The Enterprise Architect as a Crisis Manager: Insights from Lufthansa

Carsten Breithaupt[1], Jonas Vieracker[2], Alina Chircu[3], Sean Cox[4], Eldar Sultanow[5]

Abstract: In this paper we argue that the Enterprise Architect (EA) should be considered as a crisis manager. In times of a crisis organizations must create a holistic view on the situation and evaluate the proposed measures. Evaluation will be based on experience, data, upfront-created scenarios and assessments of risks, cost and benefits. The EA is already engaged in processes such as Continuity Management, Risk Management, IT Security, Business Process Management, IT Strategy, and others. Therefore, we propose that the EA is one good candidate (not the only one) for handling organizational crises. This paper presents a model of overall crisis management that incorporates an enterprise architecture view as well as related dimensions of crisis management: the ability to control a crisis, the level of communication during and after a crisis, the type of change brought by a crisis, the crisis' outcomes, its distribution within an enterprise, and an organization's criticality of business functions. Finally, we highlight how the EA role supports crisis management at Lufthansa, a top German aviation company.

Keywords: Crisis Management; Enterprise Architecture; Lufthansa

1 Introduction

Major, large-scale incidents such as the COVID-19 pandemic, the WannaCry cyberattack, Target's consumer data breach, the 9/11 terrorist attacks, Volkswagen's emissions scandal, or the Exxon Valdez and BP oil spills have repeatedly demonstrated that organizations are prone to significant internal and external threats as well as risks resulting from mismanagement of how threats are addressed [Bu17, Ko20, PC98]. These events can all be characterized as an organizational crisis – *"an event perceived by managers and stakeholders as highly salient, unexpected and potentially disruptive"* [Bu17]. For the most part, companies do not anticipate these kinds of crises and suffer severe losses, during and even after the crises – perhaps because each predicament is different and needs special treatment in order to prevent, detect and control the impact, avoid damage and accelerate recovery. Thus, the better a risky situation is analyzed and the more sophisticated the crisis management capability of an enterprise is, the better an organization can handle crisis situations. Thus,

[1] Deutsche Lufthansa AG, Von-Gablenz-Straße 2-6, 50679 Köln, Germany, carsten.breithaupt@dlh.de
[2] Capgemini, Bahnhofstraße 30, 90402 Nuremberg, Germany, jonas.vieracker@capgemini.com
[3] Bentley University, 175 Forest Street, Waltham, MA, USA, achircu@bentley.edu
[4] RatPacDune Entertainment, Los Angeles, CA, USA, sean.cox@ratpacent.com
[5] Capgemini, Bahnhofstraße 30, 90402 Nuremberg, Germany, eldar.sultanow@capgemini.com

doi:10.18420/inf2020_14

crisis management is a strategic business matter that affects a company's performance in achieving its goals [Ah12, p. 63].

The crisis management principles and strategies championed by an enterprise's senior executives (CxOs) need to be operationalized in order to take effect within the entire organization. A key way to integrate strategy into a company's organizational design, processes, and overall operations is Enterprise Architecture Management (EAM). EAM is a management philosophy that embraces holistic and sustainable change and provides an opportunity to drive strategic and operational changes while considering existing and required future business capabilities and assets [Ah12, p. 57]. An Enterprise Architect (EA) is an experienced business and technology professional, usually reporting directly to a CxO, who is responsible for EAM implementation, specifically for the alignment of the business objectives with information technology (IT) strategy and principles.

In this paper, we analyze the role of EAM and the EA from the perspective of crisis management, and propose that an EA's duties should include building and maintaining crisis management capabilities, which should be incorporated in the EAM architecture. An EA's skill set and the related EAM practices provide the structure with which all relevant activities are managed to conceptualize, implement and execute enterprise strategies. As a result, EA can also design and implement crisis management to respond to an unforeseen threat [Ah12, p. 61]. We build on this idea by proposing a holistic approach to manage crises. The goal is to provide a model with which a crisis management capability can be created as a part of EAM, turning the EA into the lead crisis manager of the organization.

2 Understanding the Role of EAM and EAs in Crisis Management

2.1 Crises and crisis management

Over the past few decades, many scholars have studied organizational crises and crisis management from a variety of disciplinary perspectives [Bu17, KW17, PC98]. They define a crisis as *"low-probability, high-impact event that threatens the viability of the organization and is characterized by ambiguity of cause, effect, and means of resolution, as well as by a belief that decisions must be made swiftly"* [PC98]. Crisis management, in turn, is *"a systematic attempt by organizational members with external stakeholders to avert crises and to effectively manage those that occur"* [PC98]. Crises can be understood from several different perspectives, including internal organizational preparedness and external stakeholder relationships [Bu17], or psychological, social-political and technology-structural perspectives [PC98]. Crises also share similar stages – pre-crisis prevention, ongoing management, and post-crisis outcomes [Bu17, Ko20].

Many typologies of crises exist. Crises can occur due to internal organizational failures, external undermining threats, or mismanagement by crisis responders [Ko20]. Crises are also characterized by their controllability, severity, undesirability and intentionality [Bu17].

From a responsibility perspective, crises affect organizations as victims, accidents, or preventable situations [Bu17]. Crisis types include armed conflict/humanitarian aid, business, climate/environment, pollution/toxic effects, natural disasters, critical infrastructure, health, ICT/cyber, riots/crowds, and terrorism, and crisis concerns include risk, preparedness, political leadership, crisis communication, decision making, organizing for safety, community resilience, crisis transboundary, and aftermath [KW17], as well as crisis detection, containment, business resumption, learning, reputation, resource availability an decision making [PC98].

Researchers have also posited that the success or failure of crisis management depends on how well an organization can minimize potential risks before a triggering event, mobilize key stakeholders and support sense-making in response to a triggering event, and re-adjusting assumptions and responses for recovery after a triggering event – all of which are affected by the executive mindset, the adoption of organizational practices, and the environmental context [PC98].

2.2 EAM, EAs, and crisis management

EAM is usually implemented using frameworks - with TOGAF being a widely-known one [Th18]. It provides methods, models and patterns to create, maintain and improve enterprise architecture capabilities. It distinguishes between four architectural layers – from the business architecture that supports an agreed upon architectural vision, down to the data and application architecture to finally defining the technology of the architecture. This enables an end-to-end alignment and integration of business and IT objectives. EAM enables EAs to make sense of the situation and construct shared meaning with organizational stakeholders, design organizational structures and coordinate complex systems - which are exactly the foundation of crisis management [Bu17, PC98]. The following subsections describe how each one of the architectural layers relates to crisis, and how EAs can perform crisis management activities in each case.

Business and strategy

According to TOGAF 9.2 [Th18, p. 407] the business architecture defines the business strategy, governance, organization and key business processes. It further represents holistic, multi-dimensional views of capabilities, end-to-end value delivery, information, and organizational structure as well as the relationships between these business views and strategies, products, policies, initiatives and stakeholders. TOGAF applies the business architecture to an entire organization. Although crisis management can be a part of the domain of governance it should be considered as unique architecture capability, which consists of strategy, governance and key business processes that define how the crisis management is set up within an enterprise. During a crisis, EAs can focus on business continuity by using the architectural model to answer business and strategy key questions such as:

- Can we continue generating revenue with our current business model?
- Can the crisis be overcome by focusing the business in other regions?
- Which measures can we take to stabilize our market?
- Are there possibilities to ensure liquidity during the time of crisis?
- How can we cover our fixed cost?

Data

The data architecture describes the structure of an organization's logical and physical data assets and data management resources and how they interact [Th18, p. 409]. The data structure and data management are defined by the capabilities laid out within the business architecture. However, the data architecture also influences the strategy made on the business level of crisis management. By leveraging the power of data analysis, EA can deploy the right crisis management strategies and methods during a crisis. EAs can also use the extracted information to prevent future incidents. Therefore, the data layer is closely linked to the ability to control (which is described later in this paper).

The better the overall data models are, the more implication can be drawn from them. For instance, data can support the prevention of crisis situations that arise from inside of the company (e.g. drop in demands, quality issues of products). Further, with reliable data, crisis situations can be simulated in order to take the most effective measures during a crisis. This keeps costs low and can speed up the recovery from a crisis. Another important aspect of preventing crisis on a data layer is taking measures to circumvent any kind of data loss or fraud. Data loss and data fraud are not limited to external attacks. Data loss is also caused through the failure of systems as well as infrastructure, and companies are continuously struggling with its prevention. By implementing standardized methods regarding information security, a huge step can be taken to prevent potential data risks.

Applications

The application architecture provides a blueprint to deploy the individual applications and to manage their interactions and their relationships to core business processes of the organization. In other words, applications support the business architecture to deliver key business functions and manage data assets [Th18, p. 21]. Throughout the history of big organizations, the application portfolio grows in order to cope with imminent business needs, and oftentimes applications are built on a heterogenous technology landscape with multiple applications serving the same or similar purposes and resulting in cost increases. When demand is low, but applications still need to be maintained, a heterogenous and "none-lean" application portfolio wastes money that is needed to ensure business continuity. Therefore, EAs need to evaluate the application portfolio frequently. By leveraging the foundation implemented within the data layer, the number of applications can be reduced to the ones needed for business delivery. Further, in times of crisis a reliable data model helps

EAs pinpoint the applications critical to business continuity, allowing the focus to be on these applications.

Technology

According to TOGAF [Th18, p. 12], the technology architecture describes the logical software and hardware capabilities that are required to support the deployment of business, data and application services; this includes IT infrastructure, middleware, networks, communications, processing, standards, etc. Analog to the application portfolio, technologies used in infrastructure can be heterogenous, resulting in huge maintenance costs. As a best practice, an EA should homogenize the technology portfolio to save cost. In addition, workflows in IT infrastructure are still characterized by manual tasks. Although the focus is shifting to platform strategies with a high amount of standardization and automation, not all units of an enterprise are implementing these measures. An important solution in this area is cloud computing. Cloud computing can increase the resilience of the infrastructure to handle crises (i.e. avoid outages) and can decrease infrastructure costs when properly managed. During a crisis, additional cloud capacity can be used to meet high workload demands. This results in lower cost, as an organization does not need to purchase and run the entire infrastructure necessary to handle peak demand situations in times of crisis.

2.3 Developing EA crisis management capabilities through EAM

EAM frameworks such as TOGAF describe the development of architecture capabilities and provide related methods, best practices and standards. An EA can use these tools to develop much-needed crisis management capabilities as well, by combining top-down and a bottom-up approaches. In the top-down approach, the EA develops and maintains a crisis management capability hierarchically, starting with the business and strategy layer. The directives set on this layer define the development of crisis management on the data, application and technology levels. The EA can use the bottom-up approach to gather data and information from underlying layers in order to adapt or influence the decisions made on business and strategy level. Figure 1 depicts this closed loop of developing a crisis management capability (see Figure 1).

Furthermore, by integrating the information gathered on lower levels, such as usage data of applications, health data of the IT infrastructure or general environmental data a continuous improvement of crisis management capability can be derived. Therefore, it can be stated that data is the crucial factor of crisis management and the data layer needs to be adapted to leverage the data.

Several crisis management dimensions are useful to further guide the development of crisis management capabilities by EAs, as described in the next paragraphs.

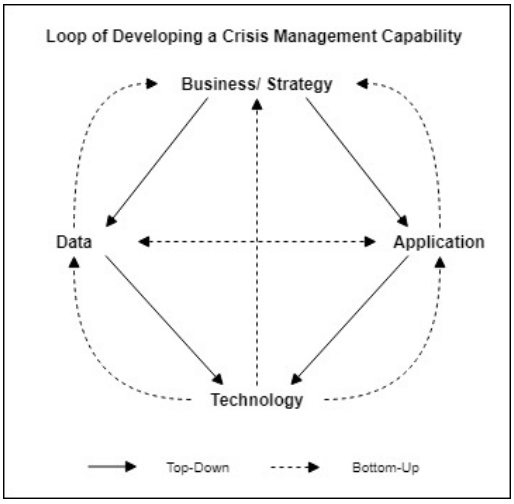

Fig. 1: Developing a Crisis Management Capability (Source: authors' own representation)

Type of change

According to Kovoor-Misra [Ko20] there are four types of changes possible in a crisis:

- **Unintentional change** occurs when the crisis changes are undesirable and are not intentional, and crate disruptions that need to be addresses.
- **Mindfully reactive change** comprises changes made by the organization after a crisis occurs in order to contain and recover from it.
- **Intentional and transformational change** is intentionally undertaken by the organization in response to or in preparation for a crisis, and may include changes in organizational structures, systems, norms and behaviors.
- **Proactive change** involves measures to prevent or address a potential crisis.

Ability to control

The ability to control describes the timing and extent of controlling and respectively manipulating (in the sense of "changing") the impacts to the organization, which increases with rising applicability of transparency [Su15, p. 9]. Ability to control is one way to characterize a crisis [Bu17]. Several types of control exist:

- **Post-preventive (corrective)** control includes measures taken after a crisis occurs. This ability does not require the detection or anticipation of influences related to the crisis. However, it demands resistance against the influences and a repository for storing the measures taken to cope with the influences.

- **Intervening (detecting)** control takes measures against influences when they occur. It requires immediate detection of influences throughout the management of the crisis.
- **Preventive** control involves taking measures for avoiding potential future influences. This indicates a need to anticipate the influences in order to take appropriate precautions.
- **Continuous** control involves a continuous effect across a time continuum. The ability of control is continuous if it is in an internal state or is natural.

Crisis outcomes

This dimension describes how enterprises emerge from a crisis [Au00]:

- **Loss through crisis** occurs when a company's business is negatively affected, for example through loses sales, orders or customers. Examples include the negative impact on airline companies from terrorist attacks or the worldwide COVID-19 pandemic.
- **Benefits from crisis** occur when the crisis positively affects the organization by creating opportunities for growth. For instance, in the case of Covid-19, the manufacturers of personal protective equipment (PPE) have benefited significantly from the increased demand for their products.

According to Watters, the focus on crisis outcomes rather than causes is important because "*there are infinite possible causes. A real risk is that you can spend all your life doing risk assessments and are not ready for what comes along. A better approach is to focus on the impacts and how they manifest themselves in terms of outcomes. It makes much more sense to do this because, for an infinite number of potential causes, the possible impacts boil down into only five outcome scenarios. That means you focus first on preparing the basic elements of business continuity so that you can survive the five possible outcome scenarios*" [Wa14, p. 8].

Level of communication

According to Laverdet et al. [La18, p. 150], effective crisis management requires organizations to communicate with stakeholders in a timely manner. This includes using the preferred communication channels of the organization to explain and provide regular updates for the current situation (to help organizational stakeholders understand the kind of crisis they are dealing with and how it is evolving) and provide instructions on how to deal with the evolving situation (at both organizational and individual level). After a crisis has ended, crisis managers should enter a learning phase and receive feedback from other members of the organization about the effectiveness of their approach in order to improve crisis management capabilities [Bu17, La18]. This approach can be adopted by an EA assuming crisis manager responsibilities. The EA can develop a crisis communication

plan together with relevant departments, such as corporate communication, orchestrate communication among different stakeholders, and filter the information available during a crisis in order to transmit the correct level of information to different groups and individuals in an organization, for example on a social intranet. Note that in our model, the dimension of communication is considered as a transversal dimension across all other dimensions, as the entire model influences communication during crisis situations.

Affected areas

According to Kovoor-Misra [Ko20] crisis can affect various areas, as follows:

- **Natural environmental** area includes the air, water, land and other natural resources associated with an organization.
- **Technical** area includes resources associated with computer, electrical, chemical and mechanical technologies, as well as raw materials used in manufacturing.
- **Economic** area includes the company's financial resources and the related management mechanisms (i.e. financial reporting and monitoring systems, etc.).
- **Human and social** area includes the physical, psychological and social aspects of the organization (i.e. individual health and behavior and organizational culture, identity and human resource structures and processes).
- **Political/reputational** area refers to the power and influence of the organization on its stakeholders, including perceptions of brand and reputation.
- **Legal** area includes the laws and regulations the organizations is subject to and the parts of the organization involved in compliance efforts.
- **Ethical** area includes the moral conduct principles and standards accepted within the organization.

Criticality of an organization's business functions

In times of crisis, an organization's priority is to ensure continuing core activities – i.e. transforming input to output at levels that satisfy the needs of key customers, with minimal interruptions or delays [PC98]. As a result, the importance of business functions within an enterprise changes during a crisis. The criticality of an organization's sub-units can be defined by using several categories [Hi00, Wa14]:

- **Vital/mission critical** business functions are necessary for survival – i.e. basic operations requirements, minimum acceptable work or service levels, or required legal aspects.

- **Essential** business functions are necessary for normal business activity – a reduction or delay in these functions will not cause an immediate negative impact, but they contribute to maintaining business continuity during the crisis.
- **Important** business functions are needed for normal operations but only have a small impact if disrupted during a crises. They support the first two types of functions, but are lower in importance.
- **Noncritical/not important** business functions have low/zero demand during a crisis, and can be put "on the back burner" in order to decrease costs and make scarce resources available for other functions.

Thus, in times of crisis the focus on an organization should be on ensuring the continuity of vital/mission critical and essential business functions. Furthermore, an organization should minimize the efforts for noncritical business functions and stabilize the performance of important functions.

Distribution of crisis management

This dimension describes the degree of centralization of the crisis management processes the success of crisis management in global organizations. We differentiate in:

- **Centralized** crisis management involves using a central point (such as the company's headquarters, or a centralized disaster management location) for all crisis management decisions. Especially when it comes to a global crisis, a standard in handling the crisis must be established centrally. While centralization ensures consistency, it can create unacceptable delays in responses to a crisis. A certain degree of freedom for subsidiaries and local managers may be needed to adjust the common crisis response to local conditions and reduce delays.
- **Decentralized** crisis management consists of local control over responses to a crisis. This implies that subsidiaries, business units, and local managers can come up with their own solutions. Decentralized crisis management is of high importance for companies with multiple business units and locations that differ in significant ways, such as due to different geographical, cultural, or economic factors. Giving these units the freedom to act and respond independently increases the chance of act quickly and achieve successful (but perhaps different) outcomes in each unit, but it can also create a disorganized, less effective and more resource-intensive response.

2.4 Relationship to other IT disciplines

Other IT management frameworks, also cover some, but not all aspects of crisis management. For example, COBIT (The Control OBjectives for Information Technology), includes IT

Risk Management AP012 and IT Continuity Management (DSS04) in its model. These areas provide processes on how to define business requirements with regards to the need for a continuous IT operations and potential risks for the IT as experienced and assessed by the business users. In addition, it is worth mentioning the "BSI IT-Grundschutz Handbuch". It is published by the German Federal Office for Information Security and defines a method to assess the protection level of an application, implicating how to deal with those applications before, during and after crises [Bu].

Evaluating other frameworks while developing an architectural approach on dealing with crisis is important as these frameworks exhibits that IT should be driven by business and its requirements. Knowing how to define such primarily non-functional requirements is integral for assessing means for crisis management.

3 Applying the model – insights from Lufthansa

To demonstrate the usefulness of our model, we applied it to a top European aviation company based in Germany – Lufthansa. Figure 2 shows the model instantiated with the Lufthansa details – including the architectural model and the six crisis management dimensions discussed previously (see Figure 2). The following sections describe relevant company practices for each component of the model.

3.1 Type of change

Lufthansa is primarily focusing on change that is initiated by the company – mindfully reactive, intentional, transformative and proactive change. The practices that are supporting the initiation of necessary change to the organization and its processes and governance include:

- **IT Strategy** is the key driver for change. By evaluating internal and external factors for its IT strategy, Lufthansa can anticipate crises and initiate change in time. For instance, Lufthansa transformed its IT operations towards being more agile in order to adjust quicker to changes in demand and other external factors.
- **IT and Business Continuity Management (ITCM/ BCM)** assesses, amongst others, the criticality of business processes and IT applications. This supports crisis management in clustering processes and applications and initiating change for the protection of the most critical systems. This is closely linked to the model's dimension on the criticality of business functions. The more critical systems are, the higher their need for continuity is. Lufthansa assesses the criticality of processes and systems on a regular basis.

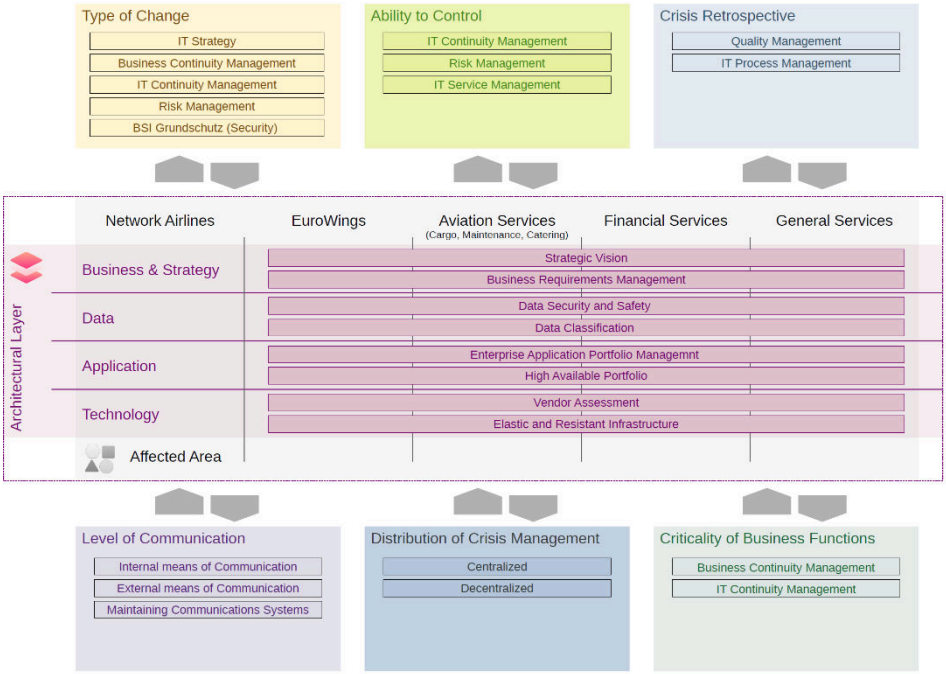

Fig. 2: Overall model applied to Lufthansa (Source: authors' own representation)

- **Risk Management** identifies threats for business and IT, as well as possible mitigation mechanisms. Being aware of risks supports the EA to initiate changes preventively in order to avoid letting risks become a crisis.
- **BSI Grundschutz** describes another initiator for change at Lufthansa based on an assessment of applications need for data protection. Its goal is to ensure a high level of confidentiality, integrity and availability. Based on the assessment outcomes, specific data security and data safety measures are taken in order to ensure the necessary protection of application data.

An EA, in his role as crisis manager, needs to understand these practices and initiate necessary measures and actively promote the associated change within the application portfolio and its underlying infrastructure. Note that the type of change dimension is not limited to these four practices. Other practices can be used to get an even more detailed perspective on needed change.

3.2 Ability to control exercised by Lufthansa in crisis situations

At Lufthansa, the Continuity Management process mentioned above helps to define different types of preventive, detective and correcting control measures to ensure IT and business continuity (ITCM/BCM). Depending on the nature of the measures, they detect the situation and act accordingly or monitor it with manual intervention as part of the measure. Concepts from the design of highly available systems, like hot, warm, and cold standby, are relevant here. The Risk Management process includes mitigations (i.e. corrective control). IT Service Management also contains the concept of service monitoring and improving, which can help to continuously detect errors or problems and identify corrective actions. Based on all these processes, the EA gets various inputs for control needs. The EA function translates this into requirements towards monitoring, supervision processes and the application behavior.

3.3 Crisis outcomes at Lufthansa

For the global aviation industry, crises generally have negative impacts resulting in losses (i.e. pandemics like SARS or COVID-19, volcano eruptions disrupting travel routes, or cyberattacks). In terms of Quality Management / IT Governance, the actions and measures defined by the practices described in previous sub-sections (Risk, Continuity, etc.) can be evaluated. Governance management is very helpful to gain some insights about the effect of the identified measures in the event of a crisis. With respect to IT Process Management, we need to have a view of the process landscape and see how the linkage of the different processes will help optimize them. At the very least it helps to identify missing links and/or gaps. The EA can thus be part of the Plan-Do-Check-Act cycle and helps continuously improve crisis outcomes.

3.4 Level of communication exercised within Lufthansa

Lufthansa employs various communication channels. These are in place during nomal business operations and can be used right away in times of crisis by posting current information, depending on release timelines and degree of formality required. For external communication, Lufthansa uses, amongst others, press conferences, social media channels, the company's public blog and press releases. For internal crisis communication, Lufthansa uses e-mail, web casts and the social intranet. In times of crisis the EA is installed as communicator and consolidates information provided by different business units. The EA is closely connected to the responsible parties for internal and external communication to distribute information as effectively as possible.

3.5 Distribution of crisis management in the context of Lufthansa

Lufthansa is a global organization, and it employs decentralized and centralized mechanisms for crisis management. The German headquarters have crisis management procedures in place to be implemented by subsidiaries around the world. However, each subsidiary has its own freedom to adapt these regulations to local standards and needs. This is the most effective approach. The central crisis management team cannot design a "one-size-fits-allßtrategy on crisis management, as each country has its own external and internal factors that need to be incorporated into its specific crisis response. EAs for global business lines incorporate regional differences in the crisis strategy plans to ensure enough freedom for local adaptions. Local EAs have to know local laws, regulations and best practices in order to tailor the strategy to the local needs.

3.6 Criticality of business functions applied to Lufthansa

As explained previously, BCM and ITCM are used to assess the criticality of an organizations business processes, functions and capabilities. These assessments are continuously applied by Lufthansa in order to get a comprehensive and up-to-date overview of its most critical business functions. Based on the outcomes of the BCM and ITCM assessment, initiatives can be started to conceptualize plans on how to ensure continuity of business functions in times of crisis and on how to prevent potential hazards for these business functions. The EA is both the consumer and producer of these assessments. In the role of producer, the EA is delivering valuable input for assessing a business function's criticality. As a consumer, the EA is using the output to start initiatives to ensure business function continuity.

3.7 Lufthansa's architectural approach to crisis management

The main benefit of our model is the ability to connect the dots across all model dimensions through the architectural perspective.

Business and strategy

The business and the strategy layer deliver important input to the EA. As described above, the assessment of the criticality of business processes and the vision of the strategy with regards to disruption, agility and reliability are translated into requirements for the IT landscape. The following example shows the link between these areas. Flight operations are vital to the business continuity of Lufthansa. Ensuring ongoing flights is the key focus of crisis management as flights are the biggest revenue stream. During a crisis, Lufthansa must at least cover the cost of operations in order to ensure long-term continuity. Booking and re-booking flights is considered as an essential business function. Irrespective of the crisis, it must still be possible to book flights in order to ensure ongoing flight operations.

Marketing campaigns are important business functions in order to maintain the brand image and associated value of Lufthansa. However, in times of crisis, marketing campaigns can be postponed—ultimately saving money.

Data

The classification of the data according to the required data protection level is important to identify the effective measures and actions for protecting the data layer. The EA's task is to translate these actions into concrete architectures (reference, domain, and solution) or alternatives, if possible. The assessment of the alternatives regarding the coverage of requirements and the cost efficiency is one of the main tasks of the EA. Measures applied at Lufthansa range from encrypting data at rest and in transit, setting up High Availability in order to optimize metrics such as Recovery-Time-Objective and Recovery-Point-Objective. An example for data classification at Lufthansa shows the following: the integrity of all flight-related data is crucial. Nevertheless, parts of flight data (e.g. arrival and departure times) have only low needs regarding confidentiality. Therefore, different measures of data protection need to be applied. Defining these measures based on the assessment is a main task of the EA.

Application

The application layer is another integral part that Lufthansa's EAs focus on. Their practices are characterized by implementing a lean application portfolio by applying different enterprise application portfolio management techniques. The most important thing for Lufthansa is to ensure high availability of applications (based on their criticality assessment) while getting rid of redundant applications. This ensures business continuity and cost reductions in the long run.

Technology

Together with assessing the crisis resistance of its infrastructure as part of the technology layer, Lufthansa is also evaluating its vendors as part of the overall risk management process. In times of crisis, a lack of support from vendors due to the unexpected circumstances can severely harm the application portfolio of an organization. Therefore, highly reliable, crisis-resistant technology vendors need to be considered during the buying decisions. For example, the infrastructure and applications cloud vendors need to show that their crisis management processes cover the requirements of an organization such as Lufthansa.

3.8 Future directions

Our ongoing research efforts are focused on identifying crisis management requirements for the IT landscape, as EAs have to do through the processes described earlier in the paper. We are following the usual steps as depicted by architecture development frameworks like TOGAF and therefore are developing the needed architecture building blocks serving

to fulfill all of the requirements. Based on the experiences reported in this paper and anticipated future developments, we have created a first set of requirements. These are comprised of: data backup and recovery (data must be recoverable - requirement derived from the BSI Grundschutz), application and server virtualization or containerization (applications must be recoverable by instantiating the image - requirement derived from ITCM and Risk Management), unlimited elasticity and financial flexibility (applications must provide scale up and down capability without boundaries in regards to workload and costs - requirement derived from Risk Management and IT-Strategy), resilience and fault tolerance (applications must able to cope with failures – requirement derived from ITCM and Risk Management), desktop and workplace virtualization (as well as the applications, the workplaces must be recoverable – requirement derived from ITCM and Risk Management), unified communication, collaboration and social media (specific communication channels and collaboration tools - requirement derived from communication needs and types).

4 Conclusions

In this paper, we build a model connecting EAM and crisis management through multiple dimensions that showcase crisis management responsibilities an EA can undertake, and then instantiate the model with insights from a large global aviation company, Lufthansa. Our work showcases a novel interdisciplinary model that connects crisis management concepts (derived primarily from the management and crisis and disaster research fields) with enterprise architecture concepts (derived primarily from IT research and practice). We hope that this model can help other organizations evaluate their enterprise architecture for crisis readiness, and show how enterprise architects can adopt crisis management responsibilities. Future research can apply this model to different organizations in other industries, and test its usefulness for different types of crises.

Bibliography

[Ah12] Ahlemann, F.; Stettiner, E.; Messerschmidt, M.; Legner, C. (Eds): Strategic Enterprise Architecture Management. Heidelberg, Germany: Springer, 2012.

[Au00] Augustine, N. R.: Managing the Crisis You Tried to Prevent. Harvard Business Review on Crisis Management. Harvard Business School Press, 2000.

[Bu] Bundesamt für Sicherheit in der Informationstechnik. Lektion 4: Schutzbedarfsfeststellung.

[Bu17] Bundy, J.; Pfarrer, M.D.; Short, C.E.; Coombs, W.T.: Crises and crisis management: Integration, interpretation, and research development. Journal of Management, 43/6, 2017, pp.1661-1692.

[Hi00] Hiatt, C. J.: A Primer for Disaster Recovery Planning in an IT Environment. Hershey, PA: Idea Group Publishing, 2000.

[Kl19] Klotz, M.: IT-Compliance nach COBIT 2019, 2019.

[Ko20] Kovoor-Misra, S.: Crisis Management Resilience and Change. Thousand Oaks, CA: SAGE Publications, 2020.

[KW17] Kuipers, S.; Welsh, N.H.: Taxonomy of the crisis and disaster literature: Themes and types in 34 years of research. Risk, Hazards & Crisis in Public Policy, 8/4, 2017, pp.272-283.

[La18] Laverdet, C.; Weiss, K.; Bony-Dandrieux, A.; Tixier, J.; Caparos, S.: Digital Training for Authorities: What is the Best Way to Communicate During a Crisis?. In Sauvagnargues, S. (Ed.), Decision-making in Crisis Situations, ISTE Ltd and John Wiley & Sons, Inc., 2018, pp. 149-174.

[PC98] Pearson, C.M.; Clair, J.A.: Reframing crisis management. Academy of Management Review, 23/1, 1998, pp.59-76.

[Su15] Sultanow, E.: Real World Awareness in kollaborativen Unternehmensprozessen. Berlin, Germany: Gito, 2015.

[Th18] The Open Group. The TOGAF Standard Version 9.2., 2018.

[Wa14] Watters, J.: Disaster Recovery, Crisis Response, and Business Continuity. Apress, 2014.