TOWARDS AN APPROACH FOR INTEGRATING BUSINESS CONTINUITY MANAGEMENT INTO ENTERPRISE ARCHITECTURE

Hanane Anir, Mounia Fredj and Meryem Kassou

AlQualsadi team, ENSIAS, Mohammed V University, Rabat, Morocco

ABSTRACT

In today's global and complex business environment, security is a major issue for any organization. All organizations should have the capability to plan and respond to incidents and business disruptions. Business continuity management is part of information security management and the process of Business continuity management (BCM) can meet these needs. Indeed, Business Continuity refers to the ability of a business to continue its operations even if some sort of failure or disaster occurs. Business continuity management (BCM) requires a holistic approach that considers technological and organizational aspects. Besides, Enterprise architecture (EA) is a comprehensive view of organizational architecture, business, and technology architecture and their relationships. EA is also considered by several studies as a foundation for BC and security management. Our research aims at studying how BCM aspect can be embedded into the enterprise architecture. In this sense, this paper proposes a metamodel and an implementation method that considers BC in the design and implementation of EA.

KEYWORDS

Business Continuity Management, Enterprise Architecture, Security Management, Enterprise Risk Management, MetaModeling.

1. INTRODUCTION

In a global, complex and connected world, organizations find themselves confronted with challenging environmental factors that create an undeniabledependency between Business and IT. Technologies and information systems become essential and constitute levers allowing businesses to grow, to be more efficient and competitive.

In this context,security and risk management is a major issue for any organization.Indeed, information unavailability can lead the enterprise to financial losses, and loss of confidence of its stakeholders and customers.It canalso affect its brand image, legal ramifications and, in some extreme cases, the company's existence.

Business Continuity (BC) refers to the ability of a business to continue its operations even if some sort of failure or disaster occurs. Several factors affect the level of BC such as data availability, application availability, networking reliability, operating system's reliability, etc.[1].

Business Continuity Management (BCM) is considered as a holistic management process that identifies potential threats to an organization and their impacts to business operations.

The purpose of BCM is to build an organizational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation and brand.

DOI: 10.5121/ijcsit.2019.11201

BCM should be an essential part of any contemporary organization's information management [1].

Currently, there is a lack of scientifically validated solutions to support continuity planning that are based on standards and best practice frameworks, capable of addressing the complexity and specific needs of organizations[2]. That's why BCM requires a global approach that considers several technological and organizational aspects.

Besides, Enterprise Architecture (EA) is a holistic view of organizational, business, and technology architectures and their relationships[3]. Moreover, EA is widely accepted as an essential mechanism for ensuring agility and consistency, compliance and efficiency; it can also be regarded as a foundation of business continuity planning, service management, and security management[4], [5].

If the interest of BCM and EA is greatly recognized, the integration of BCM in EA remains very limited.

Indeed, BCM is carried out independently of EA implementation or, at most,itis based on the EA as a base input [6].

Thus, it appears that BCM should be integrated into enterprise strategic planning to ensure proper alignment to meet business objectives and regulatory requirements [7].

The purpose of our research is to merge EA and BCM approaches. In this paper, we propose at first a metamodel for designing an EA enriched by BCM properties and metrics.Afterwards, we present an EA implementation lifecycle that considers the business continuity aspect upstream. This paper should profit to Small and Medium-sized enterprises (SMEs)by raising their awareness because they don't realize that the loss or unavailability of data would have a financial impact and undermine the credibility of their business [8]. SMEs can benefit from the results of this paper to design and implement a resilient enterprise architecture.

The remainder of this paper is organized as follows: Section 2 provides an overview of the theoretical background. Section 3 depicts related work. The details of our contribution are described in Section 4. The paper ends with a conclusion and an outlook on future research activities.

2. Foundations

2.1. Enterprise Architecture

According to the literature in the field [3], [9]–[14], EA is a comprehensive view of organizational, business, and technology architecture and their relationships. Enterprise Architecture is a concept that has been adopted by large companies for legal, economic and strategic reasons[15].

The primary aim of EA is to provide a greater understanding of an enterprise.It allowsconnecting the business drivers through business processes, organizational roles and responsibilities to the underlying IT Systems[16].

A well-implemented enterprise architecture helps a company to innovate and easily change by providing both stability and flexibility.

To build an EA, fulfilling a methodology or a process is required. Enterprise architecture Implementation Methodology (EAIM) covers the aspects of the EA lifecycle, including the planning, the analysis of business requirements, the design of systems, and the on-going enhancements[17].

While EA models represent as-is or to-be architectures of organizations, an EA framework provides[6]:

- One or more metamodel(s) for EA description,
- One or more method(s) for EA design and evolution,
- A common vocabulary for EA
- Reference models that can be used as templates or blueprints for EA design and evolution.

In a previous work related to Systematic Literature Review of Security and Enterprise Architecture [18], we provide many insights on how security is addressed in the most used enterprise architecture Frameworks like Zachman Framework, TOGAF, FEA, DoDAF and MODAF, through embedding the risk management or weaving with Enterprise Information Security Architecture (EISA)like SABSA.

2.2. Business Continuity Management (Bcm)

This section introduces some concepts related to BC. Business Continuity is defined by ISO 22301 and ISO 22313 as ‘the capability of the organization to continue delivery of products or services at acceptable predefined levels following a disruptive incident’.

ISO 22301 is based on the 'Plan-Do-Check-Act' model and sets out the requirements for a business continuity management system (BCMS), whereasISO22313 provides guidance for planning, implementing, monitoring and continually improving.

Business Continuity Management is a holistic management process that identifies potential threats to an organization and the business. Furthermore, It provides a framework for building organizational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities[1].

We can also find the concept of Business Continuity Plan (BCP), which is a documented collection of procedures and information in readiness for use in case of an incident. It enables an organization to continue to deliver its critical products and services at an acceptable predefined level.

3. Related Work

This section analyses and summarizes related works that have been carried out to link EA and BC by integration or alignment of their related models.

We have also considered in the analysis, researches related to risk management and model driven enterprise engineering.

Zadeh et al mentioned in their paper, that business continuity is regarded as one of the business principles of TOGAF.While implementing an EA using the Framework TOGAF, business continuity is taken into account in inherent manner.[19].

Tovstukhaproposes to align Enterprise Architecture model and Security Risk Management through ISSRM domain model (ISSRM DM).The alignment between EA and SRM was based on mapping of Archi Mate, an EA modeling language and MAD, a risk-oriented modeling language [20].

InnerHofer and Breu, in their approach, propose to use the advantages covered by the discipline of enterprise architecture to support an enterprise-wide holistic information security risk management.For that purpose, they make a bridge between their proper enterprise architecture metamodel and security model supported by relevant security information. This bridge reflects the status of the entire security process and connects the model elements with security artefacts such as threats, requirements, risks and countermeasures[21].

Rejeb et al. propose a definition of a methodological framework to implement continuity management that is part of a model-driven enterprise engineering approach based on ISO19440[22].The authors define specific views like Failure View, BCP View with properties related to continuity management such as criticality, Maximum tolerable period of disruption (MTPD), availability.

Mayer et al. claim that a connection between risk management and Enterprise Architecture Management (EAM) contributes in addressing the information security governance. Also, they motivate the added value of EAM to improve security risk management[4], [23].

The work of Gomes et al.provides adequate EA viewpoints, to assist BCP initiatives using the COBIT 5 manage continuity process. Also, they validate the EA's usefulness for assisting BCP[2].

Brazand Guerreiro propose a new approach to complement the management of the BCP, supported by a conceptual integration of the Design & Engineering Methodology for Organization (DEMO) and the Business Continuity Planning.The integration of DEMO with business continuity plan pretends to leverage the knowledge of business processes in place, in order to have a more broad and common understanding on the existing processes. In their work, the authorsmentionedthat compliance management, BCP, enterprise governance, risk management, IT service management are pointed as core application examples that can benefit from using EA-based approaches[24].

Our objective throughout this section is to give a synthesis of related work(eg, Table1). Therefore, we define a set of criteria to compare them:

- Dom: this criteriongives the research domain, BC (Business continuity) or RM (Risk Management), EA (Enterprise Architecture or MDEE (Model Driven Enterprise Engineering) or both
- MM: this criterion specifies if the work use existing metamodel or proposesa new one.
- Align: this criterion points out if there is any alignmentof EA or MDEE and BC or RM Models
- Integ: Integration of EA or MDEE and BC or RM Models
- Meth: this criterionspecifies if the work proposes a process or a methodology
- Prop:does the work use BC or Risk properties and metrics?

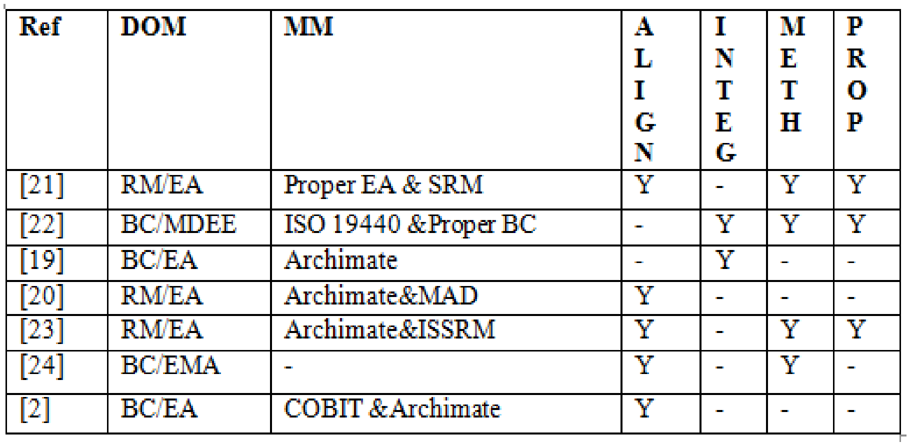
From this review (eg, Table1), we note that most existing works have taken up the issue of linking BC/RM and EA by aligning their models or taking the enterprise architecture as a baseline. Only one paper (Rejeb et al., 2012) designs a metamodel based on a model driven engineering “ISO 19440” integrated with BC model and enriched by the inherent notion of business continuity.

Furthermore, we noticed that there is no work that presents an approach considering the integration of business continuity management into EA metamodel and an implementation methodology considering the business continuity upstream.

According to this analysis, our objective is to propose:

- A new EA metamodel integrating business continuity through a set of BC properties
- An approach for embedding the business continuity aspect into the EA through an implementation Lifecycle.

Table 1. Related work analysis.



Ref	DOM	MM	ALIGN	INTEG	METH	PROP
[21]	RM/EA	Proper EA & SRM	Y	-	Y	Y
[22]	BC/MDEE	ISO 19440 &Proper BC	-	Y	Y	Y
[19]	BC/EA	Archimate	-	Y	-	-
[20]	RM/EA	Archimate&MAD	Y	-	-	-
[23]	RM/EA	Archimate&ISSRM	Y	-	Y	Y
[24]	BC/EMA	-	Y	-	Y	-
[2]	BC/EA	COBIT &Archimate	Y	-	-	-

4. CONTRIBUTION

Our contribution covers three main disciplines: enterprise architecture, business continuity and metamodeling.

According to the design research reference process[25] , this paper documents theconstruction of an artefact (EA metamodel integrating business continuity aspect).

In this context, we present first an EA metamodelintegrating business continuity aspect. We highlight some business continuity metrics and their related properties that we will define, and we will include in the proposed enterprise architecture model. Then, we propose an EA implementation Lifecycle. After that, we carry outthe mapping between thisLifecycle and a selected business continuity Lifecycle.

4.1. Enterprise Architecture Metamodelintegrating BC(Eaibc)

An EA metamodel formalizes the definition of enterprise architecture perspectives and the relationships between their components.

Based on the most used frameworks for enterprise architecture[14], [26]–[28] and different researches axed on defining Metamodel for designing of EA[5], [6], [29]–[33], we distinguish four major perspectives:

- Strategy/Business
- Process/Organizational
- Application/Integration/Information
- Software/Technical/Technology

For the EA metamodel that we propose, we discern four main perspectives, focusing on different levels of abstraction: business, information System (IS), technology, and an additional and new one for business continuity. The different perspectives are interconnected, and these interconnections depict the dependencies.

We use the UML notation to construct the design of the meta model.

The business perspective's objective is to have a clear picture of the vision, to identify the target strategy and to determine the mission and goals with stakeholders and operational staff.This perspective describes the processes that the business uses to meet its goals and the functional requirements.Furthermore, it is the base for identifying the requirements for IS, which support the business activities.

The Information Systemperspective describes the systems and applications, how they are designed and how they interact with one another.Also,it depicts how the enterprise data stores are organized and accessed.

The technology perspective exposes the network/cloud related standards and technologies and describes the hardware and software infrastructures that support the applications and their interactions.

Regarding the business continuity perspective,it exposes the business continuity objectives and retraces the likely risks and their impact. Also, it contains the BCP and countermeasures which the organisation must operate to overcome these risks.

We present in detail below (eg, Figure 1) the different perspectives as a metamodel.

Hereafter we present some definitions of the concepts used in the proposed metamodel.
A mission is the statement of purpose from which a company, business or individual operates. The mission statement is designed to guide the everyday actions and decisions made by a business or organization.

Goals have specific results that are achievable, measurable and temporal. A goal is a stated result or specific aim that an individual or team works toward. The goal would be a bit more specific and attempts to define accomplishment of the mission.

A strategy is the way to develop, direct and coordinate action plans to achieve a specific goals, programmed over the short or long term.

A stakeholder is an individual or group having an interest in the performance or success of an organization [34]. Every stakeholder has different business concerns and requirements. Without agreement from most of stakeholders, it is difficult to keep progress towards the goals. Indeed, the consensus of the stakeholders is essential to the smooth running of the strategy.

Requirements define needs and expectations from the perspective of the stakeholders depending of their roles in the business.

These requirements respond to stakeholder concerns regarding the efficiency, economy and effectiveness of monies. And by addressing these concerns it implies maintaining good relationships with stakeholders and sustaining long-term profitability.

A function is an area that the organization wants to pay attention in order to support its business goals.

A business service represents the added value that an organization delivers to its environment. One can make a distinction between internal and external services [35].

An organizational unit is a collection of people who work together toward a common goal and govern various business service. It can be an internal or external unit.

A business process is a collection of related, structured activities or tasks which in a specific sequence produce a service or product.

A business role is a group of related skills with a level of authority to perform a given task.

An Actor is an active element with responsibility within the organization. This can be an internal or external person, or a group of people who has a role that initiates or interacts with activities.

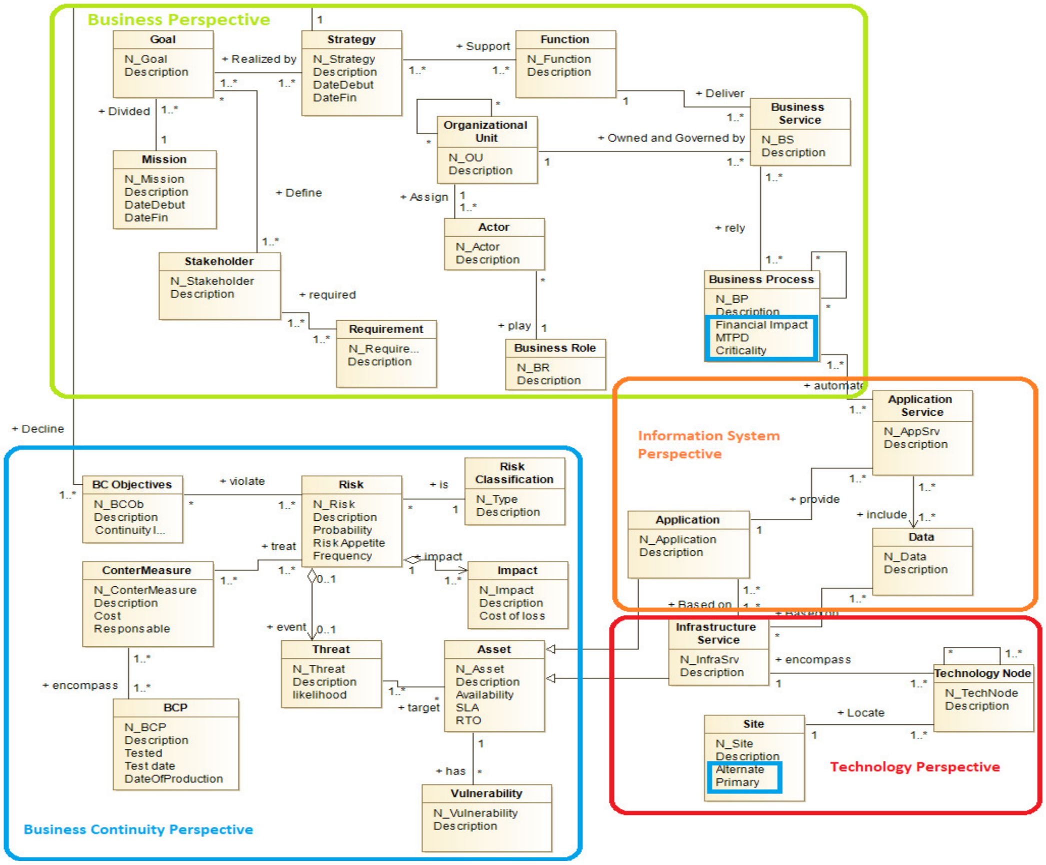


Figure 1. Our proposed EA metamodel Integrating BC (EAiBC)

An *application* is a deployed and operational IT system that supports business functions and services (for example, anHR Information system).

An *application service* is a service provided by the application to support the business process (for example, a HR Self-service or payroll).

*Data*is information used as a basis for reasoning, discussion, or calculation and is represented or coded in some form suitable for better usage or processing.

*Asset*is any tangible or intangible thing or characteristic that has value to an organization. In our case we mean by asset the technical platforms and applications.

An *infrastructure service* is thetechnical platforms that supports applications and data (for example, a cluster).

A *technology node*refers to a component whose infrastructure is based on (for example, a network, switch, virtual machine).

*Site*is the spatial location of an actual or planned datacentre. It can be an alternate site held in readiness for use during a Business Continuity invocation to continue the urgent and important processes of an organization.

Countermeasure invokes decisions, requirements and controls, which should be implemented to prevent or mitigate possible risks.

Vulnerability can be characterized as any weakness in an asset such as application, servers, or infrastructure that could be intentionally or unintentionally exploited by a threat.

Risk is the possibility that an event will occur and adversely affect the achievement of objectives.
Threat is a negative event that targets a corporate assetand can lead to loss or a disruption of the organization's operations, services, or functions.

Business Continuity Objective (BCO) is used to define strategic and tactical objectives for assurance of business continuity.BCO shall take account of the minimum level of products and services that is acceptable to the organization to achieve itsbusiness objective.For instance,create and disseminate a positive image and reputation of the enterprise, avoid supply chain disruptions.
BCP is a plan to help ensure that business processes can continue during a time of emergency or disaster.

Impact is the consequence of the occurrence of a risk. It may be financial, technical, economic or political.

RiskClassification is a typology of risk. For instance, natural, hazard, terrorism...
Risk management and continuity management approaches complement each other. Business continuity management puts more emphasis on impact analysis and measures to reduce these impacts.

In this context, to model the business continuity perspective, we got based on the basic concepts of risk management and have completed it with the concepts of business continuity.

We have enhanced the enterprise architecture metamodel proposed above (eg, Figure 1) by BC properties and their related metrics. It will allow to:

- Evaluate the criticality of the business processes and the financial impact of downtime
- Assess the impact of the inherent risks
- Estimate the probability of production of a threat
- Determine what level of resiliency and availability is required
- Define the business objectives of business continuity

In the proposed metamodel, we surroundedin blue the classes related to BC and the properties added to other classes in the Business and technology perspective.

Based on literature review [14], [17], [22], [27], [28], [36]–[43], we conduct a synthesis of BC metrics and concepts(eg,Table2).

Table 2.BC Metrics and Concepts.

Ref	**BCM Concepts**	**BCM Metrics**
[22]	BCP Failure Impact Disruptive event	Criticality Maximum tolerable period of disruption (MTPD) Availability Time of unavailability Sensitivity to time Probability Impact severity level
ISO22313 [40, p. 22313]	Business continuity objectives Business Impact analysis Risk Assessment BCP	Minimum acceptable level of operation Recovery time objective Recovery point objective Risk Appetite
COSO ERM [17]	Enterprise risk management	Risk Appetite Risk Tolerance Risk capacity Likelihood Impact
ISACA/ COBIT [41]	Business continuity objectives Business Impact analysis BCP Incident response	Recovery time objective Recovery point objective SLA Criticality Cost Availability Capacity
NIST [42], [43]	Preventive control Alternate Site	Recovery Priority Criticality Impact Availability Cost Allowable outage time SLA

We distinguish from these metrics those we consider relevant and we enhance our proposed metamodel, namely:

- Financial impact: an assessment of the revenue loss for the company in the case of disruption of a business process, in other terms the cost of downtime.

- We prefer to use this term because it's more significant than the use of cost.
- Maximum Tolerable Period of Disruption (MTPD) [39]: The MTPD expresses the maximum acceptable downtime. This metric is determined by the business unit, defined on business processes and depends on organization goals.
- The Existence of SLA: a service-level agreement (SLA) is a contract between a service provider and its internal or external customers that documents what services the provider will furnish and defines the performance standards the provider must meet.
- Recovery Time Objectives (RTO) [37], [39]: is the maximum tolerable length of time that an asset can be down after a failure or disaster occurs.
- Recovery Point Objectives (RPO) [37], [39]: is the maximum amount of data that is acceptable to lose during a failure. Quantifying the RPO defines the backup objectives, which requires knowing the volume.
- Availability ensures reliability and timely access to data and resources to authorized individuals.
- Criticality: an assessment of the critical functions or process of company which prevent the company to undertake its activities and can cause financial losses.
- Risk appetite can be defined as 'the amount and type of risk that an organization is willing to take in order to meet their strategic objectives' [36], [38].
- Likelihood is the possibility of occurrence of risk
- Probability is the possibility of a threat occurring
- Frequency is as a number of exposure risk for a unit of time.

4.2 EA LIFECYCLE

The literature review shows that various Enterprise Architecture Implementation Methodologies (EAIM) are proposed, such as ADM for TOGAF, Collaborative Planning Methodology for FEAF and MODAF and DODAF 2.0 Method for DODAF.

Hereafter, we propose a simple process inspired by these different EAIM (eg, Figure 2).

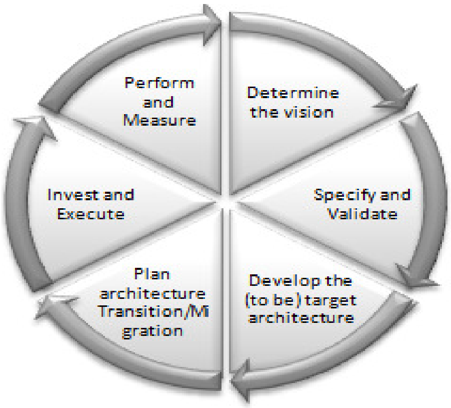

Perform and Measure
Determine the vision
Specify and Validate
Develop the (to be) target architecture
Plan architecture Transition/Mi gration
Invest and Execute

Figure 1. The proposed EA Lifecycle

The proposed process is an iterative and cyclical process, which consists of six phases:

1. Determine the vision phase During this phase, it is a question of identifying and defining the stakeholder's requirements, business objectives and purpose, key drivers, and critical issues and risks.

2. Specify and validate phase In this step, it is about defining the scope, characterizing and analysing the baseline architecture, and validating and prioritizing the needs and the target performance metrics
3. Develop the target Architecture phase As part of this phase, the emphasis is to develop the Target Architecture that describes how the enterprise needs to operate to achieve the business goals and respond to the strategic drivers while leveraging the experiences and opportunities.
4. Plan architecture Transition / Migration phase Throughout this phase, the gap between the as-is and to-be architecture is analysed, in order to define the road map to address the business needs. In other words, this phase is an opportunity to determine the business constraints for EA implementation before defining the migration/transition plan.
5. Invest and Execute phase The purpose of this phase is to execute the migration plan and to implement successfully the planned changes.
6. Perform and Measure phase This phase corresponds to a governance level.The purposeis to measure performance outcomes against the target performance metrics. It is indeed essential to establish a continual monitoring and change process, to ensure that the architecture responds to the needs of the enterprise and maximizes the value of the architecture to the business.

4.3 EMBEDDING BUSINESS CONTINUITY LIFECYCLE INTO EA LIFECYCLE

In this section, we will map the proposed Lifecycle with a selected BCM Lifecycle to produce finally an EA lifecycle integrating business continuity.

We have selected the Business Continuity Management Lifecycle(eg,Figure 3) defined by ISO 22301:2012 and ISO 22313: 2012, and the Business Continuity Institute Good Practice Guidelines GPG 2013.[40], [44].

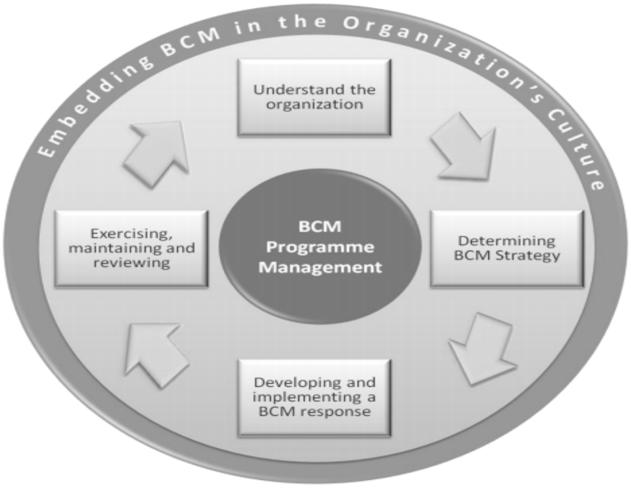

Embedding BCM in the Organization's Culture
Understand the organization
Determining BCM Strategy
Developing and implementing a BCM response
Exercising, maintaining and reviewing
BCM Programme Management

Figure 2. Business Continuity Management Lifecycle (ISO 22301:2012)

The BCM Lifecycle is divided into 4 stages:

1) Understand the organization

During this phase, it is a question of:

- Identifying key products, services and critical activities which support them
- Identifying organizations objectives, obligations
- Identifying supporting activities, assets, and resources
- Assessing the impact of failure of activities, assets, and resources
- Identifying and evaluating threats
- Identifying all interdependencies of activities

2) Determining BCM Strategy

In this step, it is about:

- Definition of incident response structure enabling an effective response & recovery
- Identification of restart timescales and service levels following a disruption
- Agreement of timescales to restore normal service levels
- Modification of the strategy as an output of management review in response to internal or external events

3) Developing and implementing a BCM response

During this phase, it is a question of:

- Alignment to the objectives of the organization's BCM strategy
- Development of plans to effectively manage a business disruption to the point it is contained
- Creation of business continuity plans designed to facilitate the resumption of critical activities

4) Exercising, maintaining and reviewing

In this step, it is about

- Validating effectiveness of plans
- Ensuring understanding of plans, roles & responsibilities
- Identifying improvement opportunities
- Maintaining relevance of plans as result of business changes

After analysing the BCM Lifecycle presented above, we have proposed a mapping between the BCM lifecycle phases with the proposed EA lifecycle process phases.

The emphasis is put on clarifying how the business continuity process can be part of the enterprise architecture lifecycle.

All the activities planned in the first phase of BCM Lifecycle are included in the first phase of EA Lifecycle.

The Specify and validate phase can be supported by a business impact analysis and risk assessment and the definition of a business continuity management strategy, to determine the critical business functions.

On the other hand, during the phase Develop target architecture of EA, we can foresee the alignment to the objectives of the organization's BCM strategy. The Business Continuity Plan can be one of the outputs of the process of this phase.

In the Perform and Measure phase of enterprise architecture, it is necessary also to govern the business continuity aspect, because an effective business continuity plan should be regularly reviewed and tested.

Hereafter, a diagram that summarizes the mapping of the EA and BCM Lifecycles (eg,Table 3). We highlight the BCM aspect in bold.

Table 3: Mapping of the EA and BCM Lifecycles.

EA Lifecycle ex BC	**Activities**
Determine Vision Phase	• Identify the stakeholder's requirements • Define Business objectives and purpose, key drivers
Specify and validate	• Define the scope • Characterize and analyse the base line architecture • Validate and prioritize the needs and the target performance metrics • **Business impact analysis and risk assessment**
Develop target Architecture	• Develop the Target Architecture **based on the proposed meta model** • **Define the business continuity management strategy**
Plan architecture Transition / Migration	• Analyse the gap between the as-is and to-be architecture • Define the road map to address the business needs • Comply the capability of the enterprise to undergo the change • Define the migration/transition plan
Invest and Execute	• Execute the migration plan • Implement successfully the planned changes • **Establish and implement business continuity procedures** • **BC Plan Development** • **Perform tests and simulations of business continuity plan**
Perform and Measure	• Govern and measure performance outcomes against identified metrics • Perform enterprise architecture compliance compared to the company goals • **Maintenance and training about the business continuity plan**

5. Conclusion And Future Work

Throughout this paper, we have proposed at first an enterprise architecture metamodelincluding a specific perspective dedicated to BC.Furthermore, we have defined a set of metrics and their related properties focused on business continuity aspect. We have also enhanced our proposed EA metamodel by these properties. Regarding the enterprise architecture implementation Lifecycle, it was extended by activities related to business continuity.

Our future work will focus on eliciting Business Continuity metrics and using them for a quantitative analysisfor assessing the level of consideration of BC in the EA.

Hence,putting into practice the proposed concepts through the development of a modelling tool. Finally,we will validateour contribution by a case study through applying it for selected SMEs, to evaluate the value of our proposal.

REFERENCES

[1] N. Bajgoric et Y. B. Moon, « Enhancing systems integration by incorporating business continuity drivers », Ind. Manag. Data Syst., vol. 109, no 1, p. 74-97, janv. 2009.

[2] P. Gomes, G. Cadete, et M. M. da Silva, « Using Enterprise Architecture to Assist Business Continuity Planning in Large Public Organizations », 2017, p. 70-78.

[3] N. Banaeianjahromi et K. Smolander, « What do we know about the role of enterprise architecture in enterprise integration? A systematic mapping study », J. Enterp. Inf. Manag., vol. 29, no 1, p. 140-164, févr. 2016.

[4] N. Mayer, E. Grandry, C. Feltus, et E. Goettelmann, « Towards the ENTRI Framework: Security Risk Management Enhanced by the Use of Enterprise Architectures », in Advanced Information Systems Engineering Workshops, vol. 215, A. Persson et J. Stirna, Éd. Cham: Springer International Publishing, 2015, p. 459-469.

[5] R. Winter et R. Fischer, « Essential layers, artifacts, and dependencies of enterprise architecture », in 2006 10th IEEE International Enterprise Distributed Object Computing Conference Workshops (EDOCW'06), 2006, p. 30–30.

[6] T. Bucher, R. Fischer, S. Kurpjuweit, et R. Winter, « Analysis and application scenarios of enterprise architecture: An exploratory study », in Enterprise Distributed Object Computing Conference Workshops, 2006. EDOCW'06. 10th IEEE International, 2006, p. 28–28.

[7] Andrew Hiles, Definitive Handbook of Business Continuity Management. John Wiley & Sons, 2011.

[8] S. Snedaker et C. Rima, Business continuity and disaster recovery planning for IT professionals, 2. ed. Waltham, Mass: Elsevier, Syngress, 2014.

[9] S. Bernard, An Introduction To Enterprise Architecture: Second Edition 2nd Edition. 2012.

[10] S. Bente, U. Bombosch, et S. Langade, Collaborative Enterprise Architecture: Enriching EA with lean, agile, and enterprise 2.0 practices. Newnes, 2012.

[11] Charles Tupper, Data architecture: from zen to reality. Elsevier, 2011.

[12] K. D. Niemann, From enterprise architecture to IT governance: elements of effective IT management, 1. ed. Wiesbaden: Vieweg, 2006.

[13] B. Scholtz, A. Calitz, et A. Connolley, « An analysis of the adoption and usage of enterprise architecture », in Enterprise Systems Conference (ES), 2013, 2013, p. 1–9.

[14] J. Zachman, « The zachman framework for enterprise architecture », Zachman Int., p. 79, 2002.

[15] R. V. McCarthy, « Toward a unified enterprise architecture framework: An analytical evaluation », Issues Inf. Syst., vol. 7, no 2, p. 14–17, 2006.

[16] J. Ralyté, S. España, et Ó. Pastor, Éd., The Practice of Enterprise Modeling, vol. 235. Cham: Springer International Publishing, 2015.

[17] M. S. Beasley, B. V.Handcock, et B. C.Branson, « Strengthening Enterprise Risk Management for Strategic Advantage ». Coso, 2009.

[18] H. Anir, M. Kassou, et M. Fredj, « Systematic Literature Review of Security and Enterprise Architecture », présenté à 4th International Workshop on Advanced Information Systems for Enterprises (IWAISE'16), Rabat Morocco, 2016.

[19] M. E. Zadeh, G. Millar, et E. Lewis, « Mapping the Enterprise Architecture Principles in TOGAF to the Cybernetic Concepts--An Exploratory Study », 2012, p. 4270-4276.

[20] I. Tovstukha, « Management of Security Risks in the Enterprise Architecture using ArchiMate and Mal-activities », p. 53, 2014.

[21] F. Innerhofer-Oberperfler et R. Breu, « Using an Enterprise Architecture for IT Risk Management. », in ISSA, 2006, p. 1–12.

[22] O. Rejeb, R. Bastide, E. Lamine, F. Marmier, et H. Pingaud, « A model driven engineering approach for business continuity management in e-Health systems », in Digital Ecosystems Technologies (DEST), 2012 6th IEEE International Conference on, 2012, p. 1–7.

[23] N. Mayer, J. Aubert, E. Grandry, C. Feltus, E. Goettelmann, et R. Wieringa, « An integrated conceptual model for information system security risk management supported by enterprise architecture management », Softw. Syst. Model., févr. 2018.

[24] J. Brás et S. Guerreiro, « DEMO Business Processes Design to Improve the Enterprise Business Continuity Plans », in Advances in Enterprise Engineering XI, vol. 284, D. Aveiro, R. Pergl, G. Guizzardi, J. P. Almeida, R. Magalhães, et H. Lekkerkerk, Éd. Cham: Springer International Publishing, 2017, p. 99-107.

[25] K. Peffers, T. Tuunanen, M. A. Rothenberger, et S. Chatterjee, « A Design Science Research Methodology for Information Systems Research », J. Manag. Inf. Syst., vol. 24, no 3, p. 45-77, déc. 2007.

[26] C. M. Pereira et P. Sousa, « A method to define an Enterprise Architecture using the Zachman Framework », in Proceedings of the 2004 ACM symposium on Applied computing, 2004, p. 1366–1371.

[27] A. Role et D. Role, « The DoDAF Architecture Framework Version 2.0 », 2011.

[28] The Open Group, TOGAF® Version 9.1. Van Haren Publishing, ZaltBommel, 2011.

[29] S. Aier, C. Fischer, et R. Winter, « Construction and evaluation of a meta-model for enterprise architecture design principles », 2011.

[30] F. J. Armour, S. H. Kaisler, et S. Y. Liu, « Building an enterprise architecture step by step », IT Prof., vol. 1, no 4, p. 31–39, 1999.

[31] J. Hoogervorst, « Enterprise architecture: Enabling integration, agility and change », Int. J. Coop. Inf. Syst., vol. 13, no 03, p. 213–233, 2004.

[32] F. Innerhofer et R. Breu, « USING AN ENTERPRISE ARCHITECTURE FOR IT RISK MANAGEMENT », p. 12.

[33] R. Winter et J. Schelp, « Enterprise architecture governance: the need for a business-to-IT approach », in Proceedings of the 2008 ACM symposium on Applied computing, 2008, p. 548–552.

[34] L. B. FBCI, « Dictionary of Business Continuity Management Terms », 2011.

[35] M. Lankhorst, Enterprise Architecture at Work. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009.

[36] « ISO/Guide 73:2009 ». 1, nov-2009.

[37] P. Kirvan, « The Importance of Performance Metrics in Business Continuity », 2014.

[38] RIMS, « Exploring Risk Appetite and Risk Tolerance ». RIMS, 2012.

[39] E. Zambon, D. Bolzoni, S. Etalle, et M. Salvato, « A model supporting business continuity auditing and planning in information systems », in Internet Monitoring and Protection, 2007. ICIMP 2007. Second International Conference on, 2007, p. 33–33.

[40] ISO, « ISO 22313 ». 2012.

[41] A. Singh, « CoBIT 5: Managing Continuity Aspects With A Practical Approach », p. 25, 2015.

[42] M. Swanson, P. Bowen, A. W. Phillips, D. Gallup, et D. Lynes, « Contingency planning guide for federal information systems », National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-34r1, 2010.

[43] M. Swanson, A. Wohl, L. Pope, T. Grance, J. Hash, et R. Thomas, « Contingency planning guide for information technology systems :: recommendations of the National Institute of Standards and Technology », National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-34, 2002.

[44] ISO, « ISO 22301 ». 2012.