Adaptive Enterprise Resilience Management

Adaptive Action Design Research in Financial Services Case Study

Asif Qumer Gill and Eng K. Chew
Faculty of Engineering and IT (FEIT)
University of Technology Sydney (UTS)
Sydney, Australia
{asif.gill; eng.chew}@uts.edu.au

David Kricker and Geoff Bird
Information Technology
Reserve Bank of Australia (RBA)
Sydney, Australia

***Abstract*— Resilience is the ability of an enterprise to absorb, recover and adapt from a disruption. Being resilient is a complex undertaking for enterprises operating in a highly dynamic environment and striving for continuous efficiency and innovation. The challenge for enterprises is to offer and run a customer-centric and interdependent large portfolio of resilient services. The fundamental research question is: how to enable service resilience in the practical enterprise resilience context? This paper addresses this important research question, and reports findings from on-going (2014-2016) research on adaptive enterprise resilience management in an Australian financial services organization (FSO). This research is being conducted using the adaptive action-design research (ADR) method to iteratively research, develop and deliver the desired resilience framework in short increments. This paper presents the overall evolved adaptive enterprise resilience management framework and its "service resilience" element details as one of the key outcomes from the second adaptive ADR increment.**

Keywords— adaptability; architecture; operations; service; resilience; model-driven.

I. INTRODUCTION

Resilience is the ability of an enterprise to effectively scan and sense expected or unexpected disruptions, interpret and analyse; decide, respond and recover quickly to such disruptions [1-4]. Resilience is often linked to "operational resilience" and "organisational change", and is a strategic imperative for any service-centric enterprise such as financial services studied in this paper. [1, 5-6]. Lack of an effective resilience capability or practice would lead to frequent service disruptions resulting in poor service quality and customer satisfaction, and may potentially cause regulatory implications or financial penalties. The challenge for financial services enterprises is how to enable service resilience in the practical enterprise resilience context? There is an urgent need from organizations to formulate a framework for enterprise resilience that meets business needs [7]. This paper reports findings from our ongoing adaptive action-design research (ADR) [8] project in an Australian financial services organization, (coded name FSO) on service resilience. This two-year (2014-2016) project aims to contribute to filling the research and practice gap by investigating and developing the service-centric and architecture-driven (model-driven) adaptive enterprise resilience management (AERM) framework appropriate for the Australian FSO local context. The scope of this research and framework is limited to technology operational resilience management. The AERM framework elements (Fig. 1) are evolving as our research is progressing and delivering elements in increments.

The first project increment (2014-15) discovered the major (A) "strategy" and (B) "service" elements for the AERM framework. The strategy element focused on understanding the strategic resilience related goals, objectives and drivers. The service element focused on developing the service architecture, service portfolio and service lifecycle models as part of the overall AERM framework for FSO's services, which are critical to organizational resilience. These models were then delivered via the services configuration information system (CiS). The first increment was a pre-requisite for the second increment and helped us to identify, understand and profile the complex interlinked services of FSO. The details of the first increment were reported in [42]. During the Ssecond project increment (2015-16), building on the first and incorporating stakeholders' feedback, we discovered two more major elements - "service resilience" and "service operations" for the AERM framework. Thus, this research has so far discovered four major elements in total for the AERM framework: strategy, service, service resilience and service operations. This indicates the adaptive and evolving nature of this research and resultant framework elements. This paper presents the overall updated and evolved AERM framework and its "service resilience" element details as one of the key outcomes from the second increment.

This paper is organized as follows. Firstly, it provides the theoretical background and research problem. Secondly, it discusses the adaptive ADR method. Thirdly, it presents the AERM framework, resilience characteristics and FSO resilience management capability model. Finally, it discusses the lessons learnt and further research directions.

II. THEORETICAL BACKGROUND AND RESEARCH PROBLEM

A. Resilience

Resilience is the ability of a system to absorb, adapt and recover rapidly from a disruption so that normal levels of the service delivery can resume [9]. Resilience can be characterized by a number of properties such as defence or

resistance to attacks, efficiency or recovery (immediate response for stability) and adaptability or evolution (to a new 'better' state) [10]. These capabilities can be supported by a number of resilience processes: anticipation, monitoring, responding, and learning/adapting [6]. Resilient organizations or high reliability organizations (HRO's) or learning organizations [11] demonstrate their mastery by balancing systemic stability and efficiency with flexibility and adaptability, which allows for adaptations in the face of uncertainties and disruptions without losing control [9].

B. Financial Services Enterprises and Resilience

Financial services enterprises offer a range of financial services to their customers [12]. These service could be impacted by a number of expected or unexpected disruptions such as service failures, datacenter failures, equipment obsolescence, unforeseen intersystem interactions, human errors, cyber-attacks, regulatory changes, market changes, customer changes and technology changes [1-2, 12]. The concept of resilience which originated in the context of reliability engineering and system safety [13-14], is getting significant interest among financial services [12]. Financial services need to offer and run resilient services to operate effectively under stress [13], and to have the ability to adapt in response to disruptions to avoid any potential losses [4, 15]. A resilient service would be able to quickly recover from a disruption or disaster state and not experience undesirable long term service disruptions [16]. The rationale of being resilient is clear, the challenge for FSO (industry research partner) is: how to enable service resilience in the practical enterprise resilience context of FSO? This research paper aims to address this important research question by using the adaptive ADR method.

III. RESEARCH METHOD

ADR is an appropriate practice research method [8, 17] for designing, developing and evaluating artifacts that aim to address a practical phenomenon in its practical context, such as FSO context in our paper. ADR aims to release research results early and frequently as the project progresses. The adaptive ADR method incorporates three main elements: adaptive, action and design research. The "adaptive" element indicates the iterative nature of the ADR method in which desired artifacts are iteratively and concurrently developed, evaluated and communicated in increments for early feedback and adjustments. The "action" element indicates the interventionist and collaborative nature of the ADR method, where researchers and practitioners actively engage and collaborate to solve a practical problem or co-create value through intervention [18]. The "design" element indicates the constructive nature of the ADR method, which is aimed to contribute to the knowledge body by designing, developing and evaluating artifacts [19].

In order to address the practical research problem at hand, this research proposes the development of service-centric and architecture-driven AERM framework for FSO that requires iterative resilience framework element and related artifact development. Hence, based on [8, 20-21], we tailored and applied the adaptive ADR method in alignment with the FSO environment, which is anticipated as an appropriate approach for iteratively developing and evaluating the resilience framework. Artifacts and artifact knowledge are the two key outcomes of this ADR project, which can be generalized and transferred to other contexts. The ADR method is organized into four stages to incrementally deliver the desired framework elements: 1. Research Initiative [intuition/ idea and strategic initiative], 2. Initiate [problem formulation and objectives], 3. Integrated Discover and DevOps [building, intervention and evaluation (BIE) and reflection and learning (RL)], and 4. Close [formalization of learning and final feedback].

Researchers from UTS were approached by FSO in 2014 to cooperatively investigate service resilience within their organization. Intuition or idea for resilience project was discussed and scoped during the research idea workshops and meetings. This was then proposed as a strategic initiative, during the initial engagement and collaboration stage of the research initiative stage between the UTS researchers and FSO practitioners. This research initiative had the sponsorship and backing of the FSO CIO, which is extremely important for the success of any project or initiative. The research initiative triggered the Initiate stage, which further focused on defining the ADR project problem and objectives (vision and scope). The integrated Discover and DevOps (development and operations) stages involved the iterative discovery, development and operationalization of the desired resilience framework artifacts for FSO use. This refers to the continuous building, intervention, and evaluation (BIE), and reflection and learning (RL) of the artifacts in small increments. Finally, the Close stage will focus on formalizing of learning and final feedback at the end of the project. This project involves two researchers from UTS who actively worked (action research intervention) with the FSO team to design the resilience framework artifacts for solving the problem at hand. The core of the FSO team members come from enterprise strategy and architecture (enterprise architect), project delivery (business analysts, project manager and development team) and operations (operations delivery manager, analysts and senior manager) areas.

As discussed earlier, this paper builds on the first increment of the ADR [42], which was focused on understanding and analyzing the strategic initiative and FSO services. The initial ADR increment results (e.g. Service models and CiS system) and paper laid a foundation for this second increment of ADR. This paper presents the results from second increment of the ADR, in which we have updated the overall AERM framework (Fig. 1) and developed the FSO resilience characteristics and management capability model. The feedback from this second increment will be used to inform and deliver the subsequent increments of the AERM framework architecture elements and artifacts.

IV. THE AERM FRAMEWORK: BUILDING, INTERVENTION AND EVALUATION (BIE)

The AERM framework is being incrementally developed using the BIE activities (integrated Discover and DevOps stage) of the ADR method for service resilience in the overall FSO context of enterprise operational resilience. This involves

the review and analysis of existing related work with design and review workshops. The context of the focus area is important when considering enterprise resilience. An enterprise (private or public) operates in a relevant industry context such as the financial services industry context. Industry operates in a national and international regulatory context. These contexts have their own cultural context. This research is addressing the problem space from a particular enterprise context of public FSO, which operates in a financial services industry context in the overall national regulatory Australian context. One of the limitations of this research is that design of the AERM framework (Fig. 1) for FSO has been done in the local Australian context, however, the AERM framework can be further investigated and tailored for other contexts (e.g. industry, public/private, international). The current version of the AERM framework has four major elements with underlying artefacts (Fig. 1): *Strategy, Service, Service Resilience, and Service Operations.* The first increment [42] of the ADR project was focused on strategy and service elements. Second and third increments focus on service resilience. Finally, fourth increment focuses on service operations element.

A. Strategy (Increment 1)

Enterprise resilience must be in alignment with the enterprise strategy and stakeholders' value expectation [22]. To develop the AERM framework, we need to understand and analyze strategic intent, and use it to identify and develop framework elements. A series of stratgey workshops took place at FSO to understand and analyze the resilience project related strategic requirements (e.g. goals, objectives and value drivers (based on the BMM [23]). This includes increased service availability, reduced response time, and reduced security breaches. There are over 200 technology services in FSO. This strategic analysis provided the overall enterprise context and was used to identify an initial set of high value services from a criticality and availability perspective (targeting those services assessed as requiring Critical Availability (Tier 1) or Increased Availability (Tier 2) services) which are subject to resilience. This adaptive approach was adopted, as opposed to a traditional big bang approach, to initially focus on the most important services. An initial list of six services (e.g. email service, payment service) and related high level strategic resilience requirements were identified and a prioritized backlog of services developed.

B. Service (Increment 1)

A service is a fundamental unit of exchange in a service enterprise, where individuals or organizations voluntarily interact, co-create, offer and consume services for mutual benefits [24]. For enterprise resilience, firstly we need to identify and describe the enterprise services, beginning with the high value services. A series of service element design workshops were organised at FSO to iteratively develop the service element artifacts of the AERM framework (Fig. 1). The service element comprises of three key artifacts: service architecture model, service portfolio model and service lifecycle model. For instance, Fig. 2 describes the FSO service reference architecture model, which was developed (based on [25-26]) and used to describe and classify the FSO services in terms of human, technology and facility services, and their relationships (type and relationship strength). It can be seen from Fig. 2 that a service can self-reference and has relationship to other services. This paper's service-centric view does not detail the underlying components of each service due to privacy concerns of critical FSO environment information. However, details of each service and underlying components were modelled in detail in the service architecture model.

The Service Portfolio model was developed to manage the information about FSO's services across all three layers – human (business, social, information and professional services), technology (application, platform and infrastructure services), and facility (spatial, energy and ancillary services). A Service Lifecycle model was defined to manage the information about these different types of FSO services throughout their lifecycle. A service lifecycle model is a staged (e.g. in-pipeline, in-operation and retired services) approach to manage the services status across the various functions and processes. It is important to mention here that this research only addresses the resilience of services in-operation (operational resilience). Others may study the resilience of services in-pipeline, which is beyond the scope of this paper and research project.

These models were then recorded in a services Configuration Information System (CiS). The CiS was developed during increment 1 for managing the service architecture, portfolio and lifecycle information within the overall "service-centric" context of the AERM framework. CiS is one of the most critical systems supporting service resilience as it coordinates the recording, management and reporting of information about services and complex dependencies, which are subject to resilience. In a nutshell, the service element of the AERM was developed in increment 1 to identify and provide the information about the high value prioritized services (in alignment with the enterprise strategy), which are subject to resilience. Service element forms the basis and is a pre-requisite for the service resilience element (increment 2), which is the scope of this paper and is discussed in the next section.

C. Service Resilience (Increments 2 and 3)

Service resilience (item C in Fig. 1) is a large and core element of the AERM framework and is being delivered over two increments (2 and 3). The service resilience element has five major related artifacts: resilience characteristics, resilience management capability model, resilience requirements model, resilience assessment model and resilience assessment tool. It is important to mention here that similar to service element, the design of the service resilience element involves the review and analysis of the existing related work and design workshops. Service resilience element artifacts build on the existing resilience relevant concepts, models, methods and frameworks (see Table 1 and Appendix A & B). These well-known literature items were reviewed and used in design workshops to develop and evaluate the AERM framework elements for FSO. The focus of the framework is on operational resilience of the service, therefore, service

resilience workshops involved researchers from UTS and practitioners from FSO's operations management area.

1) Resilience Characteristics

Increment 2 presents the resilience characteristics and resilience management capability model in detail with updated evolving AERM framework and shared requirements model (shared between increments 2 and 3) (Fig. 1). The scope of this paper is limited to present the outcome from increment 2 for on-going communication and feedback. Increment 3 is focused on developing the resilience assessment model and tool, which is required to continuously assess and improve the resilience capabilities. These items from the service resilience element will be developed and presented after the completion of increment 3 in future communication.

The concept of resilience has been described differently by different authors in the literature (as discussed earlier in Section III). Before answering the research question: "how to enable service resilience…?", there is a need to contextualize the understanding of resilience concept for the FSO context. Therefore, based on the review of related work (see Table 1 and Appendix B) and applying to the FSO context, the resilience concept has been described in terms of 3 key resilience characteristics: defend (protection), respond (immediate response for sustainment) and evolve (adaptation). Resilience characteristics form the basis for identifying the resilience requirements (requirement model) and capabilities (resilience capability model) to defend the service and immediately respond and evolve in response to disruptions.

The resilience requirements model captures the specific resilience requirements to achieve the desired resilience goals or strategic requirements. For instance, in order to achieve the high availability goal with the associated requirements, the capability model includes a process called "availability management".

FSO needs to offer and run customer centric resilient services that are protected, sustained and adaptive to deliver an effective, efficient and stable customer experience. Defence is extremely critical for FSO and refers to minimizing and exploiting risks resulting from exposure to threats, vulnerabilities or disruptions. Immediate response refers to quick recovery for keeping the FSO services operational under stress (rebound and robustness). Evolution refers to the ability to adapt to exploit expected or unexpected changes for efficiency (routine changes and continuous improvement) and explore new practices for innovation (growth and transformation).

2) Resilience Capability Model

Service resilience can be enabled by defining, operating, managing, supporting and continuously adapting (optimizing) an integrated resilience management capability [5]. FSO needs to be supported by an integrated resilience capability. Resilience characteristics and requirements were used to guide the identification of the relevant operational capabilities. Resilience management capability model (Fig. 3) was co-created through several design and review workshops (see Appendix A for some workshop photos) both based on the review of literature (Table 1 and Appendix B) and existing FSO service operations. Service operations is a fourth element, which will be discussed in next section.

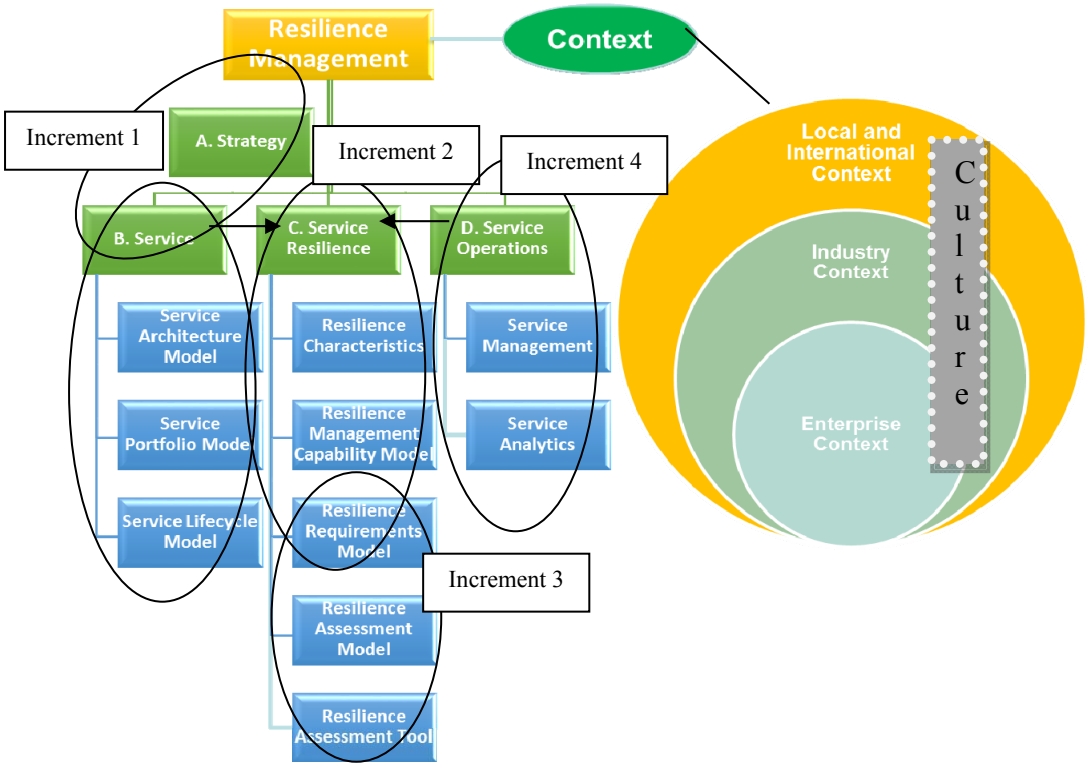


Fig. 1. The AERM Framework

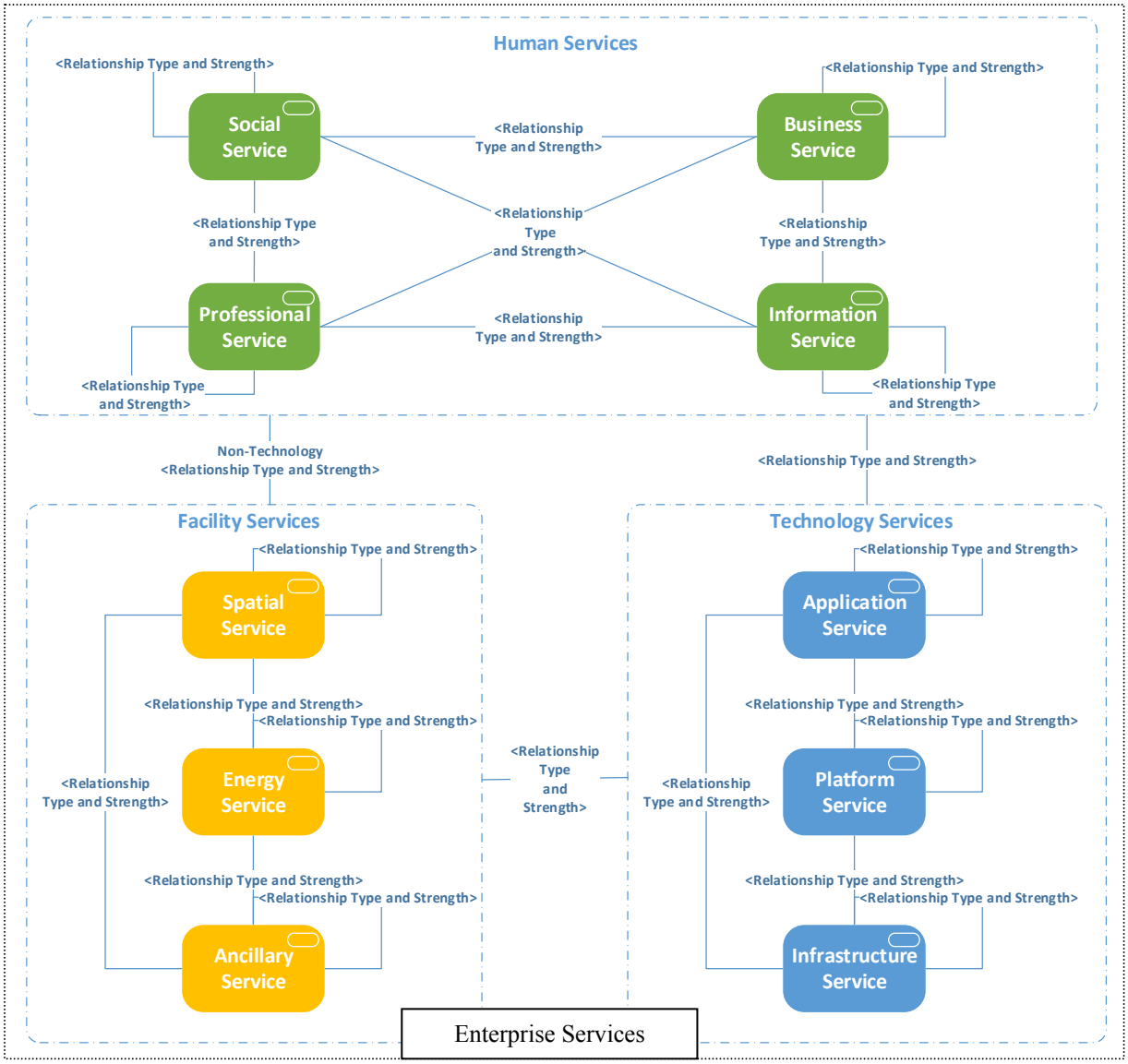


Fig. 2. FSO Service (Reference) Architecture Model (developed based on [25-26])

Resilience management capability model presents core and supporting capabilities/functions (i.e. Fig. 3 shapes with up arrow and blue color) and processes (i.e. shape with right arrow and yellow color). It was modelled using the ArchiMate (architecture modelling) standard. The FSO resilience capability model presents 39 resilience capabilities and relevant processes (Fig. 3). Traditionally, resilience capabilities such as continuity, availability and security management operate in isolation of each other with limited to no integrated engagement and governance [29]. This framework focuses on the integrated engagement and governance of different stakeholders across core and supporting resilience capabilities for the effective defence, fast response to routine changes and evolution for continuous improvement (efficiency), growth and transformation (innovation). It is important to note here that this paper does not claim that the capability model is complete or universal. This model has been designed to address the specific needs of the FSO in this action design research project. However, learnings from this model can be used to develop models for other enterprise contexts.

In summary, the capability model was developed through the careful analysis, mapping and review of the existing resilience models, methods, frameworks and standards (see Table 1) published in the public domain, and FSO operational capabilities and processes matching to the relevant resilience characteristics and requirements such as defend, respond and evolve. This is a good example of integrating theory and practice creating an actionable artifact. For instance, based on the Information Security Management Standard [27], the FSO information security management operational capability was identified as a core capability that is responsible to defend the services, and therefore, has been placed under the defend characteristic. Similarly, risk management capability was identified as supporting capability based on analysis of well-known COBIT 5.0 framework [28], IT4IT 2.0 reference model [29] and FSO risk management capability. Please see Appendix A for photos from design workshop examples and

Appendix B for detailed analysis and mapping of the resilience management capability model items to corresponding reference models, methods, frameworks and standards.

D. Service Operations

Service Operations have two key elements: service management and service analytics. FSO operates in a highly regulated and yet dynamic environment. Service management capabilities are organized into service strategy, design, transition, operation and continual improvement. FSO needs to defend and respond to maintain a steady internal state and yet evolve to address the ever-changing and emergent business, social, information and technology landscape whilst addressing disruptions. This is a challenging conflicting requirement – exploit the status quo on one hand and explore new ways of operating on the other. This requires an analytics-enabled adaptive approach to service management. Adaptive service management involves monitoring and analyzing large amount of operational service data and involves a number of processes associated with the services and underlying service components (technology and non-technology components), which are broadly known as service configuration items (CI). In this context, a service, being a part of another service, is also a CI, traditionally recorded in the CMDB (Configuration Management Data Base). Complex dependencies and integration management of several internal and external services of an enterprise is a reality.

Service analytics for planning, designing and implementing resilient and adaptive service are important and getting increased attention from service management professionals. Service management is a data-intensive decision-making capability involving continuous monitoring of services, collecting and analyzing data and information for different reporting metrics to enable sound operational decisions and actions to be made in a timely manner. Despite having the large amount of service data and information, predicting and effective decision making is still an arduous tasks for service management professionals. Whilst traditional reporting delivers high level overviews and statuses of services at a point in time, they do not offer the support needed by today's service management professionals. In contrast to traditional approach, contemporary analytics [30] can be applied to get useful and actionable insights through the complex linking of data and information for various service management related activities such as event, incident, problem, change, and capacity management. Thus, management of resilient and adaptive services can be assisted through the application of service analytics.

Analytics offers a range of powerful techniques such as trend analysis, root-cause analysis, regression analysis, forecasting and predictive modelling. These techniques can help service managers to go beyond traditional reporting and focus on extracting insights from the available information to enable appropriate adaptive actions to be taken. The applicability of the service analytics driven approach for resilient and adaptive service management seems useful to deal with the complex handling of known and unknown service disruptions. Therefore, service analytics has been identified and represented on the resilience management capability model (Fig. 3). Increment 4, future research (subject to funding beyond 2016), will focus on developing the analytics-enabled service management to support the overall AERM framework.

Table 1: Review of related work

Items	**Key Sources**
Resilience characteristics	[7, 31-37]
Systemic Resilience Model	[6]
CERT Resilience Management Model V1.2 (SEI)	[5]
CMMI Capability Maturity Model V1.3 (SEI)	[38]
Adaptive Capability Maturity Model V3.0	[25]
Integrated Service Innovation Method (iSIM)	[22]
IBM Resilience Framework	[39]
ITIL Framework V3.0	[40]
IT4IT Framework V2.0	[29]
The Gill Framework V2.0	[25]
COBIT 5.0	[28]
Information Technology Service Management Standard	[41]
Information Security Management Standard	[27]

V. Discussion : Reflection and Learning (RL)

FSO requires a framework for resilience, which is called here the AERM framework. This framework is being iteratively developed in short iterations and used at FSO. This paper (section IV) reported the outcomes (artefacts) from the Building, Intervention, and Evaluation (BIE) stage of the ADR method from the second increment. This section discusses a number of important observations and lessons learnt from this second increment, as a part of the Reflection and Learning (RL) stage of the ADR method.

Firstly, literature is scarce on service resilience, in particular within the financial services industry context. FSO is keen on adopting resiliency, however, they are unsure how to enable service resilience. This paper contributed to both theory and practice by filling this research gap and reported a research and practice based enterprise resilience framework to enable service resilience in the broader context of enterprise resilience.

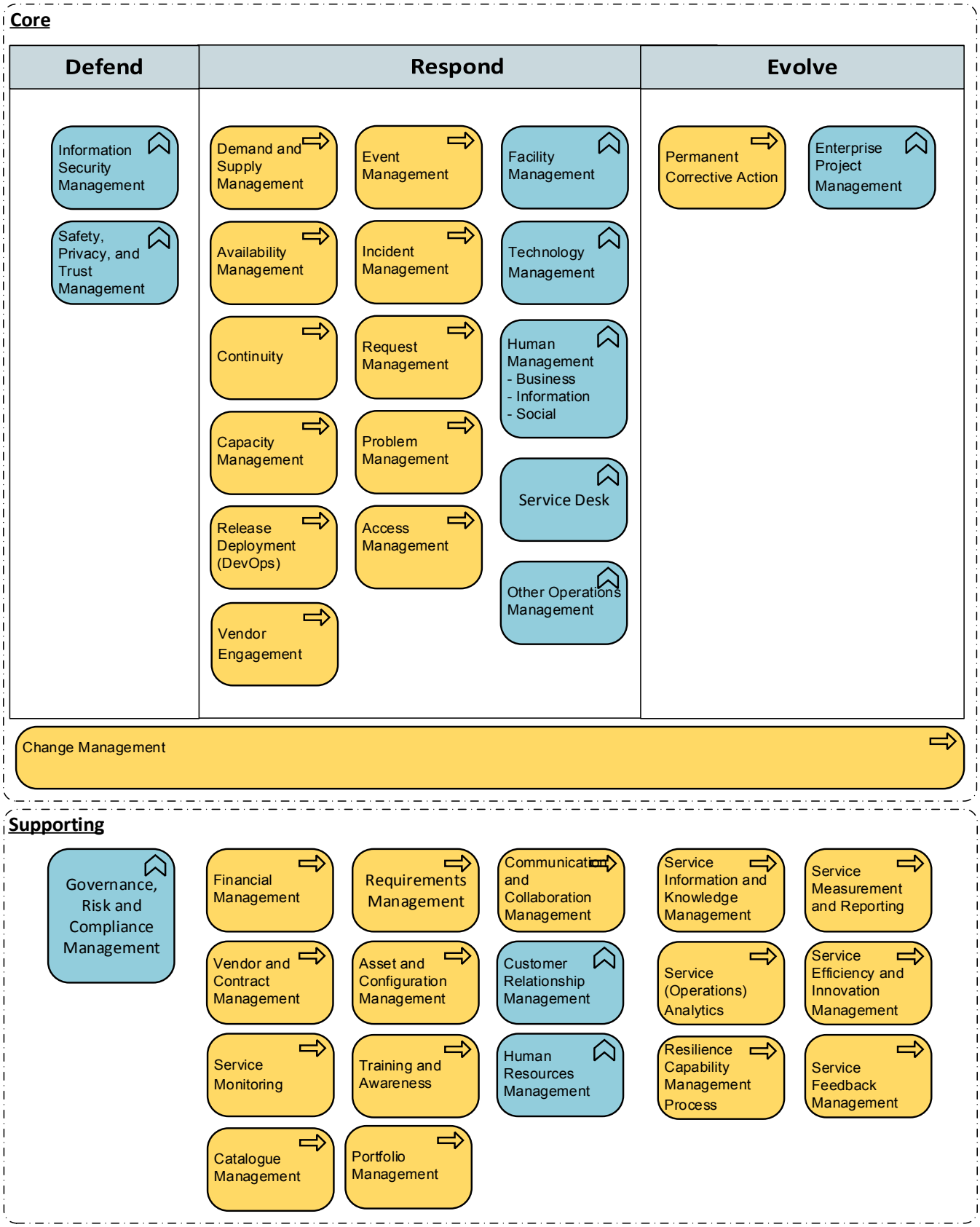


Fig. 3. FSO Resilience Management Capability Model (sub-capabilities and processes)

Secondly, developing such a large framework is not an easy task. It has been learnt that an adaptive or iterative approach to deliver the framework elements in small increments is appropriate by using the ADR method. A detailed upfront framework design and big bang delivery at the end of the project was considered risky, thus, we let the framework elements emerge in small increments. This demonstrated the value of ADR approach and incremental research benefits to the participating FSO organization where short increments trigger the benefit-response reaction leading to more engagement and higher quality result.

Thirdly, researchers (UTS) and practitioners (FSO) were actively engaged and participated in the framework design workshops for co-creating and evaluating the framework artefacts. The value co-creation concept from the service science body of knowledge has been found useful and guided to leverage the knowledge of researchers (UTS) and practitioners (FSO) for co-creating both theory and practice based artifacts for the desired framework.

Fourthly, while developing the resilience capability model (artefact), we learnt that traditionally isolated capabilities such as continuity, availability and security management need to be integrated for effective holistic enterprise resilience.

Fifthly, it is clear from this ADR research project that action-design is an impact and value driven research approach. It is a way to effectively link practice (practitioners) and research (academics) in co-creating innovative artifacts that target the challenges of industry. Instead of starting with a blank slate, we learnt that industry based existing frameworks and theory based academic literature informed the design workshop sessions. They were extremely productive and useful input in driving constructive discussions for developing the framework elements and underpinning artifacts.

Finally, it is important to highlight that the on-site researchers, active collaboration, availability and extensive industry experience of senior FSO practitioners and executive CIO ownership and sponsorship motivated the team and gave them necessary 'trust' and 'intellectual' power, and guidance to probe deeper the FSO environment. Further, the ADR research for a single FSO case could be considered a limitation when generalizing the results of this study. However, this paper lays a foundation for future action-design research cases in this important area of service resilience. Despite the single case limitation, a main research and practical contribution of this paper is the important demonstration of how to iteratively develop a large and complex framework for service resilience using the ADR research approach.

VI. Conclusion

This paper presented our ADR project results, from second increment, discussing the updated AERM framework, resilience characteristics and resilience management capability model for the FSO. The resilience management capability model is one of the important artefacts (part) of the overall AERM framework (whole) for enabling service resilience (main research question). The resilience capability model presents 39 capabilities (core and supporting) and processes in total, which are required to enable the resilience of 200+ technology services of FSO. The capability model design is guided and grouped by the three key characteristics of resilience: defend, respond and evolve. This capability model laid a foundation for ongoing research work with FSO, which will focus on developing resilience capability assessment model (metrics) and tooling, and service analytics to support the identified resilience capabilities. The research presented in this paper has both practical and research implications. The overall AERM framework and the resilience capability model and ADR approach discussed in this paper can be used and extended by other practitioners and researchers and can be tailored as appropriate to their local context. In future, we intend to further report the learnings to community from our ongoing action-design research at FSO.

Acknowledgment

We wish to extend our sincere thanks to FSO for providing financial support for this industry-academia collaboration action-design research project. Please also note that any views expressed in this paper are those of the author/s and not necessarily those of the FSO. Use of any results from this paper should clearly attribute the work to the author/s and not to the FSO. All the information contained in this paper is provided for educational and informational purposes only. No responsibility can be taken for any results or outcomes resulting from the use of this information. While every attempt has been made to provide information that is both accurate and effective, the authors do not assume any responsibility for the use or misuse of this information.

References

[1] R. Schneider, and J. Sledge, "The Future of Financial Services: Recommendations for Asset Building", Centre for Financial Services Innovation, 2011. http://www.cfsinnovation.com/content/future-financial-services-0.

[2] J. Mylonakis, "A Review of Banking Institutions' Transformation in Balkan Transition Economies: 1990-2000", *International Journal of Financial Services Management*, 2007, (2)1/2, pp. 100-117.

[3] IBM, "Business resilience: The best defense is a good offense: Develop a best practices strategy using a tiered approach", 2009. http://www.ibm.com/smarterplanet/global/files/us__en_us__security_resiliency__buw03008usen.pdf.

[4] A.Q. Gill, "Social architecture considerations in assessing social media for emergency information management applications". The Australian Journal of Emergency Management, 30(1), 17-21, Jan 2015:

[5] R.A. Caralli, J.H. Allen, and D.W. White. CERT Resilience Management Model. SEI. 2011.

[6] J. Lundberg, and B.J. Johansson, Systemic resilience model. Reliability Engineering and System Safety, 141, 22-32, 2015.

[7] D.D. Woods, Four concepts for resilience and the implicaitons for the future of resilience engineering. Reliability Engineering and System Safety, 141, 5-9, 2015.

[8] N. Papas, R. O'Keefe and P. Seltsikas, 'The action research vs design science debate: reflections from an intervention in eGovernment', European Journal of Information Systems, vol.21:2, pp. 147-59, 2012.

[9] L. Shen, and L. Tang, A Resilience Assessment Framework for Critical Infrastructure Systems. In Proceedings of 43rd Annual IEEE/IFIP Conference on Dependable Systems and Networks Workshop (DSN-W), 2013.

[10] E.A.M. Limnios, T. Mazzarol, A. Ghadouani, and S.G. Schilizzi, The resilience architecture framework: four organizational archetypes. European Management Journal, 32(1), pp.104-116, 2014.

[11] K. Furuta, and T.Kanno, Key Issues in Service Systems Resilience. In Proceedings of 43rd Annual IEEE/IFIP Conference on Dependable Systems and Networks Workshop (DSN-W), 2013.

[12] A.Q. Gill, D. Bunker, and P. Seltsikas, Moving Forward: Emerging Themes in Financial Services Technologies' Adoption. Communications of the Association for Information Systems, 36, 2015.

[13] C.S. Holling, Resilience and stability of ecological systems. Annual review of ecology and systematics, pp.1-23, 1973.

[14] A.W. Riggi, T.A. Saurin, and P. Wachs, A systematic literature review of resilience engineering: Research areas and a research agenda proposal. Reliability Engineering and System Safety, 141, 142-152, 2015.

[15] A. Rose and S.Y. Liao, Modeling regional economic resilience to disasters: A computable general equilibrium analysis of water service disruptions*. Journal of Regional Science, 45(1), pp.75-112, 2005.

[16] O. Erol, M. Mansouri and B. Sauser, A framework for enterprise resilience using service oriented Architecture approach. In Systems Conference, 2009 3rd Annual IEEE (pp. 127-132). IEEE, 2009.

[17] N.K. Denzin, and Y.S. Lincoln, "Handbook of Qualitative Research", 2nd ed, 2000.

[18] R. Baskerville and M.D. Myers, "SPECIAL ISSUE ON ACTION RESEARCH IN INFORMATION SYSTEMS: MAKING IS RESEARCH RELEVANT TO PRACTICE—FOREWORD", MIS Quarterly, 28(3), pp. 329-335, September 2004.

[19] A.R. Hevner, S.T. March, J. Park, and S. Ram, "Design science in information systems research", MIS Quarterly, 28(1), 75-105, 2004.

[20] R. Baskerville and A.T. Wood-Harper, Diversity in information systems action research methods. European Journal of information systems, 7(2), pp.90-107, 1998.

[21] M. Sein, O. Henfridsson, S. Purao, M. Rossi and R. Lindgren, Action design research, 2011.

[22] E.K. Chew, iSIM: An integrated design method for commercializing service innovation. Information Systems Frontiers, pp.1-22, 2015.

[23] OMG, Business Motivation Model (BMM), 2014. Available: http://www.omg.org/spec/BMM/, 2014.

[24] J. Spohrer, S. Vargo, N. Caswell, P. Maglio, "The Service System is the Basic Abstraction of Service Science", 41st Annual HICSS Conference Proceedings, 2008.

[25] A.Q. Gill, "Adaptive Cloud Enterprise Architecture", World Scientific Publishing, First Edition, 2015.

[26] A.Q. Gill, "Towards the Development of an Adaptive Enterprise Service System Model", AMCIS 2013, Chicago, USA.

[27] ISO/IEC 27001 - Information security management. http://www.iso.org/iso/home/standards/management-standards/iso27001.htm.

[28] COBIT 5.0. http://www.isaca.org/cobit/pages/cobit-5-framework-product-page.aspx.

[29] IT4IT 2.0. http://www.opengroup.org/IT4IT.

[30] J.G. Lou, Q. Lin, R. Ding, Q. Fu, D. Zhang and T. Xie, Software analytics for incident management of online services: An experience report. In Automated Software Engineering (ASE), 2013 IEEE/ACM 28th International Conference on (pp. 475-485). IEEE, 2013.

[31] E.H. Grotberg, The International Resilience Research Project, 1997.

[32] D. Robb, Building Resilient Organizations, 2000.

[33] E. Hollangel, D. Woods, N. Leveson, Resilience engineering: concepts and precepts. Ashgate Publishing, 2006.

[34] D.L. Alderson, and J.C. Doyle, Contrasting views of complexity and their implications for network-centric infrastructures. Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on, 40(4), pp.839-852, 2010.

[35] J. Allspaw, Fault injection in production. Communications of the ACM, 55(10), pp.48-52, 2012.

[36] L.H. Caporale and J. Doyle, In Darwinian evolution, feedback from natural selection leads to biased mutations. Annals of the New York Academy of Sciences, 1305(1), pp.18-28, 2013.

[37] S. Dekker, Second victim: Error, guilt, trauma, and resilience. CRC press, 2013.

[38] CMMI 1.3. http://www.sei.cmu.edu/cmmi/.

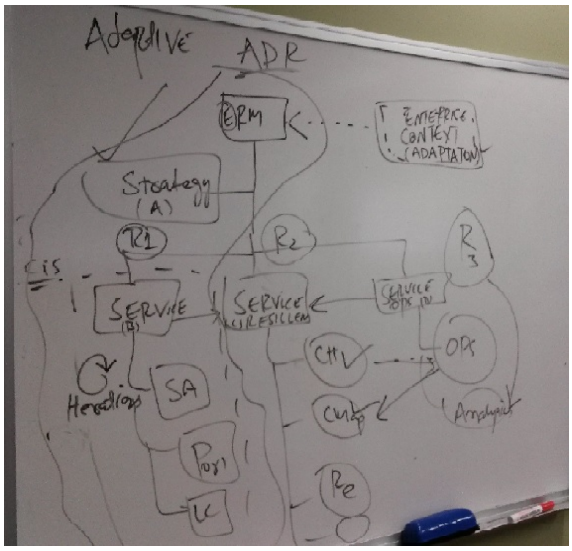
[39] IBM. IBM Resilience Framework. http://www-935.ibm.com/services/us/en/it-services/resilience-strategy-design.html.

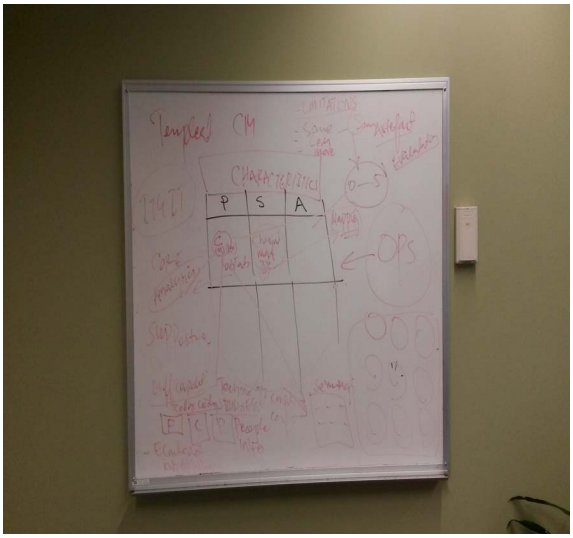
[40] ITIL 3.0. https://www.axelos.com/best-practice-solutions/itil.

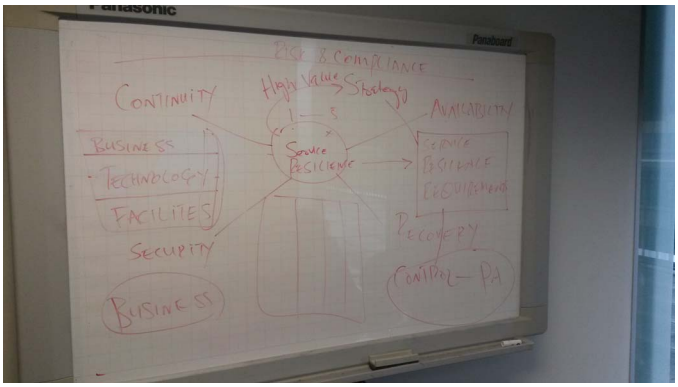
[41] Information Technology Service Management Standard. http://www.iso.org/iso/catalogue_detail?csnumber=51986.

[42] A.Q. Gill, E. Chew, G. Bird and D. Kricker, "An Agile Service Resilience Architecture Capability: Financial Services Case Study," 2015 IEEE 17th Conference on Business Informatics, Lisbon, 2015, pp. 209-216.

APPENDIX A: SERVICE RESILIENCE DESIGN WORKSHOPS EXAMPLES AND PHOTOS







APPENDIX B: DEATILED EXISTING WORK ANALYSIS AND MAPPING/ GENERATION OF RESILIENCE MANAGEMENT CAPABILITY MODEL

Items	**Type**	**Key Sources**
Defend (Protection); Respond (Sustainment) Evolve (Adaptation),	Characteristics	[7, 31-37]
Information Security Management; Safety, Privacy, and Trust Management	Core – Defend	Information Security Management Standard [27] ITIL Framework V3.0 [40]
Demand and Supply Management; Availability Management; Continuity; Capacity Management; Release Deployment (DevOps); Event Management; Incident Management Request Management; Problem Management; Access Management; Facility Management; Technology Management; Human Management; Service Desk; Vendor Engagement; Other Operations Management	Core – Respond	ITIL Framework V3.0 [40] Information Technology Service Management Standard [41] IT4IT Framework V2.0 [29] The Gill Framework V2.0 [25] CERT Resilience Management Model V1.2 (SEI) [5] IBM Resilience Framework [39]
Permanent Corrective Action; Enterprise Project Management	Core - Evolve	ITIL Framework V3.0 [40] Information Technology Service Management Standard [41] IT4IT Framework V2.0 [29] The Gill Framework V2.0 [25]
Change Management	Core - All	Systemic Resilience Model [6] ITIL Framework V3.0 [40] Information Technology Service Management Standard [41] IT4IT Framework V2.0 [29] Integrated Service Innovation Method (iSIM) – [22] The Gill Framework V2.0 [25]
Governance, Risk and Compliance Management (GRC); Portfolio Management; Catalogue Management; Financial Management; Vendor and Contract Management; Service Monitoring; Requirement Management; Asset and Configuration Management; Training and Awareness; Communication and Collaboration Management ; Customer Relationship Management; Human Resource Management; Service Information and Knowledge Management; Service (Operations) Analytics; Resilience Capability Management Process; Service Measurement and Reporting; Service Efficiency and Innovation Management; Service Feedback Management	Supporting	CERT Resilience Management Model V1.2 (SEI) [5] Systemic Resilience Model [6] ITIL Framework V3.0 [40] CMMI Capability Maturity Model V1.3 (SEI) [38] Integrated Service Innovation Method (iSIM) [22] Adaptive Capability Maturity Model V3.0 [25] IT4IT Framework V2.0 [29] COBIT 5.0 [28]