,7 and 8) and how these would be applied to contextualise environmental data [3, 17].

In application, the result is an integrated Conceptual Data Model that is a representation of the system of interest which is the Business Continuity Management System in the Context of the Banking System.

Steps applied to derive the result were as follows [3, 2, 17]:

1. Identification of Banking Process (credit life-cycle use case) and associated key risk indicator.
2. Identification of Business Continuity Management Process (derived from the ISO22301 Standard). This represents the requirement of the problem statement represented in figure 8.1, which is to test the feasibility of integrating the data context with a ISO22301 compliant BCMS.
3. Deriving the system components. The results of which are shown in the system conceptual architecture in figure 8.3.
4. Translation of system concepts into data concepts. This is shown in the conceptual data model in figure 8.2.
5. Mapping the system concepts to the industry reference model and the standard. This mapping is given in table 8.1.

The conceptual data model forms the basis on which the resilience and system data is mapped to build the logical and physical data models. In application these steps are necessary to implement the physical data model and to load the data according to the SEMP and its associated V-model. (figure 6.6).

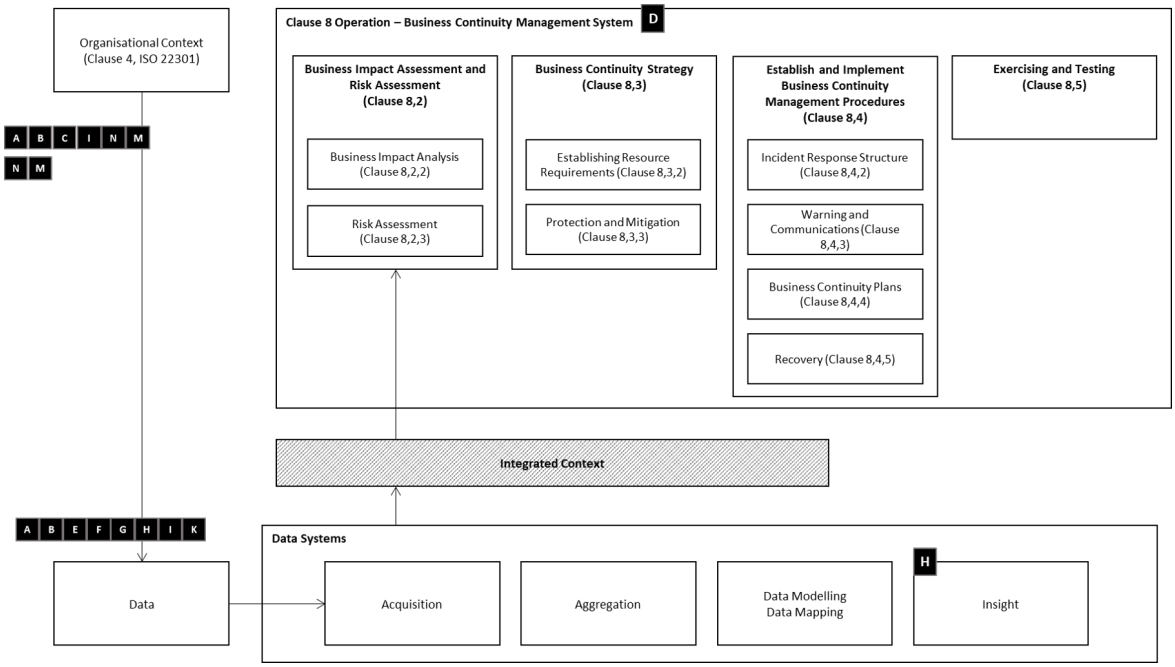


Figure 8.1: Step 2: System Requirement Mapping - in relation to the system problem statement [2, 3]

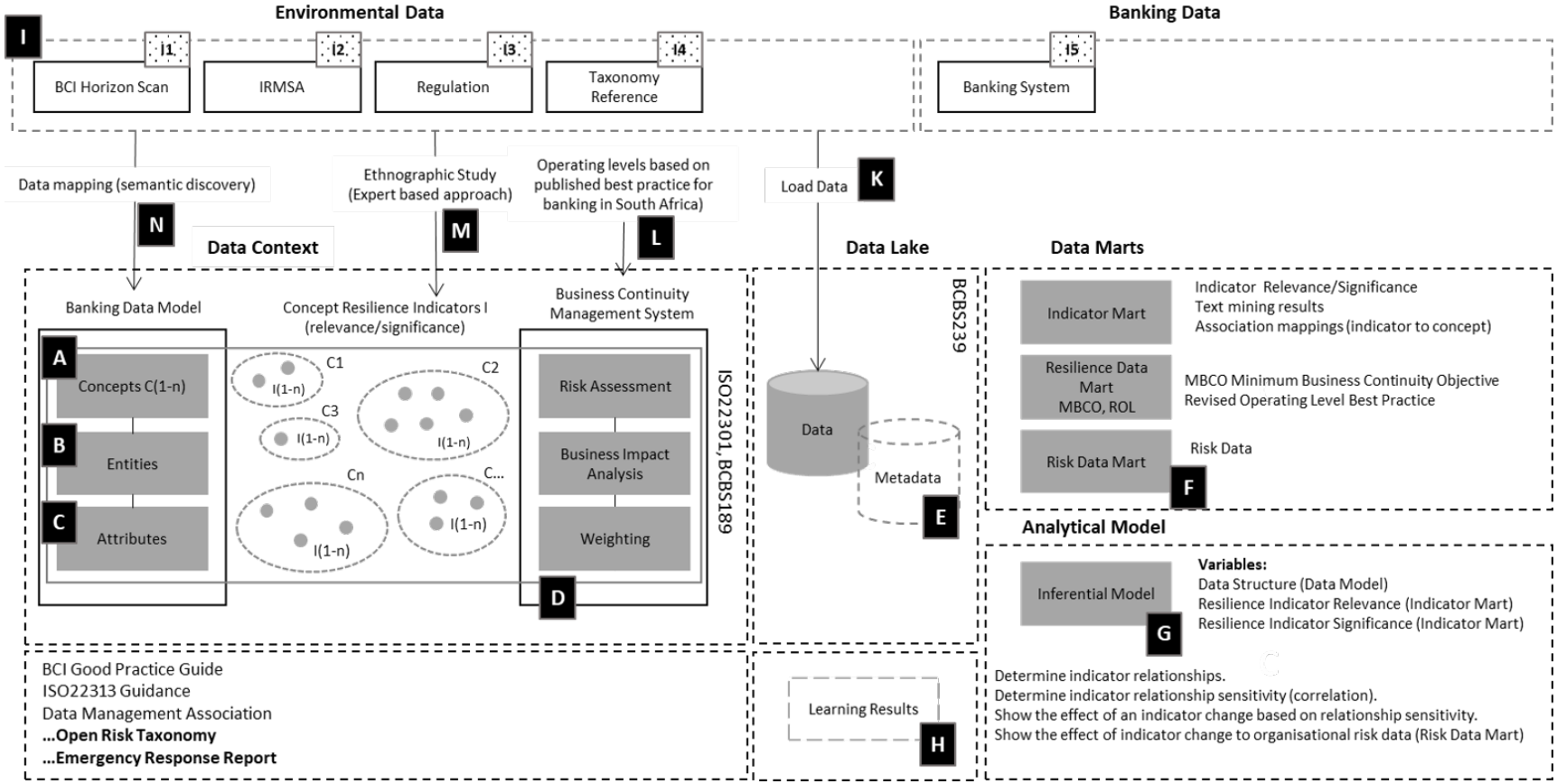


Figure 8.2: Step 3: System Conceptual Model in Context

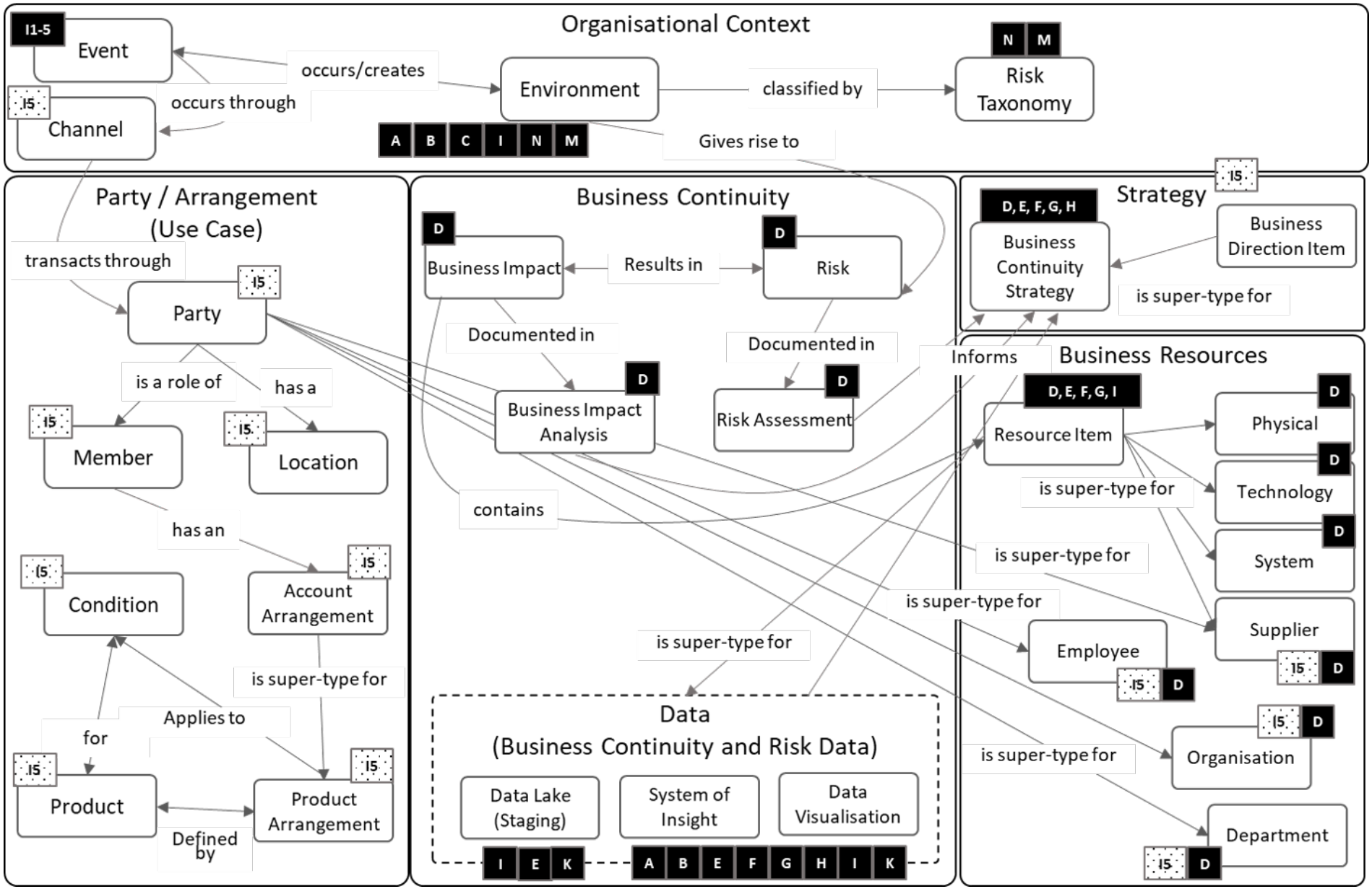


Figure 8.3: Step 4: Conceptual Data Model - System Representation in Data Terms

Table 8.1: Step 5: Conceptual Systems to Conceptual Data Model Mapping

Data Concept Mapping		**System Component Mapping**		**ISO22301 Standard**
Banking Data Model				
Party Arrangement *	Event	I1-5	BCI Horizon Scan, IRMSA, Regulation, Taxonomy Reference, Banking System	Clause 4
	Channel	I5	Banking System	Clause 4
	Party	I5	Banking System	Clause 4
	Member	I5	Banking System	Clause 4
	Location	I5	Banking System	Clause 4
	Condition	I5	Banking System	Clause 4
	Account Arrangement	I5	Banking System	Clause 4
	Product	I5	Banking System	Clause 4
	Product Arrangement	I5	Banking System	Clause 4
	Strategy	I5	Banking System	Clause 4

Data Concept Mapping		**System Component Mapping**		**ISO22301 Standard**
Strategy	Business Direction Item *	D	BCMS	Clause 6, 7
	Business Continuity Strategy	D, E, F, G, H	BCMS, Data Lake, Data Marts, Inferential Model, Learning Results	Clause 5, Clause 8
Business Resources	Resource Item *	D, E, F, G, I	Environmental and Banking Data, Data Lake, BCMS, Data Marts, Inferential Model	Clause 4 and 8
	Physical	D	BCMS	Clause 8
	Technology	D	BCMS	Clause 8
	System	D	BCMS	Clause 8
	Supplier (Party)	I5, D	Banking System, BCMS	Clause 8
	Employee (Party)	I5, D	Banking System, BCMS	Clause 4 and 8
	Organisation (Party)	I5, D	Banking System, BCMS	Clause 4 and 8
	Department (Party)	I5, D	Banking System, BCMS	Clause 4 and 8
	Data Lake Staging	I, E, K	Banking System, Data Lake, Load Data	Clause 4 and 8
	System of Insight	E, F, G, H, I, K	Data Lake, Data Mart, Inferential Model, Learning Results, Banking System, Load Data	Clause 4, 8, 10
	Data Visualisation	A, B, C, I, E, K	Concepts, Entities, Attributes, Banking Data, Data Lake, Load Data	Clause 4, 8, 10

Data Concept Mapping		**System Component Mapping**		**ISO22301 Standard**
Environment	Environment	A, B, C, I, N, M	Concepts, Entities, Attributes, Environmental and Banking Data, Data Mapping, Ethnographic Study	Clause 4
Business Continuity	Risk Taxonomy	N, M	Data Mapping, Ethnographic Study	Clause 4
	Business Impact	D	BCMS	Clause 8
	Risk	D	BCMS	Clause 8
	Business Impact Analysis	D	BCMS	Clause 8
	Risk Assessment	D	BCMS	Clause 8
** (Industry Model Reference)*				

In application, the conceptual system model was successfully expressed in data terms aligned to the ISO22301 standard, providing the possibility to manage and store the context of environmental data in suitably standardised and compliant data structures. This also satisfied the BCBS239 Principle 1 and 2 and provides a foundational basis for the implementation of the remaining principles. Principles have been included in figure 8.4. This diagram has been adapted from the BCBS239 legislation and representation of the legislation as currently published by Deloitte [17, 67].

BCBS239 Principles		
Governance and Infrastructure	**1. Governance** The bank's risk data aggregation capabilities are subject to management oversight and review.	• Documenting end to end processes of all components involved. • Incorporating a process for independent validation. • Developing Data Strategy (risk, impact, solution and timeline) when the bank acquires or develops a new product.
	2. Data and IT Architecture A bank should design, build and maintain a Data Architecture and IT infrastructure that is scalable and supports risk data aggregation and reporting.	• Assessing impacts to business continuity and planning processes. • Developing integrated data taxonomies and infrastructure.
Risk Data Aggregation Capabilities	**3. Accuracy and Integrity** The ability to generate consistent and correct data for normal and stress/crisis reporting requirements.	• Developing controls and efficient reconciliation processes. • Developing standardised operating procedures. • Identify authoritarian (golden sources), systems and mechanisms in which personnel can access risk data to aggregate, validate and reconcile to regulatory and management reports.
	4. Completeness The ability to provide all material risk data across the various lines of business as well as entities.	
	5. Timeliness The ability to provide data point on risk factors based on the frequency as required.	
	6. Adaptability The ability to generate a broad range of on demand reporting requests.	
Risk Reporting Practices	**7. Accuracy** Reports are reconciled and validated, enabling management to make informed decision about risk.	• Develop automated check functions on reasonableness and on validations. • Develop procedures for reporting and explaining data errors.
	8. Comprehensiveness The ability to provide detailed information on all material risks within the organisation.	
	9. Clarity and usefulness Communicating risk information that includes a balance among analysis, interpretation and tailored to the needs of the receiver.	
	10. Frequency Reflect the needs of recipients, nature of risk reported, and the speed at which the risk can change.	
	11. Distribution Risk management reports that have a clear procedure for rapid collection and analysis of risk data and timely dissemination to all appropriate recipients while ensuring confidentiality.	

Figure 8.4: BCBS239 Principles derived from the standard and based on currently published Deloitte methodologies [17, 67].

8.2 Logical Data Model

Further implementation of the logical and physical data models have been applied in data system simulation. Advantages of this translation provides for ease of adoption and re-usability. This contributes to the field by providing a reference model for future work and more detailed development. If future work proves that the conceptual model needs adaptation, the standardisation against industry best practice remains foundational and a reference point for change.

The logical Data Model is constructed according to the high level data concept mapping (L0) which includes: Environment (Organisational Context), Party/Arrangement (use case), Business Continuity, Strategy and Business Resources as a foundation to constructing a physical data environment (Data Lake, System of Insight and Data Visualisation).

8.2.1 Organisational Context L0 and L1

Organisational Context L0 is representative of the data that the system both generates and consumes as part of its operation. Standardisation and classification business rules are applied and the results of these are stored in two L1 logical entities including Environment and Risk Taxonomy. Organisational Context attributes are shown in figure 8.5

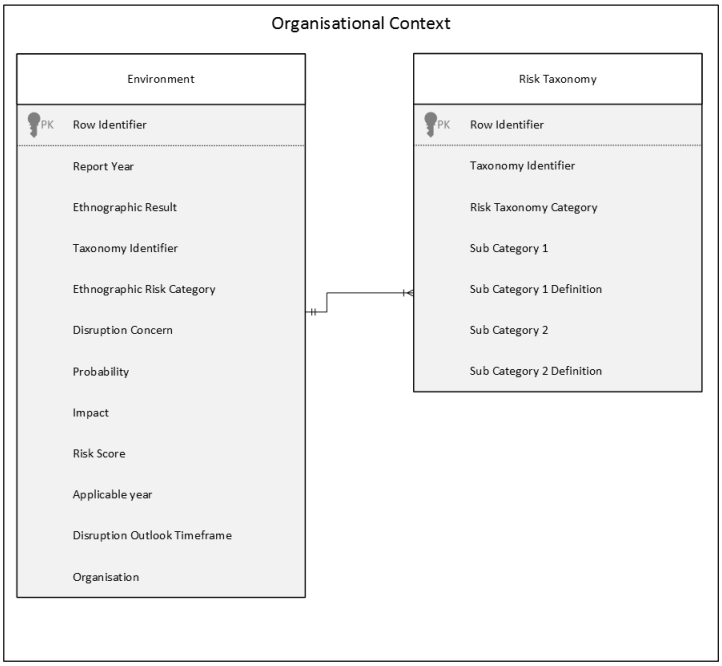


Figure 8.5: L0 Organisational Context Logical Data Model [3, 18]

L1 Definitions:

1. Environment: External risk data sources captured and classified. Stored results for V1 (Contextualisation variable component V1.1).
2. Taxonomy: Open Risk Taxonomy sub-set reference data as identified and mapped to the source data Ethnographic Result (Contextualisation variable component V1.2).

8.2.2 Party/Arrangement (Use Case) L0 and L1

Party and Arrangement L0 is representative of the banking system use case data (loan book). The details of the interested party (member), their arrangement (personal loans) and the terms of the loan in condition in the L1 entities.

L1 represents the loan book which is a flat file (data lake table). This table has all the attributes associated with the party and the arrangement.

The physical data model for the L1 Loan entity has been included in detail in the Appendix. This is a very wide entity and is rich in data attributes.

8.2.3 Business Resources L0 and L1

Business Resources L0 includes the items applicable to the organisation and its operations. In this report, business resources are specifically related in sub-type to the simulated BCMS. In a more extensive representation of the organisation all resources that apply to the parties would be included in the entities that form part of Business Resources L0. Business Resource attributes are shown in figure 8.6.

L0 definition according to the ISO22301 Standard 2012 clause 3.47 is "all assets, people, skills, information technology (including plant and equipment), premises, and supplies and information (whether electronic or note) that an organisation has to have available to use, when needed, in order to operate and meet its objective [3]."

L1 Definitions [3]:

1. Disruption Required Resources: see above L0 definition according to the standard.
2. Disruption Required Technology: specific technology resources including IT systems and other hard systems required in business operations.
3. Disruption Required Systems: includes specific systems that need to be activated and/or recovered in the event of a disruption.

4. Disruption Required Supplier Services: includes the details of the suppliers as well as their levels of service required in the event of a disruption. Suppliers are part of the interested parties and therefore this is also a sub type of party.

5. Disruption Required Department: defined under clause 3.33 of the ISO22301 Standard as follows: "person, group of people that has its own function with responsibilities, authorities, and relationships to achieve its objectives. Note: for organisations with more than one operating unit, a single operating unit can be defined as an organisation."

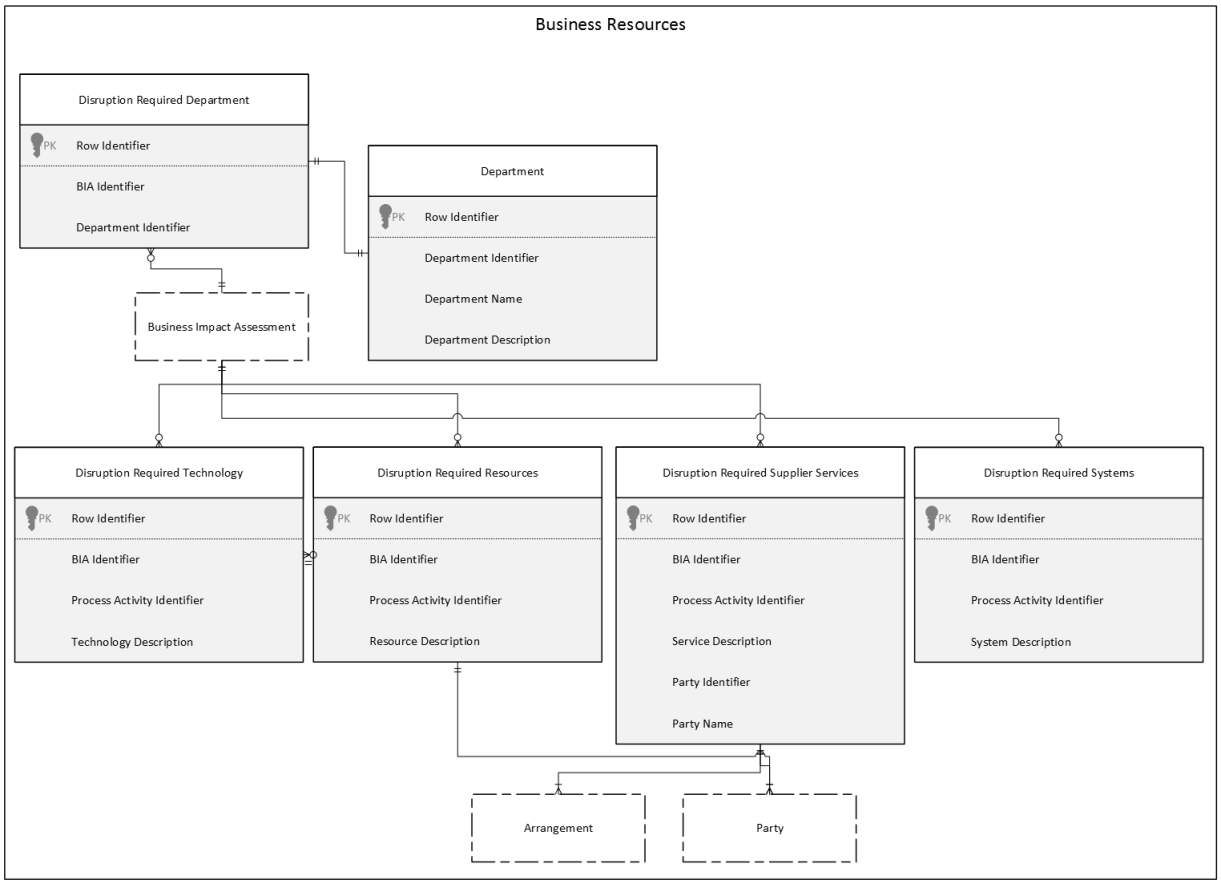


Figure 8.6: L0 Business Resources Logical Data Model [3, 18]

8.2.4 Business Continuity L0 and L1

Business Continuity L0 includes the items that represent the core of the BCMS and its L1 entities. L1 entities have been modelled using the ISO22301 as a basis and therefore the definitions of these have been inherited from the standard.

L1 Definitions [3]:

1. Business Impact Analysis (ISO22301 clause 8.22): "documented evaluation process (results) for determining continuity and recovery priorities, objectives and targets. Including; identifying activities that support the provision of products and services, assessing the impacts over time of not performing these activities, setting prioritised time frames for resuming these activities at a specified minimum level, taking into consideration the time which the impacts of not resuming them would become unacceptable and identifying dependencies and supporting resources for these activities, including suppliers, outsource partners and other relevant interested parties."

2. Business Impacts: The consequence of a disruption caused by an emerging environmental risk.

3. Impact Category: The classification of types of impacts that include: staff, public, regulatory, reputational, financial, service and environmental impacts as identified categories applicable to this report.

4. Risk Assessment (ISO22301 clause 8.23): "formal documented risk assessment process that identifies, analyses and evaluates the risk of disruptive incidents to the organisation."

The Business Continuity logical data model includes the derivation results from the risk evaluation (operating context). These attributes include relevance and significance. Relevance indicates the applicability of the derived environmental risk to the industry and significance contains the frequency of the risk occurring in the survey as well as the average associated risk scores over time.

In the Conceptual Systems Architecture and subsequent Logical Data Model representation:

1. Risk Identifier: is derived from the environmental risk assessment and standardisation process and is a stored result representing C(n) in figure 8.2.

2. Key Risk Indicator: is the risk indicator identified either through legislation or though definition to be measured and watched. This is a stored result representing I(n) in the system conceptual model in figure 8.2.

3. Relevance: is derived from organisational industry context evaluation as set out in clause 4 of the ISO22301 Standard [3]. This is a stored result for V2 (contextualisation variable V2.1).

4. Significance: calculated significance is based ion the environmental risk assessment and is a stored result for V2 (contextualisation variable V2.2).

The Business Continuity Logical Model is shown in figure 8.7

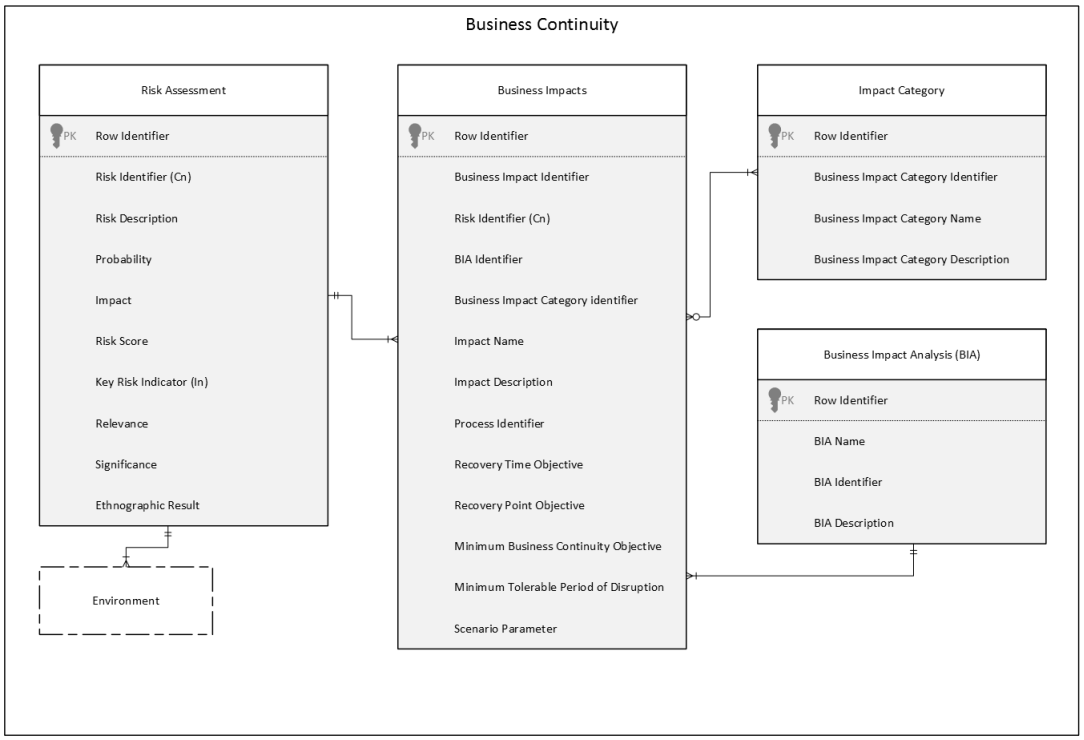


Figure 8.7: L0 Business Continuity Logical Data Model [3, 18]

8.2.5 Strategy L0 and L1

Strategy L0 includes the items that describe the direction of the organisation and its associated activities and processes. Strategy in this report, specifically refers to clause 8.3 of the ISO22301 standard as follows "the outputs of the business impact analysis and risk assessment" and also the need for the determination of strategy as follows [3]:

The ISO22301 Standard states that "The organisation shall determine an appropriate business continuity strategy for [3]:

1. Protecting prioritised activities,
2. stabilising, resuming and recovering prioritised activities and their dependencies and supporting resources and
3. mitigating, responding to and managing impacts."

L0 in this case, makes provision to store the identified activities that form part of the BIA Processes Activities and Process Activity Impact Timeframe entities as part of

the L1 construct. Insight results are contained in the data marts which is the basis of the system of insight.

L1 Definitions [3]:

1. Process Activities: Activities that require protection in the event of a disruption (clause 8.3.1 ISO22301 Standard).
2. Impacted Timeframe: "Prioritised time frames for the resumption of activities" including the Recovery Time Objective (RTO), Recovery Point Objective (RPO), Minimum Business Continuity Objective (MBCO) and Maximum Tolerable Period of Disruption (MTPD).
3. Incident Response Structure: "procedures and a management structure to respond to a disruptive incident using personnel and with the necessary responsibility, authority and competence to manage an incident (clause 8.4.2)."

The Logical Data Model for Strategy is shown in figure 8.8

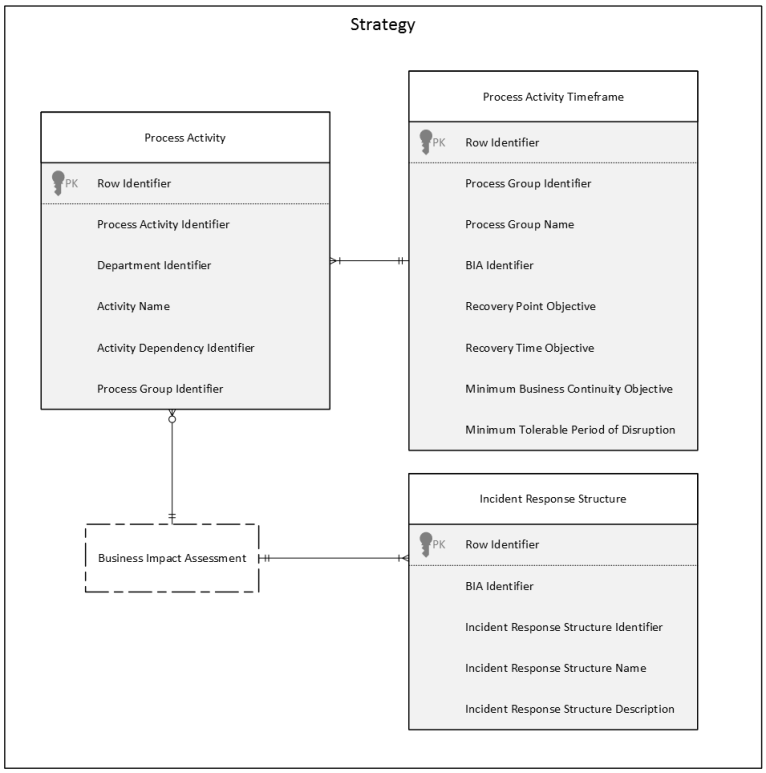


Figure 8.8: L0 strategy Logical Data Model [3, 18]

8.3 Physical Data Model

The detailed Physical Data Model metadata mapped to the Logical Data Model L0 and L1 is included in the Appendix. Scripting of the creation of the database is based on this mapping.

Sections in the Appendix include:

1. Section 10.2 Physical Data Model Standards - Table and column name standards mapping and standard data types.
2. Section 10.3 Physical Data Model - Mapping of the Logical Data Model Entities and Attributes to Tables and Columns along with their definitions.
3. Section 10.4 Database Scripting - SQL Scripting that creates the tables on the server, data profile results and data loading procedures.

8.4 Data Contextualisation Analytical Model

8.4.1 The Concept of Dynamic Contextualisation

To illustrate the concept of dynamic data conceptualisation (DC) a decomposition of variable components is required. These include:

1. Contextualisation variable V1 which is composed of the ethnographic result (V1.1) and the taxonomy identifier (V1.2)
2. Contextualisation variable V2 which is composed of the significance (V2.1) and relevance (V2.2) of risks assessed.

8.4.2 Organisational Context: Contextualisation Variable V1(1-n)

1. Ethnographic Result is (V1.1): derived by grouping key words and risk descriptions across multiple risk reports. The risk types standardised and assigned a numeric (integer) value. This field is used as an input to the taxonomy mapping.
2. Taxonomy Identifier (V1.2): is assigned based on the definition of risk in the Open Risk Taxonomy.

The Organisational Context concept contains the data that is gathered through system components I and adopts the system processes of N,M,L and K. The entities

(L1) are shown in figure 8.5 and these provide a consolidation of ethnographic study results mapped to standard risk categories in the taxonomy.

All results of the BCI and IRMSA reports covering five years of history are modelled into the Environment entity. Standardisation and classification results are stored in the Ethnographic Result and Taxonomy Identifier attributes respectively and are based on the source data variable V0 which is the Ethnographic Risk Category which contains all risks described in these sources of data.

The disadvantage of consolidation of the organisational context analysis into a single entity could not address the variances in report nuances and changes over time, making data visualisation challenging. Additional work would be required to develop standardised and comparable quantitative measures for risk. Alternatively a suitable standardisation algorithm. In this report, the variances can be visualised in two separate trends using the applicable report year attributes depending on whether the reader requires a retrospective or outlook based view.

The advantage of consolidation of the analysis into a single entity results in the standardisation of risk categories. This also provides the basis for mapping to standard taxonomy references. The output of this process is a derivation of V1 from the input variable Ethnographic Risk Category (V0) which is contained in the source data (industry risk reports).

V1 = Ethnographic Result : Taxonomy Identifier

V1 = Ethnographic result V1.1 (1-n)) : Taxonomy Identifier V1.2 (1-n)

The adoption of the usage of value pairs is to allow for additional dynamic conceptualisation sub variables to be added over time to provide flexible extension.

8.4.3 Environmental Risk Assessment: Contextualisation Variable V2(1-n)

The Name Value Pair - Ethnographic Result (V1.1) is inherited into the Risk Assessment (RSK_ASMT) table following which a Standardised Risk Description (C(1-n)) is written into the Risk Description (RSC_DESC) field. Key Risk Indicators are assigned to these according to industry standard or though derivation and stored into the Key Risk Indicator (KRI) field. Relevance (V2.1) is based on the average risk score over a three to five year period for an assessed risk. Standardisation of scoring is essential in ensuring comparability.

Significance (V2.2) is assigned according to organisational operating context based on expert judgement per record in the risk assessment. It is noted however that a framework of significance could be developed for the organisation on which to base the evaluation. There are several methods in which risk significance can be approached, for example a parameter for risk significance can be derived based on the

frequency of risk occurrences in industry risk reporting (environmental scanning). For the purposes of this report, significance ratings have been categorised into high, medium and low based on relevance and quantitative evidence.

V2 = Relevance : Significance

V2 = Relevance Result V2.1 (1-n) : Significance Result : V2.2 (1-n)

8.4.4 Data Contextualisation Variable Result Stated

Following the above analysis the final Data Contextualisation Variable (DC(1-n)) result is stated as follows:

$$DC(1-n) = (V1.1(1-n) : V1.2(1-n))\| \ (V2.1(1-n) : V2.2(1-n))$$

for C(1-n) and I(1-n) where C is the Standardised Risk Description and I is the Risk / Resilience Indicator

8.4.5 Integrated Context with the Business Continuity Management System

In application, the risk description (C(1-n)) can be applied to identify the business impacts associated with the identified risk. This association is stored in the Business Impact table (BUS_IMP) as a reference data field Risk Description (RSK_DESC), thereby always maintaining reference to the Dynamic Context (DC(1-n)) variable.

$$DC(1-n) = (V1.1(1-n) : V1.2(1-n))\| \ (V2.1(1-n) : V2.2(1-n))$$

8.4.6 System of Insight

The derived system of insight provides the consolidation of the results of the system which can be used to inform Strategy.

1. A final array of Integrated Risks and associated Impacts in their Context (DC(1-n)), which can be dynamically maintained as additional environmental data becomes available. This is shown as part of system component F (Indicator Mart) in the System Conceptual Model in figure 8.2.
2. Risk Data Marts in the Financial Services industry contain the results of identified key risk indicators, for example; calculated expected loss (applied use

case in this report). This is shown in figure 8.2. A calculation of a simulated expected loss is provided in the illustrative example. Through the association to the risk description in the Business Continuity Logical Data Model this association is maintained as part of the Risk Assessment and Business Impact Analysis.

3. Resilience Data Mart, which provides an integrated visualisation of the Risk Assessment and Business Impact Analysis which dynamically updates as changes in the system occur through continuous improvement.

Although inferential modelling was not included in the final result, by having the data available in the System of Insight data marts, sensitivity measures and correlations can be modelled to determine the sensitivity of a Key Risk Indicator against changing environmental context features.

8.5 Illustrative Data Results

In this section, the results of the environment scan are used to discuss the derivation of a data contextualisation variable and its application in the Business Continuity Management System. While the example provides an end to end illustrative system subset of the results analysed, the risks analysed include all risks identified and standardised over a period of 5 years. This data profile is included in the appendix of this report.

8.5.1 Derivation of V1.1 and V1.2

The analysis of V0 is shown in figure 8.9. 395 Risk categories were captured over the five year environment scan period along with their risk scoring measures. In this figure all risk categories analysed regardless of risk scoring calculation are shown. It is noted that in instances where the same risk category keywords in sequence were observed, these were counted distinctly.

More consistently reported distinct risks show with higher counts. Less consistently reported risks have lower counts and therefore on a continuum smaller count values indicated either an emerging risk or an isolated time based risk for a particular reporting period.

Should the counted values in the study increase over time, planning for consistently re-occurring risk is an important consideration, however these should be continuously assessed.

Emerging risks require additional planning attention and close monitoring of re-occurrence over time.

Isolated risks with a count value less than 1 over a three year period would likely be isolated risk categories. Thresholds could be applied to eliminate isolated risk occurrences, however these should still be evaluated on merit.

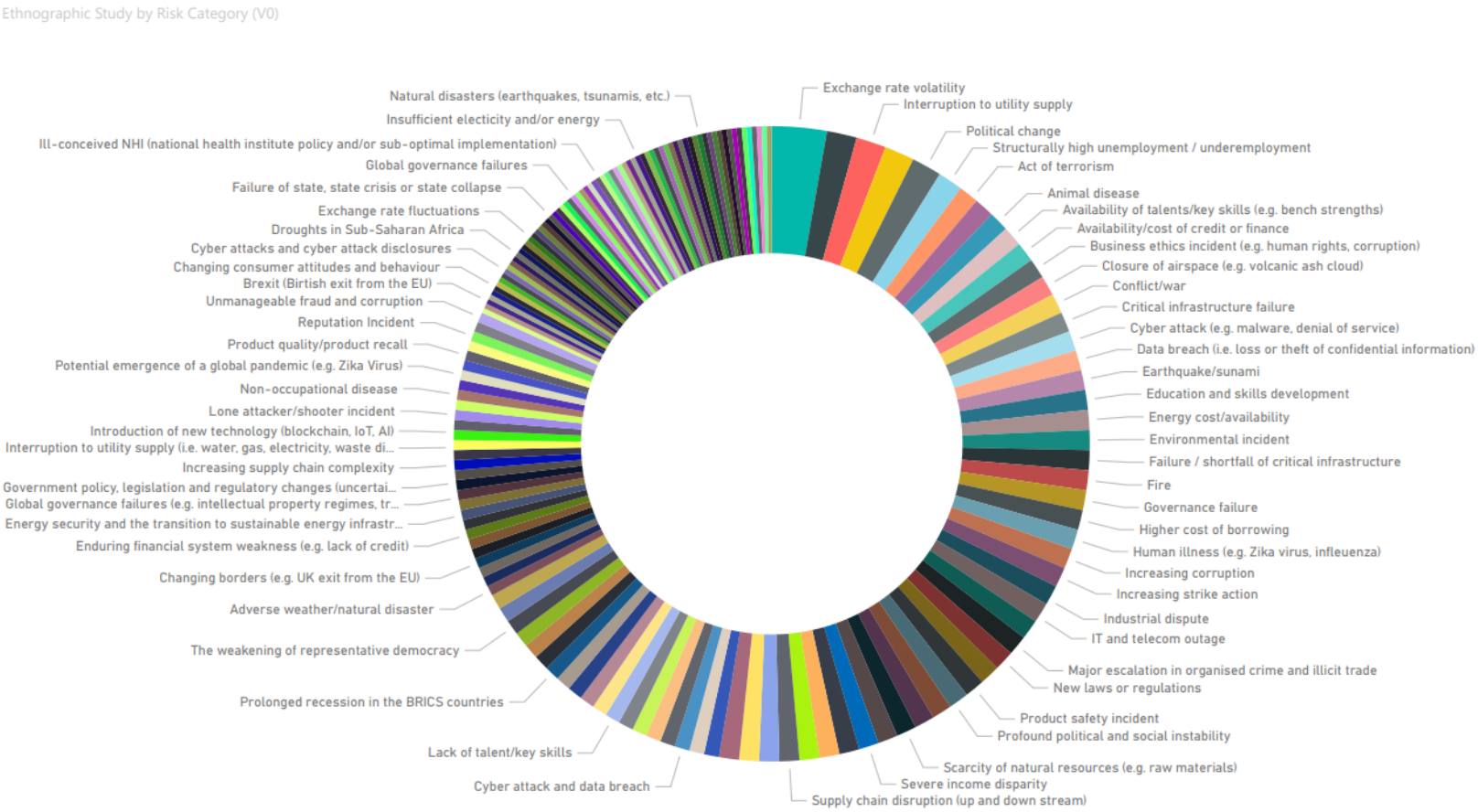


Figure 8.9: Ethnographic Study by Risk Category

The aggregated risk score (averages) post standardisation based on the ethnographic result (V1.1) is shown in figure 8.10. In these results a single risk scoring method was used i.e. probability and impact. Additional risk scoring methods would require either a standardisation in measure or additional risk scoring algorithms to obtain a standardised risk score. To accommodate this, the data model could be extended to include additional attributes for risk score results.

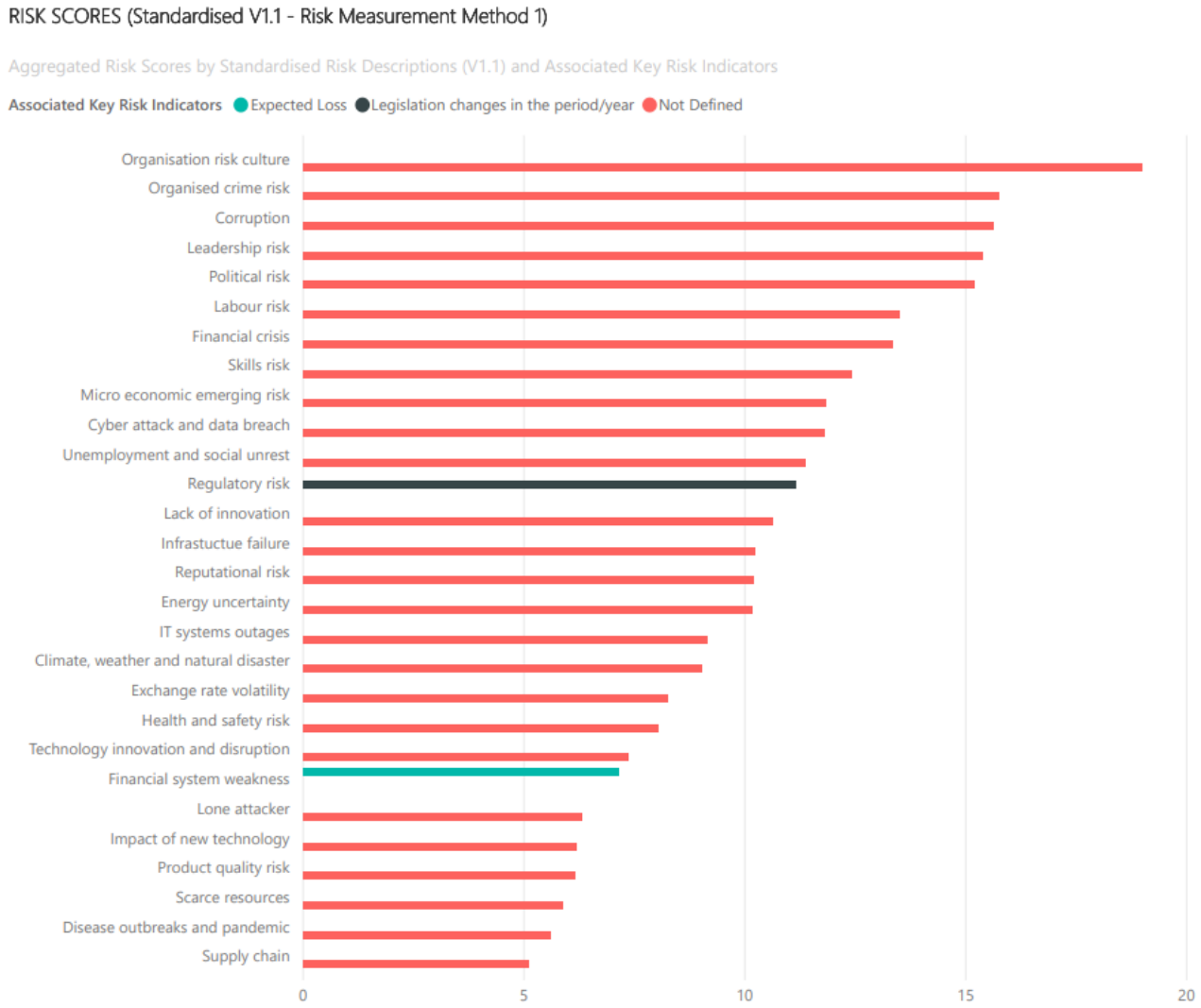


Figure 8.10: Aggregated Risk Scores by Standardised Risk Descriptions (V1.1) and Associated Key Risk Indicators

Results are integrated into the Risk Assessment (clause 8.2.3) as derived risk scores in the risk register. This provides the Business Continuity Professional with a recommended risk score on which to base their expert judgement. Derived risk scores at a macro level do not eliminate the need for direct expert judgement processes to ensure adjustment for the specific organisation. Risk score adjustment could further be automated by applying a risk score weighting parameter. This is provided for

in the System Conceptual Architecture 8.2 BCMS components D. The data model would be extended to include this attribute should this be the preferred method adopted within the specific situation and preferred method of assessment.

This process fulfils the requirement of the ISO22301 Standard to "systematically identify, analyse and evaluate the risk of disruptive incidents to the organisation" [3] at a macro level to which further impact analysis can be based. In addition to this, it provides a documented historical record of risk changes over time along with their risk scores. It is noted that all dynamic changes occurring over time would be stored as appended records in a time dependent data mart. This provides a basis on which risk trend analysis can be performed within the BCMS.

Risk classification is an important factor in establishing related data sources from industry and also provides for a record of authoritative sources (master and reference data principles). The Open Risk Taxonomy provides clarity of risk categorisation and definition and also provides associated sources of data mapped to these. This is a powerful method that can be used to quickly obtain peer reviewed sources of data that further inform a specific risk.

Worked Example: Pandemic Data Sources obtained through the taxonomy;

Taxonomy
Category = Business risk
Sub Category 1 = Operational risk
Sub Category 2 = Disease and pandemic

In the relevant section of the taxonomy, live associated risk events are crowd sourced.

In the example in this report, regulatory risk and financial system weakness have been selected as an associated key risk indicator. The identification of indicators can also be derived from industry regulation and standardised indicator sources again associated to risk taxonomy standardisation and categorisation.

Financial system weakness parameters and regulatory risk are material to banking operations and therefore have been selected here. The model caters for all risk types and therefore the selection of financial services risk indicators does not constrain the model to this specific industry.

The taxonomy mapping results for variable V1.2 are shown in figure 8.11

Ethnographic Results V1.1	Taxonomy Identifier V1.2	Ethnographic Risk Category V0
8	8	Availability/cost of credit or finance
8	8	Capital availability (credit risk)
25	14	Changes in legislation and regulations
25	14	Continuing private and public governance failures
8	8	Enduring financial system weakness
8	8	Enduring financial system weakness (e.g. lack of credit)
25	14	Enforcement by regulator
25	14	Failure of governance (private and public)
25	14	Global governance failures
25	14	Global governance failures (e.g. intellectual property regimes, trade regulations, geopoloitical risks)
25	14	Governance failure
25	14	Government policy, legislation and regulatory changes (uncertainty)
8	8	Higher cost of borrowing
25	14	Ill-conceived land reform policy and/or sub-optimal implementation
25	14	Ill-conceived NHI (national health institute policy and/or sub-optimal implementation)
25	14	New laws or regulations
25	14	New regulations and increased regulatory scrutiny
25	14	Regulatory / legislative changes
25	14	Regulatory changes

Figure 8.11: Taxonomy Mapping

Taxonomy structures are shown in figures 8.12. The associated definitions for this subset of the Open Risk Taxonomy (applied in this report) are shown in figures 8.13 and 8.14.

TAXONOMY (Organisational Context (L0))

V1.2	Taxonomy Risk Category	Sub Category 1	Sub Category 2
1	Business Risk	Operational Risk	Physical Damage
2	Climate Related Risk	Sustainable Finance	Climate Change
3	Business Risk	Operational Risk	Business Continuity
4	Business Risk	Operational Risk	IT Risk
5	Business Risk	Operational Risk	Disease and Pandemic
6	Business Risk	Revenue Risk	Market Share
7	Market Risk	Foreign Excahange Risk	Foreign Exchange
8	Business Risk	Funding Risk	Funding Risk
9	Business Risk	Operational Risk	Employment Practices
10	Business Risk	Leadership Risk	Leadership
11	Business Risk	Human Resources Risk	Human Resources
12	Market Risk	Exposure Risk	Exposure
13	Credit Risk	Country Risk	Political Risk
14	Business Risk	Operational Risk	Legal Risk
15	Business Risk	Franchise Risk	Business Model Risk
16	Business Risk	Operational Risk	External Fraud
16	Business Risk	Operational Risk	Internal Fraud
17	Business Risk	Strategic Risk	Strategic Risk

Figure 8.12: Taxonomy Distinct Categories (applied)

8.5.2 Taxonomy Reference Data Definitions

Risk Taxonomy Category
Business Risk
Climate Related Risk
Credit Risk
Market Risk

Sub Category 1	Definition	Associated Category
Exposure Risk	Exposure. Exposure (also Risk Exposure) is a general term in Risk Management that aims to capture the potential financial loss inherent in a contract, transaction, portfolio etc. It aims to capture the extent to which an individual or organization is unprotected and open to damage, danger, risk of suffering a loss, or uncertainty. The potential susceptibility to loss; the vulnerability to a particular risk.	Market Risk
Foreign Excahange Risk	Foreign Exchange Risk is the probability of the loss occurring from an adverse movement in Foreign Exchange rates.	Market Risk
Country Risk	Risks arising from credit events (default) or other unexpected economic or political events associated with a sovereign entity	Credit Risk
Sustainable Finance	Sustainable Finance denotes financial services and products that are integrating environmental, social and governance (ESG Criteria) into business or investment decisions.	Climate Related Risk
Franchise Risk	Franchise risk captures the impact of external or internal risk factors on the perceived long term franchise value of the firm	Business Risk
Funding Risk	The funding risk category covers risks linked to uncertainty around the availability of future external funds for financing operations	Business Risk
Human Resources Risk	Human Resources, in risk management context, denotes a set of challenges to the firm's business plan and franchise value due to adverse climate among its employees.	Business Risk
Leadership Risk	No definition	Business Risk
Operational Risk	Operational Risk concerns threats to the normal operations of the firm. In the Open Risk Taxonomy is it categorized as part of general Business Risk.	Business Risk
Revenue Risk	Revenue Risk covers all risks pertaining to the ability to persist or grow profitable business operations	Business Risk
Strategic Risk	Strategic Risk (also Strategy Risk) denotes the risk arising from forward looking activities that modify the Business Plan of the firm (significant changes to policies, products, targeted market segments, acquisitions or any other business building activities) which may incur investment costs but below expected returns	Business Risk

Figure 8.13: Taxonomy Definitions

Risk Taxonomy Category
Business Risk
Climate Related Risk
Credit Risk
Market Risk

Sub Category 1	Definition	Associated Category
Exposure Risk	Exposure. Exposure (also Risk Exposure) is a general term in Risk Management that aims to capture the potential financial loss inherent in a contract, transaction, portfolio etc. It aims to capture the extent to which an individual or organization is unprotected and open to damage, danger, risk of suffering a loss, or uncertainty. The potential susceptibility to loss; the vulnerability to a particular risk.	Market Risk
Foreign Excahange Risk	Foreign Exchange Risk is the probability of the loss occurring from an adverse movement in Foreign Exchange rates.	Market Risk
Country Risk	Risks arising from credit events (default) or other unexpected economic or political events associated with a sovereign entity	Credit Risk
Sustainable Finance	Sustainable Finance denotes financial services and products that are integrating environmental, social and governance (ESG Criteria) into business or investment decisions.	Climate Related Risk
Franchise Risk	Franchise risk captures the impact of external or internal risk factors on the perceived long term franchise value of the firm	Business Risk
Funding Risk	The funding risk category covers risks linked to uncertainty around the availability of future external funds for financing operations	Business Risk
Human Resources Risk	Human Resources, in risk management context, denotes a set of challenges to the firm's business plan and franchise value due to adverse climate among its employees.	Business Risk
Leadership Risk	No definition	Business Risk
Operational Risk	Operational Risk concerns threats to the normal operations of the firm. In the Open Risk Taxonomy is it categorized as part of general Business Risk.	Business Risk
Revenue Risk	Revenue Risk covers all risks pertaining to the ability to persist or grow profitable business operations	Business Risk
Strategic Risk	Strategic Risk (also Strategy Risk) denotes the risk arising from forward looking activities that modify the Business Plan of the firm (significant changes to policies, products, targeted market segments, acquisitions or any other business building activities) which may incur investment costs but below expected returns	Business Risk

Figure 8.14: Taxonomy Definitions

8.5.3 Derivation of V2.1 and V2.2

The derivation of V2.1 and V2.2 is derived against V1 which is written to the Risk Assessment Entity (RSK_ASMT). This is shown in figure 8.15.

ENVIRONMENT (Organisational Context (L0))

ID	Risk Description	Impact	Probability	Risk Score	V2.1 (Relevance)	V2.2 (Significance)	V1.1 Ethnograpgic Result
81	Organisation risk culture	4.75	4.00	19.00	19.00	Not Defined	43
80	Organised crime risk	4.08	3.86	15.74	15.74	Not Defined	42
79	Corruption	3.87	4.04	15.63	15.63	Not Defined	28
78	Supply chain	1.67	3.07	5.12	5.12	Not Defined	27
77	Reputational risk	2.84	3.59	10.19	10.19	Not Defined	26
76	Regulatory risk	2.87	3.69	11.14	11.14	H	25
75	Product quality risk	1.75	3.53	6.17	6.17	Not Defined	24
74	Unemployment and social unrest	3.03	3.75	11.36	11.36	Not Defined	23
73	Scarce resources	1.75	3.37	5.89	5.89	Not Defined	22
72	Political risk	3.72	4.09	15.21	15.21	Not Defined	21
71	Micro economic emerging risk	3.20	3.70	11.84	11.84	Not Defined	20
70	Financial crisis	3.71	3.60	13.35	13.35	Not Defined	19
69	Lone attacker	2.19	3.00	6.32	6.32	Not Defined	18
68	Skills risk	3.27	3.80	12.42	12.42	Not Defined	17
67	Leadership risk	3.87	3.70	15.37	15.37	Not Defined	16
66	Lack of innovation	3.73	2.85	10.63	10.63	Not Defined	15
65	Labour risk	3.70	3.65	13.50	13.50	Not Defined	14
64	IT systems outages	1.94	4.72	9.15	9.15	Not Defined	13
63	Impact of new technology	1.88	3.30	6.20	6.20	Not Defined	12
62	Energy uncertainty	2.60	3.91	10.16	10.16	Not Defined	11
61	Financial system weakness	2.06	3.24	7.13	7.13	H	8
60	Health and safety risk	1.67	4.83	8.05	8.05	Not Defined	7
59	Exchange rate volatility	2.23	3.70	8.25	8.25	Not Defined	6
58	Technology innovation and disruption	2.41	3.05	7.35	7.35	Not Defined	5
57	Disease outbreaks and pandemic	1.72	3.26	5.59	5.59	Not Defined	4
56	Cyber attack and data breach	2.80	4.22	11.81	11.81	Not Defined	3
55	Infrastuctue failure	2.91	3.52	10.24	10.24	Not Defined	2
54	Climate, weather and natural disaster	2.41	3.75	9.03	9.03	Not Defined	1

Figure 8.15: Risk Assessment

Relevance (V2.1) is derived from the average risk scores associated with V1.1 and V1.2. Significance is assigned based on expert judgement. The parameters for Significance can be based on any scale defined by the organisation and may be additionally classified in reference data with an associative construct against this field for further extensivity and flexibility in the model.

Weighting is an additional parameter that may be assigned to calculate a weighted risk score adjustment. This has not been added in this result as there is no quantitative expert judgement data. Future work would assess this in the context of a more specific survey for an organisation population (per country, province or region). It has however, been included in the Systems Conceptual Model as a placeholder for completeness. Expert judgement may also be applied by analysing the narratives contained in the reports.

Finally, key Risk Indicators are assigned to the risk description. There may be many Key Risk Indicators per Risk and these would be included as additional records in the RSK_ASMT (Risk Assessment) table in the database. An associative data

construct to KRI classifications is a useful method to reduce complexity for larger data sets.

8.5.4 Validation

The calculation of the DC(n) variable has been validated using an Excel model for the database result and includes one additional Risk Description i.e., Regulatory Risk. Both Risk Descriptions are highlighted in figure 8.10. Validations are shown in figures 8.16 and 8.17.

Result Validation 1 - Financial System Weakness

Entry into the Risk Assessment = Financial System Weakness											
$DC_{(8)}$ = 25:14:12,86:H											
ETH_RSLT = $V1,1_{(8)}$ = 8									Key Risk Indicator	Expected Loss (loan book)	
RSK_TAX_ID = $V1.2_{(8)}$ = 8									REL = $V2.1_{(8)}$ = 7,13	SIG - $V2.2_{(8)}$ = H	
$V1_{(8)}$ = 8:8									$V2_{(8)}$ = 7,11:H	influenced by COVID-19	
Kewords: laws, regulations, legislation, governance										Higher expected losses	
ID	RPT_YR	ETH_RSLT	RSK_TAX_ID	ETH_RSK_CAT	DIS_CNC	PROB	IMP	RSK_SC	APPL_YR	DIS_OUT_TM	ORG
11	2016	8	8	Enduring financial system weakness	0,19	-	-	-	2017	Next 12 Months	BCI
105	2017	8	8	Availability/cost of credit or finance	0,02	-	-	-	2016	Disruption Experienced Past 12 Months	BCI
106	2017	8	8	Availability/cost of credit or finance	0,05	-	-	-	2016	Disruption Concern Past 12 Months	BCI
107	2017	8	8	Enduring financial system weakness (e.g. lack of credit)	0,16	-	-	-	2017	Next 12 Months	BCI
203	2018	8	8	Availability/cost of credit or finance	0,01	-	-	-	2017	Disruption Experienced Past 12 Months	
204	2018	8	8	Availability/cost of credit or finance	0,02	-	-	-	2017	Disruption Concern Past 12 Months	BCI
205	2018	8	8	Enduring financial system weakness (e.g. lack of credit)	0,11	-	-	-	2018	Next 12 Months	BCI
206	2018	8	8	Capital availability (credit risk)	-	4,00	3,67	14,67	2018	Next 18 Months	IRMSA
300	2019	8	8	Higher cost of borrowing	-	2,10	1,48	3,11	2019	Next 12 Months	BCI
301	2019	8	8	Higher cost of borrowing	-	4,63	2,02	9,35	2018	Past 12 Months	BCI
302	2019	8	8	Capital availability (credit risk)	-	2,20	1,92	4,22	2019		IRMSA
359	2020	8	8	Higher cost of borrowing	-	1,90	1,40	2,66	2020	Next 12 Months	BCI
360	2020	8	8	Higher cost of borrowing	-	4,60	1,90	8,74	2019	Past 12 Months	BCI
Average						3,24	2,06	7,13			

Figure 8.16: Result Validations: Result 1: Financial System Weakness

Result Validation 2 - Regulatory Risk

Entry into the Risk Assessment = Regulatory Risk

$DC_{(24)}$ = 25:14:12,86:H

ETH_RSLT = $V1,1_{(24)}$ = 25
RSK_TAX_ID = $V1.2_{(24)}$ = 14
$V1_{(24)}$ = 25:14
Keywords: laws, regulations, legislation, governance

Key Risk Indicator
REL = $V2.1_{(24)}$ = 11,14
$V2_{(24)}$ = 11,14:H

Legislation changes in the period/year
SIG - $V2.2_{(24)}$ = H
influenced by COVID-19
(basel release of extraordinary measures)
https://www.bis.org/bcbs/publ/d498.pdf

ID	RPT_YR	ETH_RSLT	RSK_TAX_ID	ETH_RSK_CAT	DIS_CNC	PROB	IMP	RSK_SC	APPL_YR	DIS_OUT_TM	ORG
57	2016	25	14	New regulations and increased regulatory scrutiny	0,55	-	-	-	2017	Next 12 Months	BCI
58	2016	25	14	Regulatory / legislative changes	-	-	-	20,00	2016, 2017 (18 Months)	Next 18 Months	IRMSA
59	2016	25	14	Regulatory / legislative changes	-	-	-	25,00	2016 - 2026 (10 years)	Next 10 Years	IRMSA
60	2016	25	14	Regulatory / legislative changes	-	3,88	4,11	15,95	2015	Past 12 Months	IRMSA
61	2016	25	14	Global governance failures	0,24	-	-	-	2017	Next 12 Months	BCI
62	2016	25	14	Governance failure	-	-	-	25,00	2016, 2017 (18 Months)	Next 18 Months	IRMSA
63	2016	25	14	Governance failure	-	-	-	16,00	2016 - 2026 (10 years)	Next 10 Years	IRMSA
64	2016	25	14	Governance failure	-	4,20	3,82	16,04	2015	Past 12 Months	IRMSA
143	2017	25	14	New laws or regulations	0,14	-	-	-	2016	Disruption Experienced Past 12 Months	BCI
144	2017	25	14	New laws or regulations	0,13	-	-	-	2016	Disruption Concern Past 12 Months	BCI
145	2017	25	14	New regulations and increased regulatory scrutiny	0,46	-	-	-	2017	Next 12 Months	BCI
146	2017	25	14	Regulatory / legislative changes	-	3,64	3,51	12,78	2016	Past 12 Months	IRMSA
147	2017	25	14	Global governance failures (e.g. intellectual property regimes, trade regulations, geopoloitical risks)	0,18	-	-	-	2017	Next 12 Months	BCI
148	2017	25	14	Governance failure	-	4,09	3,79	15,50	2016	Past 12 Months	IRMSA
243	2018	25	14	New laws or regulations	0,16	-	-	-	2017	Disruption Experienced Past 12 Months	
244	2018	25	14	New laws or regulations	0,12	-	-	-	2017	Disruption Concern Past 12 Months	BCI
245	2018	25	14	New regulations and increased regulatory scrutiny	0,49	-	-	-	2018	Next 12 Months	BCI
246	2018	25	14	Government policy, legislation and regulatory changes (uncertainty)	-	4,33	4,33	18,75	2018	Next 18 Months	IRMSA
247	2018	25	14	Global governance failures (e.g. intellectual property regimes, trade regulations, geopoloitical risks)	0,19	-	-	-	2018	Next 12 Months	BCI
248	2018	25	14	Failure of governance (private and public)	-	4,50	4,50	20,25	2018	Next 18 Months	IRMSA
330	2019	25	14	Regulatory changes	-	2,95	1,63	4,81	2019	Next 12 Months	BCI
331	2019	25	14	Regulatory changes	-	4,58	2,06	9,43	2018	Past 12 Months	BCI
332	2019	25	14	Government policy, legislation and regulatory changes (uncertainty)	-	3,10	1,92	5,95	2019		IRMSA
385	2020	25	14	Regulatory changes	-	2,60	1,70	4,40	2020	Next 12 Months	BCI
386	2020	25	14	Enforcement by regulator	-	2,10	1,70	3,60	2020	Next 12 Months	BCI
387	2020	25	14	Regulatory changes	-	4,30	2,10	8,80	2019	Past 12 Months	BCI
388	2020	25	14	Enforcement by regulator	-	3,90	2,20	8,50	2019	Past 12 Months	BCI
389	2020	25	14	Changes in legislation and regulations	-	-	-	-	2020	Top risks identified with risk treatment	IRMSA
390	2020	25	14	Ill-conceived NHI (national health institute policy and/or sub-optimal implementation)	-	-	-	-	2020	Top risks identified with risk treatment	IRMSA
391	2020	25	14	Ill-conceived land reform policy and/or sub-optimal implementation	-	-	-	-	2020	Top risks identified with risk treatment	IRMSA
392	2020	25	14	Continuing private and public governance failures	-	-	-	-	2020	Top risks identified with risk treatment	IRMSA
Average						3,69	2,87	11,14			

Figure 8.17: Result Validations: Result 2: Regulatory Risk

Calculated results correlate well with the data results obtained in the system within a 3 percent variance (data profiles have been included in the appendix). The database results are integrated into the respective Business Impact Assessments for the two risks tested and are shown in figures 8.18 and 8.19 respectively.

8.5.5 Integrated BCMS Systems Result

According to the ISO22301 Standard, the Business Impact Analysis is a "formal and documented process for business impact analysis and risk assessment" that identifies "the potential impact" of disruptive incidents and prescribes the required considerations to meet the standards of recovery. This includes "risk treatments and their related costs" and other legal and regulatory requirements [3].

The organisational system (in this case the banking system) includes the data for the prescribed regulatory Key Risk Indicator(Expected Loss), which has been included in Result 1 (figure 8.18). By calculating the expected loss, the cost associated with an increasing risk and further identified impacts can be assigned. Similarly Key Risk indicators may be added to Result 2 which would indicate the volatility of regulatory change. It is also noted that there is no fixed limitation on the number of Key Risk Indicators that could be assigned to a specific risk type associated with the relevant Business Impact Analysis.

Several other Credit Key Risk Metrics can also be calculated and associated with the lending data from banking operations and associated to key risks and potential impacts shown in figure 8.20. For instance in the case of the COVID-19 pandemic, arrears data became significantly important both from a macro and micro economic perspective. Banks needed to respond in conjunction with the Reserve bank to ease interest rates and respond to the customer needs to meet their loan obligations. Reflecting this on the Business Impact Analysis with its associated Key Risk Indicators and associated costs provides an opportunity to include this holistically with other impacts and associated costs to meet the measures that need to be implemented to respond effectively to the losses incurred.

In this example, the dimensions of arrears, interest rates, losses in annual income and the loan status become important to monitor in relation to the risk description (disease outbreak and pandemic). Expected losses calculated based on the status of the loan book, provide a means for the bank to adequately provision for the impairments of these loans.

What this shows is that risks are complex and interrelated, and require systemic network analysis to be more accurate. However, with an integrated system dashboard that brings all the related data into a single data warehouse. This provides several opportunities for inferential modelling of the results.

The Data Context Variable is extensible and can contain several named values in a single matrix (preferable) or alternatively stored parameter strings to alert the interested parties of changes that become material to operations.

BUSINESS IMPACT ANALYSIS (Business Continuity L(0))

Identifier	Description
1	Business Impact Analysis for Credit Risk including accounts in arrears and potential default

RISK ASSESSMENT - Financial Use Case (Business Continuity

ID	Risk Description	Impact	Probability	Risk Score	V2.1 (Relevance)	V2.2 (Significance)	V1.1 Ethnograpgic Result	KRI
61	Financial system weakness	2.06	3.24	7.13	7.13	H	8	Expected Loss

BUSINESS IMPACTS (Business Continuity L(0))

Identifier	Category	Impact	MTPD (Impact Threshold)	MBCO	RTO	RPO	Risk Identifier	Process
7	Environment impact	2 Admin/Data Processing	0% Staff Loss	1 Staff	0.5 Day	Scenario Assumption	8	3
6	Service impact	2 Credit Risk Managers	0% Staff Loss	2 Staff	0.5 Day	Scenario Assumption	8	3
4	Reputation impact	Increased Capital Required	10.5% Capital Adquacy Ratio	8% Capital Adequacy Ratio	1 Month	Minimum Regulatory Requirement	8	2
3	Regulatory impact	Increased Risk Exposure	5% Expected Loss	7% Expected Loss	1 Month	Minimum Regulatory Requirement	8	2
1	Staff impact	Non-compliant BCBS239 Principles	100% Compliant	95% Compliant	1 Day	Scenario Assumption	8	2
2	Public impact	Reputational Damage	75%-100%	5% Reduction in applications	1 Day	Scenario Assumption	8	2
5	Financial impact	Sales Service Interruption	85%	80%	0.5 Day	Scenario Assumption	8	1

IMPACT REQUIREMENTS (Resource Items (L0))

Process	Supplier Service	Supplier Name (Party (L0)))
1	Not Required	Simulation Name
2	Legal Services	Simulation Name
3	Recruitment Services	Simulation Name

Process	Systems Requirement
1	Not Required
3	HR System
2	Credit Management System

Process	Resource Requirement
3	4 Additional Staff
2	Communications Plan, Capital Adequacy, Documented Regulatory Measures
1	None

Process	Technology Requirement
1	Loan IT System
2	Finance IT System
3	HR IT System

PROCESS/ACTIVITY - Impacted Processes (Business Continuity (L0))

Process	Process Name	Activity Description
2	Approval	Approval by Decision Makers
3	Implementation on the Credit Decision	Check Compliance with Authority Structure
2	Documentation	Complete Loan Application
1	Collect and Review Data	Completeness/Plausability Review
1	Acquisition/Credit Specific Customer Service	Customer Meeting
1	Acquisition/Credit Specific Customer Service	Debriefing
2	Collateral and Risk Assessment	Determine loan-to-value
3	Implementation on the Credit Decision	Disbursement
3	Implementation on the Credit Decision	Disbursement Review
2	Credit Review	Documentation and Other Related Factors
1	Acquisition/Credit Specific Customer Service	Establishing Contact
2	Collateral and Risk Assessment	Evaluate Exposure
1	Acquisition/Credit Specific Customer Service	Evaluate First Customer Information
1	Collect and Review Data	Follow-up
2	Approval	Follow-up

Note: Processes and Activities for business critical functions can be modelled into data terms (these can be visualised and associated on the BIA). Detailed activities have their own BCM Measures i.e. MBCO, MTPD, RPO and RTO. This level of visualisation would represent an aggregation of these. This has not been included in thisuse case, however the model has been constructed using this principle.

Figure 8.18: Systems Integration Business Impact Analysis: Result 1: Financial System Weakness

BUSINESS IMPACT ANALYSIS (Business Continuity L(0))

Identifier	Description
1	Business Impact Analysis for Credit Risk including accounts in arrears and potential default

RISK ASSESSMENT - Financial Use Case (Business Continuity

ID	Risk Description	Impact	Probability	Risk Score	V2.1 (Relevance)	V2.2 (Significance)	V1.1 Ethnograpgic Result	KRI
76	Regulatory risk	2.87	3.69	11.14	11.14	H	25	Legislation changes in the

BUSINESS IMPACTS (Business Continuity L(0))

Identifier	Category	Impact	MTPD (Impact Threshold)	MBCO	RTO	RPO	Risk Identifier	Process
7	Environment impact	2 Admin/Data Processing	0% Staff Loss	1 Staff	0.5 Day	Scenario Assumption	8	3
6	Service impact	2 Credit Risk Managers	0% Staff Loss	2 Staff	0.5 Day	Scenario Assumption	8	3
4	Reputation impact	Increased Capital Required	10.5% Capital Adquacy Ratio	8% Capital Adequacy Ratio	1 Month	Minimum Regulatory Requirement	8	2
3	Regulatory impact	Increased Risk Exposure	5% Expected Loss	7% Expected Loss	1 Month	Minimum Regulatory Requirement	8	2
1	Staff impact	Non-compliant BCBS239 Principles	100% Compliant	95% Compliant	1 Day	Scenario Assumption	8	2
2	Public impact	Reputational Damage	75%-100%	5% Reduction in applications	1 Day	Scenario Assumption	8	2
5	Financial impact	Sales Service Interruption	85%	80%	0.5 Day	Scenario Assumption	8	1

IMPACT REQUIREMENTS (Resource Items (L0))

Process	Supplier Service	Supplier Name (Party (L0)))
1	Not Required	Simulation Name
2	Legal Services	Simulation Name
3	Recruitment Services	Simulation Name

Process	Systems Requirement
1	Not Required
3	HR System
2	Credit Management System

Process	Resource Requirement
3	4 Additional Staff
2	Communications Plan, Capital Adequacy, Documented Regulatory Measures
1	None

Process	Technology Requirement
1	Loan IT System
2	Finance IT System
3	HR IT System

PROCESS/ACTIVITY - Impacted Processes (Business Continuity (L0))

Process	Process Name	Activity Description
2	Approval	Approval by Decision Makers
3	Implementation on the Credit Decision	Check Compliance with Authority Structure
2	Documentation	Complete Loan Application
1	Collect and Review Data	Completeness/Plausability Review
1	Acquisition/Credit Specific Customer Service	Customer Meeting
1	Acquisition/Credit Specific Customer Service	Debriefing
2	Collateral and Risk Assessment	Determine loan-to-value
3	Implementation on the Credit Decision	Disbursement
3	Implementation on the Credit Decision	Disbursement Review
2	Credit Review	Documentation and Other Related Factors
1	Acquisition/Credit Specific Customer Service	Establishing Contact
2	Collateral and Risk Assessment	Evaluate Exposure
1	Acquisition/Credit Specific Customer Service	Evaluate First Customer Information
1	Collect and Review Data	Follow-up
2	Approval	Follow-up

Note: Processes and Activities for business critical functions can be modelled into data terms (these can be visualised and associated on the BIA). Detailed activities have their own BCM Measures i.e. MBCO, MTPD, RPO and RTO. This level of visualisation would represent an aggregation of these. This has not been included in thisuse case, however the model has been constructed using this principle.

Figure 8.19: Systems Integration Business Impact Analysis: Result 2: Regulatory Risk

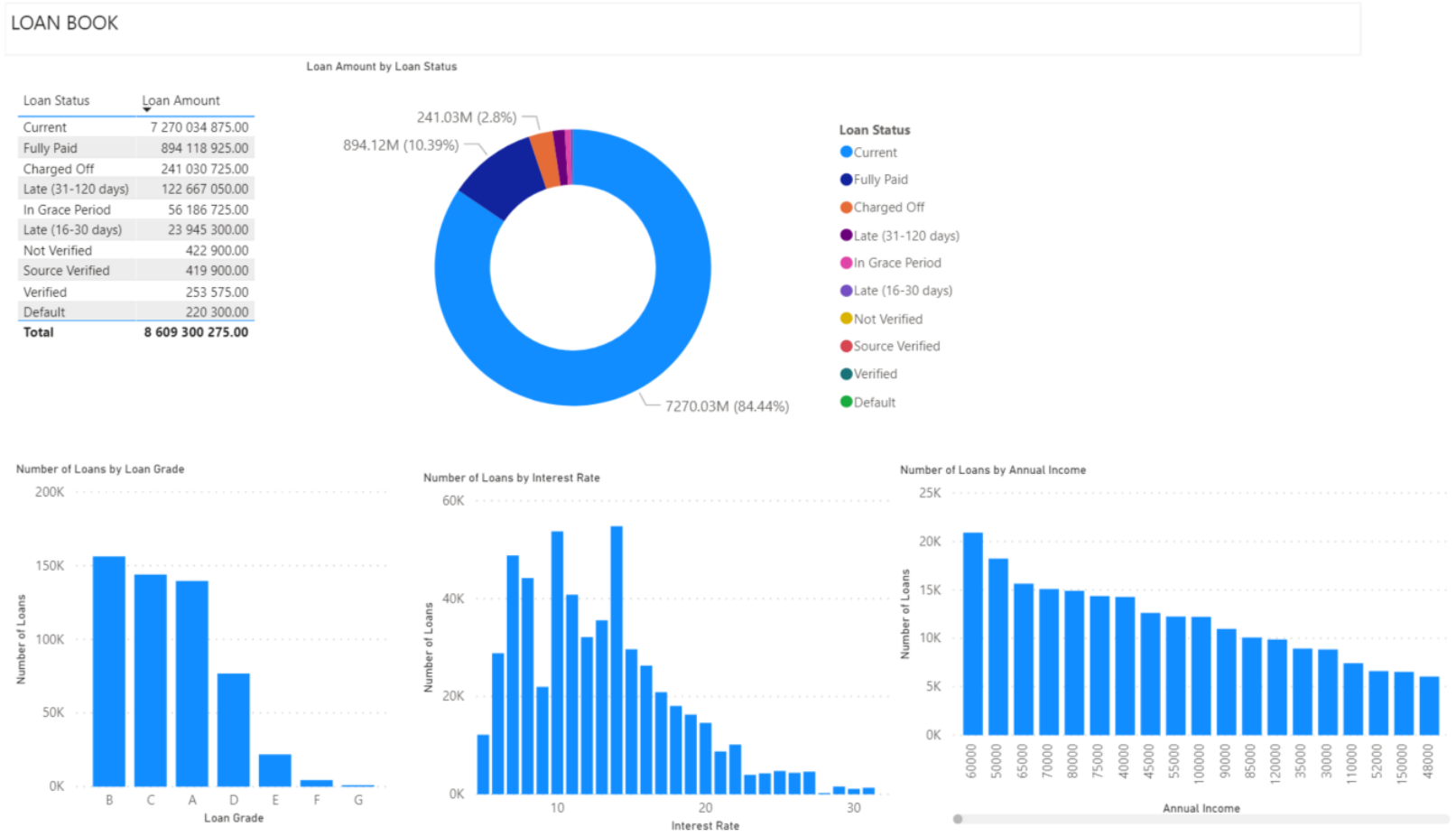


Figure 8.20: Banking Systems Data - Risk Data Mart

8.5.6 Business Continuity Strategy

For this illustrative result, the Basel committee has prescribed the necessary risk treatments with regulatory tolerance. That said, it is important to note that the addition of other risk treatments identified, these should be documented into the Corresponding Incident Response Structure. This table has been modelled with a foreign key that associates the incident response structure to a specified Business Impact Analysis Identifier.

8.5.7 Results Conclusion

The analysis described in this section illustrates the derivation of a contextualisation variable as proposed in this report. It is shown that an integrated systems based approach can be used to derive the necessary data to inform business resilience in the Business Continuity Management System.

The benefits of this approach is the ability to identify early risk warning with data sets that are operationally linked to the process of risk assessment and business impact analysis. This allows for rapid adjustment to changes in the risk landscape and pro-active anticipation of risk events. In addition to this it makes inferential modelling possible where effects of a risk landscape change can be analysed against changes in Key Risk Indicators for enhanced insight. The information seeking process is simplified through association to categorised authoritative sources of data external to the organisation. Finally, risk trend analysis becomes possible in the system of insight through historical data records stored in a time sensitive data mart.

8.5.8 Other Considerations

The proposed approach is generic and applicable to any industry system and risk landscape through the modification of industry reference model and core systems. These may be simple or complex in nature. It must however be noted that although the analysis method applies equally to many systems, it is important to consider the system of interest in the extension of the model and scaling up of complexity.

It is also important to identify the risk measurement method and standardise as complexity in this measurement can result in risk contextualisation sensitivity that may compromise the system of insight.

The systems approach does not eliminate expert judgement but is rather an enhancement to this process and the human factor is an important advantage to the systems approach. Also the system does not include organisational resilience factors which through clear risk and business continuity culture would be an advantage. Many parts of this analysis can be fully automated and additional intelligence and learning added (artificial intelligence and machine learning algorithms) which with careful implementation, provide an opportunity for Business Continuity and Resilience professionals to remain experts in the field without the overhead of data analysis, a current inhibitor according to the BCI Horizon Scan Report 2020 [1].

9

Conclusion

9.1 Summary

This report introduced dynamic data contextualisation by applying an integrated analytical data modelling and systems design approach. It was shown that contextualisation can be derived and captured into a variable represented by a name value pair that represent the categorisation, standardisation, significance and relevance of risk as it emerges on the risk horizon.

The investigation and subsequent modelling also showed that by including these variables into an additional integrated system component, a data driven approach to the risk assessment and business impact analysis becomes possible. The variable can either be applied directly in the business continuity management system itself through extending current data models for these systems or through data visualisation running alongside these systems in the analytical model described in this report. A point to note is that an ISO compliance BCMS currently do not explicitly include data as a clause, but implies its importance in clause 4, which is applied to ensure that organisations are aware of their operating context when performing risk assessment and subsequent business impact analysis.

The proposition of this report is that by including data and information as part of the system, there is an opportunity to inform organisational resilience. The availability of high value accurate data to inform business continuity strategy is one method in which this can be achieved. However if data is not representative of the operating context (clause 4) it may compromise compliance to the standard and may also yield incorrect results and deductions. Therefore the derivation of the contextualisation variable needs to be standardised. This is achieved by mapping emerging risks to a standard taxonomy which is defined and agreed.

The standardisation of the taxonomy of the system is contained in two system components i.e. the reference data and metadata of the analytical model design which are described in the list below:

1. **Reference Data**: Risk Type Classification against a taxonomy as a data source.

2. **Industry specific Reference Data Model**: for financial services which is based on the IBM Banking Data Model.

Operating context considers the risk horizon which is designed based on the resilience framework represented in figure 5.1 and applies horizon scanning and information seeking as a basis on which to define its data sources for system validation.

By applying standardisation and modelling, a dynamic data contextualisation is possible to define and apply to an analysis of risk data mapped to key risk indicator(s).

Steps in the process of derivation are summarised below:

1. Selecting of the risk scoring method and the authoritative source(s) of risk data.

2. Modelling the business operation in data terms in an enterprise data model. The first step in standardisation can also make use of industry standard data models as a reference.

3. Selection of a risk taxonomy as an authoritative reference data source.

4. Categorisation of risks according to their definitions if provided by multiple risk data sources. In this report ethnographic study was used to categorise risks.

5. Mapping of the risk category to the risk taxonomy. This provides the rules to be applied to all subsequent and future risk data sources such that these data sets can be standardised to provide comparable results and trend analysis over time.

6. Using unique identifiers, the risk category and taxonomy results can be represented in two variables; V1.1 = unique identifier of the risk category and V1.2 = taxonomy mapping identifier. If there are sub categories, these values can be linked in their respective reference data structures as associated values.

7. The results of V1.1 and V1.2 are assigned to the Key Risk Indicators that are influenced by these risk categories. These relationships are represented as an association.

8. Within the context of categorisation of V1.1 and V1.2 a risk score is derived by applying an average across the risk records in aggregation. This average is represented as a result in variable V2.1 and indicates the relevance of the risk.

9. Within the context of categorisation of V1.1 and V1.2 risk significance is derived through expert judgement, the scale of which can be defined. In this report, a three value scale has been applied to simulate the result as high, medium or low. The result of this is represented as a result in variable V2.2.

Contextualisation as a result is represented in name value pairs that consists of all four variables as follows:

$$DC_{(n)} = V1.1_{(n)} : V1.2_{(n)} : V2.1_{(n)} : V2.2_{(n)} \tag{9.1}$$

Risk contextualisation variables are stored within the BCMS data model as part of the risk assessment and are assigned to Key Risk Indicators by association.

Simulation of this system is performed in this report using sources of horizon scan data across two industry sources and linked to financial services key risk indicators. Financial services data was also simulated by loading a sample of open source data into the banking data warehouse model. Through the process of data modelling against the industry reference model, business continuity management system analytical data could be included as part of the strategic constructs.

The loading of sources of identified data yielded expected results in the system which could be subsequently visualised in an integrated fashion and also provides evidence of the system in operation.

Quantitative and mathematical models and applied qualitative approaches used to measure resilience in previous research cite future work as the ability to further quantify risk relevance and significance either retrospectively based on losses measured over the period of a disruption or through summation of key system indicator performance.

The addition of the data contextualisation variable in association with key system indicator performance in these resilience calculation methods, provides an additional operating context reference point on which to assess key system indicator performance against emerging risk. The business impact analysis provides an association to the business process and system components and is included in the results of this report to illustrate the data contextualisation variable within the Business Continuity Management Framework as a purposeful activity system.

The method proposed is shown to have the ability to provide additional context to any resilience calculation particularly by providing a quantitative standardised result for risk significance and relevance.

9.2 Conclusion

In this report, the problem of contextualising data of emerging risk in the operating context of an organisation was addressed.

A model to contextualise the data in the environment (horizon) scan component of the resilience framework provided a starting point that enhances the functioning of business continuity management systems' use of data. It has been shown that the data contextualisation variable result of named value pairs has extensible potential to include further parameters and value pairs as and when they are identified (for example, risk significance weighting).

The data model investigated is shown as industry specific to financial services, but that through the process of maintaining a reference point to an industry model and standardisation through reference data (risk taxonomy), the contextualisation model could be extended to many industries and their operations.

The main focus of this report was by using a systems approach, data and information could be applied to inform business continuity strategy within the Business Continuity Management System at the point at which risk assessment and business impact analysis are performed. It is in these activities that resilience measurement parameters are defined. A new approach based on standardisation and integrated modelling of an analytical system was introduced as an enhancement to resilience measurement methods in which a resilience measurement may be associated through a key system performance indicator to changes in operating context. For this report, a particular focus on emerging risk was applied.

Validation of the system approach used data captured in technical reports and surveys to simulate the system operation and proved that this data could be visualised as an integral component of the business impact analysis and in so doing provides information that could be captured as a foundation for the business continuity management strategy.

9.3 Future Work

The standardisation applied to the systems method in this report provides a number of opportunities for future work which are highlighted as follows:

1. The enhancement of the data model into a more inclusive standard providing a representation of the system's at scale with the flexibility to include various applications and use cases.

2. Work to increase the understanding of the dynamics of risk measurement methods to derive more accurate risk scoring results. Future work to develop a framework for risk measurement standardisation would further enhance the

performance of the proposed analytical model by allowing for a more inclusive result across data sources that use different approaches.

3. An investigation to address the most optimal measurement of risk relevance could also provide a better understanding of the sensitivity of the system to expert judgement. The addition of a quantitative approach to relevance would provide a reference point either on which to base a relevance decision or alternatively to validate a decision. This includes organisational resilience as an area for future work.

4. The overall foundation provided in this report opens the possibility for future data science work including inferential modelling to address the correlations of environment risk dynamics to key risk indicators.

10

Appendix

Each of the sections of this appendix provide more detail in terms of the standard methods adopted for the development of the system. In addition, the technical details and definitions of the system design have been included.

Appendix Section 10.1 is referenced in Section 6.8 that refers to the Systems Engineering Master Plan (Checkland's Soft System Methodology Stage 7). This section provides the details of the ISO/IEC/IEEE standard and how this has been adopted in the work. It also provides further details of the steps adopted in the development of the system along with a detailed checklist of completion criteria for each step.

Appendix Section 10.2 provides details of the approach to standardise physical database field names. These are applied in the definition of the physical data model as well as in the database scripting (Appendix Section 10.4) used to create and load the relevant data into these tables. Appendix Section 10.2 is referenced in Section 8.3 and translates the logical models defined in Section 8.2 into physical models. Data types are further standardised in support of the type of data and its data profile.

Appendix Section 10.3 is referenced in Section 8.3 and provides details of the Entity to Table mapping and Attribute to Column mapping which is a translation of the logical to physical data model. In addition, detailed field definitions are provided along with the applied data type and naming standards (Appendix Section 10.2). Where business rules have been applied and stored within the model, this is provided as part of the entity and attribute definition.

10.1 Systems Engineering Management Plan

Table 10.1: Systems Engineering Management Plan (SEMP) aligned to clauses in the ISO/IEC/IEEE 247-1:2018 Standard. Details of Clauses have been included for completeness.

Clause	Clause Statement	Stage	Section	Checklist
5.2		**Concept**		
5.2.1	"The Concept Stage begins with initial recognition of a need or a requirement for a new system-of-interest or for the modification to an existing system-of-interest. This is an initial exploration, fact finding and planning period when economic technical, strategic and market bases are asses through acquirer/market survey, business or mission analysis, solution space identification, and feasibility analysis and trade off studies. Acquirer/user feedback to the concept is obtained."		**Overview**	a. Documentation and approval of the research proposal.
5.2.2	"The Concept Stage is executed to assess new business opportunities or mission assignments and to develop preliminary system requirements and a feasible architecture and design solution."		**Purpose**	a. Qualitative research by literature review. b. Checkland 7 step method (research proposal method applied)

Clause	Clause Statement	Stage	Section	Checklist
5.2		**Concept**		
5.2.3	"a) An assessment of feasible system-of-interest concepts, with initial architectural and other solutions, including enabling systems throughout the life cycle, for closure against both technical and business or mission stakeholder objectives. b) The preparation and baselining of stakeholder requirements and preliminary system requirements (technical specifications for the selected system-of-interest and usability specifications for the envisaged human-machine interaction).c) Refinement of the outcomes and cost estimates for stages of the system life cycle model. d) Risk identification, assessment and mitigation plans for this and subsequent stages of system life cycle model. e) Identification and initial specification of the services needed from enabling systems throughout the life of the system. f) Concepts for execution of all succeeding stages. g) Definition of the enabling system services required in subsequent life cycle stages. h) Project budget and schedule baselines and life cycle ownership cost estimates. i) Satisfaction of stage exit criteria.j) Approval to proceed to the appropriate stage or stages, based on the specific life cycle model in use by the project."		**Outcomes**	a. Documented background and context. b. Definition of applicable standards and guidelines. c. Documented literature review. d. Define research method. e. Document SEMP. f. Obtain ethics clearance. g. Industry peer review. h. Research proposal presentation.

Clause	Clause Statement	Stage	Section	Checklist
5.3		**Development**		
5.3.1	"The Development Stage begins with sufficiently detailed technical refinement of the system requirements, system architecture, and the design solution and transforms these into one or more feasible products that enable one or more services during the Utilisation Stage. The system-of-interest may be a prototype in this stage. The hardware, software, operator, process and facility interfaces are specified, designed, fabricated, integrated, tested and evaluated as applicable and the requirements for production, training and support facilities , and transitions are defined."		**Overview**	a. Develop MVP experiment evaluation loop.
5.3.2	"The Development Stage is executed to develop a system-of-interest that meets stakeholder requirements and can produced, tested, evaluated, operated, supported and retired."		**Purpose**	a. Develop a prototype solution."

Clause	Clause Statement	Stage	Section	Checklist
5.3.3	"a) Plans and exit criteria for the development stage. b) Architectural and design artefacts for the system of interest. c) A system-of-interest structure comprised of, for example, hardware elements, software elements, human elements, process elements, facility elements and the interfaces (internal and external) of all such elements. d) Verification and validation documentation. e) Transition planning documentation. f) Evidence supporting a decision, with all risks and benefits considered, that the system-of-interest meets all specified requirements and is producible, operable, supportable and capable of retirement and is cost-effective for stakeholders. g) Refined and base lined requirements for the enabling systems, along with methods and tools for establishing and maintaining traceability between requirements and the developed system. h) A prototype or final system-of-interest. i) Refined outcomes and cost estimates for the Production, Utilisation, Support and Retirement Stages. j) Identification of current risks and determination of their treatment. k) Satisfaction of stage exit criteria. l) Approval to proceed to the appropriate stage or stages based on the specific life cycle model in use by the project."		**Outcomes**	a. Develop a system architecture b. Develop a prototype physical data constructs. c. Definition and development of a prototype analytical model. d. Conduct qualitative verification.

Clause 5.4	**Clause Statement**	**Stage** **Production**	**Section**	**Checklist**
5.4.1	"The Production Stage begins with the approval to produce the system-of-interest. The system-of-interest may be individually produced, assembled, integrated and tested, as appropriate, or may be mass-produced. Planning for this stage begins in the preceding stage. Production may continue throughout the remainder of the system life cycle. During this stage, the system may undergo enhancements, re-designs, the enabling systems may need to be re-configured, and production staff re-trained, in order to continue evolving cost-effective services from a stakeholder view."		**Overview**	a. Develop MVP experiment and validation loop.
5.4.2	"The Production Stage is executed to produce or manufacture the system-of-interest, test it and produce related enabling systems as needed."		**Purpose**	a. Develop MVP system solution.

Clause	Clause Statement	Stage	Section	Checklist
5.4.3	"a) Plans and exit criteria for the Production Stage. b) Qualification of the production capability. c) Acquisition of resources, material, services and system elements to support the target production quantity goals.d) The system produced according to approved and qualified production information. e) Packaged product transfer to distribution channels or acquirer. f) Updated concepts for execution of all succeeding stages. g) Current risks and mitigating actions identified. h) Quality assured systems-of-interest accepted by the acquirer. i) Satisfaction of stage exit criteria. j) Approval to proceed."		**Outcomes**	a. Update the system architecture b. Develop the system physical data constructs. c. Develop the analytical model. d. Conduct quantitative verification.

Clause 5.5	**Clause Statement**	**Stage** **Utilisation**	**Section**	**Checklist**
5.5.1	"The Utilisation Stage begins after installation and transition to use of the system. The Utilisation Stage is executed to operate the product at the intended operational sites to deliver the required services with continuing operational and cost effectiveness. This stage ends when the system of interest is taken out of service."		**Overview**	a. Validate MVP against the real world.
5.5.2	"The Utilisation Stage is executed to operate the product, to deliver services within intended environments and and help achieve continuing operational effectiveness."		**Purpose**	a. Test the solution against two case studies.
5.5.3	"a) Plans and exit criteria for the Utilisation Stage. b) Experienced personnel with the competence to be operators in the system-of-interest and provide operational services. c) An installed system-of-interest that is capable of being operated and of providing sustainable operational services. d) Performance and cost monitoring and assessment to confirm conformance to service objectives. e) New opportunities for system-of-interest enhancement through stakeholder feedback. f) Current risks and mitigation actions identified. g) Satisfaction of stage exit criteria. h) Approval to proceed to the appropriate stage or stages, based on the specific life cycle model in use by the project."		**Outcomes**	a. Update the system architecture. b. Simulate results against case study data.

Clause 5.6	**Clause Statement**	**Stage** **Support**	**Section**	**Checklist**
5.6.1	"The Support Stage begins with the provision of maintenance, logistics and other support for the system-of-interest's operation and use. Planning for this stage begins in the preceding stages. The Support stage is completed with the retirement of the system of interest and termination of support services."		**Overview**	This stage will not be required in this project.
5.6.2	"The support stage is executed to provide logistics, maintenance, and support services that enable continuing system of interest operation and sustainable service."		**Purpose**	
5.6.3	"a) Plans and exit criteria for the support stage. b) Trained personnel who will maintain the system and provide the support services. c) Organisational and enabling system interfaces for problem resolution and corrective actions. d) Maintained product and services and the provision of all related support services, including logistics, to the operational sites. e) Identification of problems or deficiencies, informing appropriate parties (user, development, production, or support) of the need for corrective action."		**Outcomes**	

Clause 5.6/5.7	**Clause Statement**	**Stage** **Retirement**	**Section**	**Checklist**
5.6.3	" f) Product and service maintenance and corrected design deficiencies. g) All required logistics support provided, including a spare parts inventory sufficient to satisfy operational availability goals. h) Current risks and mitigating actions identified. i) Satisfaction of stage exit criteria. j) Approval to proceed to the appropriate stage or stages, based on the specific life cycle model in use by the project. Ordinarily, this would be the retirement stage."		**Outcomes**	
5.7.1	" The Retirement Stage provides for the removal of a system-of-interest and related operational and support services, including appropriate disposal of specified system elements. Planning for the retirement stage begins in the preceding stages. This stage begins when the system of interest is taken out of service."		**Overview**	a. Conclusion of the research project.

Clause 5.7	**Clause Statement**	**Stage** **Retirement**	**Section**	**Checklist**
5.7.2	"The Retirement Stage is executed to provide for the removal of a system-of-interest and related operational support services, and to operate and support the retirement system itself."		**Purpose**	a. Submission of final report/dissertation. b. Ethical retirement of the system.
5.7.3	"a) Plans and exit criteria for the Retirement Stage. b) Disposal constraints are provided as inputs to requirements, architecture, design, and implementation. c) Any enabling systems or services needed for disposal are available.d) Agreement to terminate support services. e) Residual risks and mitigating actions identified. f) The system elements or waste products are destroyed, stored, reclaimed or recycled in accordance with safety and security requirements. g) The environment is returned to its original or an agreed state. h) Records of disposal actions and analysis are available. i) Satisfaction of stage exit criteria."		**Outcomes**	a. Documentation of report and findings. b. Peer review. c. Submit

10.2 Physical Data Model Standards

NAMING STANDARDS

The following naming standards have been consistently applied to name physical tables. Where data is staged in the data lake, data types are not cast but are inherited as is from the data source (system of record). Staged data tables utilise the same naming standard, but with a prefix of STAGING for example Environment is Staged as STAGING_ENV.

The physical separators in table names appear as "_" in the database scripting. For example Report Year (RPT YR) = RPT_YR in the database table.

Logical Name	**Physical Name**	**Logical Name**	**Physical Name**
ACT	Activity	ORG	Organisation
APPL	Applicable	OUT	Outlook
ASMT	Assessment	PROB	Probability
BC	Business Continuity	PROC	Process
BIA	Business Impact Analysis	REQ	Required
CAT	Category	RES	Resources
CNC	Concern	RESP	Response
DEF	Definition	Risk	RSK
DEF	Definition	RPT	Report
DEP	Dependency	RSLT	Result
DEPT	Department	SC	Score
DESC	Description	SERV	Services
DIS	Disruption	SRC	Source
DTA	Data	ST	Structure
ETN	Ethnographic	STRAT	Strategy
FM	Frame	SUPP	Supplier
GP	Group	SYS	Systems
ID	Identifier	TAX	Taxonomy
IMP	Impact	TECH	Technology
INC	Incident	TM	Time
NM	Name	YR	Year

DATA TYPE STANDARDS

Data Type	**In Application**
integer	Identifiers and integer values
varchar(100)	Descriptions
decimal(12,4)	Calculation Results in decimal values
char(50)	Names and short descriptors
char(100)	Long Descriptions

10.3 Physical Data Model

Table	Entity (L1)	Column	Attribute	Column Definition	Data Type	Results	System
L0 Organisational Context							
ENV	Environment	ID	Row Identifier	This identifies the row in the table.	integer		I1 - I2, ABCNM
ENV	Environment	RPT YR	Report Year	Indicates the year in which the report was published	integer		I1 - I2, ABCNM
ENV	Environment	ETH RSLT	Ethnographic Result	This is a derived field (result of the data analysis in the research method). This is derived by grouping key words and risk descriptions across multiple risk reports. The risk types standardised and assigned a numeric value. This field is used as an input to the taxonomy mapping. *standardisation value.	integer	V1.1	I1 - I2, ABCNM
ENV	Environment	TAX RSK ID	Taxonomy Identifier	This is the taxonomy Identifier that has been assigned in the mapping to the Taxonomy Identifier in the Environmental scanning Data.	integer	V1.2	I1 - I2, ABCNM
ENV	Environment	ETH RSK CAT	Ethnographic Risk Category	This is the input field upon which an ethnographic result has been derived and assigned a value in the Ethnographic Result Column.	varchar(150)	V0	I1 - I2, ABCNM

Table	Entity (L1)	Column	Attribute	Column Definition	Data Type	Results	System
L0 Organisational Context							
ENV	Environment	DIS CNC	Disruption Concern	This is a survey result where respondents indicated whether they felt that a risk was a concern for them in terms of associated materialised events either in the past or in the future. Expressed as a percentage of total respondent population for the applicable year.	decimal(12,4)		I1 - I2, ABCNM
ENV	Environment	PROB	Probability	This indicates the probability of a future risk arising.	decimal(12,4)		I1 - I2, ABCNM
ENV	Environment	IMP	Impact	Risk Impact which replies either to a disruption (materialised risk) or is an anticipated future impact in the outlook time frame.	decimal(12,4)		I1 - I2, ABCNM
ENV	Environment	RSK SC	Risk Score	The risk score is derived by multiplying the risk and probability. It is noted that in this data set, risk scores are either 25 or 20, depending on the survey response structure.	decimal(12,4)		I1 - I2, ABCNM
ENV	Environment	APPL YR	Applicable Year	This is the year that is applicable to the Horizon Scan and IRMSA Report. For Instance if the report was published in 2019, the applicable year would be 2018 of a 12 month retrospective and 2019 if 12 month outlook. Reports are published in March for reference. This must be read in conjunction with the report outlook f I5ld.	varchar(100)		I1 - I2, ABCNM

Table	Entity (L1)	Column	Attribute	Column Definition	Data Type	Results	System
L0 Organisational Context							
ENV	Environment	DIS OUT TM	Disruption Outlook Time Frame	This field indicates the time frame in which a disruption is likely to materialise or has already materialised.	varchar(255)		I1 - I2, ABCNM
ENV	Environment	ORG	Organisation	Indicates the organisation that conducted surveys and expert analysis and provided in the publication. In this report, the BCI and IRMSA are such organisations, however more organisations could be considered in future work and this is an extendable data set as a result.	varchar(100)		I1 - I2, ABCNM
RSK TAX	Risk Taxonomy	ID	Row Identifier	Identifies the row in the table.	integer		ID, NM
RSK TAX	Risk Taxonomy	TAX RSK ID	Taxonomy Identifier	This is the taxonomy identifier that has been assigned in the mapping to the Taxonomy Identifier in the Environmental scanning Data.	integer		ID, NM
RSK TAX	Risk Taxonomy	TAX RSK CAT	Risk Taxonomy Category	The name of the Open Risk Taxonomy Risk Type.	char(50)		ID, NM

Table	Entity (L1)	Column	Attribute	Column Definition	Data Type	Results	System
L0 Organisational Context							
RSK TAX	Risk Taxonomy	TAX SUB CAT 1	Sub Category 1	The name of the Open Risk Taxonomy Risk in the first level of the hierarchy.	char(50)		ID, NM
RSK TAX	Risk Taxonomy	SUB CAT 1 DEF	Sub Category 1 Definition	The Open Risk Taxonomy is developed in hierarchical format. This indicates the first level of the hierarchy that has been identified in the appropriate mapping to the Environmental Scanning Data.	varchar(600)		ID, NM
RSK TAX	Risk Taxonomy	TAX SUB CAT 2	Sub Category 2	The name of the Open Risk Taxonomy Risk in the second level of the hierarchy.	char(50)		ID, NM
RSK TAX	Risk Taxonomy	SUB CAT 2 DEF	Sub Category 2 Definition	The Open Risk Taxonomy is developed in hierarchical format. This indicates the second level of the hierarchy that has been identified in the appropriate mapping to the Environmental Scanning Data.	varchar(600)		ID, NM

Table	Entity (L1)	Column	Attribute	Column Definition	Data Type	Results	System
L0 Business Resources							
DIS REQ RES	Disruption Required Resources	ID	Row Identifier	Identifies the row in the table.	integer		D
DIS REQ RES	Disruption Required Resources	BIA ID	BIA Identifier	The BIA ID identifies the business impact analysis and its associated impacts.	integer		D
DIS REQ RES	Disruption Required Resources	PROC ACT ID	Process Activity Identifier	Provides a basis on which to associate the required resources in the event of a disruption to the process activity.	integer		D
DIS REQ RES	Disruption Required Resources	RES DESC	Resource Description	This is a description of the specified resources that would be required in the event of a disruption.	varchar(100)		D
DIS REQ SYS	Disruption Required Systems	ID	Row Identifier	Identifies the row in the table.	integer		D

Table	Entity (L1)	Column	Attribute	Column Definition	Data Type	Results	System
L0 Business Resources							
DIS REQ SYS	Disruption Required Systems	BIA ID	BIA Identifier	The BIA ID identifies the business impact analysis and its associated impacts.	integer		D
DIS REQ SYS	Disruption Required Systems	PROC ACT ID	Process Activity Identifier	Provides a basis on which to associate the required systems in the event of a disruption to the process activity.	integer		D
DIS REQ SYS	Disruption Required Systems	SYS DESC	System Description	Provides a description of the required systems in the event of a disruption to the process activity.	varchar(100)		D
DIS REQ TECH	Disruption Required Technology	ID	Row Identifier	Identifies the row in the table.	integer		D
DIS REQ TECH	Disruption Required Technology	BIA ID	BIA Identifier	The BIA ID identifies the business impact analysis and its associated impacts.	integer		D

Table	Entity (L1)	Column	Attribute	Column Definition	Data Type	Results	System
L0 Business Resources							
DIS REQ TECH	Disruption Required Technology	PROC ACT ID	Process Activity Identifier	Provides a basis on which to associate the required technology in the event of a disruption to the process activity.	integer		D
DIS REQ TECH	Disruption Required Technology	TECH DESC	Technology Description	Provides a description of the required technology in the event of a disruption to the process activity.	varchar(100)		D
DIS SUPP SERV	Disruption Supplier Services	ID	Row Identifier	Identifies the row in the table.	integer		D
DIS SUPP SERV	Disruption Supplier Services	BIA ID	BIA Identifier	The BIA ID identifies the business impact analysis and its associated impacts.	integer		D
DIS SUPP SERV	Disruption Supplier Services	PROC ACT ID	Process Activity Identifier	Provides a basis on which to associate the required resources in the event of a disruption to the process activity.	integer		D

Table	Entity (L1)	Column	Attribute	Column Definition	Data Type	Results	System
L0 Business Resources							
DIS SUPP SERV	Disruption Supplier Services	SERV DESC	Services Description	Provides a basis on which to associate the required resources in the event of a disruption to the process activity.	varchar(100)		D
DIS SUPP SERV	Disruption Supplier Services	MB ID	Party Identifier	The identifier of the party in the supertype.	integer		D
DIS SUPP SERV	Disruption Supplier Services	SUPP NAME	Party Name	The Supplier Contact Details **Note that this can be associated to party in the logical model for more supertype detail in addition to this additional parties can be scaled by referencing a party identifier instead of a name in this table.	char(50)		D
DIS REQ DEPT	Disruption Required Department	ID	Row Identifier	Identifies the row in the table.	integer		D
DIS REQ DEPT	Disruption Required Department	BIA ID	BIA Identifier	The BIA ID identifies the business impact analysis and its associated impacts.	integer		D

Table	Entity (L1)	Column	Attribute	Column Definition	Data Type	Results	System
L0 Business Resources							
DIS REQ DEPT	Disruption Required Department	DEPT ID	Department Identifier	The Department that is contained in the Department table which is part of the organisation to which activities can be associated.	integer		D
DEPT	Department	ID	Row Identifier	Identifies the row in the table.	integer		D
DEPT	Department	DEPT ID	Department Identifier	The department identifier used in the organisation.	integer		D
DEPT	Department	DEPT NM	Department Name	The name of the organisational department for instance “Scoring Department”.	char(50)		D
DEPT	Department	DEPT DESC	Department Description	The detailed description of the department including its function and high level activities.	varchar(100)		D

Table	Entity (L1)	Column	Attribute	Column Definition	Data Type	Results	System
L0 Business Continuity							
BIA	Business Impact Analysis	ID	Row Identifier	Identifies the row in the table.	integer		D
BIA	Business Impact Analysis	BIA ID	BIA Identifier	The BIA ID identifies the business impact analysis and its associated impacts.	integer		D
BIA	Business Impact Analysis	BIA NM	BIA Name	Name of the Business Impact Analysis.	char(50)		D
BIA	Business Impact Analysis	BIA DESC	BIA Description	The description of the BIA (Note: the BIA is specific to an organisational department).	varchar(100)		D
BUS IMP	Business Impacts	ID	Row Identifier	Identifies the row in the table.	integer		D

Table	Entity (L1)	Column	Attribute	Column Definition	Data Type	Results	System
L0 Business Continuity							
BUS IMP	Business Impacts	BUS IMP ID	Business Impact Identifier	The business identifier that is used to label the business impact that is associated with the BIA.	integer		D
BUS IMP	Business Impacts	RSK ID	Risk Identifier	The risk identifier that is used to identify the risk description in the RSK ASMT (risk assessment) table.	integer		D
BUS IMP	Business Impacts	BIA ID	BIA Identifier	The BIA ID identifies the business impact analysis and its associated impacts.	integer		D
BUS IMP	Business Impacts	IMP CAT ID	Business Impact Category Identifier	The IMP CAT ID is contained in the IMP CAT table which forms the basis upon which impacts may be categorised.	integer		D
RSK ASMT	Risk Assessment	RSK DESC	Risk Description	Detailed risk description which is an analysis and evaluation of the risk of disruption to the organisation. This is a derived output of the Ethnographic Risk Category.	varchar(100)	C(1-n)	D
BUS IMP	Business Impacts	IMP NAME	Impact Name	A short name given to the identified business impact.	char(50)		D
BUS IMP	Business Impacts	IMP DESC	Impact Description	A detailed description of the impact identified in a given scenario.	varchar(100)		D

Table	Entity (L1)	Column	Attribute	Column Definition	Data Type	Results	System
L0 Business Continuity							
BUS IMP	Business Impacts	PROC ID	Process Identifier	The PROC ID that is contained in the PROC ACT table which forms the basis upon which impacts are associated with a business process and its activities.	integer		D
BUS IMP	Business Impacts	RTO	Recovery Time Objective **	The Recovery Time Objective is the defined recovery time following a disruption each critical activity in organisation. In this table, this is a summation of associated activity timeframes from the individual activities identified.	varchar(100)		D
BUS IMP	Business Impacts	RPO	Recovery Point Objective **	The Recovery Point Objective the point in time you can recover to in the event of a disruption. In this table, this is a qualitative description that includes all objectives from the associated activities.	varchar(100)		D
BUS IMP	Business Impacts	MBCO	Minimum Business Continuity Objective **	The minimal level of Services and/or products that are acceptable to the organisation to achieve its objectives during an incident /emergency or disaster. In this table, this is a qualitative description that includes all objectives from the associated activities.	varchar(100)		D
BUS IMP	Business Impacts	MTPD	Maximum Tolerable Period of Disruption **	The maximum tolerable period of disruption is the requirement within which a recovery time objective (RTO) needs to be set. This speaks to the duration following which the organisation will be irreparably damaged if Services cannot be restored. In this table, this is a summation of associated activity timeframes from the individual activities identified.	varchar(100)		D

Table	Entity (L1)	Column	Attribute	Column Definition	Data Type	Results	System
L0 Business Continuity							
BUS IMP	Business Impacts	SCN PAR	Scenario Parameter	The scenario in which the risk indicator was set for example based on regulatory requirement and/or MBCO and MTPD.	char(50)		D
IMP CAT	Impact Category	ID	Row Identifier	Identifies the row in the table.	integer		D
IMP CAT	Impact Category	IMP CAT ID	Business Impact Category Identifier	The IMP CAT ID is contained in the IMP CAT table which forms the basis upon which impacts may be categorised.	integer		D
IMP CAT	Impact Category	IMP CAT NM	Business Impact Category Name	A name assigned to the business impact category.	char(50)		D
IMP CAT	Impact Category	IMP CAT DESC	Business Impact Category Description	The full description of the business impact category enabling standardisation of identified organisational business impact categories for example Staff Impact, Public Impact, Regulatory Impact etc.	varchar(100)		D

Table	Entity (L1)	Column	Attribute	Column Definition	Data Type	Results	System
L0 Business Continuity							
RSK ASMT	Risk Assessment	ID	Row Identifier	Identifies the row in the table.	integer		D
RSK ASMT	Risk Assessment	RSK ID	Risk Identifier (Cn)	The identifier of the risk documented.	integer		D
RSK ASMT	Risk Assessment	RSK DESC	Risk Description	Detailed risk description which is an analysis and evaluation of the risk of disruption to the organisation. This is a derived output of the Ethnographic Risk Category.	varchar(100)	C(1-n)	D
RSK ASMT	Risk Assessment	PROB	Probability	This indicates the probability of a future risk arising.	decimal(12,4)		D
RSK ASMT	Risk Assessment	IMP	Impact	Risk Impact which replies either to a disruption (materialised risk) or is an anticipated future impact in the outlook time frame.	decimal(12,4)		D

Table	Entity (L1)	Column	Attribute	Column Definition	Data Type	Results	System
L0 Business Continuity							
RSK ASMT	Risk Assessment	RSK SC	Risk Score	The risk score is derived by multiplying the risk and probability.	decimal(12,4)		D
RSK ASMT	Risk Assessment	KRI	Key Risk Indicator (In)	The risk indicator identified either through legislation or through the definition of an indicator to measure and watch.	char(50)	I(1-n)	D
RSK ASMT	Risk Assessment	REL	Relevance	The relevance of the risk derived from organisational context evaluation. Based on the average risk score over a three to five year period. Assigned to variable V2.1.	decimal(12.4)	V2.1	D
RSK ASMT	Risk Assessment	SIG	Significance	Consideration is given to industry specifics as well as operating context. indicated as high, medium and low. Assigned to variable V2.2	char(50)	V2.2	D
RSK ASMT	Risk Assessment	ETH RSLT	Ethnographic Result	References the Organisational Context Environmental Assessment.	integer	V1.1	D

Table	Entity (L1)	Column	Attribute	Column Definition	Data Type	Results	System
L0 Strategy							
PROC ACT	Process Activity	ID	Row Identifier	Identifies the row in the table.	integer		D
PROC ACT	Process Activity	PROC ACT ID	Process Activity Identifier	The Process Activity Identifier that is specific to the business and forms the basis of prioritised activities in the BIA	integer		D
PROC ACT	Process Activity	DEPT ID	Department Identifier	The Department that is contained in the Department table which is part of the organisation to which activities can be associated.	integer		D
PROC ACT	Process Activity	ACT NM	Activity Name	The process activity name that is assigned to the activity identified and to its dependent activities.	char(50)		D
PROC ACT	Process Activity	ACT DESC	Activity Description	The process activity description that is assigned to the activity identified and to its dependent activities. This contains a long description of the purpose of the activity, the roles and responsibilities associated with the activity and its required outcome.	varchar(100)		D
PROC ACT	Process Activity	ACT DEP ID	Activity Dependency Identifier	The process activity identifier (PROC ACT ID) that the Identified activity in this row is dependent on. For nodes, this is set to 0.	integer		D

Table	Entity (L1)	Column	Attribute	Column Definition	Data Type	Results	System
L0 Strategy							
PROC ACT	Process Activity	PROC GP ID	Process Group Identifier	The process group is the Identifier that logically groups critical activities together. This is specifically used where there may be a requirement to set an activity grouping timeframe.	integer		D
IMP TM FM	Impact Timeframe	ID	Row Identifier	Identifies the row in the table.	integer		D
IMP TM FM	Impact Timeframe	PROC GP ID	Process Group Identifier	The process group is the Identifier that logically groups critical activities together. This is specifically used where there may be a requirement to set an activity grouping timeframe.	integer		D
IMP TM FM	Impact Timeframe	PROC GP NM	Process Group Name	The process group is a descriptive identifier that logically groups critical activities together. This is specifically used where there may be a requirement to set an activity grouping timeframe.	char(50)		D
IMP TM FM	Impact Timeframe	BIA ID	BIA Identifier	The BIA ID identifies the business impact analysis and its associated impacts.	integer		D
IMP TM FM	Impact Timeframe	RPO	Recovery Point Objective	"point to which information used by an activity must be restored to enable the activity to operate on resumption."	char(50)		D

Table	Entity (L1)	Column	Attribute	Column Definition	Data Type	Results	System
L0 Strategy							
IMP TM FM	Impact Timeframe	RTO	Recovery Time Objective	"the period of time following an incident within which -a product or service must be resumed, or -activity must be resumed, or -resources must be recovered"	char(50)		D
IMP TM FM	Impact Timeframe	MBCO	Minimum Business Continuity Objective	"minimum level of Services and/or products that is acceptable to the organisation to achieve its business objectives during a disruption."	char(100)		D
IMP TM FM	Impact Timeframe	MTPOD	Minimum Tolerable Period of Disruption	"time it would take for adverse impacts, which might arise as a result of not providing a product/service or performing an activity, to become unacceptable."	char(100)		D

Table	Entity (L1)	Column	Attribute	Column Definition	Data Type	Results	System
L0 Strategy							
INC RSP ST	Incident Response Structure	ID	Row Identifier	Identifies the row in the table.	integer		D
INC RSP ST	Incident Response Structure	INC RESP ST ID	Incident Response Structure Identifier	The business Identifier that can be used to assign additional details of a response including "processes and procedures for the activation, operation and coordination and communication of the response" for example this can be associated to communication planning items.	integer		D
INC RSP ST	Incident Response Structure	BIA ID	BIA Identifier	The BIA ID identifies the business impact analysis and its associated impacts.	integer		D
INC RSP ST	Incident Response Structure	INC RESP ST NM	Incident Response Structure Name	The business name associated with the incident response.	char(50)		D
INC RSP ST	Incident Response Structure	INC RESP ST DESC	Incident Response Structure Description	High level description of the response based on the details required in clause 8,42 of the ISO22301 standard.	varchar(100)		D
L0 Party / Arrangement							
LOAN	Lending Data		Associated metadata from source				

10.4 Data Profile and Database Scripting

```
--L0 ENVIRONMENT (Operating Context)
--Environmental Scanning Data which includes:
--BCI Horizon Scan and IRMSA Reports - 5 year historical data
--395 Rows395
--Data Profile Results:
--MIN(RSK_SC) = 2, MAX(RISK_SC) = 25 (excludes zero values as these are not applicable to the year)
--MIN(PROB) = 1.5, MAX(PROB) = 7.5 (excludes zero values as these are not applicable to the year)
--MIN(IMP) = 1.2, MAX(IMP) = 5 (excludes zero values as these are not applicable to the year)
--MIN(APPL_YR) = 2015 , MAX(APPL_YR) = 2020
--MIN (DIS_CNC) = 0.01. MAX(DIS_CNC) = 0.83 (excludes zero values as these are not applicable to the year)
--42 Distinct Standardised Ethnographic Results (Risk Themes) (V1.1)
--17 Distinct Risk Taxonomy Identifiers associated to 395 data records indicating 17 risk descriptions to be inherited into the Risk Assessment (RSK_ASMT)

CREATE TABLE ENV (
ID                  INT     NOT NULL        IDENTITY    PRIMARY KEY,
RPT_YR              INT,
ETH_RSLT            INT,
TAX_ID              INT,
ETH_RSK_CAT         VARCHAR(150),
DIS_CNC             DECIMAL(12,4),
PROB                DECIMAL(12,4),
IMP                 DECIMAL(12,4),
RSK_SC              DECIMAL(12,4),
APPL_YR             VARCHAR (100),
DIS_OUT_TM          VARCHAR(255),
ORG                 VARCHAR(100),
);

INSERT INTO ENV
SELECT  [RPT_YR]
       ,[ETH_RSLT]
       ,[RSK_TAX_ID]
       ,[ETH_RSK_CAT]
       ,[DIS_CNC]
       ,[PROB]
       ,[IMP]
       ,[RSK_SC]
       ,[APPL_YR]
       ,[DIS_OUT_TM]
       ,[ORG]
FROM    [9101231E_FINAL_SOLUTION].[dbo].[STAGING_ENV]
WHERE   [ID] = CAST (ID AS INTEGER) and
        [RPT_YR] = CAST (RPT_YR AS INTEGER) and
        [ETH_RSLT] = CAST (ETH_RSLT AS INTEGER) and
        [RSK_TAX_ID] = CAST (RSK_TAX_ID AS INTEGER) and
        [ETH_RSK_CAT] = CAST (ETH_RSK_CAT AS VARCHAR(150)) and
        [DIS_CNC] = CAST (DIS_CNC AS DECIMAL (12,4)) and
        [PROB] = CAST (PROB AS DECIMAL(12,4)) and
        [IMP] = CAST (IMP AS DECIMAL(12,4)) and
        [RSK_SC] = CAST (RSK_SC AS DECIMAL(12,4)) and
        [APPL_YR] = CAST (APPL_YR AS VARCHAR(100)) and
        [DIS_OUT_TM] = CAST (DIS_OUT_TM AS VARCHAR(255)) and
        [ORG] = CAST (ORG AS VARCHAR(100))

--Risk Taxonomy Data which includes:
```

```
--a subset of the Open Risk Taxonomy, providing the applicable
    mapping data to the environmental Scanning Data

CREATE TABLE RSK_TAX (
ID                  INT     NOT NULL        IDENTITY    PRIMARY KEY,
TAX_RSK_ID          INT,
TAX_RSK_CAT         CHAR(50),
TAX_SUB_CAT_1       CHAR(50),
SUB_CAT_1_DEF       VARCHAR(600),
TAX_SUB_CAT_2       CHAR(50),
SUB_CAT_2_DEF       VARCHAR(600),
);

--Risk Taxonomy has been derived from an open source taxonomy
--18 Rows
--Data Profile Results (Distinct Value Combinations):
--TAX_RSK_CAT                                   TAX_SUB_CAT_1
                                            TAX_SUB_CAT_2
--Business Risk                                Funding Risk
                                            Funding Risk
--Business Risk                                Human
    Resources Risk                                  Human Resources
--Business Risk                                Leadership
    Risk                                      Leadership
--Business Risk                                Operational
    Risk                                      Business Continuity
--Business Risk                                Operational
    Risk                                      Disease and Pandemic
--Business Risk                                Operational
    Risk                                      Employment Practices
--Business Risk                                Operational
    Risk                                      External Fraud
--Business Risk                                Operational
    Risk                                      Internal Fraud
--Business Risk                                Operational
    Risk                                      IT Risk
--Business Risk                                Operational
    Risk                                      Legal Risk
--Business Risk                                Operational
    Risk                                      Physical Damage
--Business Risk                                Revenue Risk
                                            Market Share
--Business Risk                                Strategic
    Risk                                        Strategic Risk
--Climate Related Risk                         Sustainable
    Finance                                   Climate Change
--Credit Risk                                  Country Risk
                                            Political Risk
--Market Risk                                  Exposure Risk
                                            Exposure
--Market Risk                                  Foreign
    Excahange Risk                                Foreign Exchange
--Note: This is not a full representation of the taxonomy. The full
    taxonomy could be loaded to this table via application programming
     interface. The distinct value
--cobminations loaded for this report are based on mapping result.
SELECT ENV.ETH_RSLT, RSK_ASMT.RSK_ID, RSK_ASMT.RSK_DESC, RSK_ASMT.
   PROB, RSK_ASMT.IMP, RSK_ASMT.RSK_SC, RSK_ASMT.KRI, RSK_ASMT.REL,
   RSK_ASMT.SIG
FROM     ENV INNER JOIN
                  RSK_TAX ON ENV.TAX_ID = RSK_TAX.TAX_RSK_ID INNER
                     JOIN
```

```
                    RSK_ASMT ON ENV.ETH_RSLT = RSK_ASMT.ETH_RSLTSELECT
                        RSK_TAX.TAX_RSK_CAT, RSK_TAX.TAX_SUB_CAT_1,
                        RSK_TAX.TAX_SUB_CAT_2, RSK_TAX.SUB_CAT_1_DEF,
                        RSK_TAX.SUB_CAT_2_DEF, RSK_ASMT.RSK_ID, RSK_ASMT
                        .RSK_DESC, RSK_ASMT.PROB, RSK_ASMT.IMP,
95                  RSK_ASMT.RSK_SC, RSK_ASMT.KRI, RSK_ASMT.REL,
                        RSK_ASMT.SIG, ENV.ETH_RSLT
FROM     ENV INNER JOIN
                    RSK_ASMT ON ENV.ETH_RSLT = RSK_ASMT.ETH_RSLT INNER
                        JOIN
                    RSK_TAX ON ENV.TAX_ID = RSK_TAX.TAX_RSK_IDSELECT
                        RSK_TAX.TAX_RSK_ID, RSK_TAX.TAX_RSK_CAT, RSK_TAX
                        .TAX_SUB_CAT_1, RSK_TAX.SUB_CAT_1_DEF, RSK_TAX.
                        TAX_SUB_CAT_2, RSK_TAX.SUB_CAT_2_DEF, RSK_ASMT.
                        RSK_ID, RSK_ASMT.RSK_DESC, RSK_ASMT.PROB,
                    RSK_ASMT.IMP, RSK_ASMT.RSK_SC, RSK_ASMT.KRI,
                        RSK_ASMT.REL, RSK_ASMT.SIG, RSK_ASMT.ETH_RSLT
100 FROM     ENV INNER JOIN
                    RSK_ASMT ON ENV.ETH_RSLT = RSK_ASMT.ETH_RSLT INNER
                        JOIN
                    RSK_TAX ON ENV.TAX_ID = RSK_TAX.ID
INSERT INTO RSK_TAX
SELECT   [TAX_RSK_ID]
105        ,[TAX_RSK_CAT]
           ,[TAX_SUB_CAT_1]
           ,[SUB_CAT_1_DEF]
           ,[TAX_SUB_CAT_2]
           ,[SUB_CAT_2_DEF]
110 FROM    [9101231E_FINAL_SOLUTION].[dbo].[STAGING_RSK_TAX]
WHERE    [TAX_RSK_ID] = CAST (TAX_RSK_ID AS INTEGER) and
         [TAX_RSK_CAT] = CAST (TAX_RSK_CAT AS CHAR(50)) and
         [TAX_SUB_CAT_1] = CAST (TAX_SUB_CAT_1 AS CHAR(50)) and
         [SUB_CAT_1_DEF] = CAST (SUB_CAT_1_DEF AS VARCHAR(600)) and
115      [TAX_SUB_CAT_2] = CAST (TAX_SUB_CAT_2 AS CHAR(50)) and
         [SUB_CAT_2_DEF] = CAST (SUB_CAT_2_DEF AS VARCHAR(600))


--L0 BUSINESS RESOURCES
120
--Required Resources has been captured as an illustrative result

CREATE TABLE DIS_REQ_RES (
ID                  INT     NOT NULL        IDENTITY    PRIMARY KEY,
125 BIA_ID              INT,
PROC_ACT_ID         INT,
RES_DESC            VARCHAR(100),
);

130 --Required Systems has been captured as an illustrative result

CREATE TABLE DIS_REQ_SYS (
ID                  INT     NOT NULL        IDENTITY    PRIMARY KEY,
BIA_ID              INT,
135 PROC_ACT_ID         INT,
SYS_DESC            VARCHAR(100),
);

--Required Technology has been captured as an illustrative result
140
CREATE TABLE DIS_REQ_TECH (
ID                  INT     NOT NULL        IDENTITY    PRIMARY KEY,
BIA_ID              INT,
PROC_ACT_ID         INT,
```

```
TECH_DESC           VARCHAR(100),
);

--Required Suppliers has been captured as an illustrative result

CREATE TABLE DIS_SUPP_SERV (
ID                  INT     NOT NULL        IDENTITY    PRIMARY KEY,
BIA_ID              INT,
PROC_ACT_ID         INT,
SERV_DESC           VARCHAR(100),
MB_ID               INT,
SUPP_NM             CHAR(50)
);

--Required Department has been captured as an illustrative result

CREATE TABLE DIS_REQ_DEPT (
ID                  INT     NOT NULL        IDENTITY    PRIMARY KEY,
BIA_ID              INT,
DEPT_ID             INT,
);

CREATE TABLE DEPT (
ID                  INT     NOT NULL        IDENTITY    PRIMARY KEY,
DEPT_ID             INT,
DEPT_NM             CHAR(50),
DEPT_DESC           VARCHAR(100),
);

--L0 BUSINESS CONTINUITY
--Simulated Business Impact assessment which includes:
--a the master data for a simulated BIA.

--This is represented as a single record to provide the BIA Dashboard
    result for credit risk.

CREATE TABLE BIA (
ID                  INT     NOT NULL        IDENTITY    PRIMARY KEY,
BIA_ID              INT,
BIA_NM              CHAR(50),
BIA_DESC            VARCHAR(100),
);

--Simulated Business Impact which includes:
--Details of the business impacts applicable to the Business Impact
    Analysis.
--Including references to Impact Categories and Processes.
--It is noted that for this simulation: two risk results are
    represented:
--Financial System Weakness (Risk ID value V1.1 = 8)
--Regulatory Risk (Risk ID Value V1.1 = 25)

--The L1 Business Impact provides the organisational expert judgement
    to identify the potential business impacts associated to an
    assessed risk.

CREATE TABLE BUS_IMP (
ID                  INT     NOT NULL        IDENTITY    PRIMARY KEY,
BUS_IMP_ID          INT,
RSK_ID              INT,
BIA_ID              INT,
IMP_CAT_ID          INT,
IMP_NAME            CHAR(50),
```

```
IMP_DESC            VARCHAR(100),
PROC_ID             INT,
RTO                 VARCHAR(100),
RPO                 VARCHAR(100),
MBCO                VARCHAR(100),
MTPD                VARCHAR(100),
SCN_PAR             CHAR(50),
);

INSERT INTO BUS_IMP

SELECT [BUS_IMP_ID]
      ,[BIA_ID]
      ,[RSK_ID]
      ,[IMP_CAT_ID]
      ,[IMP_NAME]
      ,[IMP_DESC]
      ,[PROC_ID]
      ,[SC_PAR]
      ,[RTO]
      ,[RPO]
      ,[MBCO]
      ,[MTPD]
FROM [9101231E_FINAL_SOLUTION].[dbo].[STAGING_BUS_IMP]
WHERE [BUS_IMP_ID] = CAST (BUS_IMP_ID AS INTEGER) and
      [BIA_ID] = CAST (BIA_ID AS INTEGER) and
      [RSK_ID] = CAST (RSK_ID AS INTEGER) and
      [IMP_CAT_ID] = CAST (IMP_CAT_ID as INTEGER) and
      [IMP_NAME] = CAST (IMP_NAME AS CHAR(50)) and
      [IMP_DESC] = CAST (IMP_DESC AS VARCHAR(100)) and
      [PROC_ID] = CAST (PROC_ID AS INTEGER) and
      [SC_PAR] = CAST (SC_PAR AS CHAR(50)) and
      [RTO] = CAST (RTO AS VARCHAR(100)) and
      [RPO] = CAST (RPO AS VARCHAR(100)) and
      [MBCO] = CAST (MBCO AS VARCHAR(100)) and
      [MTPD] = CAST (MTPD AS VARCHAR(100))

--Business Impact Categories have been defined as follows:
--Staff impact ,Public impact,Regulatory impact,Reputation impact,
    Financial impact,Service impact,Environment impact

CREATE TABLE BUS_IMP_CAT (
ID                  INT     NOT NULL        IDENTITY    PRIMARY KEY,
IMP_CAT_ID          INT,
IMP_CAT_NM          CHAR(50)
IMP_CAT_DESC        VARCHAR(100),
);

--The Risk Assessment is the result of the environment scan (part of
    setting organisational context) across risk data sources and
    presents these in an integrated component of the BCMS.
--It is noted that the calculation of the Probability and Impact is a
    result of the average Risk score components in the risk data
    source where probability is the method of measurement.
--Note that there are three method of risk measurement in this report
    and the probability/impact method is the preferred choice in the
    illustrative result example.
--An extension to the logical and physical data model could be done
    to accommodate the results of other methods.
--Constraint: Multiple methods would require additional
    standardisation algorithms.
--395 Rows
--Data Profile Results:
```

```
--MIN(RSK_SC) = 5.1, MAX(RISK_SC) = 19
--MIN(PROB) = 1.5, MAX(PROB) = 2.85
--MIN(IMP) = 1.67, MAX(IMP) = 4.75
--DISTINCT ETH_RSLT Values written to the table using the chosen risk measurement:
--1, 2, 3, 4, 5, 6, 7, 8, 11,
--12, 13, 14, 15, 16, 17, 18,
--19, 20, 21, 22, 23, 24, 25,
--26, 27, 28, 42. 43
--it is noted that there are 42 Distinct Standardised Ethnographic Results (Risk Themes) (V1.1), 28 results were derived using the risk probability risk score measurement.
--17 Distinct Risk Taxonomy Identifiers associated to 395 data records indicating 17 risk descriptions to be inherited into the Risk Assessment (RSK_ASMT)
--Note: In the BCMS Operation process Clause 8.2.3, the derived risk scores in the RSK_ASMT table would be assessed and adjusted where applicable to the organisation.
--Data Quality: Check Risk Score = Probaibility * impact (derived) and calculated. with a variance of 0,032641222 3%. (due in part due to data rounding and truncation)
--Data Quality is within an acceptable limit of 5%
--Identified method of data quality remediation (longer decimal data types to avoid truncation and uneccesary rounding differences).
--Data Quality risk mitigation - acceptance of the tolerance


CREATE TABLE RSK_ASMT (
ID                  INT     NOT NULL        IDENTITY    PRIMARY KEY,
RSK_ID              INT,
RSK_DESC            VARCHAR(100),
PROB                DECIMAL(12,4),
IMP                 DECIMAL(12,4),
RSK_SC              DECIMAL(12,4),
KRI                 CHAR(50),
REL                 DECIMAL(12,4),
SIG                 CHAR(50),
ETH_RSLT            INT
);


INSERT INTO RSK_ASMT
SELECT [RSK_ID]
      ,[RSK_DESC]
      ,[PROB]
      ,[IMP]
      ,[RSK_SC]
      ,[KRI]
      ,[REL]
      ,[SIG]
      ,[ETH_RSLT]
  FROM [9101231E_FINAL_SOLUTION].[dbo].[RSK_ASMT$]
  WHERE [RSK_ID] = CAST (RSK_ID AS INTEGER) and
        [RSK_DESC] = CAST (RSK_DESC AS VARCHAR(100)) and
        [PROB] = CAST (PROB AS DECIMAL(12,6)) and
        [IMP] = CAST (IMP AS DECIMAL(12,4)) and
        [RSK_SC] = CAST (RSK_SC AS DECIMAL(12,4)) and
        [KRI] = CAST (KRI AS CHAR(50)) and
        [REL] = CAST (REL AS DECIMAL(12,4)) and
        [SIG] = CAST (SIG AS CHAR(50)) and
        [ETH_RSLT] = CAST (ETH_RSLT AS INTEGER)
```

```
SELECT RSK_TAX.TAX_RSK_ID, RSK_TAX.TAX_RSK_CAT, RSK_TAX.TAX_SUB_CAT_1
    , RSK_TAX.SUB_CAT_1_DEF, RSK_TAX.TAX_SUB_CAT_2, RSK_TAX.
   SUB_CAT_2_DEF, RSK_ASMT.RSK_ID, RSK_ASMT.RSK_DESC, RSK_ASMT.PROB,
310                RSK_ASMT.IMP, RSK_ASMT.RSK_SC, RSK_ASMT.KRI,
                       RSK_ASMT.REL, RSK_ASMT.SIG
FROM     ENV INNER JOIN
                   RSK_ASMT ON ENV.ETH_RSLT = RSK_ASMT.ETH_RSLT INNER
                       JOIN
                   RSK_TAX ON ENV.TAX_ID = RSK_TAX.ID
```

References

[1] Business Continuity Institute. (2020) Business Continuity Institute Horizon Scan Report 2020. [Online]. Available: https://www.thebci.org/resource/bci-horizon-scan-2020-webinar.html

[2] Bank of International Settlements, *BCB189 (2006) High Level Principles for Business Continuity Management.* Bank of International Settlements, 2006. [Online]. Available: https:www.bis.org/publ/bcbs189.pdf

[3] International Standards Organisation, *ISO22301: Societal Security - Business Continuity Management Systems.* BSi Standards Publication, 2012.

[4] R Elliot, G Riglietti, L Aguada, and K Muhammad, "Business Continuity Institute Horizon Scan Report 2019," Business Continuity Institute, Tech. Rep., 2019. [Online]. Available: https://www.thebci.org/resource/horizon-scan-report-2019.html

[5] Johns Hopkins Coronavirus Resource Center. (2020) Covid-19 dashboard. [Online]. Available: https://coronavirus.jhu.edu/

[6] John Hopkins University. (2020) COVID-19 map. [Online]. Available: https://coronavirus.jhu.edu/map.html

[7] South African Government. (2012) National development plan 2030 \textbackslashtextbar south african government. [Online]. Available: https://www.gov.za/issues/national-development-plan-2030

[8] Bank of International Settlements. (2020) Basel committee meets to review vulnerabilities and emerging risks, advance supervisory initiatives and promote basel III implementation. [Online]. Available: https://www.bis.org/press/p200227.htm

[9] P. Checkland, *Systems Thinking Practice*, 1st ed. John Wiley and Sons, 1999.

[10] Local Histories Organisation. (2020) A history of banks. [Online]. Available: http://localhistories.org/banking

[11] C. Herron, "Big data innovation and the application of standards for business resiliency in financial services," in *Proceedings of ELECON University of Mauritius 2018.* Springer, 2018, p. 13.

[12] A. Ismail, "The fintech frenzy: fad or financial sector transformer?" in *Proceedings of 14th BCBS-FSI high-level meeting*, 2019, pp. 1–8. [Online]. Available: http://www.southafritac.org/servlet/servlet.FileDownload?file=00P2M00000ZwQw1UAF

[13] L. Kganyago, "Strengthening financial sector supervision and current regulatory priorities," in *Proceedings of 14th BCBS-FSI high-level meeting*. South African Reserve Bank, 2019, pp. 1–9.

[14] A. P. Alex Lipton, David Shrier. (2016) Digital banking manifesto: The end of banks? [Online]. Available: https://globalriskinstitute.org/publications/digital-banking-manifesto-the-end-of-banks/

[15] Bank of International Settlements. (2017) High-level summary of Basel III reforms. [Online]. Available: https://www.bis.org/bcbs/publ/d424_hlsummary.pdf

[16] Dr. Christian Thun, "Moody's Analytics, Risk Data Management, Risk Perspectives," Moody's, Tech. Rep., 2015. [Online]. Available: https://www.moodysanalytics.com/-/media/article/2015/2015-21-07-moodys-analytics-risk-perspective-risk-data-management.pdf

[17] Bank of International Settlements, *BCBS239 Principles for Effective Risk Data Aggregation and Risk Reporting*. Bank of International Settlements, 2013. [Online]. Available: https:www.bis.org/publ/bcbs239.pdf

[18] International Standards Organisation, *ISO22313 2012: Societal Security - Business Continuity Management Systems Guideline*. BSi Standards Publication, 2012.

[19] S. Earley, *The DAMA Dictionary of Data Management*, 2nd ed. Technics Publications, LLC, 2011.

[20] C. Ellinas, N. Allan, and C. Coombe, "Evaluating the role of risk networks on risk identification, classification and emergence," *Journal of Network Theory In Finance*, vol. 3, no. 4, pp. 1–24, 2017. [Online]. Available: http://arxiv.org/abs/1801.05759

[21] Bank of International Settlements, "Covid-19 statistical resources," *Bank of International Settlements*, 2020. [Online]. Available: https://www.bis.org/ifc/covid19.htm

[22] T. Niskanen, "A resilience engineering -related approach applying a taxonomy analysis to a survey examining the prevention of risks," *Safety Science*, vol. 101, pp. 108–120, 2020. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0925753517314352

[23] M. Hellmich, B. Schuck, S. Siddiqui, M. Born, and A. Uhl, "How recent advances in IT support value creation in banking," *The Business Transformation Journal*, p. 12, 2014.

[24] Business Continuity Institute, *Good Practice Guidelines; The Global Guide to Good Practice in Business Continuity.* The Business Continuity Institute, 2018.

[25] Oxford English Dictionary, *Home : Oxford English Dictionary.* Oxford university Press, 2020. [Online]. Available: https://www.oed.com/

[26] Basel Committee. (2018) Basel committee charter. [Online]. Available: https://www.bis.org/bcbs/charter.htm

[27] Basel Committee. (2014) Basel committee history. [Online]. Available: https://www.bis.org/bcbs/history.htm

[28] S. Earley, *The DAMA Body of Knowledge*, 2nd ed. Technics Publications, LLC, 2011.

[29] T. Addagada, *Data Management and Governance Services; Simple and Effective Approaches*, 1st ed. Reedsy, 2017.

[30] C. S. Holling, "Resilience and stability of ecological systems," *Annual Review of Ecology and Systematics*, vol. 4, no. 1, pp. 1–23, 1973. [Online]. Available: http://www.annualreviews.org/doi/10.1146/annurev.es.04.110173.000245

[31] K. Burnard and R. Bhamra, "Organisational resilience: development of a conceptual framework for organisational responses," *International Journal of Production Research*, vol. 49, no. 18, p. 5581, 2011. [Online]. Available: http://0-search.ebscohost.com.innopac.wits.ac.za/login.aspx?direct=true&db=edb&AN=63634567&site=eds-live&scope=site

[32] Thimothy Vogus and Kathleen Sutcliffe. (2014) (PDF) organizing for resilience. [Online]. Available: https://www.researchgate.net/publication/255853978_Organizing_for_Resilience

[33] Open Source. (2020) Open Risk Manual. [Online]. Available: https://www.openriskmanual.org/wiki/Category:Franchise_Risk

[34] G. Cerè, Y. Rezgui, and W. Zhao, "Critical review of existing built environment resilience frameworks: Directions for future research," *International Journal of Disaster Risk Reduction*, vol. 25, pp. 173–189, 2017.

[35] Ariella Helfgott, "Operationalising resilience: Conceptual, mathematical and participatory frameworks for understanding, measuring and managing resilience." University of Adelaide, School of Mathematical Sciences, phdthesis, 2015. [Online]. Available: https://digital.library.adelaide.edu.au/dspace/handle/2440/99913?mode=full

[36] E. Coiera, "Putting the technical back into socio-technical systems research," *International Journal of Medical Informatics*, vol. 76, pp. S98–S103, 2007. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S1386505606001481

[37] R. Patriarca, G. Di Gravio, F. Costantino, A. Falegnami, and F. Bilotta, "An analytic framework to assess organizational resilience," *Safety and Health at Work*, vol. 9, no. 3, pp. 265–276, 2018. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S2093791117301968

[38] E-CSR. (2019) Resilience - definition, meaning & examples in business, psychology & urbanity. [Online]. Available: https://e-csr.net/definitions/resilience-definition-meaning-examples/

[39] Business Continuity Institute. (2016) Business Continuity Institute Horizon Scan Report 2020. [Online]. Available: https://www.thebci.org/resource/horizon-scan-2016.html

[40] S. A. Torabi, R. Giahi, and N. Sahebjamnia, "An enhanced risk assessment framework for business continuity management systems," *Safety Science*, vol. 89, pp. 201–218, 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0925753516301266

[41] S. Jackson and T. Ferris, "Resilience principles for engineered systems," *Systems Engineering*, vol. 16, no. 2, p. 152, 2019. [Online]. Available: http://0-search.ebscohost.com.innopac.wits.ac.za/login.aspx?direct=true&db=edb&AN=87075080&site=eds-live&scope=site

[42] D. Kennon, C. S. Schutte, and E. Lutters, "An alternative view to assessing antifragility in an organisation: A case study in a manufacturing SME," *CIRP Annals - Manufacturing Technology*, vol. 64, no. 1, pp. 177–180, 2015.

[43] A. Jaaron and C. Backhouse. (2014) Service organisations resilience through the application of the vanguard me...: Discovery service for university of the witwatersrand. [Online]. Available: https://0-eds-b-ebscohost-com.innopac.wits.ac.za/eds/detail/detail?vid=0&sid=cd7af6df-ade5-430d-96d2-122e8d73c502%40sessionmgr102&bdata=JnNpdGU9ZWRzLWxpdmUmc2NvcGU9c2l0ZQ%3d%3d

[44] Institute of Risk Management South Africa. (2020) PUBLICATION. [Online]. Available: https://riskreport.irmsasite.org

[45] C. Ferguson, "Business continuity and disaster management within the public service in relation to a national development plan," *Journal of Business Continuity and Emergency Planning*, vol. 11, no. 3, pp. 243–255, 2018. [Online]. Available: http://0-search.ebscohost.com.innopac.wits.ac.za/login.aspx?direct=true&db=bsu&AN=128412940&site=ehost-live&scope=site

[46] D. Henry and J. Emmanuel Ramirez-Marquez, "Generic metrics and quantitative approaches for system resilience as a function of time," *Reliability Engineering and System Safety*, vol. 99, pp. 114–122, 2012. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0951832011001748

[47] John Johnson and Adrian V. Gheorghe, "Antifragility analysis and measurement framework for systems of systems," *International Journal of Disaster Risk Reduction*, vol. Int. J. Disaster Risk Sci. 2013, 4 (4): 159–168 doi:10.1007/s13753-013-0017-7, 2013.

[48] E. H. Powley, "Reclaiming resilience and safety: Resilience activation in the critical period of crisis," *Human Relations*, vol. 62, no. 9, pp. 1289–1326, 2009. [Online]. Available: http://journals.sagepub.com/doi/10.1177/0018726709334881

[49] P. M. Senge, *The Fifth Discipline: Art and Practice of the Learning Organisation*, 1st ed. Random House, 2006.

[50] D. Couprie, Bin Li, and David Zhu. (2020) Soft systems methodology. [Online]. Available: http://plaza.ufl.edu/jtruett/abe5643c/ssmfinal.html

[51] S. Burge. (2015) Systems thinking approaches and methodologies. [Online]. Available: https://www.burgehugheswalsh.co.uk/Uploaded/1/Documents/Soft-Systems-Methodology.pdf

[52] Computer Hope. (2019) What is source data? [Online]. Available: https://www.computerhope.com/jargon/s/sourdata.htm

[53] Gartner. (2019) What is big data? - gartner IT glossary - big data. [Online]. Available: https://www.gartner.com/it-glossary/big-data/

[54] Sisense. (2019) Contextual data - what is contextual data? [Online]. Available: https://www.sisense.com/glossary/contextual-data/

[55] IBM. (2019) Industry models \textbar IBM. [Online]. Available: https://www.ibm.com/analytics/industry-models

[56] IBM. (2019) Data lakes - IBM. [Online]. Available: https://www.ibm.com/downloads/cas/ON4WK472

[57] Kimball Group, "Kimball Dimensional Modelling Techniques," Kimball University, Tech. Rep., 2016. [Online]. Available: https://www.kimballgroup.com/data-warehouse-business-intelligence-resources/kimball-techniques/dimensional-modeling-techniques/

[58] C. Biscoe. (2018) 5 benefits of an ISO 22301-conforming BCMS. [Online]. Available: https://www.itgovernance.co.uk/blog/5-benefits-of-an-iso-22301-conforming-bcms

[59] R. A. Martin, C. Liu, C.-H. Liu, Z. Martínez, Bernardo, Rubin, and Dawid, "Inferential models," Indiana University-Purdue University Indianapolis and Purdue University, Tech. Rep., 2011. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2214579617303179

[60] IBM. (2019) About Text Mining. [Online]. Available: https://www.ibm.com/support/knowledgecenter/SS3RA7_18.2.1/ta_guide_ddita/textmining/shared_entities/tm_intro_tm_defined.html?view=embed

[61] D. Marco and M. Jennings, *Universal Meta Data Models*, 1st ed. Wiley, 2004.

[62] J. Humble, J. Molesky, and B. O' Reilly, *Lean Enteprise - How High Performance Organisations Innovate at Scale*, 1st ed. O' Reilly, 2016.

[63] International Standards Organisation. (2018) ISO/IEC/IEEE 24748-1:2018. [Online]. Available: http://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/07/28/72896.html

[64] Business Continuity Institute. (2017) Business Continuity Institute Horizon Scan Report 2017. [Online]. Available: https://www.thebci.org/knowledge/horizon-scan-report-2017.html

[65] Business Continuity Institute. (2018) Business Continuity Institute Horizon Scan Report 2018. [Online]. Available: https://www.thebci.org/resource/horizon-scan-report-2018.html

[66] IBM. (2014) IBM banking data warehouse 8.2.0. [Online]. Available: https://www.ibm.com/support/pages/ibm-banking-data-warehouse-820

[67] Deloitte. (2020) BIS assessment of compliance to BCBS 239 principles. [Online]. Available: https://www2.deloitte.com/us/en/pages/regulatory/articles/bis-assessment-bcbs-239-principle-compliance.html